paloalto TECHDOCS

Guide de l'administrateur SD-WAN

3.2

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

May 20, 2024

Table of Contents

Aperçu général de SD-WAN

Apprenez-en plus sur SD-WAN et planifiez votre configuration afin de garantir un déploiement réussi.

Au sujet de SD-WAN

Le Software-Defined Wide Area Network (SD-WAN) est une technologie qui vous permet d'utiliser des services internet divers et privés pour créer un WAN intelligent et dynamique qui aide à réduire les coûts et à maximiser la qualité et l'utilisation des applications. A partir de PAN-OS® 9.1, Palo Alto Networks® offre une sécurité renforcée avec une couche SD-WAN dans un seul système de gestion. Au lieu d'utiliser des MPLS onéreux et chronophages avec des composants comme des routeurs, des pare-feux, des contrôleurs de chemin WAN et des optimisateurs de WAN pour connecter votre WAN à internet, la fonctionnalité SD-WAN sur un pare-feu Palo Alto Networks vous permet d'utiliser des services internet moins chers et moins d'équipements. Vous n'avez pas besoin d'acheter et de garder d'autres composants WAN.

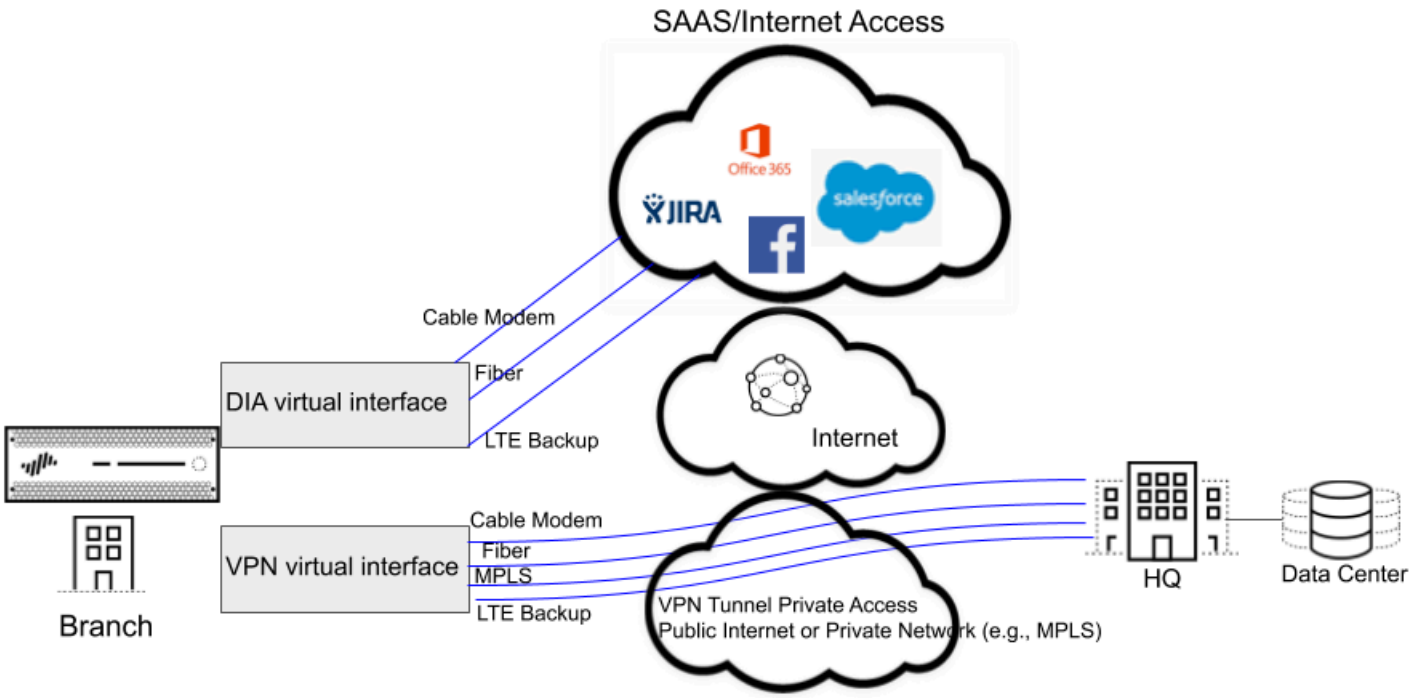
- Sécurité PAN-OS avec fonctionnalité SD-WAN
- Lien SD-WAN et Assistance pare-feu
- Prise en charge du hub d'accès Prisma
- Gestion centralisée

Sécurité PAN-OS avec fonctionnalité SD-WAN

Le plug-in SD-WAN est intégré dans PAN-OS afin que vous obteniez les fonctionnalités de sécurité d'un pare-feu PAN-OS et la fonctionnalité SD-WAN auprès d'un seul fournisseur. La couche SD-WAN permet une sélection de chemin dynamique et intelligente sur la base des applications, des services et des conditions des liens que chaque application ou service est autorisé à utiliser. La surveillance de l'état du chemin pour chaque lien comprend la latence, la gigue et la perte de paquets. Des contrôles granulaires des applications et des services permettent de prioriser les applications en fonction de leur importance métier, de leur sensibilité à la latence ou du fait qu'elles doivent répondre à certains critères d'état. La sélection de chemin dynamique évite les défaillances et les problèmes d'échec de nœud parce que des sessions basculent vers un chemin plus performant en moins d'une seconde.

La couche SD-WAN fonctionne avec toutes les fonctionnalités de sécurité PAN-OS, comme User-ID™ et App-ID™ pour offrir un contrôle de sécurité total aux sites distants. La gamme complète des capacités App-ID (décodeur App-ID, cache App-ID et liste dynamique externe source/destination [EDL] des listes d'adresses IP) identifie les applications pour le contrôle basé sur des applications du trafic SD-WAN. Vous pouvez déployer le pare-feu avec une segmentation de trafic Zero Trust. Vous pouvez configurer et gérer votre SD-WAN de façon centrale depuis l'interface web de Panorama ou le REST API de Panorama.

Vous devez avoir des services basés sur le cloud et au lieu d'avoir un flux de trafic internet depuis les branches vers la plateforme et vers le cloud, vous voulez que le trafic internet aille directement des branches au cloud en passant par un ISP connecté directement. Cet accès depuis une branche à internet est un Accès direct à internet (DIA). Vous n'avez pas besoin de gaspiller votre bande passante en central et votre argent pour le trafic internet. Le pare-feu de la branche assure déjà la sécurité et vous n'avez pas besoin que le pare-feu de la plateforme applique la sécurité au trafic internet. Utilisez DIA sur les branches pour SaaS, la navigation web ou des applications nécessitant une bande passante importante qui ne devraient pas être transportées vers un hub. La figure suivante illustre une interface virtuelle DIA se composant de trois liens depuis la branche vers le cloud. La figure illustre une interface virtuelle de tunnel VPN se composant de quatre liens qui connectent la branche au hub du siège.



Lien SD-WAN et Assistance pare-feu

Le regroupement de liens vous permet de regrouper plusieurs liens physiques (que les différents ISP utilisent pour communiquer avec la même destination) dans une interface virtuelle SD-WAN. Sur la base des applications et des services, le pare-feu choisit parmi les liens (sélection du chemin) pour le partage de la charge des sessions et pour assurer la protection par basculement en cas de défaillance ou de panne totale. Vous fournissez donc à l'application la meilleure performance possible. Le pare-feu effectue automatiquement un partage de la charge des sessions entre les liens sur l'interface virtuelle SD-WAN afin d'utiliser la bande passante disponible de façon avantageuse. Une interface SD-WAN doit avoir le même type de connexion (DIA ou VPN). Les liens VPN sont compatibles avec la topologie hub-and-spoke.

SD-WAN permet les types suivants de connexions WAN : ADSL/DSL, modem câble, Ethernet, fibre, LTE/3G/4G/5G, MPLS, micro-ondes/radio, satellite, WiFi, et tout ce qui se termine en Ethernet sur l'interface du pare-feu. Vous décidez de la stratégie appropriée d'utilisation des liens. Vous pouvez utiliser des connexions à bande passante bon marché avant d'utiliser des connexions MPLS ou LTE onéreuses. Autrement, vous pouvez utiliser des tunnels VPN spécifiques pour atteindre des points centraux spécifiques dans une région.

Consultez la les exigences du système pour le SD-WAN pour obtenir la liste complète des modèles de pare-feu prenant en charge les fonctionnalités logicielles du SD-WAN.

Si vous êtes un nouveau client qui a acheté un pare-feu nouvelle génération de Palo Alto Networks, vous utiliserez le routeur virtuel par défaut pour SD-WAN. Si vous êtes un client existant, vous pouvez choisir soit de laisser PAN-OS remplacer des routeurs virtuels existants ou

utiliser un nouveau routeur virtuel et de nouvelles zones pour SD-WAN afin de séparer le contenu SD-WAN de votre configuration préexistante.

À partir de PAN-OS 11.0, le plug-in SD-WAN 3.1 prend en charge le moteur de routage avancé qui utilise une méthodologie de configuration standard pour faciliter les tâches de l'administrateur. Bien que conceptuellement équivalent, le moteur de routage avancé utilise des routeurs logiques plutôt que des routeurs virtuels pour instancier les domaines de routage. Lorsque vous activez le routage avancé, des routeurs logiques sont créés et le moteur de routage avancé est utilisé pour le routage. Lorsque vous désactivez le routage avancé, des routeurs virtuels sont créés et le moteur hérité est utilisé pour le routage.

Prise en charge du hub d'accès Prisma

Avec le plug-in SD-WAN 2.2 et les versions ultérieures, PAN-OS Secure SD-WAN vous fournit la prise en charge du concentrateur Prisma Access pour vous donner un contrôle total sur la manière et l'endroit où les applications sont sécurisées. La prise en charge de Prisma Access Hub permet aux pare-feu PAN-OS de se connecter aux nœuds de calcul Prisma Access (NC) pour obtenir une sécurité basée sur le cloud dans une topologie en étoile SD-WAN. Cette prise en charge permet un basculement de lien transparent de la sécurité sur site vers Prisma Access et la possibilité de combiner les deux pour répondre à vos besoins de sécurité.

Dans une topologie mixte avec à la fois des pare-feu SD-WAN et des hubs Prisma Access, les hubs SD-WAN sont des CN d'accès Prisma (nœuds de terminaison IPSec) et les branches SD-WAN sont des pare-feu PAN-OS. Le SD-WAN crée automatiquement des tunnels IKE et IPSec qui connectent la branche au hub. À l'aide des profils de distribution de trafic, vous pouvez créer des politiques SD-WAN pour correspondre à des applications Internet spécifiques et les rediriger vers un pare-feu PAN-OS ou un déploiement Prisma Access de votre choix. Avec la prise en charge du hub Prisma Access, les plates-formes de sécurité sur site et cloud fonctionnent ensemble pour fournir une solution complète avec des politiques de sécurité cohérentes gérées par Panorama.

Consultez la configuration système requise pour SD-WAN pour connaître les versions minimales des plug-ins PAN-OS et SD-WAN requises pour la prise en charge de Prisma Access Hub.

La prise en charge du hub Prisma Access présente les limitations suivantes :

- L'importation et l'exportation d'une configuration SD-WAN liée à Prisma Access ne sont pas prises en charge.
- Le chargement, le chargement partiel, le retour et le retour partiel pour la configuration Prisma Access ne sont pas pris en charge.
- L'intégration à un nœud de traitement de la sécurité du réseau à distance Prisma Access (RN-SPN) existant n'est pas prise en charge. Pour une succursale existante connectée à Prisma Access, vous devez supprimer la succursale, puis la réintégrer.
- Aucune commande CLI SD-WAN n'est disponible sur les pare-feux Prisma Access.
- Sur un NC il n'y a pas de sélection de chemin pour le trafic qui provient du NC
- Les statistiques de Prisma Access ne sont pas fournies dans les rapports et les statistiques SD-WAN.

Gestion centralisée

Panorama™ donne les moyens de configurer et de gérer SD-WAN, ce qui rend la configuration de plusieurs options sur de nombreux pare-feux dispersés géographiquement plus rapide et plus facile que la configuration de pare-feux de façon individuelle. Vous pouvez modifier les configurations du réseau depuis un seul emplacement au lieu de configurer chaque pare-feu individuellement. La configuration Auto VPN permet à Panorama de configurer les branches et les hubs à l'aide de connexions sécurisées IKE/IPSec. Un cluster VPN définit les hubs et les branches qui communiquent entre eux dans une région géographique. Le pare-feu utilise des tunnels VPN pour la surveillance de l'état du chemin entre une branche et un hub afin d'assurer une détection en moins d'une seconde des conditions de défaillance.

Le tableau de bord de Panorama offre une visibilité de vos liens SD-WAN et de la performance afin que vous puissiez ajuster ls seuils de qualité du chemin et d'autres aspects de SD-WAN afin d'améliorer sa performance. Les statistiques centralisées et les rapports incluent des statistiques sur la performance des applications et des liens, des mesures de l'état du chemin et une analyse de la tendance et des points de vue spécifiques des problèmes relatifs aux applications et aux liens.

Commencez par comprendre votre utilisation de SD-WAN, puis examinez les éléments de la configuration SD-WAN, les méthodes de distribution de trafic et planifiez votre configuration SD-WAN. Afin de grandement accélérer la configuration, une bonne pratique consiste à exporter un fichier CSV de périphérique SD-WAN vide et à saisir les informations comme l'adresse IP de la branche, le routeur virtuel à utiliser, le nom du site du pare-feu, les zones auxquelles appartient le pare-feu et les informations de l'itinéraire BGP. Panorama utilise le fichier CSV pour configurer les hubs et les branches SD-WAN et fournir automatiquement des tunnels VPN entre les hubs et les branches. SD-WAN est compatible avec le routage dynamique via eBGP et est configuré à l'aide du plug-in SD-WAN de Panorama afin de permettre à toutes les branches de communiquer avec le hub uniquement ou avec le hub et les autres branches.

Si Panorama gère un multi-vsys firewall (pare-feu multi-vsys), toutes les interfaces et configurations compatibles SD-WAN doivent être configurées sur vsys1.

SD-WAN ne prend pas en charge une configuration SD-WAN sur plusieurs systèmes virtuels d'un pare-feu multi-VSYS.

Les interfaces SD-WAN doivent être configurées dans le même routeur virtuel ; ils ne peuvent pas être répartis entre les routeurs virtuels.

Configuration système requise pour le SD-WAN

Passez en revue les versions logicielles minimales, les versions de plug-in et les ressources requises pour le plug-in Panorama™ pour SD-WAN.

À partir de PAN-OS 11.0, vous pouvez configurer le routage avancé pour SD-WAN avec la version 3.1 du plug-in.

Le tableau suivant fournit les versions de plug-ins compatibles les unes avec les autres. Nous vous suggérons d'utiliser la version du plug-in de configuration cloud Prisma Access avec la version du plug-in SD-WAN compatible correspondante indiquée dans le tableau, car les versions compatibles contiennent de nouvelles fonctionnalités, des corrections de bugs ou des améliorations.

Platform (Plateforme)	PAN-OS	Configuration système requise	Plug-in de configuration Prisma Access Cloud	Plug-in SD-WAN
Panorama	11.2.3	• (Appliance virtuelle Panorama) **Disque système**—Disque système de 224 Go • **Processeur**—16 processeurs • **Mémoire**—64 Go de mémoire • **Mode système**—Mode panorama et mode gestion uniquement • (M-Series Appliance en mode Management Only uniquement) Une paire de disques de journalisation RAID de 8 To activée	—	3.3.1
	11.2.0		5.0.0-h22	3.3.0
	11.1.5		—	3.2.2
	11.1.3		5.0.0-h31	3.2.1
	11.1.0		4.0.0 et 5.0.0	3.2.0
	11.0.4		5.0.0-h21	3.1.3
	11.0.3		4.0.0 et 5.0.0	3.1.2
	11.0.2		4.0.0	3.1.2
	11.0.2		4.0.0	3.1.1
	11.0.1		3.2.1.h21	3.0.1-h6

Platform (Plateforme)	PAN-OS	Configuration système requise	Plug-in de configuration Prisma Access Cloud	Plug-in SD-WAN
	11.0.1 est la version 11.0.x recommandée.	*Les informations ci-dessus s'appliquent à un maximum de 500 appareils gérés. Pour plus d'informations sur l'utilisation d'un maximum de 1 000 appareils gérés, reportez-vous à* Configuration système requise pour l'appareil virtuel Panorama		
	11.0.0		3.2.1-h3	3.1.0-h6
	10.2.8		4.0.0-h80, 4.1.0-h49 et 5.0.0-h9	3.0.7
	10.2.7		4.0.0 et 5.0.0	3.0.6
	10.2.6		4.0.0	3.0.6
	10.2.5		4.0.0	3.0.5
	10.2.4 *10.2.4 est la version 10.2.x recommandée.*		3.2.1-h21	3.0.4
	10.2.3		3.2.1-h5	3.0.4
	10.2.1		Non pris en charge dans cette version ; prévu dans une prochaine version. Ne mettez pas à niveau vers PAN-OS 11.1 si vous utilisez	3.0.1
	10.2.0			3.0.0

Platform (Plateforme)	PAN-OS	Configuration système requise	Plug-in de configuration Prisma Access Cloud	Plug-in SD-WAN
			SD-WAN avec le plug-in de configuration de cloud Prisma Access.	
	10.1.11		4.0.0 et 5.0.0	2.2.6
	10.1.11		4.0.0	2.2.5
	10.1.10  *10.1.10 est la version 10.1.x recommandée.*		4.0.0	2.2.4
	10.1.9  *10.1.9 est la version 10.1.x recommandée.*		3.2.1-h5	2.2.4
	10.1.8		3.2.1-h5	2.2.2
	10.1.5-h1		2.1	2.2.1
	10.1.0		2.1	2.2
Pare-feu nouvelle génération	• **PAN-OS 11.1** —11.1.0 • **PAN-OS 11.0** —11.0.0 • **PAN-OS 10.2** —10.2.0	S. O.		

Platform (Plateforme)	PAN-OS	Configuration système requise	Plug-in de configuration Prisma Access Cloud	Plug-in SD-WAN
	• **PAN-OS 10.1**—10.1.4 • **PAN-OS 10.0**—10.0.8			
Nœud de calcul Prisma Access	10.0.7*	* Les nœuds de calcul d'accès Prisma (nœuds de terminaison IPSec) doivent exécuter PAN-OS 10.0.7 ou une version 10.0 ultérieure. Si nécessaire, contactez votre équipe commerciale pour demander une mise à niveau avant de tenter d'intégrer une succursale au hub Prisma Access.		

Les modèles de pare-feu suivants sont compatibles avec les capacités logicielles SD-WAN :

- PA-220 et PA-220R
- Série PA-400
- PA-820 et PA-850
- Série PA-1400
- PA-3200 Series
- Série PA-3400
- PA-5200 Series
- Série PA-5400
- PA-7000 Series
- Pare-feu VM-Series

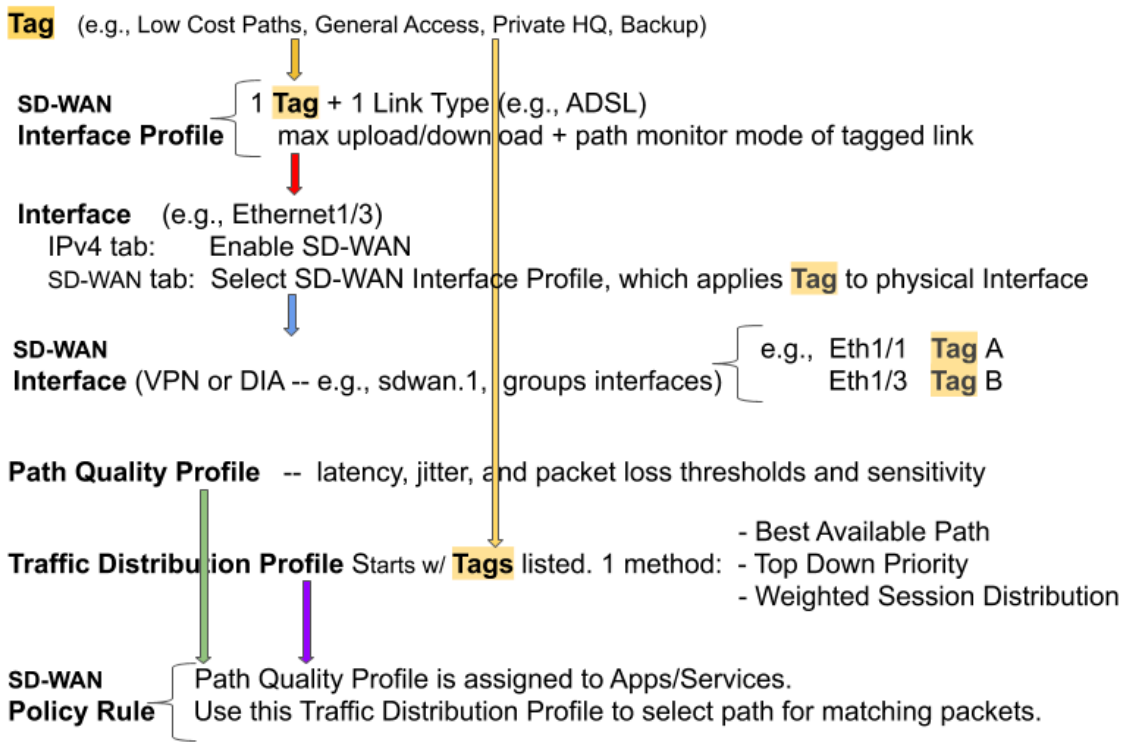
Pour plus d'informations sur une disponibilité de matériel spécifique, reportez-vous à la matrice de compatibilité.

Éléments de configuration SD-WAN

Les éléments d'une configuration SD-WAN fonctionnent ensemble, vous permettant de :

- Grouper les interfaces physiques d'Ethernet qui partagent une destination commune dans une interface SD-WAN logique.
- Spécifier les vitesses des liens.
- Spécifier les seuils auxquels un chemin détérioré (ou une défaillance ou une panne) vers un SD-WAN garantit de sélectionner le meilleur chemin.
- Spécifier la méthode de sélection de ce nouveau meilleur chemin.

Cet affichage indique les relations entre les éléments en un coup d'œil.



L'objectif d'une configuration SD-WAN est de contrôler quels sont les liens que votre trafic utilise en précisant les tunnels VPN ou l'accès internet direct (DIA) que certaines applications ou services utilisent d'une branche vers un hub ou d'une branche vers internet. Vous groupez les chemins d'accès afin que si un chemin se détériore, le pare-feu sélectionne un nouveau meilleur chemin.

- Une **Tag** (Étiquette) portant le nom de votre choix identifie un lien ; vous appliquez l'Étiquette au lien (interface) en appliquant un Profil d'Interface à l'interface, comme l'indique la flèche rouge. Un lien ne peut avoir qu'une seule Étiquette. Les deux flèches jaunes indiquent qu'une Étiquette est référencée dans le Profil d'Interface et dans le profil de Distribution du trafic. Les Étiquettes vous permettent de contrôler l'ordre d'utilisation des interfaces pour la distribution du trafic. Les Étiquettes permettent à Panorama de configurer systématiquement de nombreuses interfaces de pare-feu avec la fonctionnalité SD-WAN.

- Un **SD-WAN Interface Profile** (Profile d'interface SD-WAN) spécifie l'Étiquette que vous appliquez à l'interface physique, ainsi que le type de Lien de cette interface (ADSL/DSL, modem câble, Ethernet, fibre, LTE/3G/4G/5G, MPLS, micro-onde/radio, satellite, WiFi, ou autre). Le Profil d'Interface permet aussi de spécifier les vitesses maximales d'upload et de download (en Mbps) de la connexion de l'ISP. Vous pouvez aussi modifier la fréquence de surveillance du pare-feu ; le pare-feu surveille les types de lien de façon appropriée par défaut.
- Une **Interface** Ethernet de Couche3 avec une adresse IPv4 ou IPv6 est compatible avec les fonctionnalités SD-WAN. Vous appliquez un Profile d'Interface SD-WAN à cette interface (flèche rouge) pour indiquer les caractéristiques de l'interface. La flèche bleue indique que les interfaces physiques sont référencées et regroupées en une interface virtuelle SD-WAN.
- Une **Interface SD-WAN** virtuelle est un tunnel ou un groupe DIA d'une ou plusieurs interfaces qui constituent une interface virtuelle SD-WAN numérotée vers laquelle vous pouvez acheminer le trafic. Les chemins appartenant à une interface SD-WAN vont tous vers la même destination WAN et sont tous du même type (DIA ou tunnel VPN). (L'Étiquette A et l'Étiquette B indiquent que les interfaces physiques de l'interface virtuelle peuvent avoir des étiquettes différentes.)
- Un **Path Quality Profile** (Profil de Qualité du chemin d'accès) spécifie les seuils maximum de latence, gigue et perte de paquets. Le dépassement d'un seuil indique que le chemin s'est détérioré et que le pare-feu a besoin de sélectionner un nouveau chemin vers la cible. Un réglage de sensibilité élevée, moyenne ou faible vous permet d'indiquer au pare-feu quel paramètre de surveillance du chemin est plus important pour les applications auxquelles le profil s'applique. La flèche verte indique que vous référencez un Profil de Qualité de chemin d'accès dans une ou plusieurs règles de politique SD-WAN ; par conséquent, vous pouvez spécifier différents seuils pour les règles appliquées aux paquets ayant des applications, des services, des sources, des destinations, des zones et des utilisateurs différents.
- Un **Traffic Distribution Profile** (Profil de Distribution du trafic) spécifie comment le pare-feu détermine un nouveau meilleur chemin si le chemin préféré actuel dépasse un seuil de qualité de chemin. Vous spécifiez quelles Étiquettes la méthode de distribution utilise pour réduire la sélection d'un nouveau chemin ; par conséquent, la flèche jaune va des Étiquettes vers le profile de Distribution du trafic. Un profil de Distribution du trafic spécifie la méthode de distribution pour la règle.
- Les éléments précédents sont rassemblés dans des **Règles de politique SD-WAN**. La flèche violette indique que vous référencez un Profil de Qualité de chemin d'accès et un Profil de Distribution du trafic dans une règle, ainsi que les applications/services, sources, destinations et utilisateurs des paquets afin d'indiquer spécifiquement quand et comment le pare-feu effectue une sélection de chemin SD-WAN sur la base d'une application pour un paquet n'appartenant pas à la session. (Vous pouvez également mentionner un **SaaS Quality Profile [Profil de qualité SaaS]** et un **Error Correction Profile [Profil de correction des erreurs])**dans une règle de politique SD-WAN.)

Maintenant que vous comprenez les relations entre les éléments, examinez les traffic distribution methods (méthodes de distribution du trafic) puis Planifiez votre configuration SD-WAN.

Planifiez votre configuration SD-WAN

Planifiez la topologie complète de vos interfaces de pare-feu de branche et hub activées par SD-WAN afin de pouvoir créer des modèles Panorama™ avec des fichiers CSV puis transférer les configurations aux pare-feux.

STEP 1 | Planifiez les emplacements des branches et des hubs, les besoins en liens et les adresses IP. Depuis Panorama, vous exporterez un CSV de périphérique SD-WAN vide et l'insèrerez dans les informations des branches et des hubs.

1. Décidez du rôle de chaque pare-feu (branche ou hub).
2. Déterminez quelles branches communiqueront avec quelles hubs ; chaque groupe fonctionnel de pare-feux de branches et de hubs qui communique entre eux est un cluster VPN. Par exemple, vos clusters VPN peuvent être organisés géographiquement ou par fonction.
3. Déterminez les types de liens ISP que chaque branche et chaque hub accueille : ADSL/DSL, modem câble, Ethernet, fibre, LTE/3G/4G/5G, MPLS, micro-ondes/radio, satellite, et WiFi.
4. Déterminez la bande passante (Mbps) maximale en download et upload que les types de liens supportent et la façon dont vous souhaitez appliquer des contrôles de vitesse aux liens, tel que cela est décrit dans l'Étape 2. Enregistrez la bande passante (Mbps) maximale en download et upload du lien ISP. Cette information servira de maximum de sortie de référence si vous avez besoin de configurer un QoS pour contrôler la bande passante de l'application.
5. Rassemblez les adresses IP publiques des pare-feux des branches qu'elles aient été assignées de façon statique ou dynamique. Le pare-feu doit avoir une adresse IP public routable par internet afin de pouvoir initier et mettre un terme à des tunnels IPSec et d'acheminer le trafic de et vers internet.

   L'équipement ISP dans les locaux du client doit être directement connecté à l'interface Ethernet du pare-feu.

   Si vous avez un périphérique qui effectue un NAT se trouvant entre le pare-feu de la branche et le hub, le périphérique NAT peut empêcher le pare-feu de constituer des tunnels IKE par peering et IPSec. Si le tunnel échoue, travaillez avec l'administrateur du périphérique NAT distant pour résoudre le problème.
6. Rassemblez les préfixes et les numéros de série des pare-feux des branches et des plateformes du réseau privé.
7. Décidez du type de lien de chaque interface de pare-feu.

   Allouez les mêmes types de lien aux mêmes interfaces Ethernet sur les pare-feux de la branche afin que la configuration soit plus simple. Par exemple, Ethernet 1/1 est toujours le modem câble.
8. Décidez des conventions de dénomination de vos sites et périphériques SD-WAN.

   N'utilisez pas des noms d'hôte simples comme «hub» ou «branche» car la configuration VPN Auto utilise des mots clés pour générer différents éléments de configuration.

9. Si vous avez déjà mis des zones en place avant de configurer SD-WAN, décidez du mappage de ces zones en fonction des zones prédéfinies que SD-WAN utilise pour la sélection du chemin d'accès. Vous allez mapper des zones en fonction des zones prédéfinies appelées zone-internal, zone-to-hub, zone-to-branch et zone-internet.

   Les informations que vous allez saisir dans un CSV (afin de pouvoir ajouter plusieurs périphériques SD-WAN en une fois) comprennent : le numéro de série, le type de périphérique (branche ou hub), noms des zones à mapper selon les zones prédéfinies (clients préexistants), adresse de bouclage, préfixes pour la redistribution, numéro AS, ID du routeur et nom du Virtual Router (routeur virtuel - VR).

STEP 2 | Planifiez les regroupements de liens et la sécurité VPN des liens privés.

Un regroupement de liens vous permet de combiner plusieurs liens physiques en une seule interface virtuelle SD-WAN pour les besoins de sélection du chemin d'accès et la protection par basculement. En ayant un regroupement de plus d'un lien physique, vous maximisez la qualité de l'application si un lien physique se détériore. Vous créez un regroupement en appliquant la même étiquette de lien à plusieurs liens (via le profil d'interface SD-WAN). L'étiquette du lien identifie un regroupement de liens qui ont un type similaire d'accès et un type similaire de gestion de la politique SD-WAN. Par exemple, vous pouvez créer une étiquette de lient intitulée **`low cost broadband`** (brande passante bon marché) et inclure les services de bande passante du modem câble et de la fibre.

STEP 3 | Identifiez les applications qui utiliseront SD-WAN et l'optimisation QoS.

1. Identifiez les applications professionnelles critiques et sensibles à la latence pour lesquelles vous fournirez un contrôle et des politiques SD-WAN. Ce sont des applications qui nécessitent une bonne expérience de l'utilisateur et qui ont tendance à ne pas fonctionner dans des conditions de mauvais lien.

   Commencez par les applications les plus critiques et les plus sensibles à la latence ; vous pourrez ajouter des applications une fois que le SD-WAN fonctionnera sans problème.

2. Identifiez les applications qui nécessitent des politiques QoS afin de pouvoir accorder la priorité de bande passante. Ce devrait être les même applications que vous avez identifiées comme étant critiques ou sensibles à la latence.

   Commencez par les applications les plus critiques et les plus sensibles à la latence ; vous pourrez ajouter des applications une fois que le SD-WAN fonctionnera sans problème.

STEP 4 | Déterminez quand et comment vous voulez que les liens basculent sur un lien différent si le lien original se dégrade ou échoue.

1. Décidez du mode de surveillance des chemins pour un lien bien que la bonne pratique consiste à conserver les paramètres par défaut du type de lien :

   - **Aggressive** (mode agressif) — Le pare-feu sonde les paquets à l'extrémité opposée du lien SD-WAN à une fréquence constante (cinq sondes par seconde par défaut). Le mode agressif convient aux liens pour lesquels la surveillance de la qualité du chemin est cruciale ; lorsque vous avez besoin d'une détection rapide et d'un basculement

dans des conditions de défaillance ou de panne générale. Le mode agressif offre une détection et un basculement en moins d'une seconde.

- **Relaxed** (Mode souple) — Le pare-feu respecte un délai configurable entre l'envoi de paquets de sonde pendant sept secondes (à la fréquence de sondage que vous configurez), ce qui rend la surveillance des chemins moins fréquente qu'en mode agressif. Le mode souple convient aux liens qui ont une très faible bande passante, aux liens qui coutent cher à utiliser comme le satellite ou LTE où lorsque la détection rapide n'est pas aussi importante que la préservation du coût et de la bande passante.

2. Définissez l'ordre de priorité selon lequel le pare-feu sélectionne le premier lien pour un nouvelle session et l'ordre dans lequel les liens doivent être candidats pour remplacer un lien qui bascule s'il y a plus d'un candidat.

   Par exemple, si vous souhaitez qu'un lien LTE de sauvegarde coûteux soit le dernier lien utilisé (uniquement quand les liens de bande passante bon marché sont débordés ou à l'arrêt complet), alors utilisez la méthode de distribution du trafic de Priorité descendante et placez l'étiquette qui est sur le lien LTE en dernier dans la liste d'étiquettes du profil de Distribution de trafic.

3. Pour les applications et les services, déterminez les seuils de bon état du chemin auxquels vous estimez que la qualité d'un chemin s'est suffisamment dégradée pour vouloir que le pare-feu sélectionne un nouveau chemin (basculement). Les caractéristiques de qualité sont la latence (la fourchette est de 10 à 2 000 ms), la gigue (la fourchette est de 10 à 1 000 ms) et le pourcentage de perte de paquets.

   Ces seuils constituent un profile de Qualité du chemin que vous référencez dans une règle de politique SD-WAN. Lorsqu'un seul seuil (perte de paquets, gigue ou latence) est dépassé (et que les autres critères de la règle sont remplis), le pare-feu choisit un nouveau chemin préféré pour le trafic correspondant. Par exemple, vous pouvez créer un profil de Qualité de chemin AAA avec des seuils de latence/gigue/perte de paquets de 1000/800/10 pour utiliser la Règle 1 lorsque les paquets FTP viennent de la zone source XYZ et créer un profil de Qualité de chemin BBB (avec des seuils de 50/200/5) pour l'utiliser dans la Règle 2 lorsque les paquets FTP viennent de l'adresse IP source 10.1.2.3. Les bonnes pratiques consistent à commencer avec des seuils élevés et à tester comment l'application les tolère. Si vous définissez des valeurs trop faibles, l'application peut passer d'un chemin à l'autre trop fréquemment.

   Considérez si les applications et les services que vous utilisez sont très sensibles à la latence, à la gigue ou à la perte de paquets. Par exemple, une application vidéo peut avoir un bon buffering qui limite la latence et la gigue mais sera sensible à la perte de paquets qui a un impact sur l'expérience de l'utilisateur. Vous pouvez définir la sensibilité des paramètres de qualité de chemin dans le profil sur élevée, moyenne ou faible. Si les paramètres de sensibilité de latence, gigue et perte de paquets sont les mêmes, le pare-feu examine les paramètres dans l'ordre perte de paquets, latence, gigue.

4. Décidez s'il y a des liens entre lesquels partager la charge de nouvelles sessions pour une application ou un service.

STEP 5 | Planifier les configurations BGP que Panorama transfèrera vers les branches et les hubs afin d'acheminer le trafic de façon dynamique entre elles.

1. Planifiez les informations d'acheminement BGP, y compris un numéro système autonome (ASN) de quatre octets. Chaque site de pare-feu est sur un AS séparé et

par conséquent doit avoir un ASN unique. Chaque pare-feu doit aussi avoir une ID de routeur unique.

2. Avant de mettre en œuvre SD-WAN avec routage BGP dans un environnement où BGP est déjà utilisé, assurez-vous que la configuration BGP générée par le plug-in SD-WAN n'entre pas en conflit avec votre configuration BGP existante. Par exemple, vous devez utiliser le numéro BGP AS existant et les valeurs d'ID de routeur pour les valeurs de périphérique SD-WAN correspondantes.
3. Si vous ne voulez pas utiliser le routage dynamique BGP, prévoyez d'utiliser les options de configuration du réseau de Panorama afin de mettre en avant d'autres configuration de routage. Vous pouvez effectuer un routage statique entre la branche et les hubs. Omettez simplement toutes les informations BGP dans le plug-in de Panorama et utilisez des routages statiques normaux du routeur virtuel pour réaliser un routage statique.

STEP 6 | Tenez compte des capacities of firewall models (capacités des modèles de pare-feu) des interfaces virtuelles SD-WAN, règles de politique SD-WAN, taille du journal, tunnels IPSec (y compris les ID de proxy), peers IKE, BGP et tableaux de routage statique, peers de routage BGP et la performance pour votre mode de pare-feu (App-ID™, menace, IPSec, décryptage). Assurez vous que les modèles de pare-feu de la branche et du hub que vous envisagez d'utiliser supportent les capacités dont vous avez besoin.

Configurer SD-WAN

une fois que vous avez Planifiez votre configuration SD-WAN, installez le plug-in SD-WAN et configurez le serveur de gestion Panorama™ afin de gérer de façon centrale la configuration SD-WAN de vos pare-feux de hubs et de branches. En utilisant Panorama, vous réduisez les besoins de gestion et la surcharge opérationnelle de la gestion de votre déploiement SD-WAN et vous pouvez surveiller plus facilement l'état de vos liens et régler les problèmes qui peuvent se présenter.

Si Panorama gère un multi-vsys firewall (pare-feu multi-vsys), toutes les interfaces et configurations compatibles SD-WAN doivent être configurées sur vsys1.

SD-WAN ne prend pas en charge une configuration SD-WAN sur plusieurs systèmes virtuels d'un pare-feu multi-VSYS.

- Installer le plug-in SD-WAN
- Configurer Panorama et les pare-feux pour SD-WAN
- Créer une Link Tag (Étiquette de liens)
- Configurer un Profil d'interface SD-WAN
- Configurer une interface Ethernet physique pour SD-WAN
- (Facultatif) Configurer une interface Ethernet agrégée et des sous-interfaces pour SD-WAN
- (Facultatif) Configurer les sous-interfaces de couche 3 pour SD-WAN
- Configurer une Interface virtuelle SD-WAN
- Créer un itinéraire par défaut vers l'interface SD-WAN
- Configurez les Profils de gestion des liaisons SD-WAN
- Configurer une Règle de politique SD-WAN
- Autoriser le basculement du trafic de l'accès direct à internet vers un lien MPLS
- Configuration de DIA AnyPath
- Distribuer des sessions sans correspondance
- Ajouter des Périphériques SD-WAN à Panorama
- (Facultatif) Configurer des routeurs virtuels multiples sur le hub SD-WAN
- (Facultatif) Configurer des routeurs virtuels multiples sur la branche SD-WAN
- (Facultatif) Configurer les Périphérique HA pour SD-WAN
- Créer un cluster VPN
- Création d'un cluster VPN Full Mesh avec le service DDNS
- (Facultatif) Créer une route statique pour SD-WAN
- (Facultatif) Configurer le routage avancé pour le SD-WAN

Installer le plug-in SD-WAN

Un serveur de gestion Panorama™ avec un plug-in SD-WAN est nécessaire pour configurer et gérer un déploiement SD-WAN. Si votre Panorama est connecté à internet, vous téléchargez le plug-in SD-WAN directement depuis Panorama et l'installer sur le serveur Panorama. Si votre Panorama n'est pas connecté à internet, vous téléchargez le plug-in SD-WAN directement depuis le Portail Support Client de Palo Alto Networks® et vous l'installez sur le serveur Panorama.

- Installez le plug-in SD-WAN lorsque Panorama est connecté à Internet
- Installer le plug-in SD-WAN lorsque Panorama n'est pas connecté à Internet

Installez le plug-in SD-WAN lorsque Panorama est connecté à Internet

Un serveur de gestion Panorama™ avec un plug-in SD-WAN est nécessaire pour configurer et gérer un déploiement SD-WAN. Lorsque Panorama est connecté à internet, vous téléchargez et installez le plug-in SD-WAN directement depuis l'interface web de Panorama. Le plug-in doit être installé uniquement sur le Panorama qui gère vos pare-feux SD-WAN et non sur les pare-feux individuels des branches et des hubs.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Sélectionnez **Panorama** > **Plugins** (plug-ins de Panorama), recherchez le plug-in **`sd_wan`** et **Check Now** (recherchez maintenant) la version la plus récente du plug-in.

STEP 3 | **Download** (téléchargez) et **Install** (installez) le plug-in SD-WAN.

STEP 4 | Après avoir réussi l'installation du plug-in SD-WAN, sélectionnez **Commit** (Validez) puis **Commit to Panorama** (Validez sur Panorama).

Cette étape est nécessaire avant que vous puissiez valider des modifications de la configuration de Panorama.

STEP 5 | (Mode Management Only uniquement) Activez les disques de journalisation requis pour stocker les données de surveillance SD-WAN.

- **Appliances de la série M —**Tous les appareils de la série M sont livrées avec deux paires de disques de journalisation de 8 To en RAID 1 par défaut. Lors de la gestion de pare-feu utilisant SD-WAN à partir de Panorama en mode Gestion uniquement, vous devez activer la première paire de paires de disques de journalisation pour stocker les données de surveillance SD-WAN.

  1. Connectez-vous à l'CLI de Panorama.
  2. Activez la première paire de paires de disques de journalisation incluse par défaut avec votre appareil M-Series.

```
> request system raid add A1
```


3. Vérifiez que la journalisation `de la paire de disques de journalisation A` est `disponible` :

   ```
   > show system raid detail
   ```

   Une fois la configuration RAID terminée, la réponse suivante s'affiche :

   ```
   Paire de disques A État disponible nettoyer ID de disque
    A1 Modèle actuel : St91000640NS taille : 953869 Mo :
    synchronisation active
   ```

4. Rendez les paires de disques de journalisation disponibles pour la journalisation.
   1. Sélectionnez **Panorama (Panorama)** > **Managed Collectors (Collecteurs gérés)** et modifiez le collecteur de journaux.
   2. Sélectionnez **Disks (Disques)** et **Add (Ajoutez)** chaque baie.
   3. Cliquez sur **OK** pour enregistrer vos modifications.
   4. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.
   5. Sélectionnez **Commit (Valider)** > **Push to Devices (Transmettre aux périphériques)**, sélectionnez le groupe de collecteurs, puis **Push (Appliquez)** vos changements.

- **Appareils virtuels Panorama**— Si vous avez déployé votre appareil virtuel Panorama en mode Gestion uniquement, vous devez augmenter le disque système à 224 Go pour stocker les données de surveillance SD-WAN.

STEP 6 | Continuer à Configurer Panorama et les pare-feux pour SD-WAN pour commencer à configurer votre déploiement SD-WAN.

Installer le plug-in SD-WAN lorsque Panorama n'est pas connecté à Internet

Un serveur de gestion Panorama™ avec un plug-in SD-WAN est nécessaire pour configurer et gérer un déploiement SD-WAN. Lorsque Panorama n'est pas connecté à internet, vous devez télécharger le plug-in SD-WAN depuis le Portail Support Client de Palo Alto Networks et uploader le plug-in dans Panorama. Le plug-in doit être installé uniquement sur le Panorama qui gère vos pare-feux SD-WAN et non sur les pare-feux individuels des branches et des hubs.

STEP 1 | Connectez-vous au Customer Support Portal (Portail assistance clientèle) de Palo Alto Networks.

STEP 2 | Sélectionnez **Updates** > **Software Updates**, et dans le filtre, choisissez dans la liste déroulante **Panorama Integration Plug In** (plug-in d'intégration panorama).

STEP 3 | Localisez et téléchargez le **SD-WAN Plug-in** (plug-in SD-WAN).

STEP 4 | Connectez-vous à l'interface Web Panorama.

STEP 5 | Sélectionnez**Panorama** > **Plugins** et **Upload** (uploadez) le plug-in SD-WAN.

STEP 6 | **Browse** (Naviguez) et localisez le plug-in SD-WAN que vous avez téléchargé sur le Portail Support Client et cliquez sur **OK**.

STEP 7 | **Install** (installez) le plug-in SD-WAN.

STEP 8 | Après avoir réussi l'installation du plug-in SD-WAN, sélectionnez **Commit** (Validez) puis **Commit to Panorama** (Validez sur Panorama).

Cette étape est nécessaire avant que vous puissiez valider des modifications de la configuration de Panorama.

STEP 9 | (Mode Management Only uniquement) Activez les disques de journalisation requis pour stocker les données de surveillance SD-WAN.

- **Appliances de la série M —**Tous les appareils de la série M sont livrées avec deux paires de disques de journalisation de 8 To en RAID 1 par défaut. Lors de la gestion de pare-feu utilisant SD-WAN à partir de Panorama en mode Gestion uniquement, vous devez activer la première paire de paires de disques de journalisation pour stocker les données de surveillance SD-WAN.

  1. Connectez-vous à l'CLI de Panorama.
  2. Activez la première paire de paires de disques de journalisation incluse par défaut avec votre appareil M-Series.

     ```
     > request system raid add A1
     ```

  3. Vérifiez que la journalisation `de la paire de disques de journalisation A` est `disponible` :

     ```
     > show system raid detail
     ```

     Une fois la configuration RAID terminée, la réponse suivante s'affiche :

     ```
     Paire de disques A État disponible nettoyer ID de disque
      A1 Modèle actuel : St91000640NS taille : 953869 Mo :
      synchronisation active
     ```

  4. Rendez les paires de disques de journalisation disponibles pour la journalisation.
     1. Sélectionnez **Panorama (Panorama)** > **Managed Collectors (Collecteurs gérés)** et modifiez le collecteur de journaux.
     2. Sélectionnez **Disks (Disques)** et **Add (Ajoutez)** chaque baie.
     3. Cliquez sur **OK** pour enregistrer vos modifications.
     4. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.
     5. Sélectionnez **Commit (Valider)** > **Push to Devices (Transmettre aux périphériques)**, sélectionnez le groupe de collecteurs, puis **Push (Appliquez)** vos changements.

- **Appareils virtuels Panorama**— Si vous avez déployé votre appareil virtuel Panorama en mode Gestion uniquement, vous devez augmenter le disque système à 224 Go pour stocker les données de surveillance SD-WAN.

STEP 10 | Continuer à Configurer Panorama et les pare-feux pour SD-WAN pour commencer à configurer votre déploiement SD-WAN.

Configurer Panorama et les pare-feux pour SD-WAN

Avant de pouvoir commencer à configurer votre déploiement SD-WAN, vous devez ajouter vos pare-feux de hub et de branche en tant qu'appareils gérés et créer les modèles et configurations de groupes d'appareils nécessaires afin de soutenir correctement votre configuration SD-WAN des pare-feux SD-WAN.

- Ajouter vos pare-feux SD-WAN en tant que Périphériques gérés
- Créer un Modèle de réseau SD-WAN
- Créer les Zones prédéfinies dans Panorama
- Créer des Groupes de périphériques SD-WAN

Ajouter vos pare-feux SD-WAN en tant que Périphériques gérés

Avant de pouvoir commencer à configurer votre déploiement SD-WAN, vous devez d'abord Installer le plug-in SD-WAN et ajouter vos pare-feux de hub et de branche en tant que périphériques gérés au serveur de gestion Panorama™. Dans le cadre de l'ajout de votre pare-feu SD-WAN en tant que périphérique géré sur le serveur de gestion Panorama™, vous devez activer la licence SD-WAN pour utiliser la fonctionnalité SD-WAN pour le pare-feu.

Dans le cadre de l'ajout de vos pare-feux SD-WAN en tant que périphériques gérés, vous devez configurer vos pare-feux gérés pour transférer les journaux à Panorama. Panorama collecte les informations de plusieurs sources, comme les journaux de configuration, les journaux de trafic et les mesures des caractéristiques des liens, pour générer la visibilité de l'application SD-WAN et des informations sur l'état des liens.

Faites en sorte que la connexion de votre serveur de gestion Panorama ne dépende pas uniquement de la superposition SD-WAN. Pour maintenir une connexion fiable dans laquelle le Panorama est toujours accessible aux pare-feu PAN-OS, nous vous recommandons de créer un tunnel IPSec dédié à partir des pare-feu PAN-OS pour atteindre Panorama (c'est-à-dire à l'extérieur de la superposition SD-WAN entre le hub/les branches où se trouve le Panorama). Grâce à cette approche, vous pouvez garantir l'accessibilité au serveur de gestion Panorama à tout moment, même en cas d'impact sur la superposition SD-WAN.

STEP 1 | Launch the Firewall Web Interface (Lancez l'interface web du pare-feu).

STEP 2 | Activate your SD-WAN license (Activer votre licence SD-WAN) pour utiliser la fonctionnalité SD-WAN sur le pare-feu.

Chaque pare-feu que vous avez l'intention d'utiliser dans votre déploiement SD-WAN nécessite un code d'authentification pour activer la licence. Par exemple, si vous avez 100

pare-feux, vous devez acheter 100 licences SD-WAN et activer chaque licence SD-WAN sur chaque pare-feu en utilisant un des 100 codes d'authentification unique.

Pour les pare-feux VM-Series, vous appliquez le code d'authentification SD-WAN au pare-feu VM-Series spécifique. si vous deactivate the VM-Series firewall (désactivez le pare-feu VM-Series), le code d'authentification SD-WAN ne peut être activé sur un pare-feu VM-Series différent du même modèle.

Assurez-vous que votre licence SD-WAN reste valable pour continuer à utiliser SD-WAN. Si la licence SD-WAN expire, ce qui suit se produit :

- *Un avertissement s'affiche lorsque vous **Validez** des modifications de configuration mais aucun échec de validation ne se produit.*
- *Votre configuration SD-WAN ne fonctionne plus mais n'est pas supprimé.*
- *Les pare-feux ne surveillent plus et ne rassemblent plus les mesures d'état des liens et arrêtent d'envoyer des sondes de surveillance.*
- *Les pare-feux n'envoient plus de mesures de l'état des applications et des liens à Panorama.*
- *La logique de sélection du chemin SD-WAN est désactivée.*
- *Nouvelles sessions à tour de rôle sur virtual SD-WAN interface (l'interface virtuelle SD-WAN).*
- *Les sessions existantes restent sur le lien spécifique sur lequel elles étaient lorsque la licence a expiré.*
- *Si une coupure d'internet se produit, le trafic se poursuit en utilisant l'itinéraire standard et ECMP s'il est configuré.*

STEP 3 | Ajoutez l'adresse IP de Panorama au pare-feu.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et Edit (Modifiez) les paramètres de Panorama.
2. Saisissez l'adresse IP de Panorama dans le premier champ.

   Le FDQN (nom de domaine complet) de Panorama n'est pas compatible avec SD-WAN.
3. (Facultatif) Si vous avez configuré une paire haute disponibilité dans Panorama, entrez l'adresse IP du Panorama secondaire dans le deuxième champ.
4. Vérifiez que vous **Enable pushing device monitoring data to Panorama** (avez activé l'application des données de surveillance des périphériques à Panorama).
5. Cliquez sur **OK**.
6. **Commit (Validez)** vos modifications.

STEP 4 | Configure log forwarding to Panorama (Configurez le transfert des journaux à Panorama).

Transférer les journaux depuis vos pare-feux SD-WAN vers Panorama est nécessaire pour afficher Surveillance et Création de rapports les données.

L'inspection HTTP/2 est automatiquement activée par défaut si le décryptage du trafic des applications est activé. Les sessions parents qui utilisent une connexion HTTP/2 ne génèrent pas de journaux du trafic, car elles n'acheminent aucun trafic d'application. Cependant, les sessions enfants générées par les flux au sein de la session parent HTTP/2 continuent de générer des journaux de trafic. Pour obtenir de plus amples informations sur la consultation des journaux des connexions HTTP/2, reportez-vous à la base de données de connaissance de Palo Alto Networks.

STEP 5 | Ajoutez un ou plusieurs pare-feu à Panorama.

Pour plus d'informations sur l'ajout des pare-feux à Panorama, consultez Add a Firewall as a Managed Device (Ajouter un pare-feu en tant que périphérique géré).

1. Connectez-vous à l'interface Web Panorama.
2. Sélectionnez **Panorama** > **Managed Devices (périphériques gérés)** > **Summary (Résumé)**et **Add** (Ajoutez) les pare-feux.
3. Saisissez les numéros de série des pare-feux.
4. Si vous ajoutez des pare-feux lorsque les groupes et les modèles de périphériques nécessaires sont déjà créés, activez (cochez) **Associate Devices** (Périphériques associés) pour attribuer de nouveaux pare-feux aux groupes et à la pile de modèles de périphériques appropriés.
5. pour ajouter plusieurs pare-feux en utilisant un fichier CSV, cliquez sur **Import** (Importer) et **Download Sample CSV** (télécharger le fichier CSV d'exemple) pour peupler avec les informations du pare-feu, puis **Browse** (Naviguez) pour importer les pare-feux.
6. Cliquez sur **OK**.

STEP 6 | Sélectionnez **Commit** (valider) et **Commit and Push** (validez et appliquez) votre configuration.

STEP 7 | Répétez les Etapes 2 à 5 sur chaque pare-feu que vous avez l'intention d'utiliser lors de votre déploiement SD-WAN.

Créer un Modèle de réseau SD-WAN

Créez un modèle contenant tous les objets de configuration de réseau pour vos plateformes et vos branches SD-WAN. Vous devez créer un modèle et une pile de modèles séparés pour les pare-feux de votre hub et un modèle et une pile de modèles séparés pour les pare-feux de votre branche. Une bonne pratique consiste à limiter le nombre de modèles et de piles de modèles utilisés pour gérer la configuration de votre périphérique SD-WAN. Limiter le nombre de modèles et de piles de modèles utilisés sur les hubs et les branches réduit grandement la surcharge opérationnelles de la gestion des configurations de plusieurs hubs et branches SD-WAN. Utilisez template or template stack variables (variables de modèle ou de pile de modèles) pour réduire le nombre de modèles utilisés.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Créez le modèle de réseau de plateforme SD-WAN.

1. Sélectionnez **Panorama** > **Templates (Modèles)** et cliquez sur **Add** (Ajouter) un nouveau modèle.
2. Donnez un **Name (Nom)** descriptif au modèle.
3. (Facultatif) Saisissez une **Description** de l'interface.
4. Cliquez sur **OK** pour enregistrer les modifications de votre configuration.

STEP 3 | Créez une pile de modèle pour hub.

1. Sélectionnez **Panorama** > **Templates (Modèles)**, puis cliquez sur **Add Stack** (Ajouter une pile) pour ajouter une nouvelle pile de modèles.
2. Donnez un **Name (Nom)** descriptif à la pile de modèles.
3. (Facultatif) Saisissez une **Description** de l'interface.
4. **Add** (Ajoutez) le modèle de réseau SD-WAN que vous avez créé dans l'Étape 2.
5. Dans la section **Devices** (Périphériques), cochez les cases de tous les pare-feux de hubs SD-WAN.
6. Cliquez sur **OK** pour enregistrer les modifications de votre configuration.

STEP 4 | Créez le modèle de réseau de branche SD-WAN.

1. **Add** (Ajouter) un nouveau modèle.
2. Donnez un **Name (Nom)** descriptif au modèle.
3. (Facultatif) Saisissez une **Description** de l'interface.
4. Cliquez sur **OK** pour enregistrer les modifications de votre configuration.

STEP 5 | Créez une pile de modèle pour branche.

1. Cliquez sur **Add Stack** (Ajouter une pile) pour ajouter une nouvelle pile de modèles.
2. Donnez un **Name (Nom)** descriptif à la pile de modèles.
3. (Facultatif) Saisissez une **Description** de l'interface.
4. **Add** (Ajoutez) le modèle de réseau SD-WAN que vous avez créé dans l'Étape 4.
5. Dans la section **Devices** (Périphériques), cochez les cases de tous les pare-feux de branche SD-WAN.
6. Cliquez sur **OK** pour enregistrer les modifications de votre configuration.

STEP 6 | **Commit (validez)** vos modifications de configuration.

Créer les Zones prédéfinies dans Panorama

Les règles de politique SD-WAN utilisent des zones prédéfinies pour la sélection du chemin d'accès internet et pour des besoins de transfert de trafic. Il existe deux cas d'utilisation ; votre utilisation dépend de si vous activez SD-WAN sur vos pare-feux actuels PAN-OS® qui ont des règles de politique de sécurité existantes ou si vous commencez un tout nouveau déploiement PAN-OS sans règles de politique de sécurité antérieures. Si vos pare-feux actuels ont des règles de politique de sécurité en place, vous mappez vos zones existantes selon les zones prédéfinies que les politiques SD-WAN utilisent.

Le moteur SD-WAN utilise les zones prédéfinies pour transférer le trafic. De plus, la création des zones prédéfinies dans les modèles Panorama™ offre une visibilité cohérente entre les pare-feux gérés et Panorama :

- **Zone Internet**— Pour le trafic sortant et entrant d'un internet non approuvé.
- **Zone to Hub** (Zone vers hub) — Pour le trafic allant des pare-feux de la branche vers les pare-feux du hub et pour le trafic entre les pare-feux du hub.
- **Zone to Branch** (Zone vers branche) — Pour le trafic allant des pare-feux du hub vers les pare-feux de la branche et pour le trafic entre les pare-feux de la branche.
- **Zone Internal** (Zone interne) — Pour le trafic interne d'un emplacement spécifique.
- **Zone to PA Hub (Zone vers le hub PA)** — Pour que le trafic interne atteigne le hub Prisma Access.

Si vous ne créez pas de zones prédéfinies, le plug-in SD-WAN créera automatiquement les zones prédéfinies sur votre pare-feu de branche et de hub mais vous ne les verrez pas dans Panorama.

Il existe deux cas principaux d'utilisation pour les zones prédéfinies :

- **Existing Zones** (Zones existantes) — Vous avez déjà des zones préexistantes que vous avez créées pour une utilisation dans User-ID™ ou différentes politiques (règles de politique de sécurité, règles de politique QoS, protection de zone et protection de la mémoire tampon des paquets). Vous devez mapper les zones préexistantes selon les zones prédéfinies que SD-WAN utilise afin que le pare-feu puisse transférer correctement le trafic. Vous devez continuer à utiliser vos zones prédéfinies dans toutes vos politiques car les nouvelles zones prédéfinies sont utilisées uniquement pour le transfert SD-WAN. Vous effectuerez le mappage des zones lorsque vous Ajouter des Périphériques SD-WAN à Panorama en créant votre fichier CSV. (Si vous n'utilisez pas de fichier CSV, vous mapperez les zones lorsque vous configurerez **Panorama** > **SD-WAN** > **Devices** (périphériques SD-WAN de Panorama) et ajoutez les zones existantes à **Zone Internet**, **Zone to Hub**, **Zone to Branch**, and **Zone Internal**.)

  Le résultat du mappage est que le pare-feu d'une branche ou d'un hub peut effectuer une boucle de transfert pour déterminer l'interface de sortie SD-WAN et donc la zone de sortie. Si vous n'effectuez pas le mappage des zones préexistantes selon les zones prédéfinies, une session autorisée n'utilisera pas SD-WAN. Le mappage est nécessaire car les clients existants ont des noms de zone différents en place et le pare-feu doit réduire le nombre de ces noms de zone jusqu'aux zones prédéfinies. Vous n'avez pas forcément besoin de mapper les zones selon

toutes les zones prédéfinies mais vous devez mapper les zones préexistantes selon au moins les zones **`Zone to Hub`** et **`Zone to Branch`**.

- **No Existing Zones** (Aucune zone existante) — Vous avez un tout nouveau déploiement de pare-feux et SD-WAN de Palo Alto Networks®. Dans ce cas, vous n'avez pas de zones à mapper ; nous vous conseillons d'utiliser les zones prédéfinies dans vos politiques PAN-OS et User-ID pour simplifier le déploiement.

Avant de commencer à configurer votre déploiement SD-WAN, dans les deux cas d'utilisation ; vous devez créer les zones prédéfinies nécessaires dans Panorama appelées **`zone-internet`**, **`zone-internal`**, **`zone-to-hub`**, **`zone-to-branch`** et **`zone-to-pa-hub`**. lorsque vous embarquerez vos pare-feux de hub et branche, vous devrezAjouter des Périphériques SD-WAN à Panorama. Pour les clients préexistants, le plug-in SD-WAN mappera en interne les zones préexistantes selon les zones prédéfinies lors de l'exécution des règles de politique SD-WAN, des règles de politique QoS, protection de zone, User-ID et protection de la mémoire tampon des paquets, et utilisera les zones prédéfinies pour l'enregistrement des zones et la visibilité dans Panorama. Pour les nouveaux clients, vous effectuez une configuration correcte en utilisant les zones prédéfinies.

Les zones prédéfinies sont aussi nécessaires afin de configurer automatiquement les tunnels VPN entre vos hubs et branches SD-WAN lorsque vous appliquez la configuration depuis Panorama vers vos périphériques SD-WAN gérés.

Les noms de zones sont sensibles à la casse et doivent correspondre que noms donnés dans cette procédure. Votre validation échoue sur le pare-feu si les noms de zones ne correspondent pas à ceux décrits dans cette procédure.

Dans cet exemple, nous créons la zone appelée **`zone-internet`**.

STEP 1 | Connectez-vous à l'interface Web Panorama.

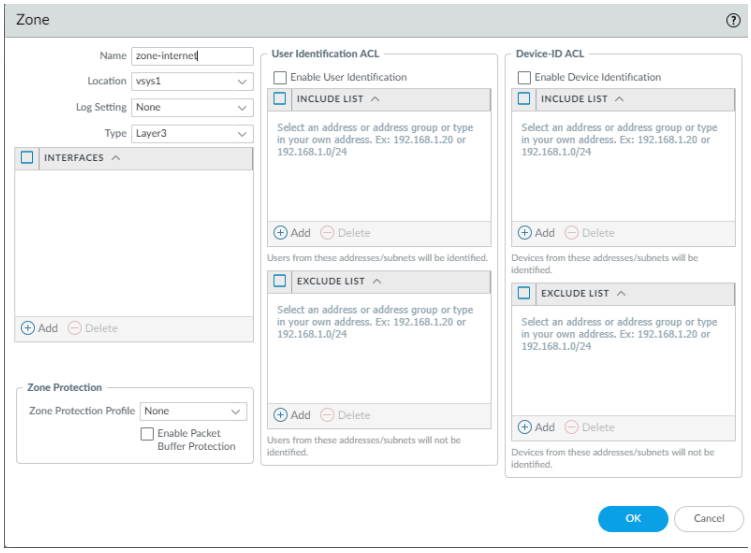
STEP 2 | Sélectionnez **Network** > **Zones** (Réseau Zones) et dans la liste déroulante du **Template** (Modèle), sélectionnez le network template (modèle de réseau) que vous avez créé au préalable.

STEP 3 | **Add** (Ajoutez) une nouvelle zone.

STEP 4 | Saisissez **`zone-internet`**, par exemple, comme **Name** (Nom) de la zone.

STEP 5 | Pour le **Type (Type)** de zone, sélectionnez **Layer3 (Couche 3)**.

STEP 6 | Cliquez sur **OK**.



STEP 7 | Répétez les étapes précédentes pour créer les zones restantes. Au total, vous devez créer les zones suivantes :

- **`zone-to-branch`**
- **`zone-to-hub`**
- **`zone-internal`**
- **`zone-internet`**
- **`zone-to-pa-hub`**

STEP 8 | **Commit** (Validez) et **Commit and Push** (Validez et appliquez) les modifications de votre configuration.

STEP 9 | **Commit (Validez)** vos modifications.

Créer des Groupes de périphériques SD-WAN

Créez des groupes de périphériques, un pour vos hubs et un pour vos branches, contenant toutes les règles de politique et les objets de configuration de vos plateformes et branches SD-WAN. Une fois que vous avez créé les groupes de périphériques pour vos hubs et branches, vous devez créer une règle de politique de sécurité dans chaque groupe de périphériques autorisant le trafic entre le hub et les zones des branches. La création de ces règles de politique de sécurité garantit que le trafic entre les zones des périphériques SD-WAN est autorisé lorsque le plug-in SD-WAN crée les tunnels VPN après que vous ayez créé un cluster VPN.

Configurez des configurations identiques sur les pare-feux de votre hub et une configuration identique sur les pare-feux de vos branches. Cela réduit considérablement la surcharge opérationnelle de la gestion des configurations de plusieurs branches et hubs SD-WAN et vous permet de dépanner, isoler, mettre à jour les problèmes de configuration plus rapidement.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Créer les Zones prédéfinies dans Panorama.

STEP 3 | Créez le Groupe de périphériques du hub SD-WAN.

1. Sélectionnez **Panorama** > **Device Groups (Groupes dé périphériques)** et **Add** (ajoutez) un groupe de périphériques.
2. Saisissez **SD-WAN_Hub** en tant que**Name** (Nom) du groupe de périphériques.
3. (Facultatif) Saisissez une **Description** de l'interface.
4. Dans la section **Devices** (Périphériques), cochez les cases pour affecter les plateformes SD-WAN au groupe.
5. Pour le **Parent Device Group** (Groupe de périphériques parent), sélectionnez**Shared** (Partagé).
6. Cliquez sur **OK**.

STEP 4 | Créez le Groupe de périphériques de la branche SD-WAN.

1. Sélectionnez **Panorama** > **Device Groups (Groupes dé périphériques)** et **Add** (ajoutez) un groupe de périphériques.
2. Saisissez **SD-WAN_Branch** en tant que**Name** (Nom) du groupe de périphériques.
3. (Facultatif) Saisissez une **Description** de l'interface.
4. Dans la section **Devices** (Périphériques), cochez les cases pour affecter les branches SD-WAN au groupe.
5. Pour le **Parent Device Group** (Groupe de périphériques parent), sélectionnez**Shared** (Partagé).
6. Cliquez sur **OK**.

STEP 5 | Créez une règle de politique de sécurité pour contrôler le trafic depuis les branches vers la zone interne du hub et depuis la zone interne du hub vers les branches.

1. Sélectionnez **Policies** > **Security** (Polices Sécurité) dans la liste déroulante **Device Group** (Groupe de périphériques), sélectionnez le groupe de périphériques **SD-WAN_Hub**.
2. **Add** (Ajoutez) une nouvelle règle de politique.
3. Saisissez un **Name** (Nom) pour la règle de politique, comme **SD-WAN access--hub DG**.
4. Sélectionnez **Source** > **Source Zone** (Source Zone de la source) et **Add** (Ajoutez) **zone-internal** et **zone-to-branch**.
5. Sélectionnez **Destination** > **Destination Zone** (Zone de de destination) et **Add** (Ajoutez) **zone-internal** et **zone-to-branch**.
6. Sélectionnez **Application** et **Add**(ajoutez) les applications à autoriser.

   Vous devez autoriser BGP si vous utilisez un routage BGP.
7. Sélectionnez **Actions** et **Allow** (Autoriser) pour autoriser les applications que vous avez sélectionnées.
8. Sélectionnez **Target** (Cible) et spécifiez les périphériques cibles auxquels Panorama™ devra appliquer cette règle.

STEP 6 | Créez une règle de politique de sécurité pour contrôler le trafic en provenance des zones internes des branches vers le hub et depuis le hub vers les zones internes des branches.

1. Sélectionnez **Policies** > **Security** (Polices Sécurité) dans la liste déroulante **Device Group** (Groupe de périphériques), sélectionnez le groupe de périphériques **SD-WAN_Branch**.
2. **Add** (Ajoutez) une nouvelle règle de politique.
3. Saisissez un **Name** (Nom) pour la règle de politique, comme **`SD-WAN access--branch DG`**.
4. Sélectionnez **Source** > **Source Zone** (Source Zone de la source) et **Add** (Ajoutez) **zone-internal** et **zone-to-hub**.
5. Sélectionnez **Destination** > **Destination Zone** (Destination Zone de la destination) et **Add** (Ajoutez) **zone-internal** et **zone-to-hub**.
6. Sélectionnez **Application** et **Add**(ajoutez) les applications à autoriser.

   Vous devez autoriser BGP si vous utilisez un routage BGP.

7. Sélectionnez **Actions** et **Allow** (Autoriser) pour autoriser les applications que vous avez sélectionnées.
8. Sélectionnez **Target** (Cible) et spécifiez les périphériques cibles auxquels Panorama devra appliquer cette règle.

STEP 7 | Validez et appliquez vos modifications de configuration.

1. **Commit** (Validez) et **Commit and Push** (Validez et appliquez) les modifications de votre configuration.
2. Dans la partie Push Scope (cadre d'application), cliquez sur **Edit Selections** (Modifier les sélections).
3. Activez (cochez) **Include Device and Network Templates** (inclure les modèles de périphériques et de réseau) et cliquez sur **OK**.
4. **Commit and Push** (Validez et appliquez) les modifications de votre configuration.

   *Deux opérations de validation sont réalisées automatiquement lorsque vous validez et appliquez la configuration du groupe et des modèles de périphériques. Affichez les **Tasks** (Tâches) pour vérifier que la deuxième validation a réussi. Sur ces deux opérations de validation, la première échoue tout le temps.*

Créer une Link Tag (Étiquette de liens)

Créez une étiquette de liens afin d'identifier un ou plusieurs liens physiques que vous souhaitez que les applications et les services utilisent dans un ordre spécifique au cours d'une distribution de trafic SD-WAN et d'une protection par basculement. Le regroupement de plusieurs liens physiques vous permet de maximiser la qualité des applications et des services si l'état du lien physique se détériore.

Lorsque vous planifiez comment regrouper vos liens, tenez compte de l'utilisation ou de l'objectif des liens et regroupez les en conséquence. Par exemple, si vous configurez des liens prévus pour un trafic à faible coût ou non crucial pour l'entreprise, créez une étiquette de liens et groupez ces interfaces ensemble afin de vous assurer que le trafic prévu passe principalement sur ces liens et pas sur des liens plus onéreux qui peuvent avoir un impact sur des applications ou des services critiques pour l'entreprise.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Sélectionnez **Objects** > **Tags** (Objets Étiquettes) puis sélectionnez le groupe de périphériques dans la liste déroulante **Device Group** (Groupe de périphériques).

STEP 3 | **Add** (Ajoutez) une nouvelle étiquette.

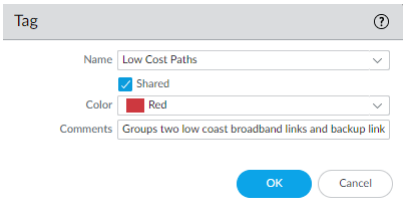
STEP 4 | Donnez un **Name (Nom)** descriptif à l'étiquette. par exemples ; Chemins à faible coût, Chemins onéreux, Accès général, HQ privé ou Sauvegarde.

STEP 5 | Activer (cocher) **Shared** pour rendre le Link Tag disponible à tous les groupes de périphériques sur le serveur de gestion PanoramaTM et à vsys par défaut sur un seul hub ou branche vsys, ou à vsys1 sur tout hub ou branche multi-vsys sur lequel vous poussez.

En configurant une Étiquette de liens partagée, Panorama peut référencer les Étiquettes de liens dans la validation de la configuration du pare-feu et valider et appliquer la configuration aux branches et hubs. La validation échoue si Panorama n'est pas capable de référencer une Étiquette de liens.

STEP 6 | (Facultatif) Sélectionnez une **Color** (couleur) pour l'étiquette.

STEP 7 | Saisissez des **Comments** (commentaires) utiles au sujet de l'étiquette. Par exemple, **`Regroupez deux liens de bande passante à faible coût et un lien de sauvegarde pour l'accès général à internet`**.



STEP 8 | Cliquez sur **OK** pour enregistrer les modifications de votre configuration.

STEP 9 | **Commit** (Validez) et **Commit and Push** (Validez et appliquez) les modifications de votre configuration.

STEP 10 | Configurer un Profil d'interface SD-WAN.

Configurer un Profil d'interface SD-WAN

Créez un profil d'interface SD-WAN pour définir les caractéristiques des connexions ISP et spécifier la vitesse des liens et la fréquence selon laquelle le pare-feu surveille le lien, et spécifier une Étiquette de liens pour le lien. Lorsque vous spécifiez la même Étiquette de liens pour plusieurs liens, vous regroupez ces liens physiques dans un lot de liens ou dans un fat pipe. Vous devez configurer un profil d'interface SD-WAN et le spécifier pour une interface Ethernet activée avec SD-WAN avant de pouvoir sauvegarder l'interface Ethernet.

Groupez les liens sur la base d'un critère commun. Par exemple, groupez les liens en fonction de la préférence de chemin depuis le plus préféré ou moins préféré ou groupez les liens par coût.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Sélectionnez **Network** > **Network Profiles** > **SD-WAN Interface Profile** (Réseau Profils de réseau Profil d'interface SD-WAN) et sélectionnez le modèle approprié dans la liste déroulante **Template** (Modèle).

STEP 3 | **Add** (Ajoutez) un profil d'interface SD-WAN.

STEP 4 | Saisissez un **Name** (Nom) simple pour le profil d'interface SD-WAN, que vous verrez dans les rapports, les résolutions de pannes et les statistiques.

STEP 5 | Sélectionnez **Location** (emplacement) vsys si vous avez un serveur de gestion Panorama™ multi-vsys. Par défaut, vsys1 est sélectionné.

STEP 6 | Sélectionnez la **Link Tag** (Étiquette de liens) que ce profil attribuera à l'interface.

STEP 7 | Ajoutez une **Description** pour le profil.

STEP 8 | Sélectionnez le **Link Type (Type de lien)** physique dans la liste prédéfinie (**ADSL/DSL**, **Cable modem (Modem câble)**, **Ethernet**, **Fiber (Fibre)**, **LTE/3G/4G/5G**, **MPLS**, **Microwave/Radio (Micro-ondes/Radio)**, **Satellite**, **WiFi**, **Private Link1 (Lien privé1)**, **Private Link2 (Lien privé2)**, **Private Link3 (Lien privé3)**, **Private Link4 (Lien privé4)**, ou **Other (Autre)**). Avec PAN-OS 11.1.3, le plug-in SD-WAN 3.2.1 et versions ultérieures prennent en charge les types de liens privés de point à point supplémentaires tels que **Private Link1 (Lien privé1)**, **Private Link2 (Lien privé2)**, **Private Link3 (Lien privé3)**et **Private Link4 (Lien privé4)**. Nous ne prenons pas en charge le trafic de texte en clair du pare-feu de la branche SD-WAN vers le pare-feu de hub SD-WAN pour les types de liens **Private Link1 (Lien privé1)**, **Private Link2 (Lien privé2)**, **Private Link3 (Lien privé3)** et **Private Link4 (Lien privé4)**. Lorsque vous configurez l'un des nouveaux types de liaison privée, assurez-vous de disposer d'une règle de politique SD-WAN sur le hub configurée uniquement avec le type de lien public. En effet, lorsque le trafic Internet est renvoyé ou échoue vers le hub depuis la branche, il doit correspondre à cette règle de politique SD-WAN. Sinon, le trafic est abandonné, car ces liens privés (**Private Link1**

(Lien privé1), **Private Link2 (Lien privé2)**, **Private Link3 (Lien privé3)**et **Private Link4 (Lien privé4)**) font partie de l'interface d'accès direct à Internet (DIA) SD-WAN.

(Pour PAN-OS 11.1.3 et versions ultérieures, le plug-in SD-WAN 3.2.1 et versions ultérieures) Pour activer les types de liens privés de point à point supplémentaires, vous devez vérifier ce qui suit :

- *Le serveur de gestion Panorama doit fonctionner sur PAN-OS 11.1.3*
- *Les appareils gérés par Panorama doivent fonctionner sur PAN-OS 11.1.3*
- *La version du plug-in SD-WAN doit être 3.2.1*

(Pour PAN-OS 11.2.0 et versions ultérieures, le plug-in SD-WAN 3.3.0 et versions ultérieures) Pour activer les types de liens privés de point à point supplémentaires, vous devez vérifier ce qui suit :

- *Le serveur de gestion Panorama doit fonctionner sur PAN-OS 11.2.0*
- *Les appareils gérés par Panorama doivent fonctionner sur PAN-OS 11.2.0*
- *La version du plug-in SD-WAN doit être 3.3.0*

Le pare-feu est compatible avec n'importe quel périphérique CPE qui se termine par une connexion Ethernet sur le pare-feu ; par exemple, les points d'accès WiFi, des modems LTE, des CPE laser/micro-onde peuvent tous se terminer par un raccord Ethernet.

Les types de liens suivants formeront des tunnels avec le même type de lien uniquement :

- *Types de liens publics (ou* ***Other (Autre)****) :* ***Ethernet****,* ***ASDL/DSL****,* ***Cable modem (Modem câble)****,* ***Fiber (Fibre)****,* ***LTE/3G/4G/5G****,* ***WiFi****et* ***Other (Autres)****.*

  Tout type de lien public vers tout autre type de lien public créera un tunnel avec succès. Par exemple, les types de lien Ethernet vers autre et Autre vers autre créeront les tunnels avec succès.

- *Types de liens privés et de point à point :****MPLS****,* ***Satellite****,* ***Private Link1 (Lien privé1)****,* ***Private Link2 (Lien privé2)****,* ***Private Link3 (Lien privé3)****,* ***Private Link4 (Lien privé4)*** *et* ***Microwave/Radio (Micro-ondes/Radio)****.*

  Un type de lien privé ne peut créer le tunnel qu'avec le même type de lien privé. Par exemple, les types de liens MPLS vers MPLS et satellite vers satellite sont valides et les tunnels seront donc créés avec succès, mais MPLS vers satellite ne créera pas le tunnel.

Pour les déploiements PAN-OS existants dont les zones sont définies sur les interfaces qui seront utilisées pour prendre en charge SD-WAN, Panorama peut configurer automatiquement le nom de la zone de l'interface sur l'une des zones SD-WAN prédéfinies dans les conditions suivantes :

1. *L'interface SD-WAN est configurée en tant que type de lien privé de point à point (****MPLS****,* ***Satellite****,* ***Private Link1 (Lien privé1)****,* ***Private Link2 (Lien privé2)****,* ***Private Link3 (Lien privé3)****,* ***Private Link4 (Lien privé4)*** *ou* ***Microwave (Micro-ondes)****) dans son profil d'interface.*
2. *La case****Assistance du tunnel de données VPN*** *est désactivée (décochée) sur le profil d'interface SD-WAN. Cela indique à PAN-OS de transférer le trafic en texte clair en dehors du tunnel VPN SD-WAN. Étant donné que les types de liens* ***Private Link1 (Lien privé1)****,* ***Private Link2 (Lien privé2)****,* ***Private Link3 (Lien privé3)****et* ***Private Link4 (Lien privé4)*** *ne prennent pas en charge le trafic de texte en clair du pare-feu de branche SD-WAN vers le pare-feu de hub SD-WAN, vous devez laisser l'option* ***VPN Data Tunnel Support (Prise en charge du tunnel de données VPN)*** *activée lorsque vous configurez ces types de liens privés.*

Sur le pare-feu Hub, le nom de la zone est configuré comme «`zone à branche`» lorsque la condition a) est remplie. Sur le pare-feu de la succursale, le nom de la zone est configuré

comme «zone à hub» lorsque les conditions a) et b) sont remplies. Panorama automatise cette étape pour simplifier la configuration afin d'assurer une communication correcte entre le hub et les pare-feu des succursales. Si vous avez des stratégies de pare-feu préexistantes qui font référence à l'ancien nom de zone, vous devez mettre à jour les stratégies pour refléter le nouveau nom de zone SD-WAN prédéfini.

STEP 9 | Spécifiez la vitesse de **Maximum Download (Mbps)** (téléchargement maximum (Mbps) de l'ISP en mégabits par seconde (la fourchette va de 0 à 100 000; il n'y a pas de valeur par défaut). Vous pouvez saisir une plage contenant un maximum de trois décimales, par exemple, 10,456. Demandez à votre ISP la vitesse du lien ou prenez un échantillon des vitesses maximales du lien à l'aide d'un outil comme speedtest.net et prenez la moyenne des maximales sur une bonne durée de temps.

STEP 10 | Spécifiez la vitesse de **Maximum Download (Mbps)** (téléchargement maximum (Mbps) de l'ISP en mégabits par seconde (la fourchette va de 0 à 100 000 ; il n'y a pas de valeur par défaut). Vous pouvez saisir une plage contenant un maximum de trois décimales, par exemple, 10,456. Demandez à votre ISP la vitesse du lien ou prenez un échantillon des vitesses maximales du lien à l'aide d'un outil comme speedtest.net et prenez la moyenne des maximales sur une bonne durée de temps.

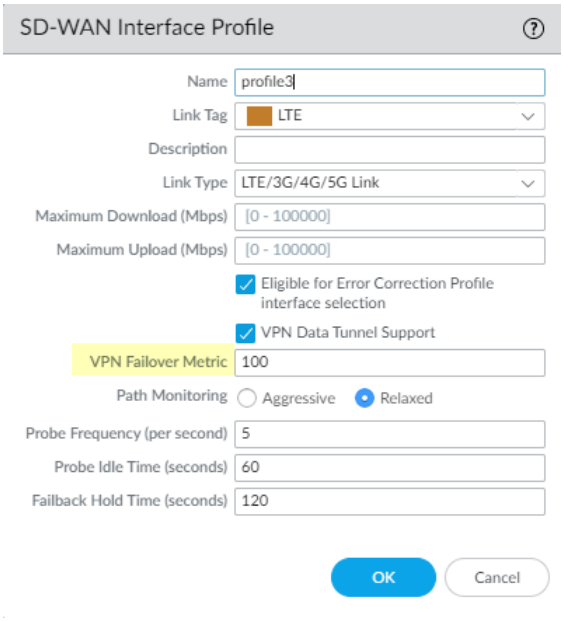
STEP 11 | Sélectionnez **Eligible for Error Correction Profile interface selection (Admissible à la sélection d'interface de profil de correction des erreurs)** pour activer le transfert de correction des erreurs (FEC) ou la duplication de paquet pour les interfaces. Vous devez activer cette option sur les pare-feu de cryptage et de décryptage ; vous devez également créer un profil de correction des erreurs à appliquer à la règle de politique SD-WAN des applications spécifiées.

STEP 12 | **VPN Data Tunnel Support (Assistance de tunnel de données VPN)** détermine si le trafic de la branche vers le hub et le trafic de retour passent par un tunnel VPN pour plus de sécurité (méthode par défaut) ou passe en dehors du tunnel VPN afin d'éviter la surcharge du cryptage.

- Laissez **VPN Data Tunnel Support** (Assistance du tunnel de données VPN) activé pour les types de liens publics qui ont des connexions internet directes ou une capacité d'interruption d'internet, comme le modem câble, l'ADSL et les autres connexions internet.
- Vous pouvez désactiver l'option **VPN Data Tunnel Support (Prise en charge du tunnel de données VPN)** pour les types de liens privés tels que MPLS, satellite ou micro-ondes qui n'ont pas de capacité de dérivation Internet , sauf des types de liens **Private Link1 (Lien privé1)**, **Private Link2 (Lien privé2)**, **Private Link3 (Lien privé3)**et **Private Link4 (Lien privé4)**. Cependant, vous devez d'abord vous assurer que le trafic ne peut pas être intercepté parce qu'il sera envoyé en dehors du tunnel VPN.
- (Plug-in SD-WAN 3.2.1 et versions ultérieures) Étant donné que les types de liens **Private Link1 (Lien privé1)**, **Private Link2 (Lien privé2)**, **Private Link3 (Lien privé3)**et **Private Link4 (Lien privé4)** ne prennent pas en charge le trafic de texte en clair du pare-feu de branche SD-WAN vers le pare-feu de hub SD-WAN, vous devez maintenir l'option **VPN Data Tunnel Support (Prise en charge du tunnel de données VPN)** activée lorsque vous configurez ces types de liens privés.
- La branche peut avoir un trafic DIA qui nécessite de basculer sur le lien MPLS privé se connectant au hub et atteindre internet depuis le hub. Le réglage de **VPN Data Tunnel Support (Assistance du tunnel de données VPN)** détermine si les données privées passent

par le tunnel VPN ou en dehors du tunnel et le trafic qui a basculé utilise l'autre connexion (que le flux de données privées n'utilise pas). Le pare-feu utilise des zones pour segmenter le trafic qui a bascule en DIA depuis le trafic MPLS privé.

STEP 13 | Si vous Configuration de DIA AnyPath, une interface virtuelle principale peut comporter plusieurs interfaces virtuelles de plate-forme. Vous devez donc prioriser l'ordre de sélection d'une plate-forme donnée lors d'un basculement. Pour ce faire, configurez la **VPN Failover Metric (Mesure de basculement VPN)** des tunnels VPN regroupés dans l'interface virtuelle de plate-forme où ce profil est appliqué. Plus la mesure est faible, plus la priorité d'être sélectionnée lors d'un basculement est élevée. Si plusieurs interfaces virtuelles de plate-forme possèdent la même valeur de mesure, SD-WAN leur envoie le nouveau trafic de session au moyen de la permutation circulaire.



STEP 14 | (Facultatif) Sélectionnez le mode **Path Monitoring** (surveillance des chemins) dans lequel le pare-feu surveille les interfaces auxquelles vous appliquez le profil d'interface SD-WAN.

*Le pare-feu sélectionne ce qu'il considère être la meilleure méthode de surveillance sur la base du **Link Type** (Type de lien). Conservez le réglage par défaut pour le type de lien sauf si une interface (à laquelle vous appliquez ce profil) a des problèmes qui nécessitent une surveillance des chemins plus agressive ou plus souple.*

- **Aggressive** (mode agressif) — (Par défaut pour tous les types sauf LTE et Satellite) Le pare-feu sonde les paquets à l'extrémité opposée du lien SD-WAN à une fréquence constante. Utilisez ce mode si vous avez besoin d'une détection rapide et d'un basculement dans des conditions de défaillance ou de panne générale.
- **Relaxed** (Mode souple) —(Par défaut pour les types de lient LTE et Satellite) Le Pare-feu patiente quelques secondes (le**Probe Idle Time**) (délai d'attente de la sonde) entre l'envoi d'ensemble de paquets de sondage, ce qui rend la surveillance des chemins moins fréquente. Lorsque le délai d'attente de la sonde expire, le pare-feu envoie des sondes pendant sept secondes selon la **Probe Frequency** configurée. Utilisez ce mode lorsque vous avez des liens de bande passante faibles, des liens qui chargent en fonction de l'usage

(comme LTE) ou lorsque la détection rapide n'est pas aussi importante que la préservation du coût et de la bande passante.

STEP 15 | Réglez la **Probe Frequency (per second)** (Fréquence de sondage (par seconde), qui correspond au nombre de fois par seconde où le pare-feu envoie un paquets de sondage à l'extrémité opposée du lien SD-WAN (la fourchette est de 1 à 5 ; la valeur par défaut est de 5). Les paramètres par défaut permettent une détection en moins d'une seconde des conditions de défaillance et de panne générale.

*Si vous modifiez la Fréquence de sondage pour un modèle Panorama, vous devez aussi ajuster le seuil du pourcentage de **Packet Loss** (perte de paquets) dans un profil de Qualité du chemin pour un groupe de périphériques de Panorama.*

STEP 16 | Si vous sélectionnez le mode de surveillance des chemins **Relaxed** (souple), vous pouvez régler le**Probe Idle Time (seconds)** (délai d'attente de la sonde (secondes)) pendant lequel le pare-feu attend entre des ensembles de paquets de sondage (la fourchette va de 1 à 60 ; la valeur par défaut est 60).

STEP 17 | Saisissez le **Failback Hold Time (seconds)** (délai d'attente avant basculement (en secondes) pendant lequel le pare-feu attend qu'un lien récupéré soit qualifié avant que le pare-feu réaffecte ce lien en tant que lien préféré après le basculement (la fourchette va de 20 à 120 ; la valeur par défaut est 120).

STEP 18 | Cliquez sur **OK** pour enregistrer le profil.

STEP 19 | **Commit** (Validez) et **Commit and Push** (Validez et appliquez) les modifications de votre configuration.

STEP 20 | Surveillez les mesures d'état de votre application et du chemin de vos liens et générez des rapports sur la performance d'état de l'application et des liens. Pour plus d'informations, consultez Surveillance et Création de rapports.

Configurer une interface Ethernet physique pour SD-WAN

Dans Panorama, configurez une interface physique Ethernet Couche 3 et activez la fonctionnalité SD-WAN. Pour configurer une interface physique, vous devez lui attribuer une adresse IPv4 ou IPv6, ou les deux. Vous devez attribuer également à l'interface une passerelle de saut suivant entièrement qualifiée et un profil d'interface SD-WAN. (SD-WAN ne prend en charge qu'un type d'interface Couche 3 ; il ne prend pas en charge les réseaux Couche 2 tels que VPLS.)

Après avoir utilisé Panorama pour créer un cluster VPN et exporté les informations de votre branche et de votre hub dans le fichier CSV, une configuration Auto VPN du plug-in SD-WAN utilise ces informations pour générer une configuration pour les branches et les hubs associés qui incluent les zones SD-WAN prédéfinies et crée des tunnels VPN sécurisés entre les branches et les hubs SD-WAN. La configuration Auto VPN génère aussi la configuration BGP si vous saisissez des informations BGP dans le fichier CSV ou dans Panorama lorsque vous ajoutez une branche ou un hub SD-WAN.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**, sélectionnez le modèle approprié dans la liste déroulante **Template (modèle)**, sélectionnez un numéro d'emplacement, comme Slot1, et sélectionnez une interface (par exemple, ethernet1/1).

STEP 3 | Sélectionnez **Interface Type** (Type d'interface) en tant que **Layer3** (Couche 3).

STEP 4 | Dans l'onglet **Config**, pour un moteur de routage existant, sélectionnez un **Virtual Router (routeur virtuel - VR)** ou créez un nouveau routeur virtuel. Pour Advanced Routing Engine (Moteur de routage avancé), sélectionnez un **Routeur logique** ou créez un nouveau routeur logique.

STEP 5 | Attribuez la**Security Zone** (Zone de sécurité) appropriée à l'interface que vous configurez.

Par exemple, si vous créez une liaison montante vers un ISP, vous devez savoir que l'interface Ethernet que vous choisissez va vers une zone non approuvée.

STEP 6 | Pour activer SD-WAN sur une interface IPv4, sélectionnez l'onglet **IPv4** et **Enable SD-WAN (Activer SD-WAN)**.

Le plug-in SD-WAN 3.2.0 et les versions ultérieures vous permettent de configurer jusqu'à quatre adresses IP pour une interface compatible SD-WAN. Le plug-in SD-WAN utilise uniquement la première adresse IP de la liste d'adresses IP configurées pour créer le tunnel SD-WAN.

Le SD-WAN tient uniquement compte de la première adresse **IP** de la **Next Hop Gateway (Passerelle du saut suivant)** et ignore les adresses **IP** restantes de la liste.

(Déploiements HA uniquement) Si vous souhaitez rétrograder de la version 3.2.0 du plug-in SD-WAN vers la version 3.1.0 ou antérieure, supprimez les configurations HA active/passive sur les deux pare-feu avant de tenter de réaliser une procédure de rétrogradation, comme la rétrogradation des versions de plug-in PAN-OS et SD-WAN.

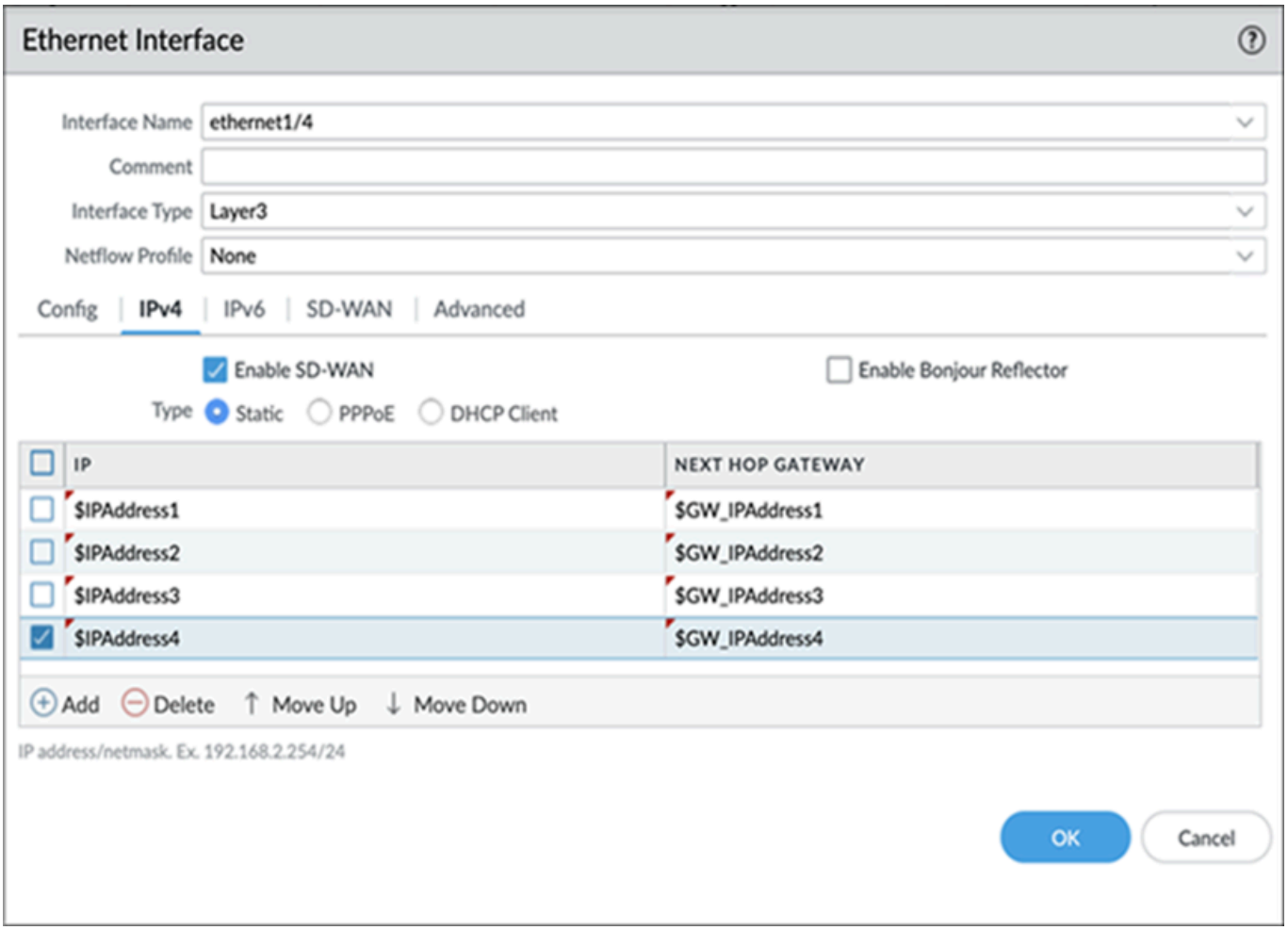
STEP 7 | Pour une interface IPv4, sélectionnez **Type** d'adresse :

- **Static** (statique) — Dans le champ**IP**, **Add** (Ajoutez) une adresse IPv4 et une longueur de préfixe pour l'interface. Vous pouvez utiliser une variable définie comme $uplink avec une fourchette d'adresses. Saisissez l'adresse IPv4 du **Next Hop Gateway (Portail de saut suivant)** (le saut suivant de votre adresse IPv4 que vous venez de saisir). La Passerelle du saut suivant doit être sur le même réseau secondaire que l'adresse IPv4. La Passerelle du saut suivant est l'adresse IP du routeur par défaut de l'ISP que l'ISP vous a donné lorsque vous avez acheté le service. Dans l'adresse IP du saut suivant vers laquelle le pare-feu envoie le trafic pour atteindre le réseau de l'ISP et, en dernier lieu, internet et le hub.
- **PPPoE**—**Enable (Activez)** l'authentification PPPoE des liaisons DSL, saisissez le **Username (Nom d'utilisateur)** et le **Password (Mot de passe)**, puis **Confirm Password (Confirmez le mot de passe)**.
- **DHCP Client (Client DHCP)** – Il est crucial que le DHCP attribue une passerelle par défaut, également appelée passerelle du saut suivant pour la connexion ISP. L'ISP fournira toutes

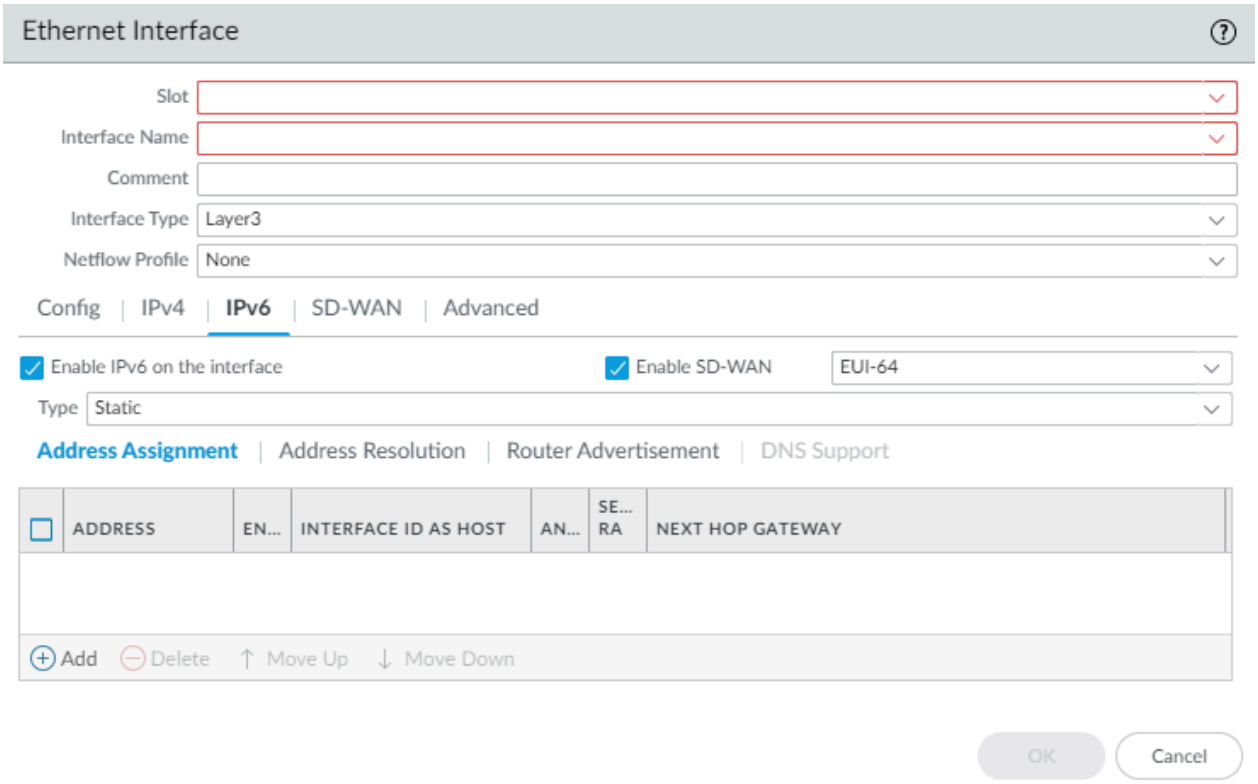
les informations nécessaires, comme l'adresse IP dynamique, les serveurs DNS et la passerelle par défaut.

*Bien que le client DHCP soit pris en charge pour une interface de hub ou de branche, il vous est préférable d'attribuer une adresse **Static (Statique)** sur une interface de hub au lieu du client DHCP. L'utilisation de DHCP sur un concentrateur nécessite le service DDNS de Palo Alto Networks. L'utilisation d'une adresse statique sur le site hub crée un environnement plus stable, car DDNS n'est pas impliqué lors de la résolution des modifications d'adresse IP DHCP et parce que le service DDNS peut prendre quelques minutes pour enregistrer la nouvelle adresse IP lors de sa modification. Si vous avez plusieurs sites de branches connectés au site d'un hub, la stabilité est essentielle pour maintenir le réseau en cours de fonctionnement.*

*Si vous sélectionnez le Client DHCP, veillez à désactiver l'option **Automatically create default route pointing to default gateway provided by server (Créer automatiquement un itinéraire par défaut en direction de la passerelle par défaut fournie par le serveur)**, qui est activée par défaut.*



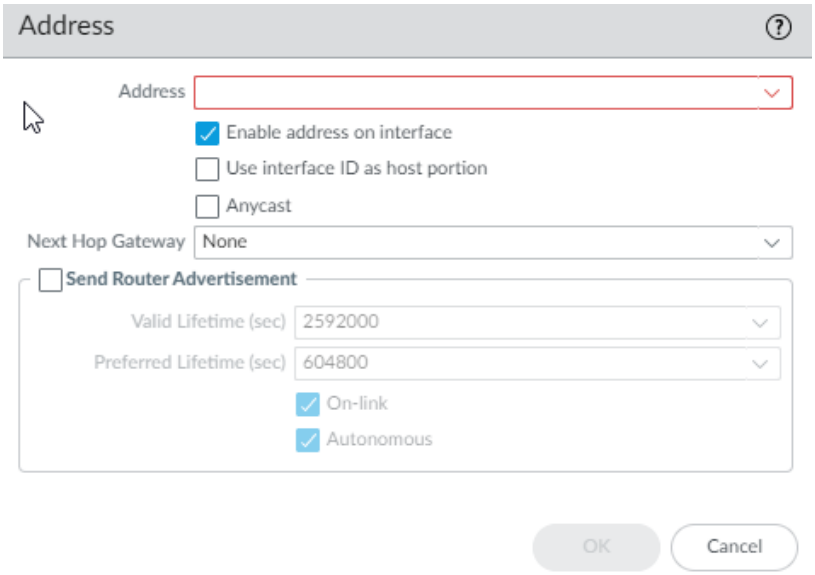
STEP 8 | Pour activer SD-WAN sur une interface IPv6, sélectionnez l'onglet **IPv6**, **Enable IPv6 on the interface (Activer IPv6 sur l'interface)** et **Enable SD-WAN (Activer SD-WAN)**.



STEP 9 | Dans le champ **EUI-64 (default 64-bit Extended Unique Identifier) (identifiant unique étendu 64 bits par défaut)**, saisissez EUI 64 bits au format hexadécimal. Si ce champ n'est pas renseigné, le pare-feu utilise l'identifiant unique étendu sur 64'A0;bits (EUI-64) généré à partir de l'adresse MAC de l'interface physique. Si vous activez l'option **Use interface ID as host portion (Utiliser l'ID de l'interface comme partie hôte)** lors de l'ajout d'une adresse, le pare-feu utilise l'ID de l'interface comme partie hôte de l'adresse.

STEP 10 | Pour une interface IPv6, sélectionnez le **Type** d'adresse sur **Static (Statique)**. Sélectionnez l'onglet **Address Assignment (Attribution d'adresse)**.

1. **Add (Ajoutez)** une **Address (Adresse)** IPv6 pour l'interface ou sélectionnez **New Variable (Nouvelle variable)** pour créer la variable. SD-WAN prend en charge une adresse IPv6 par interface physique.
2. **Enable address on interface (Activer l'adresse sur l'interface)**.



3. **Use interface ID as host portion (Utiliser l'ID d'interface comme partie hôte)** – Consultez l'étape précédente pour une explication.
4. **Anycast** – Sélectionnez cette option pour faire de l'adresse IPv6 (itinéraire) une adresse Anycast (itinéraire), ce qui veut dire que plusieurs emplacements peuvent publier le même préfixe et que l'adresse IPv6 envoie le trafic anycast au nœud qu'il considère le plus près selon les coûts associés au protocole de routage et d'autres facteurs.
5. **Next Hop Gateway (Passerelle du saut suivant)** – Saisissez l'adresse IPv6 de la Passerelle du saut suivant (le prochain saut à partir de l'adresse IPv6 que vous avez saisie). La Passerelle du saut suivant doit se trouver sur le même sous-réseau que l'adresse IPv6. La Passerelle du saut suivant est l'adresse IP du routeur par défaut de l'ISP que l'ISP vous a donné lorsque vous avez acheté le service. Il s'agit de l'adresse IP du saut suivant à laquelle le pare-feu envoie le trafic pour atteindre le réseau de l'ISP et, en fin de compte, l'Internet et le hub.
6. **Send Router Advertisement (Envoyer la publicité de routeur)** – Sélectionnez cette option pour permettre au pare-feu d'envoyer cette adresse dans les publicités de routeur, auquel cas vous devez également activer l'option **Enable Router Advertisement (Activer la publicité de routeur)** globale pour l'interface (dans l'onglet **Router Advertisement (Publicité de routeur)**).
7. **Valid Lifetime (Durée de vie valide) (sec)** – Saisissez la durée de vie valide (en secondes) pendant laquelle le pare-feu considère l'adresse comme valide. La durée de vie valide doit être supérieure ou égale à la valeur **Preferred Lifetime (Durée de vie préférée)** (valeur par défaut de 2 592 000).
8. **Preferred Lifetime (Durée de vie préférée) (sec)** – Saisissez la durée de vie préférée (en secondes) pendant laquelle l'adresse valide est préférée, ce qui signifie que le pare-feu

peut l'utiliser pour envoyer et recevoir du trafic. Lorsque la durée de vie préférée expire, le pare-feu ne peut plus utiliser l'adresse pour établir de nouvelles connexions, mais toutes les connexions existantes restent valides jusqu'à l'expiration de la durée de vie valide (valeur par défaut de 604 800).

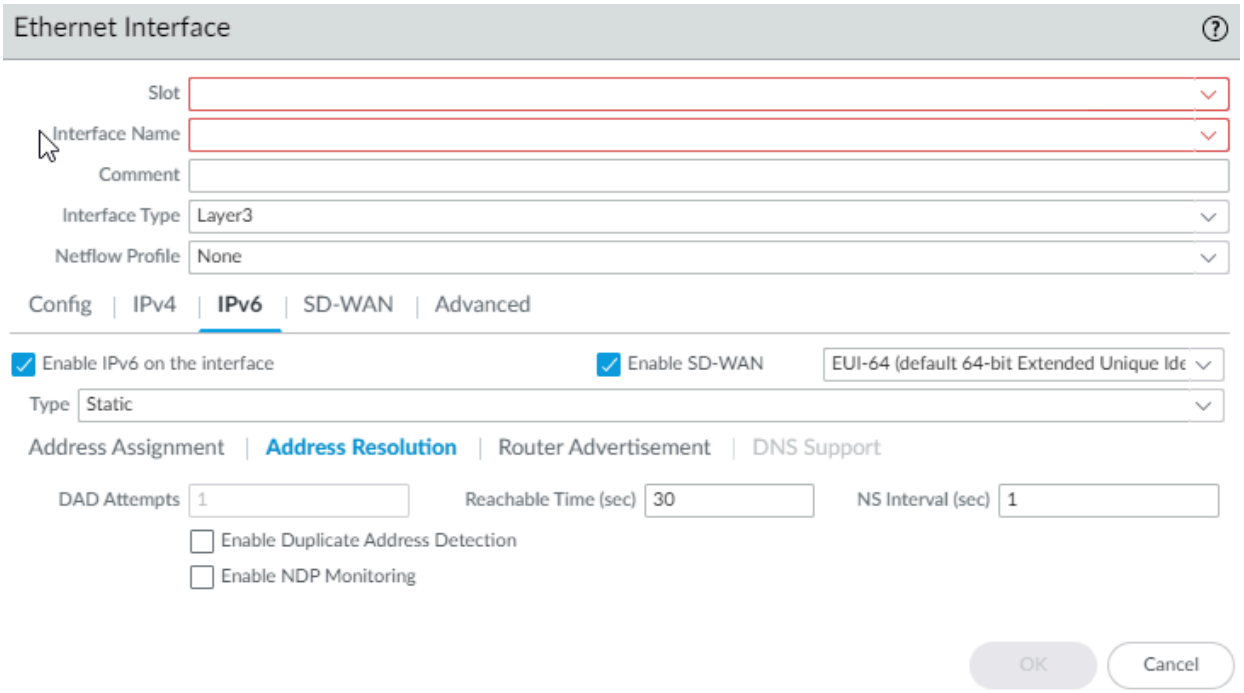
9. **On-link (Sur la liaison)** - Sélectionnez si les systèmes qui disposent d'adresses dans le préfixe sont accessibles sans routeur.
10. **Autonomous (Autonome)** – Sélectionnez cette option si les systèmes peuvent créer une adresse IP de façon indépendante en combinant le préfixe publié avec un ID d'interface.
11. Cliquez sur **OK**.

STEP 11 | Pour une interface IPv6 statique, configurez la résolution d'adresses.

1. Sélectionnez **Address Resolution (Résolution d'adresse)**.
2. Activez **Duplicate Address Detection (Détection d'adresses en double (DAD))** si vous souhaitez que l'unicité d'une adresse IPv6 potentielle soit vérifiée avant qu'elle ne soit affectée à l'interface (la valeur par défaut est activée).
3. Si vous avez sélectionné **Enable Duplicate Address Detection (Activer la détection des adresses en double)**, spécifiez le nombre de **DAD Attempts (tentatives DAD)** dans l'intervalle de sollicitation de voisinage (NS) avant l'échec de la tentative d'identification des voisins ; plage comprise entre 1 et 10 ; la valeur par défaut est 1.
4. Entrez le **Reachable Time (sec) (temps d'accessibilité (sec))**, la durée pendant laquelle le client suppose qu'un voisin est joignable après avoir reçu un message de confirmation d'accessibilité ; la plage est comprise entre 10 et 36 000 ; la valeur par défaut est 30.
5. Entrez **NS Interval (sec) (intervalle NS (sec))** (intervalle de sollicitation de voisin), la durée entre les sollicitations de voisins ; plage comprise entre 1 et 3 600 ; la valeur par défaut est 1.
6. **Enable NDP Monitoring (Activez NDP Monitoring)** pour activer la surveillance du protocole de découverte des voisins. Lorsqu'il est activé, vous pouvez sélectionner l'icône NDP dans la colonne Features (Fonctionnalités) et consulter des informations

telles que l'adresse IPv6 d'un voisin découverte par le pare-feu, l'adresse MAC correspondante, l'ID utilisateur et l'état (selon la situation la plus favorable).

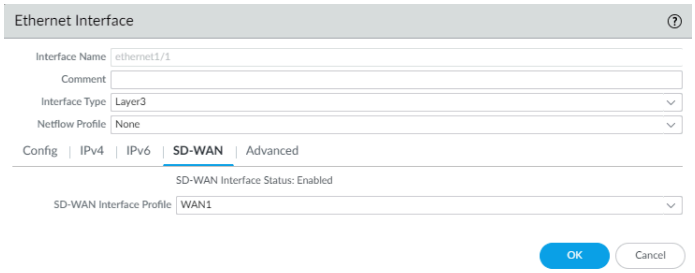
7. Cliquez sur **OK**.



STEP 12 | Si vous souhaitez permettre à l'interface d'envoyer des publicités de routeur (RA) IPv6 et éventuellement de régler les paramètres RA, configurez la Publicité du routeur comme indiqué dans la section Configurer les interfaces de couche 3 du Guide de l'administrateur réseau PAN-OS.

STEP 13 | Dans l'onglet **SD-WAN**, sélectionnez un **SD-WAN Interface Profile** (profil d'interface SD-WAN) que vous avez créé (ou créez un nouveau SD-WAN Interface Profile(profil d'interface SD-WAN)) à appliquer à cette interface. Le Profil d'interface SD-WAN a une étiquette de liens associée et les interfaces auxquelles ce profil s'applique auront cette étiquette de liens associée. Une interface ne peut avoir qu'une seule étiquette de lien.

STEP 14 | Cliquez sur **OK (OK)** pour enregistrer l'interface ethernet.

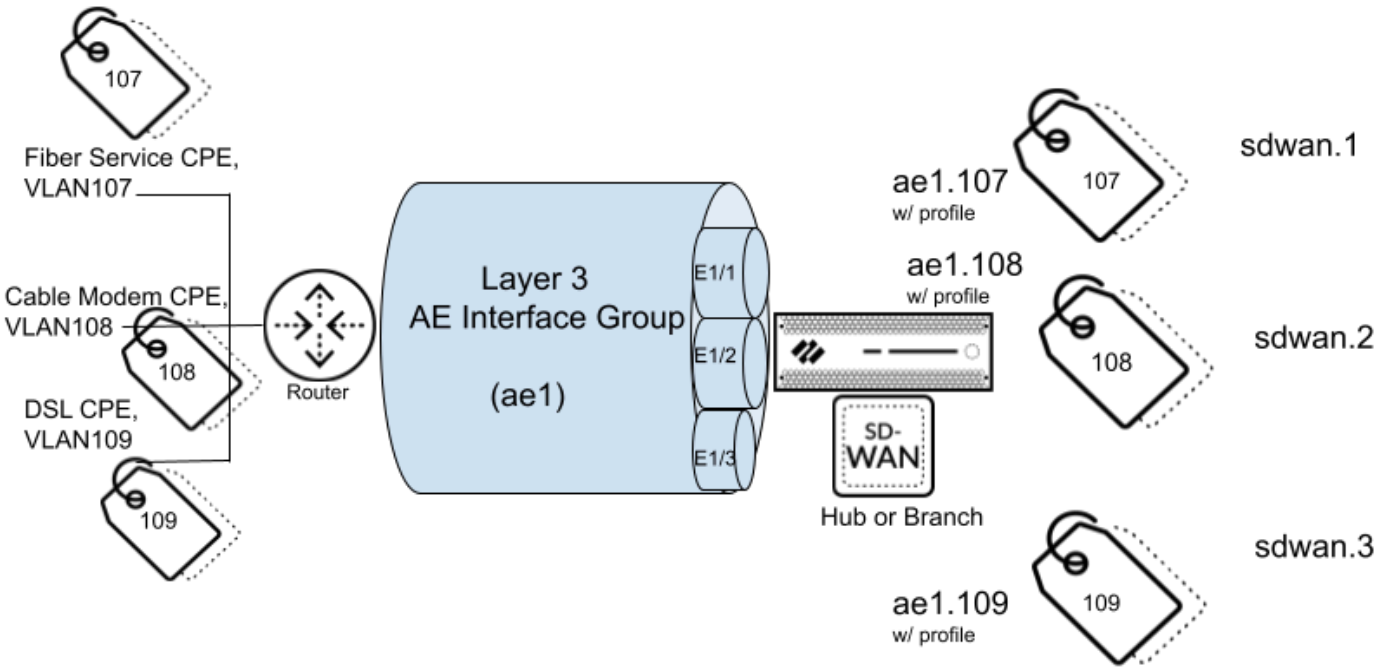


STEP 15 | **Commit** (Validez) et **Commit and Push** (Validez et appliquez) les modifications de votre configuration.

STEP 16 | (Configuration SD-WAN manuelle uniquement) Configurer une Interface virtuelle SD-WAN.
La configuration Auto VPN effectuera cette tâche si vous utilisez Auto VPN.

Configurer une interface Ethernet agrégée et des sous-interfaces pour SD-WAN

Les pare-feu physiques exécutant PAN-OS 11.0 et SD-WAN Plugin 2.1.0 prennent en charge SD-WAN sur des interfaces Ethernet agrégées (AE) afin qu'un pare-feu SD-WAN dans un centre de données, par exemple, puisse avoir un groupe d'interfaces agrégées (bundle) d'interfaces Ethernet physiques qui assurent la redondance des liaisons. SD-WAN prend en charge les interfaces AE avec ou sans sous-interfaces. Vous pouvez créer une interface AE avec des sous-interfaces que vous pouvez baliser pour différents services ISP afin de fournir une segmentation du trafic de bout en bout. Ainsi, vos services ISP peuvent atteindre plusieurs laboratoires ou bâtiments sans avoir besoin d'une paire de fibres dédiée pour chaque connexion. Un groupe d'interfaces de couche 3 AE se connecte à un routeur, comme illustré dans la figure suivante :



Les pare-feux VM-Series ne prennent pas en charge les interfaces AE. Un hub SD-WAN ou un pare-feu de branche doté d'une interface AE ne doit pas appartenir au même cluster VPN qu'un hub SD-WAN ou un pare-feu de branche VM-Series car les interfaces AE ne sont pas prises en charge sur les pare-feu VM-Series.

PPPoE n'est pas pris en charge sur les sous-interfaces.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Configurer un Profil d'interface SD-WAN pour chaque connexion ISP (sous-interface) dans le groupe d'interfaces AE pour définir ses attributs de lien.

STEP 3 | Créez un groupe d'interfaces AE.

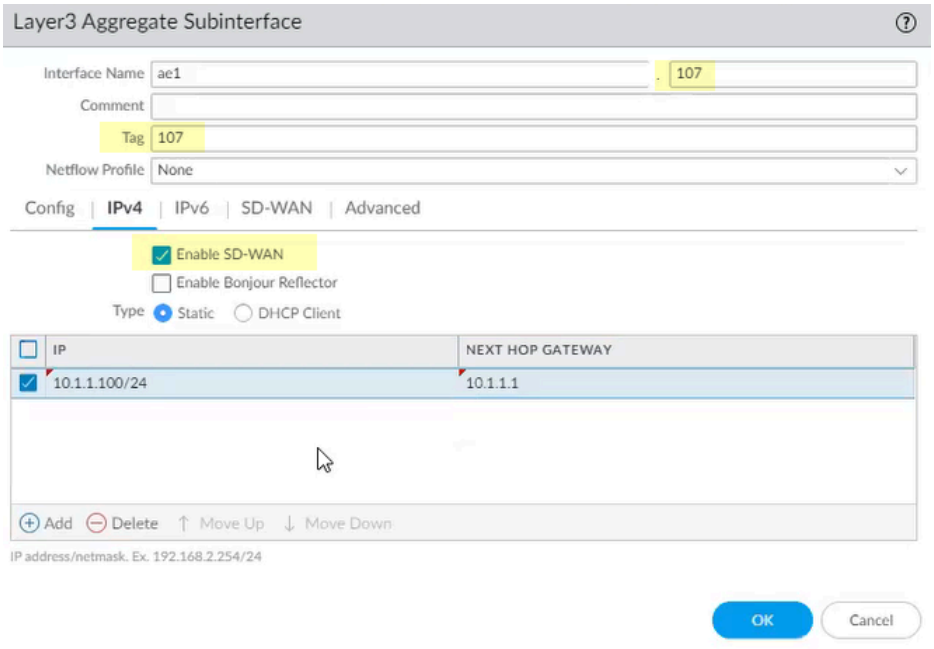
1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**, sélectionnez un **Template (modèle)** de Panorama et **Add Aggregate Group (ajoutez un groupe d'agrégats)**.
2. Pour **Interface Name (Nom de l'interface)**, entrez le numéro pour identifier le groupe agrégé ; la plage est de 1 à 16.
3. Sous **Interface Type (Type d'interface)**, sélectionnez **Layer3 (Couche 3)**.
4. Cliquez sur **OK**.

STEP 4 | Attribuez des interfaces physiques au groupe agrégé.

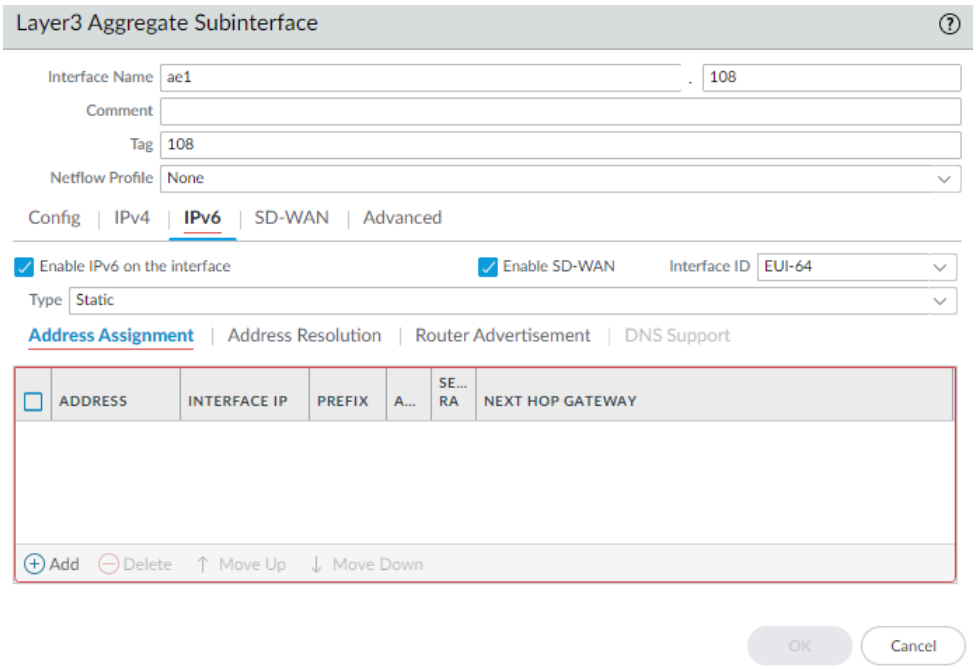
1. Sélectionnez **Network (réseau)** > **Interfaces** > **Ethernet** et sélectionnez l'interface que vous souhaitez affecter au groupe agrégé.
2. Sélectionnez pour **Interface Type (type d'interface)** **Aggregate Ethernet (Ethernet agrégé)**.
3. Sélectionnez le **Aggregate Group (groupe d'agrégats)** que vous avez créé ; par exemple, ae1.
4. Dans l'onglet **Advanced (Avancé)**, sélectionnez **Link Speed (vitesse de liaison)**, **Link Duplex (duplex de liaison)** et **Link State (état de liaison)**.
5. Cliquez sur **OK**.
6. Répétez cette étape pour chaque interface que vous souhaitez affecter au groupe agrégé.

STEP 5 | Pour le groupe agrégé, créez une sous-interface qui utilise une adresse IP statique.

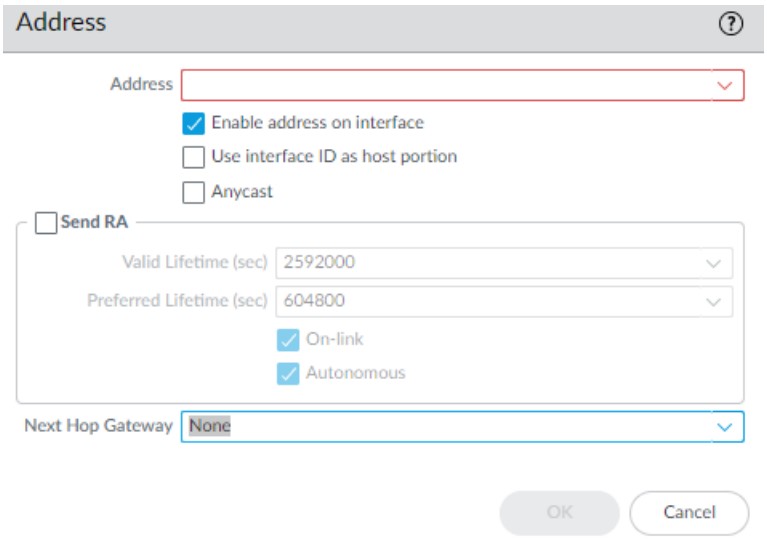
1. Sélectionnez **Network (réseau)** > **Interfaces** > **Ethernet**, mettez en surbrillance l'interface agrégée, telle que ae1, et cliquez sur **Add Subinterface (Ajouter une sous-interface)** en bas de l'écran.
2. Pour **Interface Name (Nom de l'interface)**, entrez un nombre après le point, tel que 107.
3. Saisissez la **Tag (balise)** VLAN pour différencier les sous-interfaces. Donnez à la balise le même numéro que l'ID de la sous-interface pour simplifier son utilisation.
4. Pour configurer une adresse IPv4 statique pour la sous-interface, sélectionnez l'onglet **IPv4** et **Enable SD-WAN (Activer SD-WAN)**.



5. Sélectionnez le **Type** d'adresse : **Static (Statique)**
6. **Add (Ajoutez) IP (adresse IP)** (et le masque de sous-réseau) de la sous-interface.
7. Saisissez l'adresse IP de **Next Hop Gateway (passerelle Next Hop)**.
8. Pour configurer une adresse IPv6 statique pour la sous-interface, sélectionnez l'onglet **IPv6**, **Enable IPv6 on the interface (Activer IPv6 sur l'interface)** et **Enable SD-WAN (Activer SD-WAN)**.



9. Dans le champ **EUI-64 (default 64-bit Extended Unique Identifier) (identifiant unique étendu 64 bits par défaut)**, saisissez EUI 64 bits au format hexadécimal. Si ce champ n'est pas renseigné, le pare-feu utilise l'identifiant unique étendu sur 64'A0;bits (EUI-64) généré à partir de l'adresse MAC de l'interface physique. Si vous activez l'option **Use interface ID as host portion (Utiliser l'ID de l'interface comme partie hôte)** lors de l'ajout d'une adresse, le pare-feu utilise l'ID de l'interface comme partie hôte de l'adresse.
10. Sélectionnez **Address Assignment (Attribution d'adresse)** et **Add (Ajoutez)** une **Address (Adresse)** IPv6 pour l'interface ou sélectionnez **New Variable (Nouvelle variable)** pour créer la variable.



11. **Use interface ID as host portion (Utiliser l'ID d'interface comme partie hôte)** ; voir la sous-étape précédente pour **EUI-64**.
12. Sélectionnez **Anycast** pour faire de l'adresse IPv6 (itinéraire) une adresse Anycast (itinéraire), ce qui veut dire que plusieurs emplacements peuvent publier le même préfixe

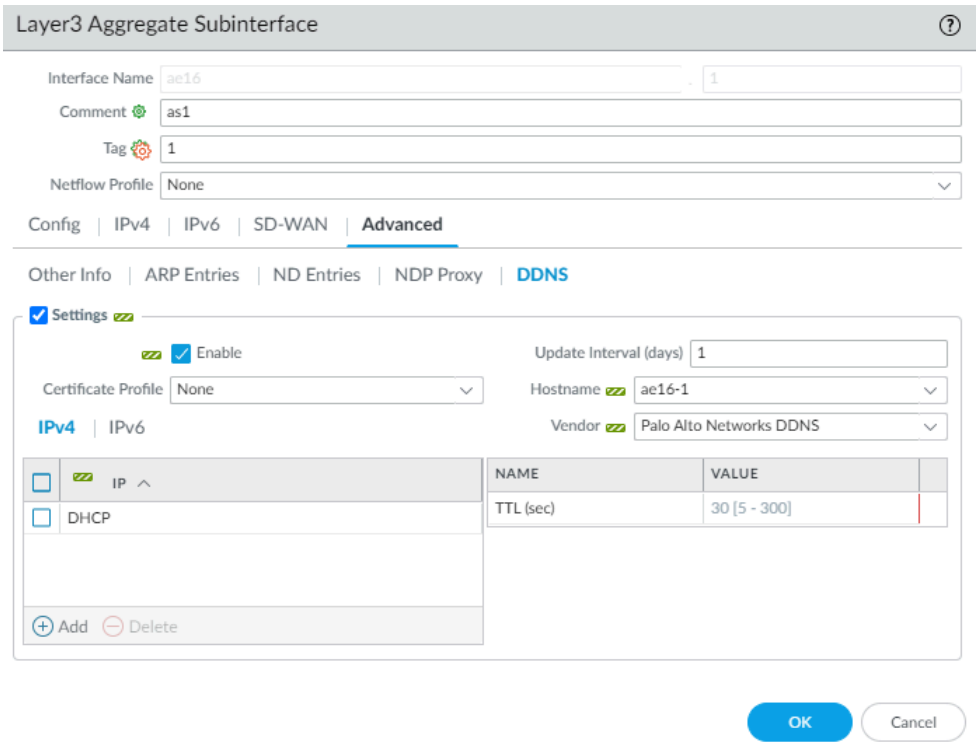
et que l'adresse IPv6 envoie le trafic anycast au nœud qu'il considère le plus près selon les coûts associés au protocole de routage et d'autres facteurs.

13. Saisissez l’adresse IPv6 de **Next Hop Gateway (Passerelle du saut suivant)** (le saut suivant de votre adresse IPv6 que vous venez de saisir). La Passerelle du saut suivant doit se trouver sur le même sous-réseau que l’adresse IPv6. La Passerelle du saut suivant est l’adresse IP du routeur par défaut de l’ISP que l’ISP vous a donné lorsque vous avez acheté le service. Il s'agit de l'adresse IP du saut suivant à laquelle le pare-feu envoie le trafic pour atteindre le réseau de l’ISP et, en fin de compte, l’Internet et le hub.
14. Sélectionnez **Send Router Advertisement (Envoyer la publicité de routeur)** pour permettre au pare-feu d'envoyer cette adresse dans les publicités de routeur, auquel cas vous devez également activer l'option **Enable Router Advertisement (Activer la publicité de routeur)** globale pour l'interface (dans l'onglet Router Advertisement (Publicité de routeur)).
15. Saisissez la **Valid Lifetime (Durée de vie valide) (sec)** en secondes pendant laquelle le pare-feu considère l'adresse comme valide. La durée de vie valide doit être supérieure ou égale à la valeur **Preferred Lifetime (Durée de vie préférée)** (valeur par défaut de 2 592 000).
16. Saisissez la **Preferred Lifetime (Durée de vie préférée) (sec)** en secondes pendant laquelle l’adresse valide est préférée, ce qui signifie que le pare-feu peut l’utiliser pour envoyer et recevoir du trafic. Lorsque la durée de vie préférée expire, le pare-feu ne peut plus utiliser l’adresse pour établir de nouvelles connexions, mais toutes les connexions existantes restent valides jusqu’à l’expiration de la durée de vie valide (valeur par défaut de 604 800).
17. Sélectionnez **On-link (Sur la liaison)** si les systèmes qui disposent d’adresses dans le préfixe sont accessibles sans routeur.
18. Sélectionnez **Autonomous (Autonome)** si les systèmes peuvent créer indépendamment une adresse IP en combinant le préfixe publié avec l'ID de l'interface.
19. Cliquez sur **OK**.

STEP 6 | Au lieu d'une adresse statique pour le groupe agrégé, créez une sous-interface qui utilise DHCP pour obtenir son adresse.

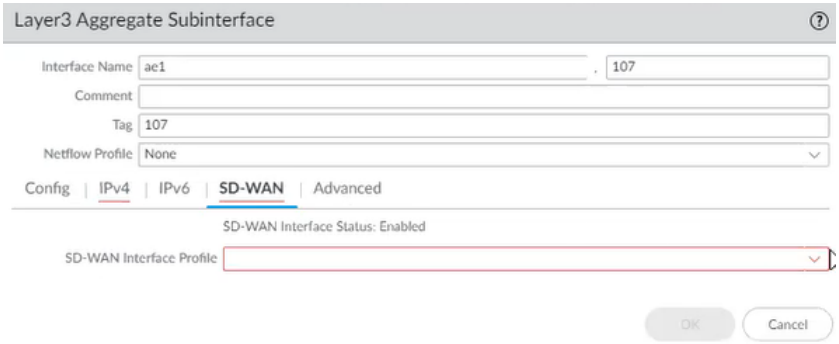
1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet** puis, dans le champ **Template (Modèle)**. sélectionnez une Pile de modèles.
2. Mettez en surbrillance l'interface agrégée, telle que ae1, et cliquez sur **Add Subinterface (Ajouter une sous-interface)** en bas de l'écran.
3. Mettez en surbrillance la sous-interface et cliquez sur **Override (Remplacer)** en bas de l'écran.
4. Mettez en surbrillance la sous-interface et pour **Interface Name (nom d'interface)**, écrivez un nombre après la période, tel que 1.
5. Saisissez la **Tag (balise)** VLAN pour différencier les sous-interfaces. Donnez à la balise le même numéro que l'ID de la sous-interface pour simplifier son utilisation.
6. Sélectionnez l'onglet **IPv4** et **Enable SD-WAN (Activez SD-WAN)**.

   Une sous-interface dans un groupe d'interfaces agrégées ne prend en charge qu'une adresse IPv4 en tant que client DHCP, pas une adresse IPv6.
7. Sélectionnez le **Type** d'adresse : **DHCP Client**.
8. Sélectionnez **Enable (Activer)**.
9. Désactivez (ne pas sélectionnez)**Automatically create default route pointing to default gateway provided by server (Créer automatiquement un itinéraire par défaut en direction de la passerelle par défaut fournie par le serveur)**.
10. Sélectionnez l'onglet **Advanced (Avancé)** et l'onglet **DDNS**.
11. Sélectionnez **Settings (Paramètres)** et **Enable (Activer)**. Le**Hostname (nom d'hôte)** est généré automatiquement par le plugin Panorama SD-WAN.
12. Sélectionnez le **Vendor (fournisseur)** en tant que **DDNS Palo Alto Networks**.
13. Cliquez sur **OK**.



STEP 7 | Appliquez un profil d'interface SD-WAN à la sous-interface.

1. Mettez en surbrillance la sous-interface que vous avez créée et sélectionnez l'onglet **SD-WAN**.
2. Sélectionnez le **SD-WAN Interface Profile (profil d'interface SD-WAN)** que vous avez créé pour ce lien ou créez un nouveau profil.



3. Cliquez sur **OK**.

STEP 8 | Répétez les étapes précédentes pour créer des sous-interfaces Layer3 supplémentaires pour le groupe d'interfaces agrégées et appliquez un profil d'interface SD-WAN à chaque sous-interface.

STEP 9 | **Commit** (Valider).

Configurer les sous-interfaces de couche 3 pour SD-WAN

Les pare-feu exécutant PAN-OS 11.0 et SD-WAN Plugin 2.1.0 prennent en charge SD-WAN sur les sous-interfaces de couche 3 afin que le pare-feu puisse segmenter le trafic à l'aide de balises VLAN. La tâche suivante montre comment créer une sous-interface Layer3 qui utilise une adresse IP statique et comment en créer une qui utilise DHCP pour obtenir son adresse. Il montre comment attribuer une balise VLAN à la sous-interface et activer SD-WAN sur la sous-interface. Créez un profil d'interface SD-WAN pour définir chaque connexion ISP et attribuez le profil à la sous-interface correspondante (une interface SD-WAN virtuelle).

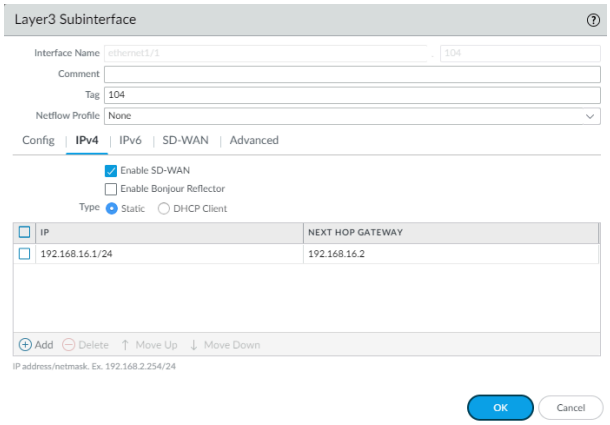
Si vous configurez des sous-interfaces SD-WAN de couche 3 sur des pare-feu VM-Series, la configuration VMware doit avoir des groupes de ports respectifs attachés à ces interfaces qui autorisent tous les VLAN.

PPPoE n'est pas pris en charge sur les sous-interfaces.

STEP 1 | Configurer un Profil d'interface SD-WAN pour chaque connexion ISP (sous-interface) pour définir ses attributs de lien.

STEP 2 | Créez une sous-interface de couche 3 qui utilise une adresse IPv4 statique.

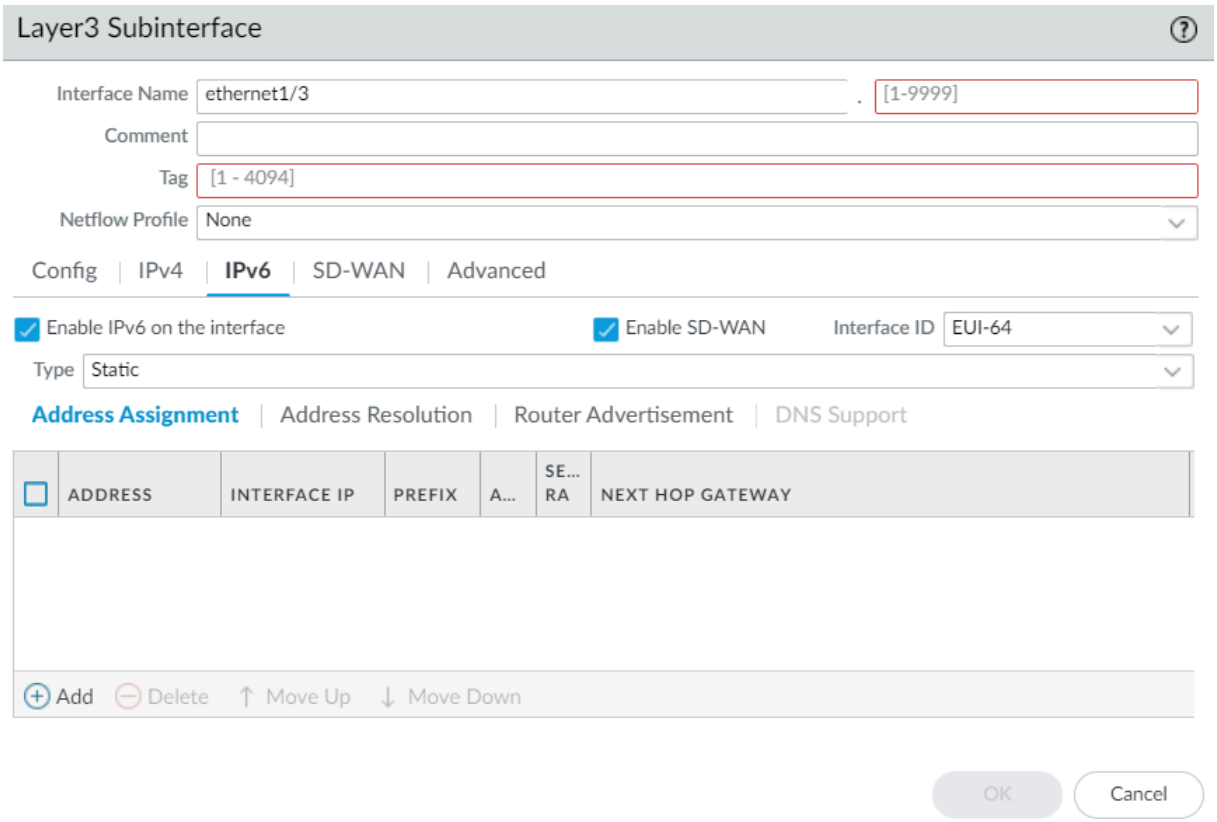
1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet** puis, dans le champ **Template (Modèle)**, sélectionnez un modèle.
2. Sélectionnez une interface.
3. Pour **Interface Type (Type d'interface)**, sélectionnez **Layer3** et cliquez sur **OK**.
4. Mettez l'interface en surbrillance et cliquez sur **Add Subinterface (Ajouter une sous-interface)** en bas de l'écran.
5. Après le **Interface Name (nom de l'interface)** et la période de l'interface, entrez le numéro de la sous-interface.
6. Saisissez une **Tag (balise)** pour la sous-interface (la plage est de 1 à 4094). Donnez à la balise le même numéro que l'ID de la sous-interface pour simplifier son utilisation.
7. Dans l'onglet **IPv4**, **Enable SD-WAN** (Activez SD-WAN).
8. Sélectionnez le **Type** d'adresse : **Static (Statique)**
9. **Add (Ajoutez) IP (adresse IP)** et le masque de sous-réseau.
10. Saisissez l'adresse IP de **Next Hop Gateway (passerelle Next Hop)**.
11. Cliquez sur **OK**.



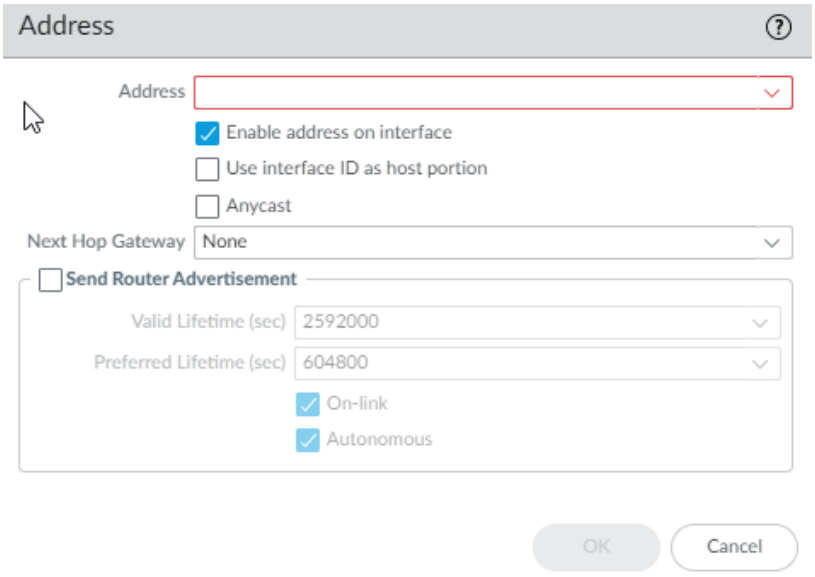
STEP 3 | Créez une sous-interface de couche 3 qui utilise une adresse IPv6 statique.

1. Réalisez les six premières sous-étapes de l'étape pour créer une sous-interface de couche 3 qui utilise une adresse IPv4 statique, car ce sont les mêmes pour une adresse IPv6.
2. Dans l'onglet **IPv6**, **Enable IPv6 on the interface (Activez IPv6 sur l'interface)** et **Enable SD-WAN (Activez SD-WAN)**.
3. Dans le champ **EUI-64 (default 64-bit Extended Unique Identifier) (identifiant unique étendu 64 bits par défaut)**, saisissez EUI 64 bits au format hexadécimal. Si ce champ n'est pas renseigné, le pare-feu utilise l'identifiant unique étendu sur 64'A0;bits (EUI-64) généré à partir de l'adresse MAC de l'interface physique. Si vous activez l'option **Use interface ID as host portion (Utiliser l'ID de l'interface comme partie hôte)** lors de l'ajout d'une adresse, le pare-feu utilise l'ID de l'interface comme partie hôte de l'adresse.
4. Sélectionnez le **Type** d'adresse : **Static (Statique)**

5. Sélectionnez **Address Assignment (Attribution d'adresse)**.



6. **Add (Ajoutez)** une **Address (Adresse)** IPv6 pour l'interface ou sélectionnez **New Variable (Nouvelle variable)** pour créer la variable. SD-WAN prend en charge une adresse IPv6 par interface physique.
7. **Enable address on interface (Activer l'adresse sur l'interface)**.

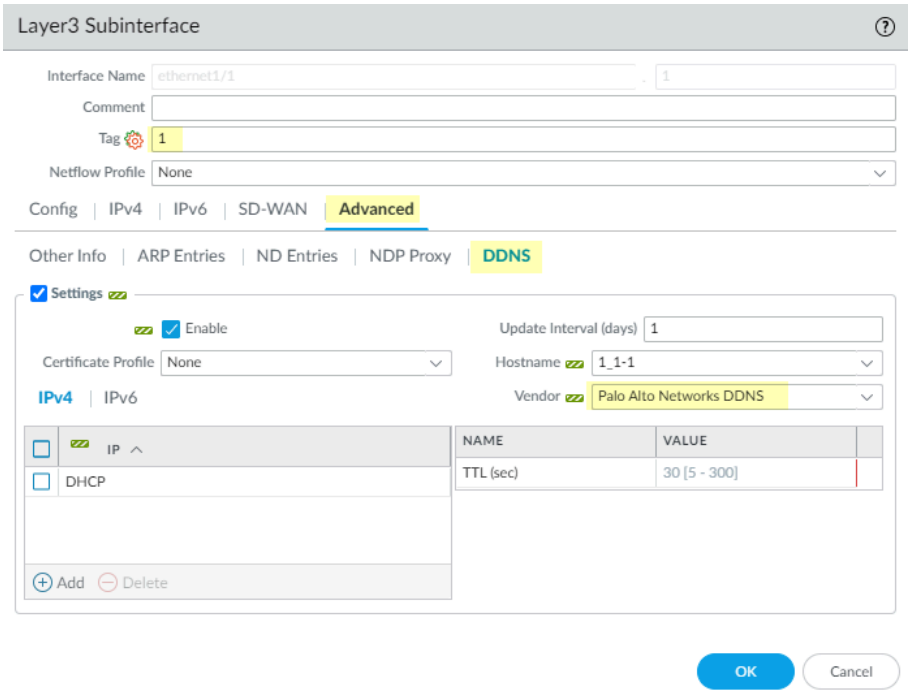


8. **Use interface ID as host portion (Utiliser l'ID de l'interface comme partie hôte)** – Consultez la troisième sous-étape ci-dessus pour une explication.

9. **Anycast** – Sélectionnez cette option pour faire de l'adresse IPv6 (itinéraire) une adresse Anycast (itinéraire), ce qui veut dire que plusieurs emplacements peuvent publier le même préfixe et que l'adresse IPv6 envoie le trafic anycast au nœud qu'il considère le plus près selon les coûts associés au protocole de routage et d'autres facteurs.
10. **Next Hop Gateway (Passerelle du saut suivant)** – Saisissez l'adresse IPv6 de la Passerelle du saut suivant (le prochain saut à partir de l'adresse IPv6 que vous avez saisie). La Passerelle du saut suivant doit se trouver sur le même sous-réseau que l'adresse IPv6. La Passerelle du saut suivant est l'adresse IP du routeur par défaut de l'ISP que l'ISP vous a donné lorsque vous avez acheté le service. Il s'agit de l'adresse IP du saut suivant à laquelle le pare-feu envoie le trafic pour atteindre le réseau de l'ISP et, en fin de compte, l'Internet et le hub.
11. **Send Router Advertisement (Envoyer la publicité de routeur)** – Sélectionnez cette option pour permettre au pare-feu d'envoyer cette adresse dans les publicités de routeur, auquel cas vous devez également activer l'option **Enable Router Advertisement (Activer la publicité de routeur)** globale pour l'interface (dans l'onglet **Router Advertisement (Publicité de routeur)**).
12. **Valid Lifetime (Durée de vie valide) (sec)** – Saisissez la durée de vie valide (en secondes) pendant laquelle le pare-feu considère l'adresse comme valide. La durée de vie valide doit être supérieure ou égale à la valeur **Preferred Lifetime (Durée de vie préférée)** (valeur par défaut de 2 592 000).
13. **Preferred Lifetime (Durée de vie préférée) (sec)** – Saisissez la durée de vie préférée (en secondes) pendant laquelle l'adresse valide est préférée, ce qui signifie que le pare-feu peut l'utiliser pour envoyer et recevoir du trafic. Lorsque la durée de vie préférée expire, le pare-feu ne peut plus utiliser l'adresse pour établir de nouvelles connexions, mais toutes les connexions existantes restent valides jusqu'à l'expiration de la durée de vie valide (valeur par défaut de 604 800).
14. **On-link (Sur la liaison)** - Sélectionnez si les systèmes qui disposent d'adresses dans le préfixe sont accessibles sans routeur.
15. **Autonomous (Autonome)** – Sélectionnez cette option si les systèmes peuvent créer une adresse IP de façon indépendante en combinant le préfixe publié avec un ID d'interface.
16. Cliquez sur **OK**.

STEP 4 | Au lieu d'une adresse statique, créez une sous-interface de couche 3 qui utilise DHCP pour obtenir son adresse IPv4.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet** puis, dans le champ **Template (Modèle)**, sélectionnez une pile de modèles (et non un modèle).
2. Sélectionnez une interface.
3. Pour **Interface Type (Type d'interface)**, sélectionnez **Layer3** et cliquez sur **OK**.
4. Mettez l'interface en surbrillance et cliquez sur **Add Subinterfaces (Ajouter des sous-interfaces)** en bas de l'écran.
5. Mettez en surbrillance la sous-interface et cliquez sur **Override (Remplacer)**.
6. Mettez en surbrillance la sous-interface et après **Interface Name (Nom de l'interface)** et la période, écrivez le numéro de la sous-interface.
7. Saisissez une **Tag (balise)** pour la sous-interface (la plage est de 1 à 4094). Donnez à la balise le même numéro que l'ID de la sous-interface pour simplifier son utilisation.
8. Dans l'onglet **IPv4**, **Enable SD-WAN** (Activez SD-WAN).
9. Sélectionnez **Type** d'adresse : **DHCP Client** et **Enable (Activer)**.
10. Désactivez (ne pas sélectionnez)**Automatically create default route pointing to default gateway provided by server (Créer automatiquement un itinéraire par défaut en direction de la passerelle par défaut fournie par le serveur)**.
11. Sélectionnez l'onglet **Advanced (Avancé)** puis l'onglet **DDNS**.
12. Sélectionnez **Settings (Paramètres)** et **Enable (Activer)**. Le**Hostname (nom d'hôte)** est généré automatiquement par le plugin Panorama SD-WAN.
13. Sélectionnez le **Vendor (fournisseur)** en tant que **DDNS Palo Alto Networks**.
14. Cliquez sur **OK**.



STEP 5 | Appliquez un profil d'interface SD-WAN à la sous-interface.

1. Mettez en surbrillance la sous-interface que vous avez créée et sélectionnez l'onglet **SD-WAN**.
2. Sélectionnez le **SD-WAN Interface Profile (profil d'interface SD-WAN)** que vous avez créé pour ce lien ou créez un nouveau profil.
3. Cliquez sur **OK**.

STEP 6 | Répétez les étapes précédentes pour ajouter plus de sous-interfaces à l'interface.

STEP 7 | **Commit** (Valider).

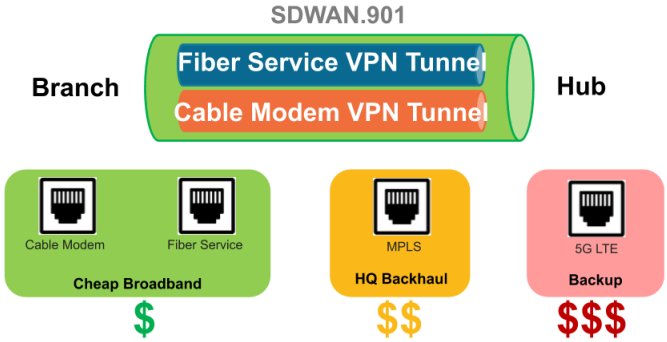
Configurer une Interface virtuelle SD-WAN

Si vous utilisez la configuration Auto VPN par le biais de Panorama, elle crée des interfaces SD-WAN pour vous, auquel cas vous ne créez pas et ne configurez pas d'interface virtuelle SD-WAN.

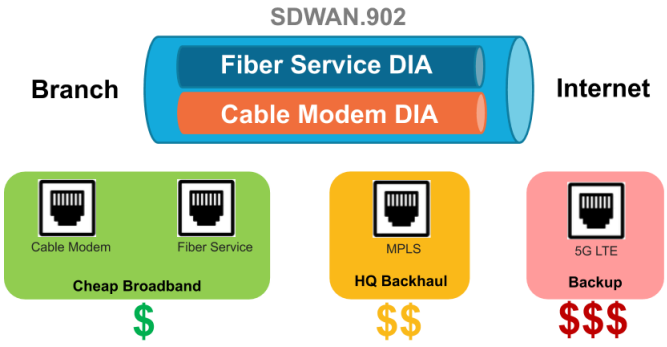
Si vous n'utilisez pas la configuration Auto VPN avec Panorama, créez et configurez une interface virtuelle SD-WAN pour spécifier une ou plusieurs ethernet interfaces (interfaces ethernet) physiques compatibles SD-WAN qui vont vers la même destination, comme une plateforme spécifique ou internet. En réalité, tous les liens d'une interface virtuelle SD-WAN doivent être du même type : tous les liens d'un tunnel VPN ou tous les liens d'accès direct à internet (DIA).

La première figure donne un exemple d'une interface SD-WAN appelée SDWAN.901 qui rassemble deux interfaces physiques qui utilisent des opérateurs différents : Ethernet1/1 (le lien du modem câble) et Ethernet1/2 (le lien du service de la fibre). Les deux liens sont un tunnel VPN depuis la branche jusqu'au hub.

Dans cette figure, les deux liens de l'interface SD-WAN utilisent la même étiquette de liens (Bande passante bon marché) mais des liens dans une interface SD-WAN peuvent avoir des étiquettes de liens différentes.



Dans la figure suivante, SDWAN.902 rassemble les liens Ethernet1/1 et Ethernet1/2, qui sont tous les deux des liens DIA de la branche jusqu'à l'Internet :



STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Sélectionnez **Network** > **Interfaces** > **SD-WAN** (Réseau Interfaces SD-WAN) et sélectionnez le modèle approprié dans la liste déroulante **Template** (Modèle).

STEP 3 | **Add** (Ajoutez) une interface logique SD-WAN en saisissant un chiffre (dans une fourchette de 1 à 9 999) après le préfixe **sdwan.**.

La configuration Auto VPN crée des interfaces SD-WAN numérotées .901, .902, etc. Par conséquent, si vous souhaitez créer les interfaces SD-WAN manuellement, n'utilisez pas le format sdwan.90x pour le nom d'une interface SD-WAN. De même, la configuration Auto VPN crée une interface SD-WAN numérotée .9016 pour une interface IPv6, n'utilisez donc pas sdwan.9016 pour le nom d'une interface SD-WAN.

STEP 4 | Saisissez un **Comment** (commentaire) descriptif.

Ajoutez un commentaire utile, comme ***`Branch to internet`*** *(branche vers Internet) ou* ***`Branch to western USA hub`*** *(branche vers un hub de l'ouest des USA) si vous êtes dans le modèle de la Branche. Votre commentaire rend la résolution des pannes plus simple plutôt que d'essayer de décrypter des noms générés automatiquement dans les journaux et les rapports.*

STEP 5 | Sélectionnez le **Protocol (Protocole)** pour indiquer le type d'interface SD-WAN virtuelle :

- **ipv4** indique une interface virtuelle DIA IPv4.
- **ipv6** indique une interface virtuelle DIA IPv6 DIA.
- **none (aucune)** indique une interface virtuelle de tunnel VPN.

STEP 6 | Dans l'onglet **Config (Configuration)**, affectez l'interface SD-WAN à un **Virtual Router (routeur virtuel)**.

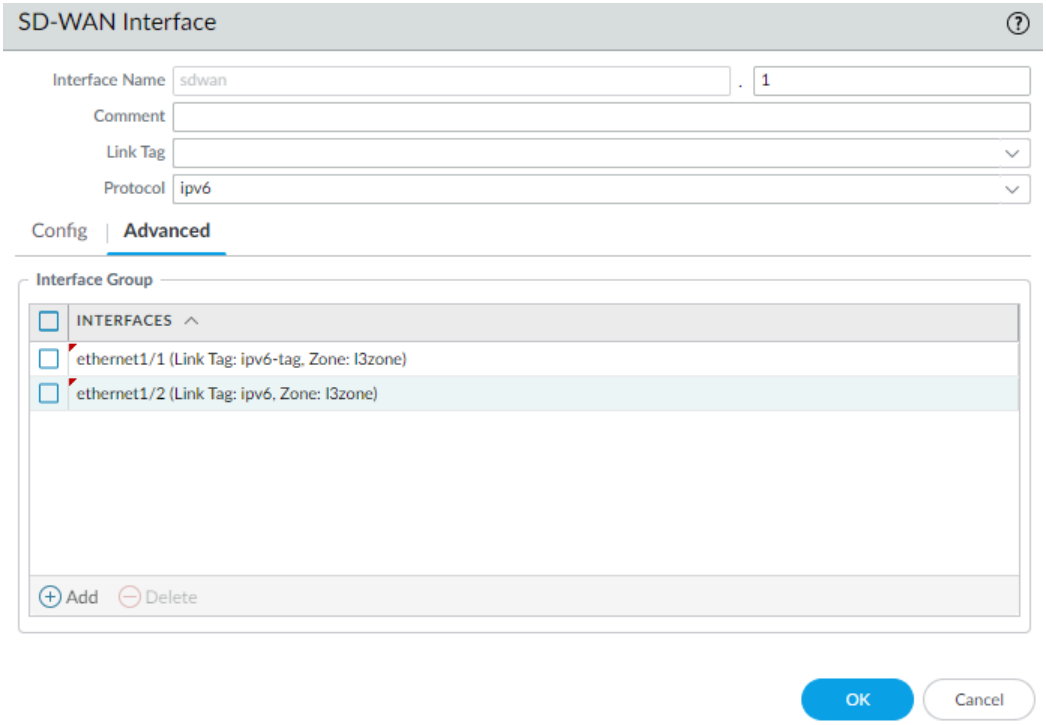
STEP 7 | Affectez l'interface SD-WAN à une **Security Zone (Zone de sécurité)**.

L'interface virtuelle SD-WAN et tout les membres de l'interface doivent être dans la même Zone de sécurité, assurant ainsi que les mêmes règles de politique de sécurité s'appliquent à tous les chemins depuis la branche jusqu'à la même destination.

STEP 8 | Dans l'onglet **Advanced** (Avancé), **Add Interfaces** (Ajoutez les interfaces) qui sont des membres qui vont vers la même destination, en sélectionnant une ou plusieurs interfaces Ethernet de Couche 3 (pour DIA) ou une ou plusieurs interfaces de tunnel VPN (pour le hub). Si vous saisissez plus d'une interface, elles doivent toutes être du même type (tunnel VPN ou DIA).

Le routeur virtuel du pare-feu utilise cette interface virtuelle SD-WAN pour acheminer le trafic SD-WAN vers un emplacement DIA ou vers un hub. Pendant l'acheminement, la table de routage détermine par quelle interface virtuelle SD-WAN (interface de sortie) le paquet sortira sur la base de l'adresse IP de destination dans le paquet. Ensuite les profils d'état du chemin SD-WAN et de Distribution du trafic dans la règle de politique SD-WAN à laquelle correspond le paquet déterminent quel chemin utiliser (et l'ordre dans lequel tenir compte des nouveaux chemins si un chemin se détériore).

STEP 9 | Cliquez sur **OK** pour enregistrer la modification de votre configuration.



STEP 10 | **Commit** (Validez) et **Commit and Push** (Validez et appliquez) les modifications de votre configuration.

Créer un itinéraire par défaut vers l'interface SD-WAN

Si vous utilisez un itinéraire de service pour accéder à Panorama™, pour afficher le pare-feu, vous devez créer un itinéraire par défaut qui renvoie vers l'interface SD-WAN que vous avez créée.

Auto VPN crée une interface virtuelle SD-WAN appelée sdwan.901 pour DIA IPv4 et une interface virtuelle SD-WAN appelée sdwan.9016 pour DIA IPv6. Il crée une interface virtuelle SD-WAN nommée sdwan.902 pour les tunnels VPN. Auto VPN crée également son propre itinéraire par défaut qui utilise les interfaces sdwan.901 (IPv4) et sdwan.9016 (IPv6) comme interface de sortie et utilise des métriques faibles, de sorte que les interfaces sdwan.901 (IPv4) et sdwan.9016 (IPv6) soient préférées à l'itinéraire par défaut que vous avez créé.e

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Sélectionnez le **Template** (Modèle) sur lequel vous travaillez.

STEP 3 | Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et sélectionnez un routeur virtuel comme **sd-wan**.

STEP 4 | Sélectionnez **Static Routes (Itinéraires statiques)**.

STEP 5 | Sélectionnez **IPv4** ou **IPv6** et **Add (Ajoutez)** une route statique par **Name (Nom)**.

STEP 6 | Pour la **Destination** IPv4, saisissez 0.0.0.0/0. Pour la **Destination** IPv6, saisissez ::/0.

STEP 7 | Pour l'**Interface** de sortie, sélectionnez une des interfaces logiques SD-WAN que vous avez créées pour afficher le pare-feu, comme.

L'interface de sortie que vous sélectionnez peut être n'importe quelle interface logique SD-WAN sauf sdwan.901, sdwan.902 ou sdwan.9016.

STEP 8 | Pour **Next Hop** (saut suivant), sélectionnez **None** (Aucun).

STEP 9 | Pour **Metric** (Mesure), saisissez une valeur supérieure à 50, afin que cet itinéraire par défaut ne soit pas favorisé par rapport à l'itinéraire par défaut que Auto VPN crée avec une métrique faible.

STEP 10 | Cliquez sur **OK**.

STEP 11 | Sélectionnez **Commit (Valider)** et **Commit and Push (Validez et appliquez)** les modifications de configuration.

STEP 12 | **Commit (Validez)** vos modifications.

STEP 13 | Répétez cette tâches pour les autres modèles sur les pare-feux qui utilisent un itinéraire de service pour accéder à Panorama.

Configurez les Profils de gestion des liaisons SD-WAN

Créez et configurez un profil de qualité de chemin, de qualité SaaS, de distribution du trafic et de correction d'erreur pour gérer les basculements de liaison SD-WAN.

- Créer un Path Quality Profile (Profil de qualité du chemin d'accès)
- Configuration de la surveillance SaaS
- Traffic Distribution Profiles (profils de distribution du trafic) SD-WAN
- Créer un Traffic Distribution Profile (profil de distribution du trafic)
- Création d'un profil de correction des erreurs

Créer un Path Quality Profile (Profil de qualité du chemin d'accès)

Créez un profil de qualité de chemin d'accès pour chaque ensemble d'applications critiques pour l'entreprise ou sensibles à la latence, les filtres d'applications, les groupes d'applications, les services, les objets de services et les objets de groupes de services qui ont des besoins (état) de qualité de réseau uniques sur la base de la latence, de l'instabilité et du pourcentage de perte de paquets. Les applications et les services peuvent partager un profil de qualité de chemin d'accès. Spécifiez le seuil maximum de chaque paramètre au-dessus duquel le pare-feu estime que le chemin d'accès s'est détérioré suffisamment pour sélectionner un meilleur chemin.

En tant qu'alternative à la création d'un profil de qualité de chemin, vous pouvez utiliser un des profils de qualité de chemin, comme **general-business**, **voip-video**, **file-sharing**, **audio-streaming**, **photo-video**, et **remote-access**, ou autres. Les profils prédéfinis sont configurés pour optimiser les seuils de latence, instabilité et perte de paquets pour le type d'applications et services suggéré par le nom du profil.

*Les profils de qualité de chemin d'accès prédéfinis pour un groupe de périphériques Panorama sont basés sur les paramètres par défaut de **Probe Frequency** (Fréquence de sondage) dans le profil d'interface SD-WAN pour un modèle Panorama. Si vous modifiez le paramètre de Fréquence de sondage par défaut, vous devez ajuster le seuil du pourcentage de **Packet Loss** (Perte de paquets) dans le profil de qualité de chemin pour les pare-feux d'un Groupe de périphériques qui sont affectés par le modèle Panorama dans lequel vous avez modifié le profil d'interface.*

Le pare-feu traite les seuils de latence, gigues et perte de paquets comme des conditions OU, ce qui signifie que si l'un des seuils est dépassé, le pare-feu sélectionne le nouveau meilleur (préféré) chemin d'accès. Tout chemin qui à une latence, une gigue ou une perte de paquets inférieure ou égale aux trois seuils est considéré comme qualifié et le pare-feu a sélectionné le chemin sur la base du profil de Distribution du trafic associé.

Par défaut, le pare-feu mesure **latency** (la latence) et **jitter** (la gigue) toutes les 200 ms et fait une moyenne des trois dernières mesures pour évaluer la qualité du chemin sur une fenêtre glissante. Vous pouvez modifier ce comportement en sélectionnant la surveillance des chemins agressive ou souple lorsque vous Configurer un Profil d'interface SD-WAN.

Si un chemin bascule parce qu'il a dépassé le seuil de **packet loss** (perte de paquets) configuré, le pare-feu continue à envoyer des paquets de sondage sur le chemin qui a basculé et calcule son pourcentage de perte de paquets lorsque le chemin se rétablit. Trois minutes peuvent être

nécessaires pour que le pourcentage de pertes de paquets sur un chemin rétabli passe en dessous du seuil de pertes de paquets configuré dans le profil de qualité de chemin d'accès. Par exemple, supposons qu'une règle de politique SD-WAN pour une application a un profil de qualité de chemin qui spécifie un seuil de perte de paquets de 1 % et un profil de Distribution du trafic qui spécifie une distribution descendante avec l'étiquette 1 (appliquée à tunnel.1) en premier sur la liste et l'étiquette 2 (appliquée à tunnel.2) en position suivante sur la liste. Lorsque tunnel.1 dépasse 1 % de perte de paquets, les paquets de données basculent sur tunnel.2. Une fois que tunnel.1 est repassé à 0 % de perte de paquets (sur la base des paquets de sondage), jusqu'à trois minutes peuvent être nécessaires pour que le taux de perte de paquets surveillé pour tunnel.1 passe en dessous de 1 %, moment où le pare-feu sélectionne tunnel.1 comme meilleur chemin à nouveau.

Le paramètre de sensibilité indique quel paramètre (latence, instabilité ou perte de paquets) est le plus important (préféré) pour les applications auxquelles le profil s'applique. Lorsque le pare-feu évalue la qualité du lien, il tient compte du paramètre qui a un réglage **high** (élevé) en premier. Par exemple, lorsque le pare-feu compare deux liens, en supposant qu'un lien a une latence de 100 ms et une gigue de 20 ms ; l'autre lien ayant une latence de 300 ms et une gigue de 10 ms. Si la sensibilité de la latence est élevée, le pare-feu choisit le premier lien. Si la sensibilité de la gigue est élevée, le pare-feu choisit le deuxième lien. Si les paramètres ont la même sensibilité (par défaut les paramètres sont réglés sur **medium** (moyen)), le pare-feu évalue la perte de paquets en premier, puis latence et en dernier, la gigue.

Comme le Traffic Distribution Profiles (profils de distribution du trafic) SD-WAN concept l'indique,la sélection du nouveau chemin d'accès se produit en moins de une seconde si vous laissez Path Monitoring and Probe Frequency (Surveillance des chemins d'accès et Fréquence de sondage) avec les paramètres par défaut ; autrement, la sélection d'un nouveau chemin d'accès pourrait prendre plus d'une seconde. Pour obtenir un basculement sur incident inférieur à la seconde basé sur la perte de paquets, vous devez définir la sensibilité de latence sur **élevée** et le seuil de latence sur 250 ms maximum.

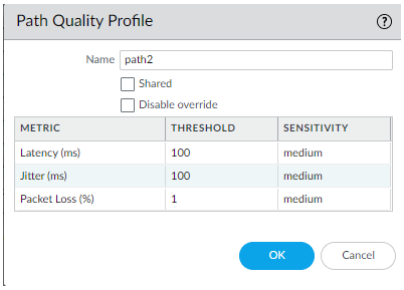
Créer un profil de qualité du chemin d'accès dans une SD-WAN policy rule (règle de politique SD-WAN) pour contrôler le seuil auquel le pare-feu remplace un chemin d'accès détérioré par un nouveau chemin pour les paquets de l'application correspondante.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Sélectionnez un **Device Group** (groupe de périphériques).

STEP 3 | Sélectionnez **Objects (Objets)** > **SD-WAN Link Management (gestion des liens SD-WAN)** > **Path Quality Profile (profil de qualité des chemins d'accès)**.

STEP 4 | **Add** (Ajoutez) un profil de qualité du chemin d'accès par **Name** (nom) en utilisant un maximum de 31 caractères alphanumériques.



STEP 5 | Pour **Latency** (latence), faites un double clic sur la valeur du **Threshold** (seuil) et saisissez le nombre de millisecondes autorisé pour qu'un paquet quitte le pare-feu, arrive à l'extrémité opposée du tunnel SD-WAN et un paquet de réponse retourne au pare-feu avant que le seuil ne soit dépassé (la fourchette va de 10 à 2 000 ; par défaut on a 100).

STEP 6 | Pour **Latency** (latence), sélectionnez **Sensitivity** (Sensibilité) (**low**, **medium**, or **high**) (faible, moyenne ou élevée). Le réglage par défaut est **medium** (moyenne).

Cliquez sur la flèche au bout de la colonne Seuil pour trier les seuils dans l'ordre numérique ascendant ou descendant.

STEP 7 | Pour **Jitter** (gigue), faites un double clic sur la valeur du **Threshold** (seuil) et saisissez le nombre de millisecondes (la fourchette va de 10 à 1 000 ; par défaut on a 100).

STEP 8 | Pour **Jitter** (gigue), sélectionnez **Sensitivity** (Sensibilité) (**low**, **medium**, or **high**) (faible, moyenne ou élevée). Le réglage par défaut est **medium** (moyenne).

STEP 9 | Pour **Packet Loss** (perte de paquets), faites un double clic sur la valeur du **Threshold** (seuil) et saisissez le pourcentage de perte de paquets sur le lien avant que le seuil ne soit dépassé (la fourchette va de 1 à 100,0 ; par défaut on a 1).

*Le réglage de la **Sensitivity (Sensibilité)** pour la **Packet Loss (Perte de paquets)** n'a aucun effet ; vous pouvez donc garder le réglage par défaut.*

*Si vous modifiez la **Probe Frequency** (Fréquence de sondage) dans un profil d'interface SD-WAN pour un modèle Panorama, vous devez aussi ajuster le seuil de perte de paquets pour un groupe de périphériques de Panorama.*

STEP 10 | Cliquez sur **OK**.

STEP 11 | **Commit** (Validez) et **Commit and Push** (Validez et appliquez) les modifications de votre configuration.

STEP 12 | **Commit (Validez)** vos modifications.

STEP 13 | Répétez cette tâche pour chaque Groupe de périphériques.

Configuration de la surveillance SaaS

Configurez un profil de qualité SaaS pour la surveillance des liaisons Direct Internet Access (Accès Internet direct ; DIA) entre une application SaaS et votre pare-feu de la branche.

La surveillance des chemins d'application SaaS est prise en charge uniquement pour les pare-feu PAN-OS compatibles SD-WAN. La surveillance des chemins d'application SaaS n'est pas prise en charge pour Prisma Access Hubs.

- Création d'un profil de qualité SaaS
- Cas d'utilisation : Configuration de la surveillance SaaS pour un pare-feu de la branche

- Cas d'utilisation : Configuration du basculement d'un pare-feu de la plate-forme pour la surveillance SaaS à partir d'un pare-feu de la branche vers la même destination des applications SaaS
- Cas d'utilisation : Configuration du basculement d'un pare-feu de la plate-forme pour la surveillance SaaS à partir d'un pare-feu de la branche vers une destination des applications SaaS différente

Création d'un profil de qualité SaaS

Si votre pare-feu de la branche dispose d'une liaison DIA à une application Saas, créez un profil de qualité SaaS pour spécifier la façon de surveiller une ou plusieurs applications SaaS. Les profils de qualité SaaS sont associés à une règle de politique SD-WAN pour déterminer la façon dont le pare-feu de la branche détermine les seuils de qualité des chemins en ce qui a trait à la latence, à la gigue et à la perte de paquets et sélectionne le chemin privilégié pour un paquet sortant.

Le profil de qualité SaaS prend en charge un maximum de quatre adresses IP statiques, ou un Fully Qualified Domain Name (nom de domaine complet - FQDN) ou une URL par profil de qualité SaaS. Lorsque plusieurs adresses IP statiques sont configurées, le pare-feu de la branche surveille une adresse IP à la fois en ordre descendant, en fonction de l'ordre des adresses IP au sein du profil de qualité SaaS. Par exemple, si vous ajoutez IP1, IP2, IP3 et IP4, le pare-feu de la branche surveille IP1 pour déterminer si les seuils de qualité du chemin ont été dépassés, puis il passe à IP2, et ainsi de suite.

Les données de surveillance et de création de rapports SD-WAN affichent l'application SaaS ainsi que l'adresse IP, le FQDN ou l'URL de l'application SaaS, selon sa configuration au sein du profil de qualité SaaS associé à la règle de politique SD-WAN, sans égard au filtre de temps appliqué lors de l'affichage de vos données de surveillance SD-WAN.

*Par exemple, il y a trois jours, vous avez initialement configuré l'adresse IP de votre application SaaS (**192.168.10.50**) dans un profil de qualité SaaS et vous avez fait correspondre le trafic à la règle de politique SD-WAN à laquelle le profil de qualité SaaS est associé. Aujourd'hui, vous avez reconfiguré le profil de qualité SaaS existant et modifié l'adresse IP de l'application Saas comme suit : **192.168.10.20**. Lorsque vous retournez consulter les données de surveillance SD-WAN, toutes les données de surveillance existantes pour cette application SaaS affichent l'adresse IP **192.168.10.20**.*

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Sélectionnez **Objects (Objets)** > **SD-WAN Link Management (Gestion des liaisons SD-WAN)** > **SaaS Quality Profile (Profil de qualité SaaS)** et spécifiez le **Device Group (Groupe de périphériques)** contenant votre configuration SD-WAN.

STEP 3 | **Add (Ajoutez)** un nouveau profil de qualité SaaS.

STEP 4 | Saisissez un **Name (Nom)** descriptif pour le profil de qualité SaaS.

STEP 5 | (Facultatif) Cochez (activez) **Shared (Partagé)** pour que le profil de qualité SaaS soit partagé entre tous les groupes de périphériques.

STEP 6 | (Facultatif) Cochez (activez) **Disable override (Désactiver le contrôle prioritaire)** pour désactiver le contrôle prioritaire de la configuration du profil de qualité SaaS sur le pare-feu local.

> *L'option **Disable override (Désactiver le contrôle prioritaire)** ne peut être activée que si l'option **Shared (Partagé)** est désactivée à l'étape précédente.*

STEP 7 | Configurez le mode de surveillance SaaS.

- Surveillez automatiquement l'état du chemin de l'application SaaS.

  Activée par défaut, la surveillance **Adaptive (adaptative)** permet au pare-feu de la branche de surveiller passivement la session des applications SaaS pour les activités d'envoi et de réception afin de déterminer si les seuils de qualité des chemins ont été dépassés. La

qualité de la santé des chemins des applications SaaS est automatiquement déterminée sans effectuer de vérifications supplémentaires de l'état de l'interface SD-WAN.

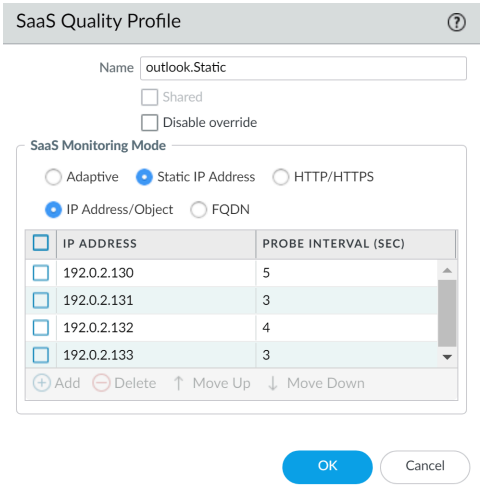
La surveillance SaaS adaptative est prise en charge pour les applications SaaS TCP.

- Configurez l'adresse IP statique de l'application SaaS.

  Créez un profil de qualité SaaS par application SaaS critique que vous devez surveiller. Si une application SaaS possède plusieurs adresses IP, configurez un profil de qualité SaaS avec les multiples adresses IP statiques pour cette application SaaS.

  La surveillance SaaS utilise beaucoup de ressources et peut impacter la performance du pare-feu si vous surveillez une grande quantité d'applications SaaS. Il est recommandé de surveiller uniquement ces applications SaaS critiques qui ont besoin d'une bonne facilité d'utilisation.

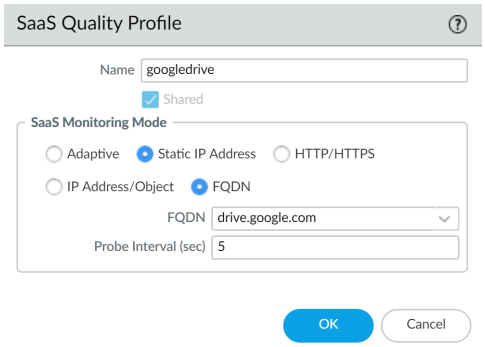
  1. Sélectionnez **IP Address/Object (Adresse IP/Objet)** > **Static IP Address (Adresse IP statique)** et **Add (Ajoutez)** une adresse IP.
  2. Saisissez l'adresse IP de l'application SaaS ou sélectionnez un objet d'adresse configuré.
  3. Saisissez le **Probe Interval (Intervalle de sondage)**auquel le pare-feu de la branche sonde le chemin de l'application SaaS pour obtenir les informations relatives à son état.
  4. Cliquez sur **OK** pour enregistrer les modifications de votre configuration.



- Configurez le Fully Qualified Domain Name (nom de domaine complet - FQDN) de l'application SaaS.

  1. Configurez un address object (objet d'adresse) FQDN de l'application SaaS.
  2. Sélectionnez **IP Address/Object (Adresse IP/Objet)** > **FQDN**, puis **Add (Ajoutez)** le FQDN.
  3. Sélectionnez l'**address object (objet d'adresse)** FQDN de l'application SaaS.
  4. Saisissez le **Probe Interval (Intervalle de sondage)**auquel le pare-feu de la branche sonde le chemin de l'application SaaS pour obtenir les informations relatives à son état.

5. Cliquez sur **OK** pour enregistrer les modifications de votre configuration.

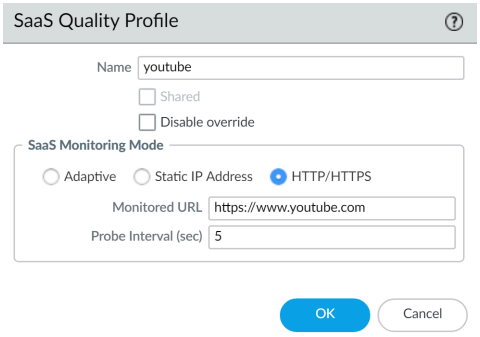


- Configurez l'URL de l'application SaaS.

  La surveillance URL n'est prise en charge que pour le trafic qui transite par les ports 80, 443, 8080, 8081 et 143.

  1. Sélectionnez **HTTP/HTTPS**.
  2. Saisissez la **Monitored URL (URL surveillée)** de l'application SaaS.
  3. Saisissez le **Probe Interval (Intervalle de sondage)**auquel le pare-feu de la branche sonde le chemin de l'application SaaS pour obtenir les informations relatives à son état.

     L'intervalle de sondage minimal pris en charge pour HTTP/HTTPS d'une application SaaS est de 3 secondes.
  4. Cliquez sur **OK** pour enregistrer les modifications de votre configuration.



STEP 8 | Sélectionnez **Commit (Valider)** et **Commit and Push (Validez et appliquez)** les modifications de configuration.

Cas d'utilisation : Configuration de la surveillance SaaS pour un pare-feu de la branche

Si votre organisation exploite une application critique à l'emplacement d'un pare-feu de la branche, vous pouvez configurer un profil de qualité SaaS et l'associer à une règle de politique SD-WAN pour surveiller les mesures d'état de la latence, de la gigue et de la perte de paquets de l'application SaaS critique et faire passer les liaisons d'un pare-feu de la branche SD-WAN en une application SaaS sur la liaison Direct Internet Access (Accès Internet direct ; DIA) pour garantir la facilité d'utilisation de l'application.

Si les seuils de la mesure de l'état des liaisons DIA des applications SaaS sont dépassés, la liaison passe à la prochaine liaison DIA configurée dans le profil de distribution du trafic pour toutes les nouvelles sessions. La session existante sur la liaison DIA détériorée ne passe pas à la prochaine liaison DIA.

STEP 1 | Configurez votre déploiement SD-WAN.

1. Installer le plug-in SD-WAN.
2. Configurer Panorama et les pare-feux pour SD-WAN.
3. Ajouter des Périphériques SD-WAN à Panorama.
4. (Configurations haute disponibilité uniquement) Configurer les Périphérique HA pour SD-WAN.
5. Créer un cluster VPN.

STEP 2 | Créer une Link Tag (Étiquette de liens) pour regrouper les liaisons DIA de l'application SaaS.

Créez plusieurs étiquettes de liaison pour vos liaisons DIA pour appliquer différents paramètres de surveillance SD-WAN à chaque liaison d'applications SaaS en fonction du type de liaison.

De plus, vous pouvez créer une seule étiquette de liaison pour plusieurs liaisons DIA afin de regrouper les liaisons en un seul ensemble de liaisons. La création d'une seule étiquette de liaison pour plusieurs liaisons DIA vous permet de cumuler la bande passante entre les liaisons regroupées et permet au pare-feu de distribuer les sessions entre plusieurs liaisons.

STEP 3 | Configurez un profil d'interface SD-WAN pour définir les caractéristiques de votre connexion ISP et spécifiez la vitesse de la liaison DIA, la fréquence à laquelle le pare-feu de la branche surveille la liaison, puis sélectionnez l'étiquette de liaison pour spécifier à quelle liaison le profil d'interface SD-WAN s'applique.

Si vous avez créé plusieurs étiquettes de liaison, vous devez configurer un profil d'interface SD-WAN pour chaque étiquette de liaison.

Si vous avez créé un ensemble de liaison en affectant plusieurs liaisons DIA à une seule étiquette de liaison, en spécifiant cette étiquette de liaison, les paramètres du profil d'interface SD-WAN seront appliqués à toutes les liaisons DIA de l'ensemble.

STEP 4 | Configurez une interface Ethernet physique pour chaque liaison DIA d'applications SaaS.

Toutes les interfaces Ethernet physiques des liaisons DIA doivent être de Couche3.

STEP 5 | Configurer une Interface virtuelle SD-WAN qui regroupe toutes les interfaces Ethernet physiques des liaisons DIA d'applications SaaS en un seul groupe d'interfaces.

Le routeur virtuel du pare-feu utilise cette interface virtuelle SD-WAN pour acheminer le trafic SD-WAN à un emplacement DIA. Les profils d'état du chemin SD-WAN et de Distribution du trafic dans la règle de politique SD-WAN déterminent quel chemin utiliser et l'ordre dans lequel tenir compte des nouveaux chemins si l'état d'un chemin se détériore.

STEP 6 | Créez un profil de qualité du chemin d'accès pour configurer la sensibilité et les mesures de latence, de gigue et de perte des paquets afin de spécifier à quel moment le pare-feu de la branche devrait passer à la liaison DIA suivante.

STEP 7 | Créez un profil de qualité SaaS pour spécifier votre application SaaS et la fréquence à laquelle la liaison DIA est surveillée.

STEP 8 | Créez un profil de distribution du trafic pour spécifier l'ordre dans lequel le pare-feu de la branche passe à des liaisons DIA en cas de dégradation de l'état d'une liaison.

STEP 9 | Configurez une règle de politique SD-WAN pour spécifier les mesures de l'état des liaisons et des applications SaaS et pour déterminer la façon dont le pare-feu sélectionne la liaison privilégiée pour le trafic critique des applications SaaS.

*À l'onglet **Application**, ajoutez l'application SaaS que vous surveillez à la règle de politique SD-WAN pour vous assurer que les paramètres de surveillance SaaS sont appliqués uniquement à l'application SaaS souhaitée.*

Cas d'utilisation : Configuration du basculement d'un pare-feu de la plate-forme pour la surveillance SaaS à partir d'un pare-feu de la branche vers la même destination des applications SaaS

Si votre organisation utilise une application SaaS au niveau d'un pare-feu de la branche, mais que le pare-feu de la branche ne dispose d'aucune liaison DIA fonctionnelle vers laquelle basculer, vous pouvez configurer le pare-feu de la plateforme en tant qu'option de basculement de rechange, ce qui vous permettra de maintenir une connexion fonctionnelle à votre application SaaS.

Si les seuils de la mesure de l'état des liaisons DIA des applications SaaS sont dépassés et qu'il n'y a aucune liaison DIA fonctionnelle sur le pare-feu de la branche, la liaison passe au prochain pare-feu de la plateforme pour toutes les nouvelles sessions. La session existante sur la liaison DIA détériorée ne passe pas au pare-feu de la plateforme.

Par exemple, supposons que vos pare-feu de la branche et de la plateforme se trouvent dans la même région et qu'ils accèdent à une application SaaS qui utilise la même adresse IP de destination. Vous pouvez configurer le basculement vers le pare-feu de la plateforme en l'absence de liaisons DIA fonctionnelles entre le pare-feu de la branche et l'application SaaS en configurant un profil de qualité SaaS portant le même nom sur les pare-feu de la branche et de la plateforme pour qu'il bascule automatiquement vers le pare-feu de la plateforme si aucune liaison DIA n'est disponible à partir du pare-feu de la branche. Vous pouvez ainsi maintenir un chemin fonctionnel pour votre application SaaS et maintenir des données bout en bout précises sur la surveillance des applications SaaS sans congestionner la bande passante de votre réseau.

STEP 1 | Configurez votre déploiement SD-WAN.

1. Installer le plug-in SD-WAN.
2. Configurer Panorama et les pare-feux pour SD-WAN.
3. Ajouter des Périphériques SD-WAN à Panorama.
4. (Configurations haute disponibilité uniquement) Configurer les Périphérique HA pour SD-WAN.
5. Créer un cluster VPN.

STEP 2 | Créer une Link Tag (Étiquette de liens) pour regrouper les liaisons DIA de l'application SaaS.

Créez plusieurs étiquettes de liaison pour vos liaisons DIA pour appliquer différents paramètres de surveillance SD-WAN à chaque liaison d'applications SaaS en fonction du type de liaison.

De plus, vous pouvez créer une seule étiquette de liaison pour plusieurs liaisons DIA afin de regrouper les liaisons en un seul ensemble de liaisons.

STEP 3 | Configurez un profil d'interface SD-WAN pour définir les caractéristiques de votre connexion ISP et spécifiez la vitesse de la liaison DIA, la fréquence à laquelle le pare-feu de la branche surveille la liaison, puis sélectionnez l'étiquette de liaison pour spécifier à quelle liaison le profil d'interface SD-WAN s'applique.

Si vous avez créé plusieurs étiquettes de liaison, vous devez configurer un profil d'interface SD-WAN pour chaque étiquette de liaison.

Si vous avez créé un ensemble de liaison en affectant plusieurs liaisons DIA à une seule étiquette de liaison, en spécifiant cette étiquette de liaison, les paramètres du profil d'interface SD-WAN seront appliqués à toutes les liaisons DIA de l'ensemble.

STEP 4 | Configurez une interface Ethernet physique pour chaque liaison DIA d'applications SaaS.

Toutes les interfaces Ethernet physiques des liaisons DIA doivent être de Couche3.

STEP 5 | Configurer une Interface virtuelle SD-WAN qui regroupe toutes les interfaces Ethernet physiques des liaisons DIA d'applications SaaS en un seul groupe d'interfaces.

Le routeur virtuel du pare-feu utilise cette interface virtuelle SD-WAN pour acheminer le trafic SD-WAN à un emplacement DIA. Les profils d'état du chemin SD-WAN et de Distribution du trafic dans la règle de politique SD-WAN déterminent quel chemin utiliser et l'ordre dans lequel tenir compte des nouveaux chemins si l'état d'un chemin se détériore.

STEP 6 | Créez des profils de qualité SaaS pour des noms identiques pour les pare-feu de la plateforme et de la branche.

Deux profils de qualité SaaS portant le même nom doivent être configurés sur les pare-feu de la plateforme et de la branche pour exploiter avec succès le pare-feu de la plateforme comme solution de basculement de rechange. Le plus facile consiste à créer un seul profil de qualité SaaS dans le groupe de périphériques partagé. Vous pouvez également créer deux profils de qualité SaaS ayant des noms identiques dans des groupes de périphériques différents et les appliquez à vos pare-feu de la plate-orme et de la branche.

1. Sélectionnez **Objects (Objets)** > **SD-WAN Link Management (Gestion des liaisons SD-WAN)** > **SaaS Quality Profile (Profil de qualité SaaS)** et, dans le menu déroulant Device Group (Groupe de périphériques), sélectionnez **Shared (Partagé)**.
2. **Add (Ajoutez)** un nouveau profil de qualité SaaS.
3. Saisissez un **Name (Nom)** descriptif pour le profil de qualité SaaS.

4. Cochez (activez) **Shared (Partagé)** pour que le profil de qualité SaaS soit partagé entre tous les groupes de périphériques.

   Cette étape est nécessaire pour rendre le profil de qualité SaaS disponible à tous les groupes de périphériques auxquels vos pare-feu de la branche et de la plateforme appartiennent.
5. Cochez (activez) **Disable override (Désactiver le contrôle prioritaire)** pour désactiver le contrôle prioritaire de la configuration du profil de qualité SaaS sur le pare-feu local.
6. Configurez le mode de surveillance SaaS à l'aide de l'une des méthodes suivantes.
   - Configurez l'adresse IP statique de l'application SaaS.

     Créez un profil de qualité SaaS par application SaaS. Si une application SaaS possède plusieurs adresses IP, configurez un profil de qualité SaaS avec les multiples adresses IP statiques pour cette application SaaS.

     1. Sélectionnez **IP Address/Object (Adresse IP/Objet)** > **Static IP Address (Adresse IP statique)** et **Add (Ajoutez)** une adresse IP.
     2. Saisissez l'adresse IP de l'application SaaS ou sélectionnez un objet d'adresse configuré.
     3. Saisissez le **Probe Interval (Intervalle de sondage)**auquel le pare-feu de la branche sonde le chemin de l'application SaaS pour obtenir les informations relatives à son état.
     4. Cliquez sur **OK** pour enregistrer les modifications de votre configuration.
   - Configurez le Fully Qualified Domain Name (nom de domaine complet - FQDN) de l'application SaaS.
     1. Configurez un address object (objet d'adresse) FQDN de l'application SaaS.
     2. Sélectionnez **IP Address/Object (Adresse IP/Objet)** > **FQDN**, puis **Add (Ajoutez)** le FQDN.
     3. Sélectionnez l'**address object (objet d'adresse)** FQDN de l'application SaaS.
     4. Saisissez le **Probe Interval (Intervalle de sondage)**auquel le pare-feu de la branche sonde le chemin de l'application SaaS pour obtenir les informations relatives à son état.
     5. Cliquez sur **OK** pour enregistrer les modifications de votre configuration.
   - Configurez l'URL de l'application SaaS.

     La surveillance URL n'est prise en charge que pour le trafic qui transite par les ports 80, 443, 8080, 8081 et 143.

     1. Sélectionnez **HTTP/HTTPS**.
     2. Saisissez la **Monitored URL (URL surveillée)** de l'application SaaS.
     3. Saisissez le **Probe Interval (Intervalle de sondage)**auquel le pare-feu de la branche sonde le chemin de l'application SaaS pour obtenir les informations relatives à son état.
     4. Cliquez sur **OK** pour enregistrer votre configuration.

STEP 7 | Créez un profil de distribution du trafic pour spécifier l'ordre dans lequel le pare-feu de la branche passe de liaisons DIA à des liaisons VPN vers le pare-feu de la plateforme, en cas de dégradation de l'état d'une liaison.

STEP 8 | Configurez une règle de politique SD-WAN pour spécifier les mesures de l'état des liaisons et des applications SaaS et pour déterminer la façon dont le pare-feu sélectionne la liaison privilégiée pour le trafic critique des applications SaaS.

*À l'onglet **Application**, ajoutez l'application SaaS que vous surveillez à la règle de politique SD-WAN pour vous assurer que les paramètres de surveillance SaaS sont appliqués uniquement à l'application SaaS souhaitée.*

Cas d'utilisation : Configuration du basculement d'un pare-feu de la plate-forme pour la surveillance SaaS à partir d'un pare-feu de la branche vers une destination des applications SaaS différente

Si votre organisation utilise une application SaaS au niveau d'un pare-feu de la branche, mais que le pare-feu de la branche ne dispose d'aucune liaison DIA fonctionnelle vers laquelle basculer, vous pouvez configurer le pare-feu de la plateforme en tant qu'option de basculement de rechange, ce qui vous permettra de maintenir une connexion fonctionnelle à votre application SaaS au moyen d'un profil de qualité SaaS qui point vers une autre destination des applications SaaS.

Si les seuils de la mesure de l'état des liaisons DIA des applications SaaS sont dépassés et qu'il n'y a aucune liaison DIA fonctionnelle sur le pare-feu de la branche, la liaison passe au prochain pare-feu de la plateforme pour toutes les nouvelles sessions. La session existante sur la liaison DIA détériorée ne passe pas au pare-feu de la plateforme.

Par exemple, présumons que vos pare-feu de la branche et de la plateforme se trouvent aux extrémités du pays et qu'ils accèdent à une application SaaS dans le cloud, déployée dans un fournisseur de cloud, comme GCP. Vous pouvez configurer le basculement vers le pare-feu de la plateforme en l'absence de liaisons DIA fonctionnelles entre le pare-feu de la branche et l'application SaaS. Pour ce faire, configurez un profil de qualité SaaS portant le même nom sur les pare-feu de la branche et de la plateforme afin de forcer le basculement automatique vers le pare-feu de la plateforme en cas d'indisponibilité de liaisons DIA fonctionnelles à partir du pare-feu de la branche. Le profil de qualité SaaS configuré sur le pare-feu de la plateforme pointe vers l'emplacement le plus près de la plateforme afin de profiter des ressources locales les plus près. Vous avez ainsi toute la souplesse nécessaire pour spécifier les chemins de basculement fonctionnels et maintenir des données bout en bout précises sur la surveillance des applications SaaS sans congestionner la bande passante de votre réseau.

STEP 1 | Configurez votre déploiement SD-WAN.

1. Installer le plug-in SD-WAN.
2. Configurer Panorama et les pare-feux pour SD-WAN.
3. Ajouter des Périphériques SD-WAN à Panorama.
4. (Configurations haute disponibilité uniquement) Configurer les Périphérique HA pour SD-WAN.
5. Créer un cluster VPN.

STEP 2 | Créer une Link Tag (Étiquette de liens) pour regrouper les liaisons DIA de l'application SaaS.

Créez plusieurs étiquettes de liaison pour vos liaisons DIA pour appliquer différents paramètres de surveillance SD-WAN à chaque liaison d'applications SaaS en fonction du type de liaison.

De plus, vous pouvez créer une seule étiquette de liaison pour plusieurs liaisons DIA afin de regrouper les liaisons en un seul ensemble de liaisons.

STEP 3 | Configurez un profil d'interface SD-WAN pour définir les caractéristiques de votre connexion ISP et spécifiez la vitesse de la liaison DIA, la fréquence à laquelle le pare-feu de la branche surveille la liaison, puis sélectionnez l'étiquette de liaison pour spécifier à quelle liaison le profil d'interface SD-WAN s'applique.

Si vous avez créé plusieurs étiquettes de liaison, vous devez configurer un profil d'interface SD-WAN pour chaque étiquette de liaison.

Si vous avez créé un ensemble de liaison en affectant plusieurs liaisons DIA à une seule étiquette de liaison, en spécifiant cette étiquette de liaison, les paramètres du profil d'interface SD-WAN seront appliqués à toutes les liaisons DIA de l'ensemble.

STEP 4 | Configurez une interface Ethernet physique pour chaque liaison DIA d'applications SaaS.

Toutes les interfaces Ethernet physiques des liaisons DIA doivent être de Couche3.

STEP 5 | Configurer une Interface virtuelle SD-WAN qui regroupe toutes les interfaces Ethernet physiques des liaisons DIA d'applications SaaS en un seul groupe d'interfaces.

Le routeur virtuel du pare-feu utilise cette interface virtuelle SD-WAN pour acheminer le trafic SD-WAN à un emplacement DIA. Les profils d'état du chemin SD-WAN et de Distribution du trafic dans la règle de politique SD-WAN déterminent quel chemin utiliser et l'ordre dans lequel tenir compte des nouveaux chemins si l'état d'un chemin se détériore.

STEP 6 | Créez des profils de qualité SaaS pour des noms identiques pour les pare-feu de la plateforme et de la branche.

Deux profils de qualité SaaS portant le même nom doivent être configurés sur les pare-feu de la plateforme et de la branche pour exploiter avec succès le pare-feu de la plateforme comme solution de basculement de rechange. Créez deux profils de qualité SaaS ayant des noms identiques, chacun pointant vers une destination pour les applications SaaS différente dans des groupes de périphériques différents et appliquez-les à vos pare-feu de la plateforme et de la branche.

1. Sélectionnez **Objects (Objects)** > **SD-WAN Link Management (Gestion des liaisons SD-WAN)** > **SaaS Quality Profile (Profil de qualité SaaS)**, puis sélectionnez le groupe de périphériques cible qui contient le pare-feu de la branche dans le menu déroulant Device Group (Groupe de périphériques).
2. **Add (Ajoutez)** un nouveau profil de qualité SaaS.
3. Saisissez un **Name (Nom)** descriptif pour le profil de qualité SaaS.
4. Cochez (activez) **Disable override (Désactiver le contrôle prioritaire)** pour désactiver le contrôle prioritaire de la configuration du profil de qualité SaaS sur le pare-feu local.

5. Configurez le mode de surveillance SaaS à l'aide de l'une des méthodes suivantes.
   - Configurez l'adresse IP statique de l'application SaaS.

     Créez un profil de qualité SaaS par application SaaS. Si une application SaaS possède plusieurs adresses IP, configurez un profil de qualité SaaS avec les multiples adresses IP statiques pour cette application SaaS.

     1. Sélectionnez **IP Address/Object (Adresse IP/Objet)** > **Static IP Address (Adresse IP statique)** et **Add (Ajoutez)** une adresse IP.
     2. Saisissez l'adresse IP de l'application SaaS ou sélectionnez un objet d'adresse configuré.
     3. Saisissez le **Probe Interval (Intervalle de sondage)**auquel le pare-feu de la branche sonde le chemin de l'application SaaS pour obtenir les informations relatives à son état.
     4. Cliquez sur **OK** pour enregistrer les modifications de votre configuration.
   - Configurez le Fully Qualified Domain Name (nom de domaine complet - FQDN) de l'application SaaS.
     1. Configurez un address object (objet d'adresse) FQDN de l'application SaaS.
     2. Sélectionnez **IP Address/Object (Adresse IP/Objet)** > **FQDN**, puis **Add (Ajoutez)** le FQDN.
     3. Sélectionnez l'**address object (objet d'adresse)** FQDN de l'application SaaS.
     4. Saisissez le **Probe Interval (Intervalle de sondage)**auquel le pare-feu de la branche sonde le chemin de l'application SaaS pour obtenir les informations relatives à son état.
     5. Cliquez sur **OK** pour enregistrer les modifications de votre configuration.
   - Configurez l'URL de l'application SaaS.

     La surveillance URL n'est prise en charge que pour le trafic qui transite par les ports 80, 443, 8080, 8081 et 143.

     1. Sélectionnez **HTTP/HTTPS**.
     2. Saisissez la **Monitored URL (URL surveillée)** de l'application SaaS.
     3. Saisissez le **Probe Interval (Intervalle de sondage)**auquel le pare-feu de la branche sonde le chemin de l'application SaaS pour obtenir les informations relatives à son état.
     4. Cliquez sur **OK** pour enregistrer votre configuration.
6. Sélectionnez **Objects (Objects)** > **SD-WAN Link Management (Gestion des liaisons SD-WAN)** > **SaaS Quality Profile (Profil de qualité SaaS)**, puis sélectionnez le groupe de périphériques cible qui contient le pare-feu de la plateforme dans le menu déroulant Device Group (Groupe de périphériques).
7. Répétez les étapes 6.2 à 6.5 pour créer un profil de qualité SaaS portant le même nom pour une application SaaS se trouvant à un autre emplacement.

   Cette étape est nécessaire pour créer un profil de qualité SaaS portant le même nom dans le groupe de périphériques auquel votre pare-feu de la plateforme appartient.

STEP 7 | Créez un profil de distribution du trafic pour spécifier l'ordre dans lequel le pare-feu de la branche passe de liaisons DIA à des liaisons VPN vers le pare-feu de la plateforme, en cas de dégradation de l'état d'une liaison.

STEP 8 | Configurez une règle de politique SD-WAN pour spécifier les mesures de l'état des liaisons et des applications SaaS et pour déterminer la façon dont le pare-feu sélectionne la liaison privilégiée pour le trafic critique des applications SaaS.

*À l'onglet **Application**, ajoutez l'application SaaS que vous surveillez à la règle de politique SD-WAN pour vous assurer que les paramètres de surveillance SaaS sont appliqués uniquement à l'application SaaS souhaitée.*

Traffic Distribution Profiles (profils de distribution du trafic) SD-WAN

Dans une typologie SD-WAN, le pare-feu détecte une défaillance, une panne et une détérioration du chemin d'accès *par application* et sélectionne un nouveau chemin d'accès afin de garantir que vous bénéficiez de la meilleure performance pour les applications cruciales de votre entreprise. Avoir plusieurs liens ISP vous permet d'échelonner la capacité de votre trafic et de réduire les coûts. La sélection du nouveau chemin d'accès se produit en moins de une seconde si vous laissez Path Monitoring and Probe Frequency (Surveillance des chemins d'accès et Fréquence de sondage) avec les paramètres par défaut ; autrement, la sélection d'un nouveau chemin d'accès pourrait prendre plus d'une seconde.

Pour mettre en place cette sélection du chemin d'accès, le pare-feu utilise les règles de politique SD-WAN, en référence au profil de Distribution de trafic qui précise comment sélectionner des chemins d'accès pour la distribution de la charge de la session et pour le basculement vers un meilleur chemin d'accès lorsque la qualité du chemin d'une application se détériore.

Décidez quelle méthode de distribution du trafic une application ou un service (qui correspond à une règle de politique SD-WAN) doit utiliser :

- **Best Available Path** (Meilleur chemin disponible) —Sélectionnez cette méthode si le coût n'est pas un facteur déterminant et les applications pourront utiliser n'importe quel chemin d'accès sur la branche. Le pare-feu utilise des mesures de la qualité du chemin d'accès pour distribuer le trafic et basculer sur un des liens appartenant à une Link Tag (étiquette de lien) dans la liste, fournissant ainsi la meilleure expérience de l'application aux utilisateurs.
- **Top-Down Priority** (Priorité descendante) — Si vous avez des liens onéreux ou à faible capacité dont vous souhaitez qu'ils soient utilisés en dernier ressort ou comme liens de secours, utilisez la méthode de Priorité descendante et placez les étiquettes qui comprennent ces liens en dernier dans la liste des Link Tags (étiquettes de liens) dans le profil. Le pare-feu utilise la première étiquette de lien de la liste afin de déterminer les liens sur lesquels charger le trafic de la session et ceux sur lesquels basculer. Si aucun des liens de la première étiquette de liens n'est validé sur la base du Path Quality profil(profil de qualité du chemin d'accès), le pare-feu sélectionne un lien dans la deuxième étiquette de liens dans la liste. Si aucun des liens de la deuxième étiquette de liens n'est validé, la procédure continue aussi longtemps que nécessaire jusqu'à ce que le pare-feu trouve un lien validé dans la dernière étiquette de liens. Si tous les liens associés sont surchargés et qu'aucun lien ne respecte les seuils de qualité, le pare-feu utilise la méthode du Meilleur chemin disponible pour sélectionner un lien vers lequel transférer le trafic. Au début d'un événement de basculement, le pare-feu démarre en haut de la liste de Priorité descendante des Étiquettes de liens pour trouver un lien sur lequel basculer.

- **Weighted Session Distribution** (Distribution de session pondérée) — Sélectionnez cette méthode si vous souhaitez charger le trafic (qui correspond à la règle) manuellement vers votre ISP et vos liens WAN et que vous n'avez pas besoin de basculer lors de conditions de défaillance. Vous indiquez manuellement la charge du lien lorsque vous appliquez un pourcentage statique de nouvelles sessions que les interfaces regroupées avec une seule Étiquette de lien obtiendront. Le pare-feu distribue les nouvelles sessions à tour de rôle entre les liens qui ont les Étiquettes de liens indiquées, jusqu'à ce que le lien auquel est assigné le pourcentage le plus faible atteigne ce pourcentage de sessions. Le pare-feu utilise le(s) lien(s) restant(s) de la même façon. Vous pouvez sélectionner cette méthode pour les applications qui ne sont pas sensibles à la latence et qui nécessitent une grande capacité de bande passante du lien, telles que les sauvegardes de branches importantes et les transferts de fichiers volumineux.

  Si le lien subit un brownout, le pare-feu ne redirige pas le trafic correspondant vers un lien différent.

En cas de condition de chemin d'accès défectueux, la méthode de distribution du trafic que vous choisissez pour une/des application(s) dans une règle de politique SD-WAN, et les Étiquettes de liens dans des groupes de liens, déterminent si et comment le pare-feu sélectionne un nouveau chemin d'accès (effectue des basculements de lien) comme suit :

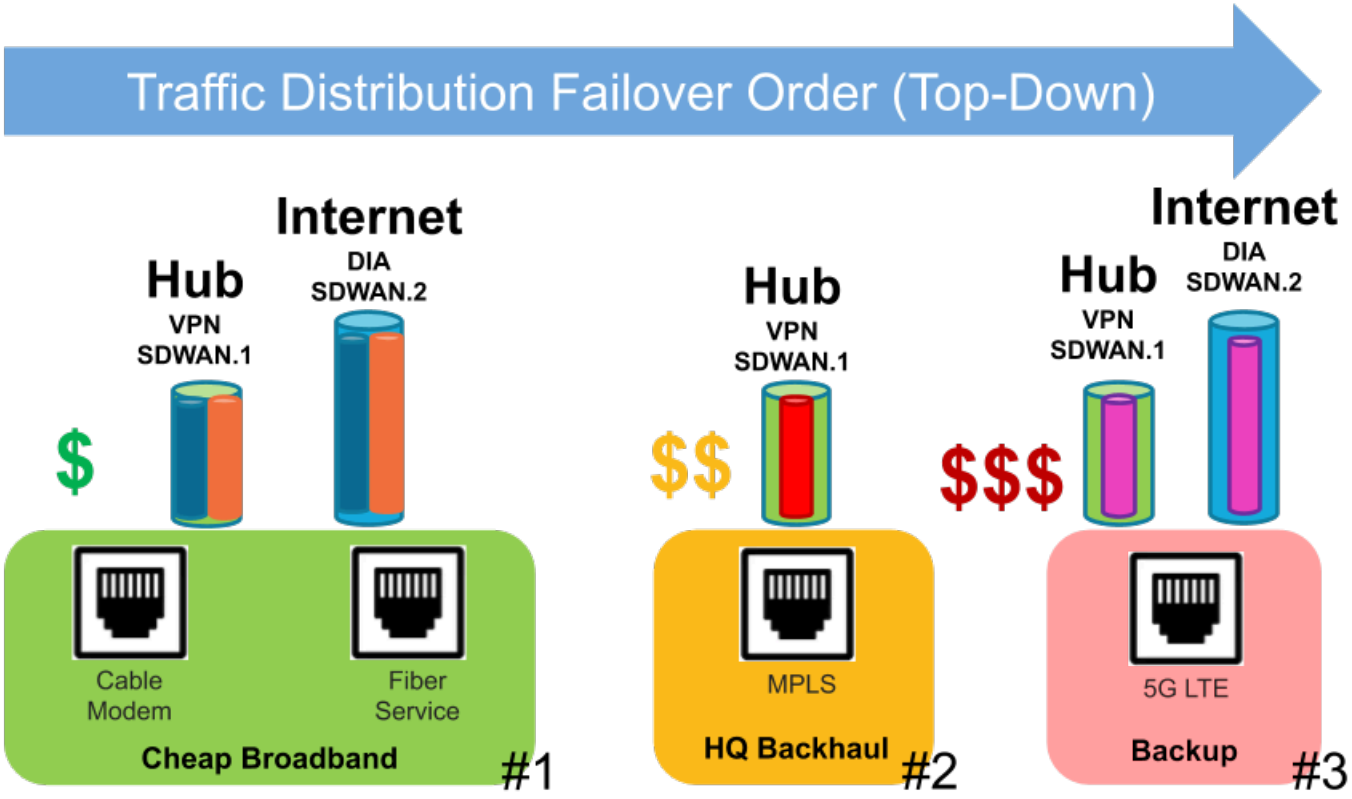
Condition du chemin d'accès	Top-Down Priority (Priorité descendante)	Best Available Path (Meilleur chemin disponible)	Weighted Session Distribution (Distribution pondérée de sessions)
La session sur un chemin d'accès existant a basculé à un seuil de bon état du chemin d'accès (restriction d'alimentation)	La session affectée bascule sur un meilleur chemin d'accès (si disponible)	La session affectée bascule sur un meilleur chemin d'accès (si disponible)	La session affectée ne bascule pas
Récupération ascendant ou du meilleur chemin disponible : le chemin existant répond toujours aux conditions (bon)	La session affectée rebascule sur le chemin d'accès précédent	La session affectée reste sur le chemin existant et ne rebascule pas	La session affectée ne bascule pas
Récupération ascendant ou du meilleur chemin disponible : le chemin existant ne réussit pas la vérification de l'état	Toutes les sessions basculent sur le chemin d'accès précédent	Des sessions sélectives rebasculent sur le chemin d'accès précédent jusqu'à ce que le chemin d'accès existant affecté soit rétabli	La session affectée ne bascule pas

Condition du chemin d'accès	Top-Down Priority (Priorité descendante)	Best Available Path (Meilleur chemin disponible)	Weighted Session Distribution (Distribution pondérée de sessions)
Le chemin d'accès existant ne fonctionne pas (défaillance)	Toutes les sessions basculent sur le meilleur chemin d'accès suivant sur la liste	Toutes les sessions basculent sur le meilleur chemin d'accès suivant	Toutes les sessions basculent sur d'autres étiquettes sur la base des paramètres de pondération
Restriction d'alimentation sans chemin qualifié (meilleur)	Prendre le meilleur chemin disponible	Prendre le meilleur chemin disponible	Prendre le meilleur chemin disponible

De plus, le pare-feu réalise automatiquement un partage de la charge de la session entre les membres de l'interface d'un seule Étiquette de liens. Après que ces interfaces aient approché leur Mbps maximum, de nouvelles sessions se dirigent vers les interfaces qui ont une Étiquette de liens différente (sur la base de la méthode de distribution du trafic) si ces interfaces ont de meilleures mesures de santé.

Condition du chemin d'accès	Top-Down Priority (Priorité descendante)	Best Available Path (Meilleur chemin disponible)	Weighted Session Distribution (Distribution pondérée de sessions)
Plusieurs liens avec la même Étiquette SD-WAN	Partage de la charge de la session de façon égale entre les liens de la même Étiquette SD-WAN	Partage de la charge de la session sur la base du meilleur chemin dans une Étiquette SD-WAN	Partage de la charge de la session sur la base du % de pondération assigné à l'Étiquette SD-WAN
Plusieurs liens avec des Étiquettes SD-WAN différentes	Partage de la charge de la session sur la base de la priorité de la liste, des liens de charge de la première Étiquette SD-WAN d'abord.	Partage de la charge de la session sur la base du meilleur chemin de toutes les Étiquettes SD-WAN	Partage de la charge de la session sur la base du % de pondération assigné aux Étiquettes SD-WAN

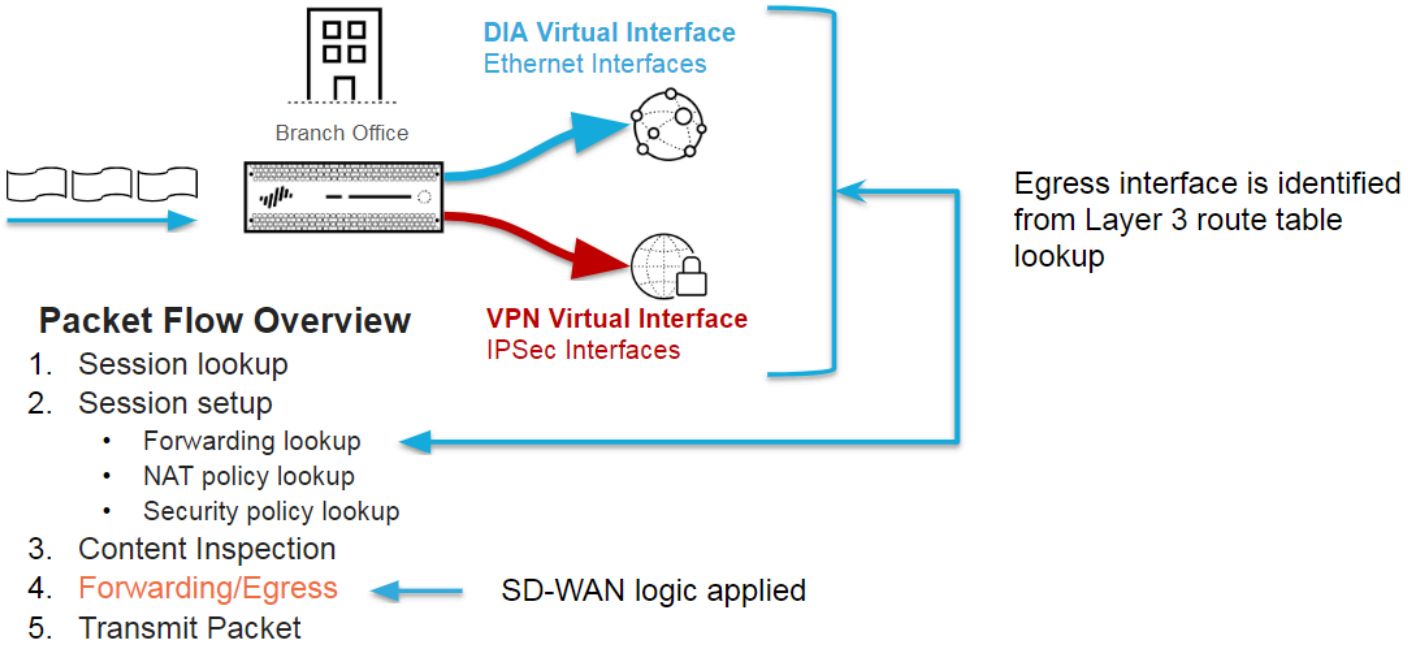
La figure suivante montre un exemple de profil de Distribution de trafic qui utilise la Méthode de Priorité descendante. Les n° 1, 2 et 3 sont l'ordre des Étiquettes de liens des liens que le pare-feu examine, si nécessaire, pour trouver un chemin d'accès sain afin d'effectuer une basculement total de session de l'application. Pour chaque basculement séparé qui se produit, le pare-feu commence au début de la liste descendante des Étiquettes de liens.



1. Dans cet exemple de Priorité descendante, les paquets d'une branche supportant une application spécifique (par exemple, office365-enterprise-access) arrivent au pare-feu. Le pare-feu utilise le tableau d'acheminement afin de déterminer le saut suivant vers la destination et l'interface sortante qui est le tunnel d'interface SD-WAN intitulé sdwan.901. La règle de politique de sécurité autorise les paquets. Les paquets correspondent ensuite à une règle de politique SD-WAN (intitulée Office365 to Hub 1) qui précise la zone de destination pour le hub. Le pare-feu utilise le profil de Qualité du chemin d'accès de la règle de politique SD-WAN, le profil de Distribution du trafic et les Étiquettes de liens de ce profil afin de déterminer quel membre de l'interface (lien) de sdwan.901 doit être utilisé. Le profil de Distribution du trafic indique trois Étiquettes de liens dans cet ordre : n°1 Largeur de bande bon marché, n°2 Interconnexion HQ et n°3 Sauvegarde (qui est l'ordre des Étiquettes de liens dont le pare-feu examine les liens afin d'en trouver un sur lequel basculer).
2. En supposant que tous les chemins sont validés (par le profil de Qualité du chemin), le pare-feu distribue les paquets à un des liens physiques associés avec la première Étiquette de liens dans la liste du profil de Distribution du trafic : Bande passante bon marché. Le tunnel sdwan.901 a deux interfaces de membre (deux transporteurs) : le tunnel VPN du modem câble et le tunnel VPN du service de la fibre. Le pare-feu examinera en premier un lien à tour de rôle et choisira le premier lien qu'il trouvera qui est qualifié, par exemple, le lien du modem câble.
3. Si le premier lien de la Bande passante bon marché (modem câble) n'est pas le lien qualifié, le pare-feu sélectionne le deuxième lien de la Bande passante bon marché (service de la fibre).
4. Si le deuxième lien de la Bande passante bon marché (service de la fibre) n'est pas un lien qualifié, le pare-feu sélectionne l'interconnexion HQ avec le lien portant l'étiquette du lien n°2, qui est un lin MPLS plus cher vers la même plateforme.

5. Si le deuxième lien de la Bande passante bon marché (service de la fibre) n'est pas un lien qualifié, le pare-feu sélectionne l'interconnexion HQ avec le lien portant l'étiquette du lien n°3, qui est un lien LTE 5G plus cher vers la même plateforme.
6. Si le pare-feu ne trouve pas de lien qualifié pour basculer, il utilise la méthode du Meilleur disponible afin de sélectionner un lien.
7. Au début d'un nouvel événement de basculement, le pare-feu démarre en haut de la liste descendante des Étiquettes de liens pour trouver un lien sur lequel basculer.

Gardez à l'esprit que la distribution du trafic SD-WAN est l'une des dernières étapes dans la logique de flux de paquets. Zoomons pour avoir un aperçu plus général du flux de paquets.

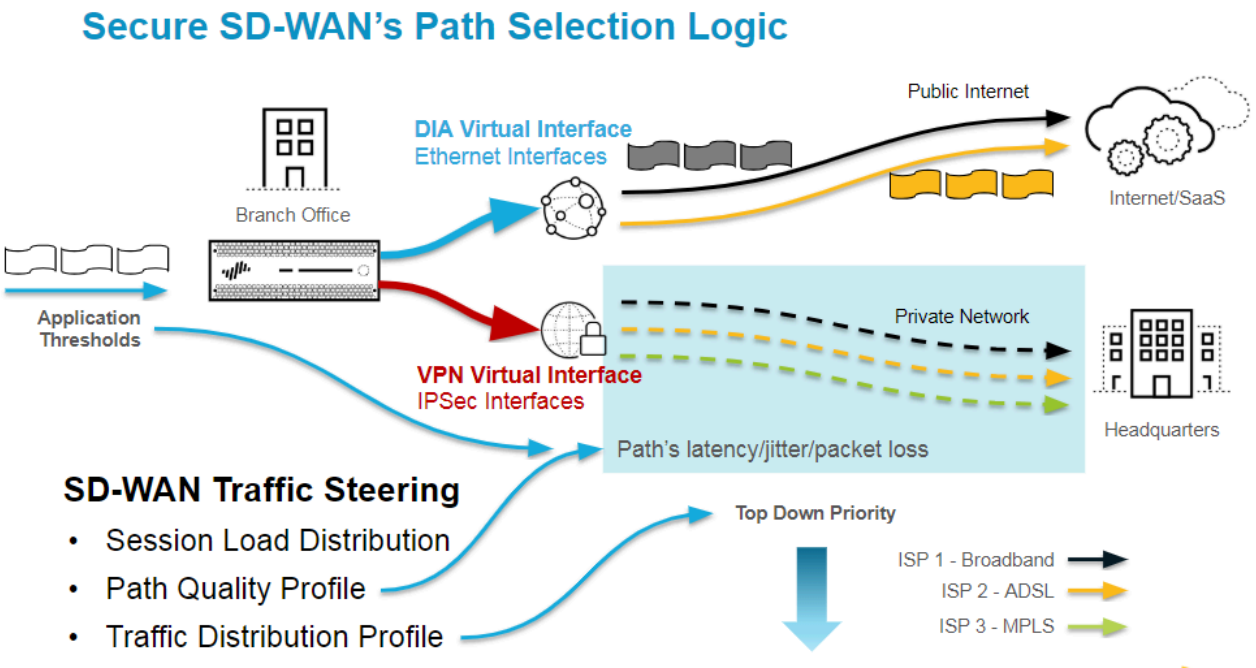


Les détails du flux de paquets de la figure sont les suivants :

1. Lorsqu'une session d'une application arrive au pare-feu, le pare-feu effectue une recherche de session afin de déterminer si la session est une session existante ou une nouvelle session.
2. Une nouvelle session passe par la configuration de session :
    1. Forwarding lookup (Transfert de la recherche) — Le pare-feu obtient la zone de sortie, l'interface de sortie et le système virtuel du tableau d'acheminement de la Couche 3 ou de la Couche 2 de Forwarding Database lookup (transfert de la recherche de base de données), etc. Pour les applications qui correspondent à une règle de politique SD-WAN, le pare-feu utilise l'interface virtuelle SD-WAN en tant qu'interface de sortie.
    2. NAT Policy lookup (recherche de politique NAT) — Si la session correspond à une règle NAT, le pare-feu effectue une autre transmission de recherche afin de déterminer l'interface et la zone de sortie finales (converties).
    3. Security Policy lookup (Recherche de politique de sécurité) —Si une règle de politique de sécurité autorise la session, la session est créée et installée dans le tableau des sessions. Le pare-feu effectue ensuite une classification supplémentaire à l'aide de App-ID™ et User-ID™.

3. Content Inspection (inspection du contenu) — Le pare-feu effectue une inspection des menaces (Anti-Spyware pour IPS [protection contre les vulnérabilités], Antivirus, filtrage d'URL , WildFire®, etc.)sur la charge utile et les en-têtes si nécessaire.
4. L'étape de Transfert/Sortie effectue une sélection du chemin d'accès et transfère les paquets. Cette étape est celle où se fait la sélection du chemin d'accès SD-WAN.
    1. Packet Forwarding Process (Procédure de transfert de paquets) — Le pare-feu utilise l'interface de sortie afin de déterminer le domaine de transfert ; il effectue l'acheminement, la transition ou le transfert par câble virtuel.
    2. La sélection du chemin d'accès SD-WAN se fait lorsque l'application correspond à une règle de politique SD-WAN ; le profil de Qualité du chemin d'accès détermine la qualification du chemin d'accès ; le profil de Distribution du trafic détermine la méthode de sélection du chemin d'accès et l'ordre dans lequel les chemins d'accès sont pris en compte lors de la sélection.
    3. Le cryptage du tunnel IPSec/SSL-VPN a lieu si nécessaire.
    4. Packet Egress Process (procédure de sortie de paquets) - QoS shaping (mise en forme de qualité de service), la réécriture DSCP et la fragmentation d'IP sont appliquées (si nécessaire).
5. Transmit Packet (Transférer le paquet) — Le pare-feu transfère le paquet à l'interface de sortie sélectionnée.

Maintenant, nous dézoomons pour examiner la logique de la sélection du chemin d'accès SD-WAN plus en détails.



1. Le pare-feu consulte le tableau d'acheminement pendant le transfert de recherche ; sur la base de l'adresse IP de la destination correspondant à un préfixe de Couche 3, le pare-feu détermine l'interface virtuelle SD-WAN de sortie. Le paquet va soit directement sur l'internet public ou retourne vers le hub par un lien VPN sécurisé.

2. Le pare-feu surveille chaque chemin d'accès en effectuant des vérifications d'état par un tunnel VPN. Chaque circuit DIA a un tunnel VPN qui surveille les informations sur l'état.
3. L'application de la règle de politique SD-WAN est associée à un profil de Qualité du chemin d'accès et le pare-feu compare les valeurs moyennes réelles de latence, gigue et perte de paquets du chemin du chemin aux valeurs seuil.
4. Tout chemin d'accès dont la valeur de latence, gigue ou perte de paquets est plus élevée que le seuil n'est pas sélectionné.
5. Tous les chemins satisfaisant aux conditions dans l'interface virtuelle SD-WAN sont ensuite soumis à la méthode de profil de Distribution du trafic et à la logique de priorité du chemin (ordre). Les étiquettes de liens SD-WAN regroupent les services ISP ensemble et l'ordre de ces étiquettes dans le profil de Distribution du trafic donne la priorité aux chemins lors de la sélection du chemin.
6. Ainsi le Path Quality Profile (Profil de Qualité du chemin d'accès) et le Traffic Distribution profile (Profil de Distribution du trafic) déterminent ensemble le meilleur chemin suivant à utiliser et le pare-feu transfère le trafic par ce lien.

Créer un Traffic Distribution Profile (profil de distribution du trafic)

Sur la base de votre planification de configuration SD-WAN, créez le Traffic Distribution Profiles (profils de distribution du trafic) SD-WAN dont vous avez besoin sur la base de la façon dont vous souhaitez que les applications de vos règles de politique SD-WAN soient chargées dans la session et basculent.

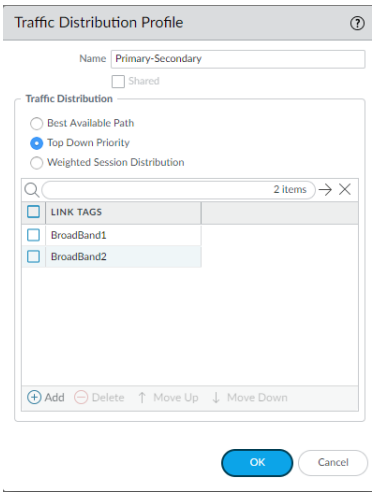
STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Assurez vous d'avoir déjà configuré les Étiquettes de liens dans un SD-WAN interface profile (profil d'interface SD-WAN), qu'elles sont validées et appliquées. Les Étiquettes de liens doivent être appliquées à vos hubs er branches afin que le Panorama™ associe bien les Étiquettes de liens que vous indiquez dans ce profil de Distribution du trafic à un profil d'interface SD-WAN.

STEP 3 | Sélectionnez un **Device Group** (groupe de périphériques).

STEP 4 | Créez un Traffic Distribution Profile (profil de distribution du trafic).

1. Sélectionnez **Objects** > **SD-WAN Link Management** > **Traffic Distribution Profile** (Objets - Gestion des liens SD-WAN - Profil de distribution du trafic).
2. **Add** (Ajoutez) un profil de distribution du trafic par **Name** (nom) en utilisant un maximum de 31 caractère alphanumériques.



3. Sélectionnez **Shared** (Partagé) uniquement si vous souhaitez utiliser ce profil de distribution du trafic pour tous les Groupes de périphériques (hubs et branches).
4. Sélectionnez une méthode de distribution du trafic et ajoutez un maximum de quatre Étiquettes de liens qui utilisent cette méthode pour ce profil.

   - **Best Available Path** (Meilleur chemin disponible) —**Add** (Ajoutez) une ou plusieurs **Link Tags** (Étiquettes de liens). Au cours des échanges de paquets initiaux, avant que App-ID n'ait classé l'application dans le paquet, le pare-feu utilise le chemin de l'étiquette qui présente les meilleures mesures d'état (sur la base de l'ordre des étiquettes). Un fois que le pare-feu a identifié l'application, il compare l'état (qualité du chemin) du chemin qu'il utilisait avec celui du premier chemin (interface) de la première Étiquette de lien. Si l'état du chemin original est meilleur, il reste le chemin sélectionné ; autrement, le pare-feu remplace le chemin original. Le pare-feu répète cette procédure jusqu'à ce qu'il ait évalué tous les chemins de l'Étiquette de lien. Le chemin final est le chemin sélectionné par le pare-feu lorsqu'un paquet répondant aux critères de correspondance arrive.

     *Lorsqu'un lien devient non qualifié et doit basculer vers le meilleur chemin suivant, le pare-feu peut migrer un maximum de 1 000 sessions par minute du lien non qualifié vers le meilleur chemin suivant. Par exemple, supposons que le tunnel.901 a 3 000 sessions ; 2 000 de ces sessions correspondent à la règle de politique SD-WAN A et 1 000 sessions correspondent à la règle de politique SD-WAN B (les deux règles ont une politique de distribution du trafic configurée à l'aide du **Best Path Available** (Meilleur chemin disponible). Si le tunnel.901 n'est plus qualifié, il faut trois minutes pour migrer les 3 000 sessions depuis le lien non qualifié vers le meilleur chemin suivant.*

   - **Top Down Priority** (Priorité descendante) —**Add** (Ajoutez) une ou plusieurs **Link Tags** (Étiquettes de liens). Le pare-feu distribue les nouvelles sessions (qui répondent aux critères de correspondance) vers les liens dans l'ordre descendant des **Link**

Tags (Étiquettes de liens) que vous avez ajoutées. Le pare-feu examine la première étiquette configurée pour ce profil et examine les chemins qui utilisent cette étiquette en sélectionnant le premier chemin qu'il trouve qui est qualifié (qui atteint les seuils de qualité du chemin ou reste en dessous pour cette règle). Si aucun chemin qualifié n'est trouvé depuis cette Étiquette de liens, le pare-feu examine les chemins qui utilisent l'Étiquette de liens suivante. Si le pare-feu ne trouve aucun chemin après avoir examiné tous les chemins de toutes les Étiquettes de liens, le pare-feu utilise la méthode du **Best Available Path** (Meilleur chemin disponible). Le premier chemin sélectionné est le chemin préféré jusqu'à ce que l'un des seuils de qualité du chemin pour ce chemin soit dépassé, après quoi le pare-feu redémarre en haut de la liste Balise de lien pour trouver le nouveau chemin préféré.

*Si vous n'avez qu'un seul lien sur le hub, ce lien prend en charge toutes les interfaces virtuelles et le trafic DIA. Si vous souhaitez utiliser les types de liens dans un ordre spécifique, vous devez appliquer un profil de distribution du trafic au hub qui spécifie la **Top Down Priority (priorité descendante)** puis ordonner aux balises de lien de spécifier l'ordre préféré. Si vous appliquez un profil de distribution du trafic qui spécifie à la place **Best Available Path (meilleur chemin disponible)**, le pare-feu utilisera le lien, quel qu'en soit le coût, pour choisir le chemin d'accès le plus performant à la branche. En résumé, Lier des balises dans un profil de distribution du trafic, la balise link appliquée à une hub virtual interface (interface virtuelle hub) et une **VPN Failover Metric (métrique de basculement VPN)** fonctionnent uniquement lorsque le profil de distribution du trafic spécifie la **Top Down Priority (priorité descendante)**.*

- **Weighted Session Distribution** (Distribution pondérée de sessions) —**Add** (Ajoutez) une ou plusieurs **Link Tags** (Étiquettes de liens) puis saisissez le pourcentage de**Weight** (pondération) pour chaque **Link Tag** (Étiquette de liens) afin que la pondération atteigne 100 %. Le pare-feu effectue une distribution de la charge des sessions entre les Étiquettes de liens jusqu'à ce que les pourcentages maximums soient atteints. S'il y a plus d'un chemin dans l'Étiquette de liens, le pare-feu distribue de façon égale en utilisant une méthode à tour de rôle jusqu'à ce que les mesures

d'état du chemin soient atteintes puis distribue les sessions aux autres membres qui n'ont pas atteint la limite.

Si plusieurs interfaces physiques ont la même étiquette, le pare-feu distribue les sessions correspondantes de façon égale entre elles. Si tous les chemins d'accès ne passe pas le seuil de bon état (qualité du chemin), le pare-feu sélectionne le chemin qui a les meilleures statistiques d'état. Si aucun lien SD-WAN n'est disponible (peut-être à cause d'une panne, le pare-feu utilise un routage statique ou dynamique pour acheminer les paquets correspondants.

Si un paquet est acheminé vers une interface virtuelle SD-WAN mais que le pare-feu ne peut pas trouver un chemin préféré pour la session sur la base du profil de Distribution du trafic de la politique SD-WAN, le pare-feu utilise implicitement la méthode du Meilleur chemin disponible pour trouver le chemin préféré. Le pare-feu distribue les sessions d'application qui ne correspondent pas à une règle de politique SD-WAN sur la base de la règle finale implicite du pare-feu, qui distribue les sessions à tour de rôle entre les liens disponibles, quel que soit le profil de Distribution du trafic.

Si vous préférer contrôler la façon dont le pare-feu distribue les sessions sans correspondance, créez une règle finale de récupération de la totalité pour Distribuer des sessions sans correspondance vers les liens spécifiques dans l'ordre que vous indiquez.

5. (En option) Après avoir ajouté les Étiquettes de liens, utilisez les flèches **Move Up** (Déplacer vers le haut) ou **Move Down** (Déplacer vers le bas) pour modifier l'ordre dans lequel vous souhaitez que le pare-feu utilise les liens pour ce profil et pour les applications sélectionnées dans la règle de politique SD-WAN.
6. Cliquez sur **OK**.

STEP 5 | **Commit** (Validez) et **Commit and Push** (Validez et appliquez) les modifications de votre configuration.

STEP 6 | **Commit (Validez)** vos modifications.

Création d'un profil de correction des erreurs

Le transfert de correction des erreurs (FEC) est une méthode utilisée pour corriger certaines erreurs de transmission de données qui se produisent sur des lignes de communication bruyantes. Il permet donc de renforcer la fiabilité des données sans exiger leur retransmission. Le FEC est utile pour les applications qui sont sensibles à la perte des paquets ou à la corruption, comme l'audio, le VoIP et la conférence vidéo. Avec le FEC, le pare-feu récepteur peut récupérer des paquets perdus ou corrompus en utilisant des bits de parité que l'encodeur qui envoie intègre dans un flux d'application. Grâce à la réparation du flux, les données SD-WAN n'ont pas à basculer vers un autre chemin, et TCP n'a pas à renvoyer les paquets. Le FEC peut également aider avec les applications UDP en récupérant les paquets perdus ou corrompus, puisque UDP ne retransmet pas les paquets.

Le FEC SD-WAN prend en charge les pare-feu de la branche et de la plate-forme qui agissent en tant qu'encodeurs et que décodeurs. Selon le mécanisme du FEC, l'encodeur ajoute des octets

redondants à un train de bits et le décodeur utilise cette information pour corriger les données reçues, au besoin, avant de les envoyer à destination.

SD-WAN prend également en charge la duplication de paquet comme méthode de rechange pour la correction des erreurs. La duplication de paquet effectue une duplication complète d'une session d'application d'un tunnel à un autre. La duplication de paquet exige plus de ressources que le FEC et doit être utilisée uniquement pour les applications critiques qui ont une faible tolérance aux paquets abandonnés.

Les applications modernes qui possèdent leurs propres mécanismes de reprise pourraient ne pas avoir besoin du FEC ou de la duplication de paquet. Appliquez la méthode FEC ou de duplication de paquet uniquement aux applications qui peuvent réellement tirer parti de ce mécanisme. Autrement, une bande passante et des ressources CPU supplémentaires sont nécessaires sans procurer d'avantages. Ni le FEC, ni la duplication de paquet n'est utile si votre problème de SD-WAN est la congestion.

La fonctionnalité du FEC et de la duplication de paquet exige que Panorama exécute PAN-OS 10.0.2 ou une version ultérieure et le plugin SD-WAN 2.0 ou toute version ultérieure qui est compatible avec la version de PAN-OS. L'encodeur et le décodeur doivent tous deux exécuter PAN-OS 10.0.2 ou toute version ultérieure. Si une branche ou une plateforme exécute une version plus ancienne du logiciel, le trafic dont l'en-tête comprend un FEC ou une duplication de paquet est abandonné au niveau du pare-feu.

À partir de PAN-OS 10.0.3, la FEC et la duplication de paquets sont prises en charge dans une topologie à maillage complet, en plus de la topologie en étoile déjà prise en charge.

Ni le FEC, ni la duplication de paquet ne doivent être utilisés sur des liaisons DIA : ils ne servent qu'aux liaisons des tunnels VPN entre une branche et une plate-forme.

FEC et la duplication de paquets sont pris en charge uniquement pour les pare-feux PAN-OS compatibles SD-WAN. FEC et la duplication de paquets ne sont pas prises en charge pour Prisma Access Hubs.

Pour configurer le FEC ou la duplication de paquet sur l'encodeur (le côté qui initie le FEC ou la duplication de paquet), utilisez Panorama pour faire ce qui suit :

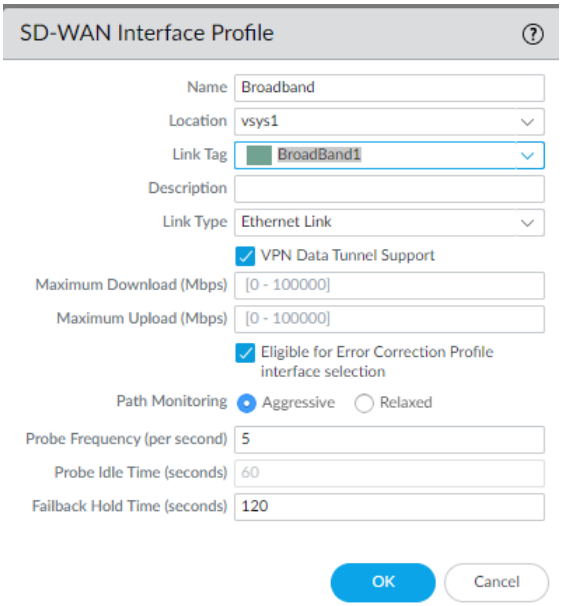
- Créer un profil d'interface SD-WAN qui spécifie **Eligible for Error Correction Profile interface selection (Admissible à la sélection d'interface de profil de correction des erreurs)** et appliquer le profil à au moins une interface.
- Créer un profil de correction des erreurs pour appliquer le FEC ou la duplication de paquet.
- Appliquer le Profil de correction des erreurs à une règle de politique SD-WAN et spécifier les applications auxquelles les règles s'appliquent.
- Appliquer la configuration aux encodeurs. (Le décodeur [le côté récepteur] n'exige aucune configuration spécifique pour le FEC ou la duplication de paquet : les mécanismes sont activés par défaut sur le décodeur tant que l'encodeur initie la correction des erreurs.)

Le FEC et la duplication de paquet prend en charge un MTU de 1 340 octets. Un paquet plus grand ne passera pas le FEC ou le processus de duplication de paquet.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Configurer un Profil d'interface SD-WAN, et sélectionnez **Eligible for Error Correction Profile interface selection (Admissible à la sélection d'interface de profil de correction des erreurs)** pour indiquer que le pare-feu peut automatiquement utiliser les interfaces (où le profil d'interface SD-WAN est appliqué) à des fins de correction des erreurs. Que cette option utilise par défaut les choix sélectionnés ou non dépend du **Link Type (Type de liaison)** que vous sélectionnez pour le profil.

*L'option **Eligible for Error Correction Profile interface selection (Admissible à la sélection d'interface de profil de correction des erreurs)** d'un profil peut être décochée, et vous pouvez appliquer le profil à une liaison 5G LTE onéreuse, par exemple, pour que la correction d'erreurs coûteuse ne soit jamais effectuée sur cette liaison.*



STEP 3 | Configurer une interface Ethernet physique pour SD-WAN et appliquez le profil d'interface SD-WAN qui vous avez créé à l'interface Ethernet.

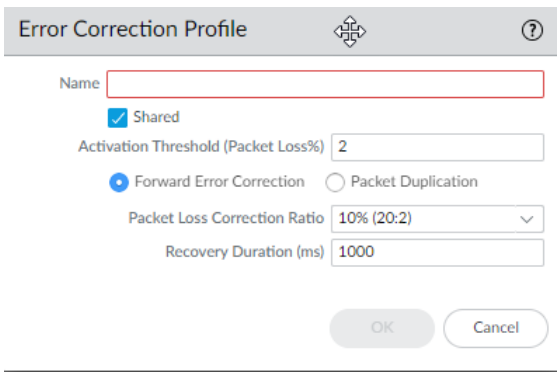
STEP 4 | Créez un profil de correction des erreurs pour le FEC ou la duplication de paquet.

1. Sélectionnez **Objects (Objets)** > **SD-WAN Link Management (Gestion des liaisons SD-WAN)** > **Error Correction Profile (Profil de correction des erreurs)**.
2. **Add (Ajoutez)** un profil de correction des erreurs et donnez un **Name (Nom)** descriptif d'un maximum de 31 caractères alphanumériques; par exemple, EC_VOIP.
3. Sélectionnez **Partagé** pour rendre le profil de correction d'erreur disponible pour tous les groupes d'appareils sur Panorama et pour le vsys par défaut sur un hub ou une branche vsys unique, ou pour vsys1 sur un hub ou une branche multi-vsys vers lequel vous poussez cette configuration.
4. Spécifiez le paramètre **Activate when packet loss exceeds (%) (Activer lorsque la perte de paquet dépasse [%]**—Lorsque la perte de paquet dépasse ce pourcentage, la méthode FEC ou de duplication de paquet est activée pour les applications configurées dans la

règle de politique SD-WAN où le profil de correction des erreurs s'applique. La plage est comprise entre 1 et 99 ; la valeur par défaut est 2.

5. Sélectionnez **Forward Error Correction (Transfert de la correction des erreurs)** ou **Packet Duplication (Duplication de paquet)** pour indiquer la méthode de correction des erreurs que le pare-feu utilise lorsqu'une règle de politique SD-WAN référence ce profil d'interface SD ; le transfert de la correction des erreurs est défini par défaut. Si vous sélectionnez la duplication de paquet, SD-WAN sélectionne une interface par laquelle envoyer les paquets reproduits. (SD-WAN sélectionne l'une des interfaces que vous avez configurées au moyen de l'option **Eligible for Error Correction Profile interface selection (Admissible à la sélection d'interface de profil de correction des erreurs)** à l'étape précédente.)
6. (Transfert de la correction des erreurs uniquement) Sélectionnez le **Packet Loss Correction Ratio (Ration de correction de la perte de paquet)** : **10% (20:2)**, **20% (20:4)**, **30% (20:6)**, **40% (20:8)** ou **50% (20:10)**—Ratio des bits de parité par rapport aux paquets de données ; la valeur par défaut est 10 % (20:2). Plus le ratio des bits de parité par rapport aux paquets de données que le pare-feu d'envoi (encodeur) envoie, plus la probabilité que le pare-feu de réception (décodeur) puisse réparer la perte de paquet est élevée. Cependant, un ratio plus élevé nécessite plus de redondance et par conséquent plus de ressources en bande passante, ce qui est un compromis permettant la correction des erreurs. Le ratio de parité s'applique à l'encodage du trafic sortant du pare-feu. Par exemple, si le ratio de parité du pare-feu de la plate-forme est de 50 % et que le ratio de parité du pare-feu de la branche est de 20 %, le pare-feu de la plate-forme recevra 20 % et le pare-feu de la branche recevra 50 %.
7. Spécifiez la **Recovery Duration (ms) (Durée de récupération [en ms])**—Nombre maximum de millisecondes que le pare-feu récepteur (décodeur) peut passer pour effectuer la récupération de paquets de données perdus en utilisant les paquets de parité qu'il a reçus ; plage de 1 à 5 000 ; valeur par défaut de 1 000. Le pare-feu envoie immédiatement les paquets de données qu'il reçoit vers la destination. Au cours de la durée de récupération, le décodeur procède à une récupération de paquets pour tous les paquets de données perdus. Lorsque la durée de récupération expire, tous les paquets de parité sont publiés. Vous configurez la durée de récupération dans le profil de correction des erreurs de l'encodeur, qui envoie la valeur de la durée de récupération au décodeur. Un paramètre de durée de récupération sur le décodeur n'a aucun impact.

   Commencez par utiliser le paramètre de durée de récupération par défaut et ajustez-le au besoin, selon les essais que vous menez avec des baisses de tension intermittentes et normales.



8. Cliquez sur **OK**.

STEP 5 | Configurer une Règle de politique SD-WAN, référencez le **Error Correction Profile (Profil de correction des erreurs)** que vous avez créé dans la règle, puis spécifiez les applications critiques auxquelles les règles s'appliquent.

Spécifiez une seule application dans la règle de politique SD-WAN lors de la configuration du FEC ou de la duplication de paquets. Vous ne devez pas combiner plusieurs applications dans une seule règle de politique pour la FEC ou la duplication de paquets.

STEP 6 | **Commit (Validez)** et **Commit and Push (Validez et appliquez)** vos modifications aux pare-feu encodeurs (branches et plateformes).

Configurer une Règle de politique SD-WAN

Une règle de politique SD-WAN spécifie les applications et/ou les services et un profil de distribution de trafic pour déterminer comment le pare-feu sélectionne le chemin préféré pour un paquet entrant qui n'appartient pas à une session existante et qui correspond à tous les autres critères comme les zones de source et destination, les adresses IP source et destination et l'utilisateur source. La règle de politique SD-WAN spécifie aussi un profil de qualité de chemin pour les seuils de latence, instabilité et perte de paquets. Lorsque l'un des seuils est dépassé, le pare-feu sélectionne un nouveau chemin pour les applications et/ou les services.

Lors du monitoring (surveillance) de votre trafic SD-WAN, le trafic en provenance d'une source derrière le périphérique du hub est évalué par rapport aux politiques SD-WAN appliquées au périphérique du hub et parce que la décision de sélection du chemin a déjà été prise, le périphérique de la banche évalue le trafic par rapport à des politiques SD-WAN lorsqu'il passe par le périphérique de la branche vers le périphérique cible final. Inversement, le trafic en provenance d'une source au-delà du périphérique de branche est évalué par rapport aux politiques SD-WAN appliquées au périphérique de la branche et non par périphérique du hub. Le serveur de gestion Panorama™ cumule les journaux de la plateforme et de la branche et, pour le même trafic, deux entrées de session s'affichent mais uniquement le périphérique SD-WAN qui a évalué le trafic à l'origine contient les informations SD-WAN.

Dans une règle de politique SD-WAN, vous pouvez mentionner un profil de correction d'erreur. Vous pourrez ainsi appliquer le transfert de correction des erreurs ou la duplication de paquet aux applications critiques spécifiées qui ont une faible tolérance aux paquets corrompus ou abandonnés.

Dans la règle de politique SD-WAN, vous spécifiez les périphériques auxquels vous souhaitez que Panorama applique la règle.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Sélectionnez **Policies** > **SD-WAN** (Politiques SD-WAN) puis sélectionnez le groupe de périphériques dans la liste déroulante **Device Group** (Groupe de périphériques).

STEP 3 | **Add** (Ajoutez) une règle de politique SD-WAN.

STEP 4 | Dans l'onglet **General (Général)**, donnez un **Name (Nom)** descriptif à la règle.

STEP 5 | Dans l'onglet **Source** (source), configurez les paramètres de la source de la règle de politique.

1. Ajoutez la **Source Zone** (Zone source) ou sélectionnez **Any** (n'importe quelle) zone source
2. **Add** (Ajoutez) une ou plusieurs adresses source, définissez une external dynamic list (liste dynamique externe - EDL), ou sélectionnez **Any** (n'importe quelle) adresse source.
3. **Add** (Ajoutez) un ou plusieurs utilisateurs source ou sélectionnez **any** (n'importe quel) Utilisateur source.

STEP 6 | Dans l'onglet **Destination**, configurez les paramètres de la destination de la règle de politique.

1. **Add** (Ajoutez) la **Destination Zone** (zone de destination) ou sélectionnez **Any** (n'importe quelle) zone de destination.
2. **Add** (Ajoutez une ou plusieurs adresses de destination, définissez une EDL, ou sélectionnez **Any** (n'importe quelle) adresse de destination.

STEP 7 | À l'onglet **Application/Service**, associez vos profils de gestion de liaisons SD-WAN et spécifiez vos applications et vos services.

PAN-OS 10.0.2 ne prend en charge l'association que d'un seul profil (profil de qualité SaaS ou profil de correction des erreurs), mais pas les deux. Si vous associez l'un de ces profils à une règle de politique SD-WAN, vous ne pouvez associer l'autre.

Par exemple, si vous associez un profil de qualité SaaS à une règle de politique SD-WAN, vous ne pouvez associer un profil de correction des erreurs à la même règle.

1. Sélectionnez la**Path Quality (Qualité du chemin)** ou Créer un Path Quality Profile (Profil de qualité du chemin d'accès).
2. Sélectionnez le **SaaS Quality Profile (Profil de qualité SaaS)** ou Création d'un profil de qualité SaaS si le pare-feu de la branche a une liaison Direct Internet Access (Accès Internet direct ; DIA) à une application SaaS. La valeur par défaut est **None (disabled) (Aucun - désactivé)**.
3. Sélectionnez le **Error Correction Profile (Profil de correction des erreurs)** ou Création d'un profil de correction des erreurspour appliquer le transfert de correction des erreurs (FEC) ou la duplication de paquet aux applications qui correspondent à la règle de politique SD-WAN. La valeur par défaut est **None (disabled) (Aucun - désactivé)**.
4. **Add Applications**(Ajoutez des applications) et sélectionnez une ou plusieurs applications dans la liste ou sélectionnez **Any** (n'importe quelles) applications. Toutes les applications que vous sélectionnez sont soumises à des seuils d'état dans le profil de Qualité du chemin que vous avez sélectionné. Si un paquet correspond à une de ces applications et que l'application dépasse un des seuils d'état dans le profil de Qualité du chemin (et

que le paquet correspond aux critères des règles restantes), le pare-feu sélectionne un nouveau chemin préféré.

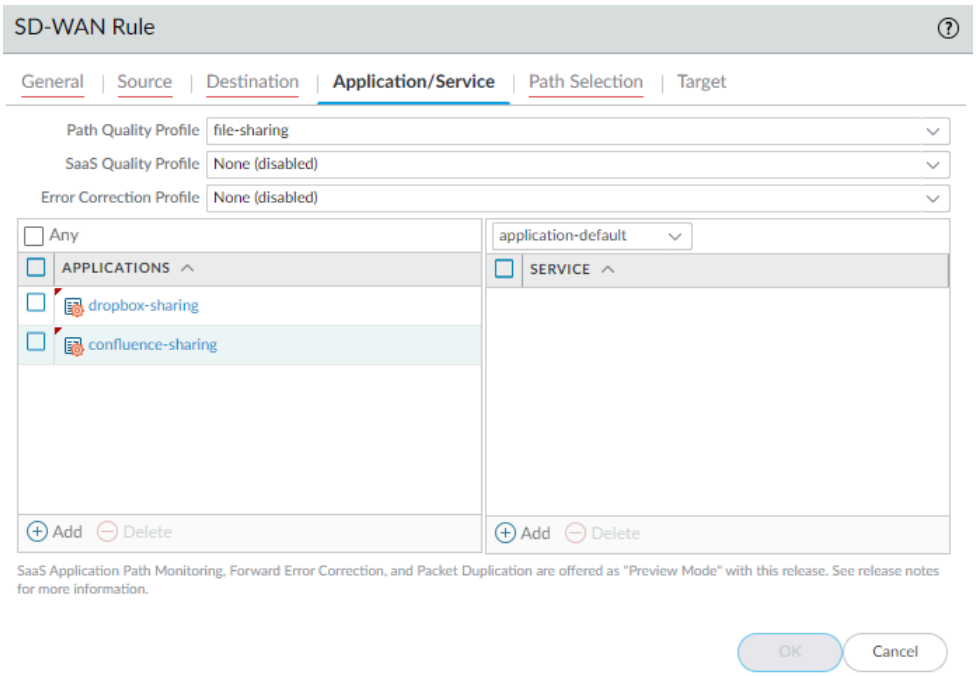
Ajoutez uniquement les applications critiques à l'entreprise et les applications qui sont sensibles aux conditions du chemin pour leur utilisation.

*Si vous associez un SaaS Quality profile (Profil de qualité SaaS) à la politique SD-WAN au mode **Adaptive (Adaptatif)**, ajoutez les applications SaaS spécifiques que vous souhaitez surveiller. L'utilisation de la surveillance adaptative pour toutes les applications qui correspondent à la règle de politique SD-WAN peut affecter la performance du pare-feu SD-WAN.*

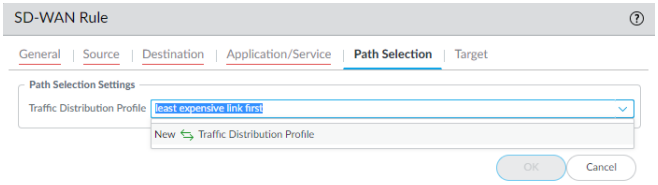
Si vous associez un SaaS Quality profile (Profil de qualité SaaS) à une application SaaS spécifiée, ajoutez l'application SaaS à la règle SD-WAN pour vous assurer que les paramètres de surveillance SaaS sont appliqués uniquement à l'application SaaS souhaitée.

5. **Add Services** (Ajoutez des services) et sélectionnez un ou plusieurs services dans la liste ou sélectionnez**Any** (n'importe quels) services. Tous les services que vous sélectionnez sont soumis à des seuils d'état indiqués dans le profil de Qualité du chemin que vous avez sélectionné. Si un paquet correspond à un de ces services et que le service dépasse un des seuils d'état dans le profil de Qualité du chemin (et que le paquet correspond aux critères des règles restantes), le pare-feu sélectionne un nouveau chemin préféré.

Ajoutez uniquement les services critiques à l'entreprise et les services qui sont sensibles aux conditions du chemin pour leur utilisation.

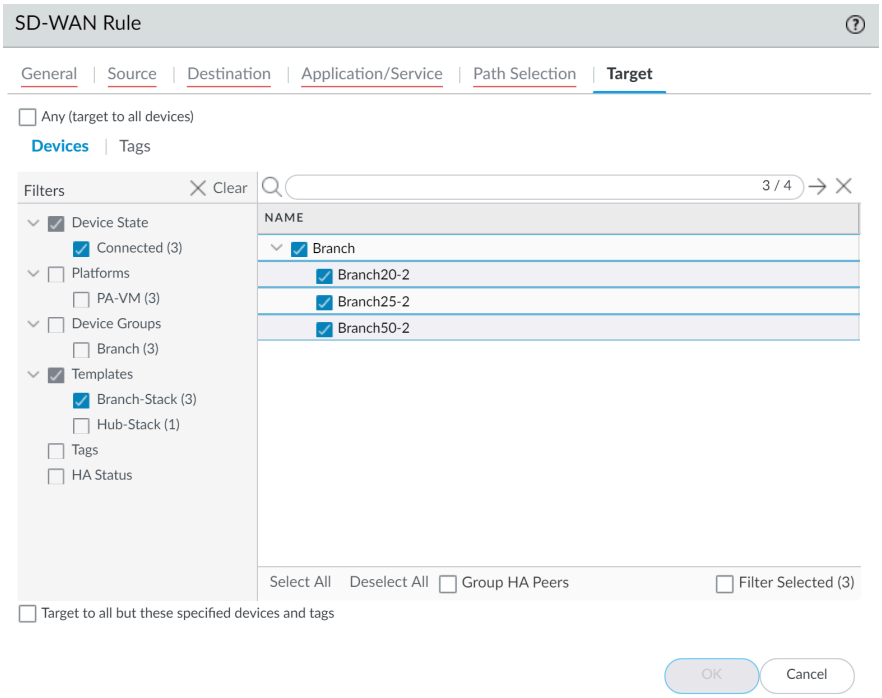


STEP 8 | Dans l'onglet **Path Selection** (sélection du chemin), sélectionnez le **Traffic Distribution Profile** (Profil de distribution du trafic) ou Créer un Traffic Distribution Profile (profil de distribution du trafic). Quand un paquet entrant (non associé avec une session) correspond à tous les critères de correspondance de la règle, le pare-feu utilise ce profil de Distribution de trafic pour sélectionner un nouveau chemin préféré.

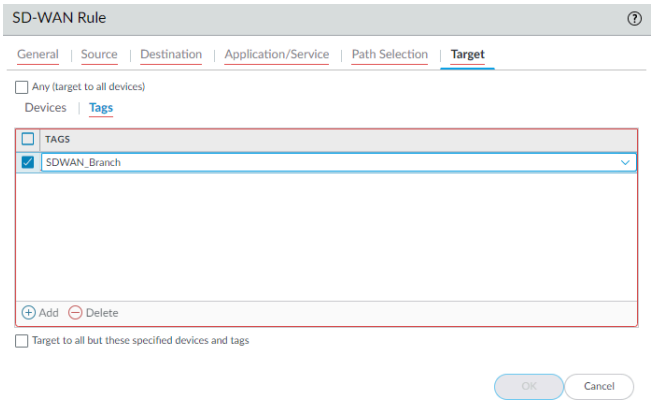


STEP 9 | Dans l'onglet **Target** (cible), utilisez une ou plusieurs des méthodes suivantes pour spécifier les pare-feux cibles dans le groupe de périphériques auxquels Panorama applique la règle de politique SD-WAN :

- Sélectionnez **Any (target to all devices)** (n'importe lequel (cible vers tous les périphériques)) (par défaut) pour appliquer la règle à tous les périphériques. Autrement, sélectionnez **Devices** (Périphériques) ou **Tags** (Étiquettes) pour spécifier les périphériques auxquels Panorama applique la règle de politique SD-WAN.
- Dans l'onglet **Devices** (Périphériques), sélectionnez un ou plusieurs filtres pour restreindre les sélections qui apparaissent dans le champ du Nom ; puis sélectionnez un ou plusieurs périphériques auxquels Panorama applique la règle, comme dans cet exemple :



- Dans l'onglet **Tags** (Étiquettes), **Add** (Ajoutez) une ou plusieurs **Tags** (Étiquettes) et sélectionnez les étiquettes pour spécifier que Panorama applique la règle aux périphériques qui sont étiquetés avec les étiquettes sélectionnées, comme dans cet exemple :



- Si vous avez spécifié des Périphériques ou des Étiquettes, vous pouvez sélectionner **Target to all but these specified devices and tags** (Cibler tous sauf les périphériques et étiquettes spécifiés) afin que Panorama applique la règle de politique SD-WAN à tous les périphériques sauf les périphériques spécifiés ou les périphériques étiquetés.

STEP 10 | Cliquez sur **OK**.

STEP 11 | **Commit** (Validez) et **Commit and Push** (Validez et appliquez) les modifications de votre configuration.

STEP 12 | (Bonne pratique) Créez une règle de politique SD-WAN de collecte de la totalité afin de Distribuer des sessions sans correspondance afin que vous puissiez contrôler quels liens des sessions sans correspondance utilisent et afficher les sessions sans correspondance dans des journaux et des rapports dans le plug-in the SD-WAN.

Si vous ne créez pas de règle de collecte de la totalité pour distribuer les sessions sans correspondance, le pare-feu les distribue à tour de rôle entre les liens disponibles parce qu'il n'y a pas de profil de distribution de trafic pour les sessions sans correspondance. La distribution à tour de rôle de sessions sans correspondance peut augmenter vos coûts de façon inattendue et avoir pour conséquence une perte de visibilité des applications.

STEP 13 | Après avoir configuré vos règles de politique SD-WAN , Create a Security Policy Rule (Créez une règle de politique de sécurité) pour autoriser le trafic (par exemple, **bgp** comme **Application**) depuis les branches vers internet, depuis les branches vers les hubs et depuis les hubs vers les branches.

STEP 14 | (Facultatif) Configure QoS (Configurer Qos) pour les applications critiques.

Si les applications SD-WAN nécessitent des capacités de bande passante garanties ou si vous ne voulez pas que d'autres applications prennent la bande passante d'applications critiques à l'entreprise, créez des règles QoS pour contrôler correctement la bande passante.

STEP 15 | Afin de configurer automatiquement un itinéraire BGP entre les membres du cluster VPN, dans le plug-in SD-WAN, Configure BGP Configurez l'itinéraire BGP entre les branches et les hubs selon un trafic d'acheminement dynamique qui sera soumis au basculement SD-WAN et au partage de la charge.

Autrement, si vous voulez configurer l'itinéraire BGP manuellement sur chaque pare-feu ou utiliser un modèle Panorama séparé pour configurer l'itinéraire BGP (pour plus de contrôle), laissez les informations BGP du plug-in vides. Au contraire, configurez l'itinéraire BGP.

STEP 16 | Configure NAT (Configurez NAT) pour les interfaces virtuelles SD-WAN destinées au public.

Autoriser le basculement du trafic de l'accès direct à internet vers un lien MPLS

Dans une branche SD-WAN, le pare-feu effectue un partage de tunnel afin que toute application qui a une adresse IP publique prenne l'interface d'accès direct à internet (DIA) vers internet, et les applications qui ont des adresses IP privées qui appartiennent au hub prennent l'interface VPN. Le pare-feu bascule automatiquement les applications DIA vers la connexion privée MPLS vers le hub si nécessaire afin que le trafic destiné à Internet prenne un chemin alternatif par le hub pour atteindre internet. Pour que cela fonctionne, vous devez faire ce qui suit :

STEP 1 | Créez un lien MPLS entre votre branche et votre hub. Lorsque vous create the SD-WAN Interface profile (créez le profil d'interface SD-WAN), le type de lien doit être **MPLS** pour le hub et pour la branche.

STEP 2 | Si vous souhaitez que le trafic privé passe par le tunnel VPN, activez **VPN Data Tunnel Support** (Assistance du tunnel de données VPN) dans le SD-WAN Interface profile (profil de l'interface SD-WAN). Si vous désactivez **VPN Data Tunnel Support** (Assistance du tunnel de données VPN), les données privées passeront en dehors du tunnel VPN.

STEP 3 | Configurer une Règle de politique SD-WAN pour des applications spécifiques, Créer un Path Quality Profile (Profil de qualité du chemin d'accès), et Créer un Traffic Distribution Profile (profil de distribution du trafic) qui spécifie la méthode de **Top Down Priority** (priorité descendante). Le profil de Distribution du trafic doit aussi spécifier un lien **MPLS** comme une des options de basculement (identifié par une étiquette). Vérifiez que les applications de la règle de politique SD-WAN référencent les bons profils de Qualité du chemin d'accès et de Distribution du trafic et que le profil de Distribution du trafic spécifie la Priorité descendante.

Une fois que l'Assistance du tunnel de données VPN est activée sur le hub et la branche et que le lien MPLS est opérationnel, le pare-feu utilise automatiquement la connexion MPLS pour basculer le trafic lorsque cela est nécessaire.

STEP 4 | Dans la configuration du hub, assurez vous que la plateforme ait un chemin vers internet et que l'itinéraire soit correctement configuré pour que le trafic du hub atteigne internet.

Le pare-feu utilise l'interface virtuelle DIA et l'interface virtuelle VPN afin de garantir que le trafic internet public reste séparé de votre trafic privé sur le même chemin ; c'est-à-dire que le trafic internet et le trafic privé ne passent pas par le même tunnel VPN. Une segmentation complète avec un zonage approprié est pleinement appliquée.

Configuration de DIA AnyPath

Lorsque vos liaisons Direct Internet Access (accès Internet direct ; DIA) d'un ISP subissent une panne ou une baisse de tension, vous avez besoin que ces liaisons basculent vers une autre liaison pour garantir la continuité des activités. Les liaisons DIA peuvent basculer vers une liaison MPLS, mais vous pourriez ne pas avoir de liaison MPLS. Les liaisons DIA doivent pouvoir basculer vers une autre liaison qui possède un chemin direct ou indirect (au moyen d'une plateforme ou d'une branche) vers Internet. Le trafic DIA peut prendre *n'importe quel chemin* disponible pour atteindre l'Internet, il ne se limite pas à DIA. DIA AnyPath prend en charge le basculement d'une liaison DIA vers un tunnel VPN privé menant à un pare-feu de la plateforme pour ensuite atteindre l'Internet. De plus, si vous disposez d'une topologie Full Mesh (branche à branche) sans plateforme, le trafic DIA peut basculer vers un pare-feu de la branche pour atteindre l'Internet.

DIA AnyPath nécessite PAN-OS 10.0.3 ou une version ultérieure de PAN-OS et la version compatible du plug-in SD-WAN, qui est indiquée dans le tableau SD-WAN de la section Plugins Panorama de la matrice de compatibilité.

Il y a plusieurs cas d'utilisation selon lesquels une liaison Internet pourrait basculer vers un tunnel VPN (DIA AnyPath) :

- Vous souhaitez abandonner une liaison MPLS dispendieuse pour adopter une ou plusieurs connexions Internet publiques, généralement auprès de divers fournisseurs.
- Vous avez plusieurs plateformes dans un cluster VPN pour permettre un basculement en cascade de la plateforme principale vers une succession de plateformes de secours.
- Dans un scénario de segmentation de tunnel, vous souhaitez qu'une seule application qui exige beaucoup de bande passante soit acheminée directement vers l'Internet via la liaison DIA de la branche au lieu de retourner à la plateforme du centre de données via le tunnel VPN, ce qui vous permet d'économiser sur les coûts liés à la bande passante WAN. Dans le cas d'une baisse de tension ou d'une panne de courant DIA, ce trafic d'application bascule vers la plateforme du centre de données pour atteindre l'Internet et, au besoin, il peut basculer vers une seconde plateforme pour atteindre l'Internet.
- Dans un scénario de segmentation de tunnel, au lieu de ramener le trafic au centre de données vous voulez que la majorité de votre trafic d'Internet sorte de la liaison DIA. Cependant, vous voulez que des applications spécifiques (qui peuvent devoir faire l'objet d'analyses supplémentaires ou d'une journalisation par un autre périphérique de sécurité) retournent au centre de données. Vous créez une règle de politique SD-WAN pour acheminer ces applications vers un chemin principal de la plateforme, plutôt que la liaison DIA normale, comme le détermine l'itinéraire par défaut dans la table d'itinéraires du pare-feu. En cas de baisse de tension ou de panne de courant, ces applications basculent pour prendre l'interface DIA de la branche.

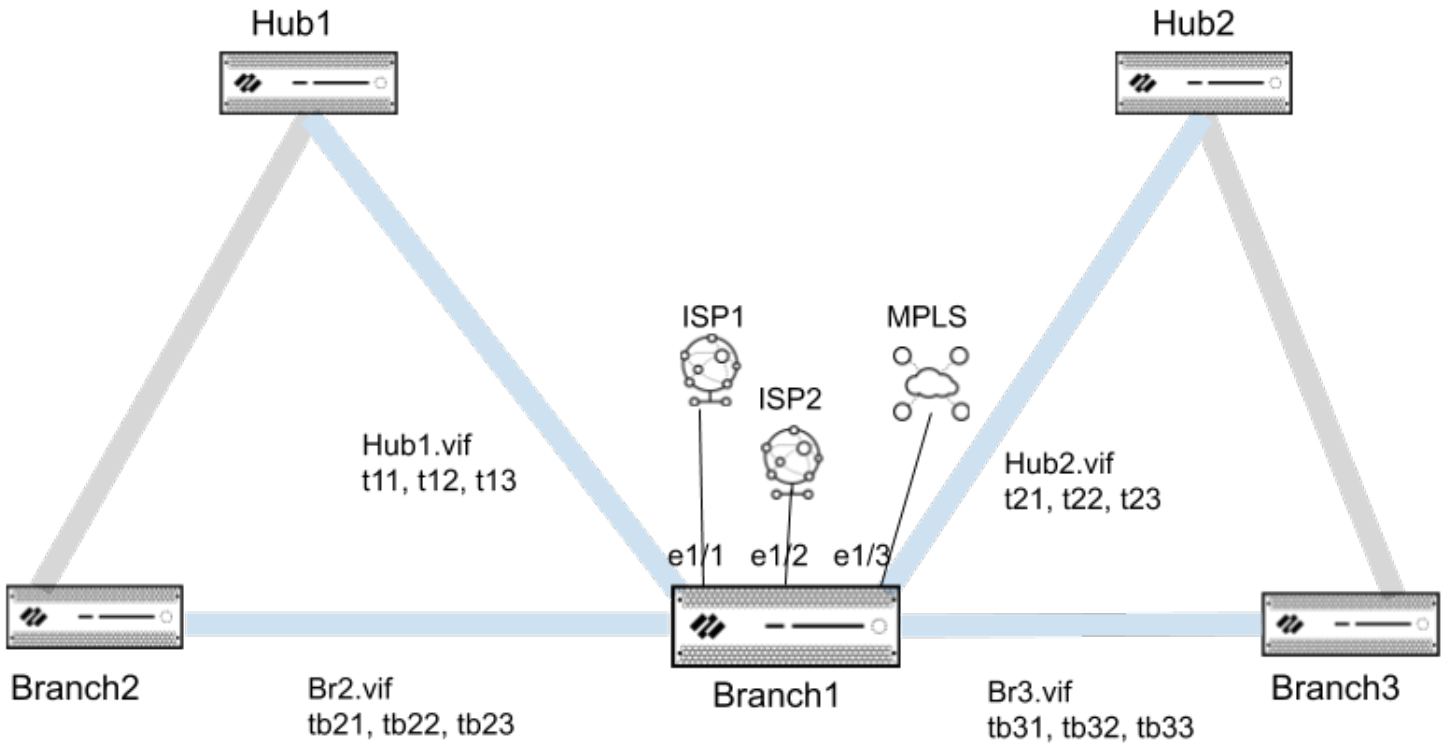
DIA AnyPath introduit le concept d'une *interface virtuelle principale*, qui peut comprendre des liaisons DIA et des *interfaces virtuelles de plateforme* et des *interfaces virtuelles de branche* imbriquées (tunnels VPN) qui comprennent chacune leurs propres liaisons. L'interface virtuelle principale peut comporter un maximum de neuf interfaces (Ethernet) DIA, interfaces virtuelles de plateforme et interfaces virtuelles de branche. Vous affectez une étiquette de liaisons à une plateforme lorsque vous ajoutez le périphérique de la plateforme à Panorama. Supposons que vous utilisiez le plugin SD-WAN, Auto VPN affecte cette étiquette de liaison à l'interface virtuelle

de la plateforme, ce qui vous permet de spécifier l'étiquette dans un profil de distribution de trafic afin de contrôler l'ordre de basculement des interfaces virtuelles.

Dans les commandes CLI, on fait référence à une interface virtuelle principale comme suit : DIA-VIF.

Une interface virtuelle principale peut posséder plusieurs membres d'interfaces qui appartiennent à différentes zones de sécurité. Toutefois, la meilleure pratique consiste à faire en place toutes les interfaces membres de l'interface virtuelle principale dans la même zone de sécurité. Une autre bonne pratique consiste à avoir au moins une interface membre dans l'interface virtuelle principale de type Ethernet, mode câble, ADSL, fibre, LTE ou WiFi.

L'exemple de topologie suivant montre Branche1 avec deux connexions ISP et une liaison MPLS. Branche1 possède également une interface virtuelle Plateforme1 avec trois tunnels VPN se connectant à la Plateforme1, et une interface virtuelle Plateforme2 de trois tunnels VPN se connectant à Plateforme2. Branche1 possède également une interface virtuelle branche2 avec trois tunnels VPN se connectant à la branche2, et une interface virtuelle branche3 de trois tunnels VPN se connectant à branche3. L'objectif de DIA AnyPath consiste à configurer l'ordre selon lequel DIA peut basculer vers des tunnels VPN pour atteindre l'Internet directement ou indirectement et, par conséquent, maintenir la continuité des activités.



Lorsque vous configurez une interface virtuelle principale, celle-ci devient automatiquement l'itinéraire par défaut pour que le trafic Internet soit acheminé comme il se soit vers l'un des

membres de l'interface virtuelle principale (liaisons DIA et tunnels VPN). La sélection des chemins se fonde sur les profils de qualité des chemins SD-WAN et sur les profils de distribution de trafic, que vous définiriez pour utiliser la méthode de distribution Priorité descendante pour contrôler l'ordre de basculement. Dans l'exemple de topologie, un profil de distribution du trafic peut indiquer l'étiquette de l'interface virtuelle principale en premier, puis l'étiquette de l'interface virtuelle Plateforme1, et ensuite l'étiquette de l'interface virtuelle Plateforme2.

Si l'on fait un gros plan sur un niveau plus approfondi de priorité de basculement, une interface virtuelle de la plateforme possède plusieurs membres-tunnels, vous avez donc besoin d'une façon de prioriser l'ordre de basculement des membres, par exemple, un tunnel VPN à large bande passante est utilisé avant un tunnel VPN LTE. Vous spécifiez la priorité au moyen de la **VPN Failover Metric (Mesure de basculement VPN)** indiquée dans le profil d'interface SD-WAN que vous appliquez à l'interface Ethernet. Plus la valeur est faible, plus la priorité du tunnel à sélectionner lors du basculement est élevée. Dans l'exemple de topologie, dans l'interface virtuelle Plateforme1, si t11 possède une mesure de basculement VPN plus faible que t12, le trafic Internet basculera donc vers t11 avant t12. Si plusieurs tunnels d'une interface virtuelle possèdent la même mesure, SD-WAN envoie le nouveau trafic de session aux tunnels au moyen de la permutation circulaire.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Spécifiez la priorité de basculement d'un tunnel VPN regroupé dans une interface virtuelle de la plateforme ou une interface virtuelle de la branche.

1. Sélectionnez ou Configurer un Profil d'interface SD-WAN.

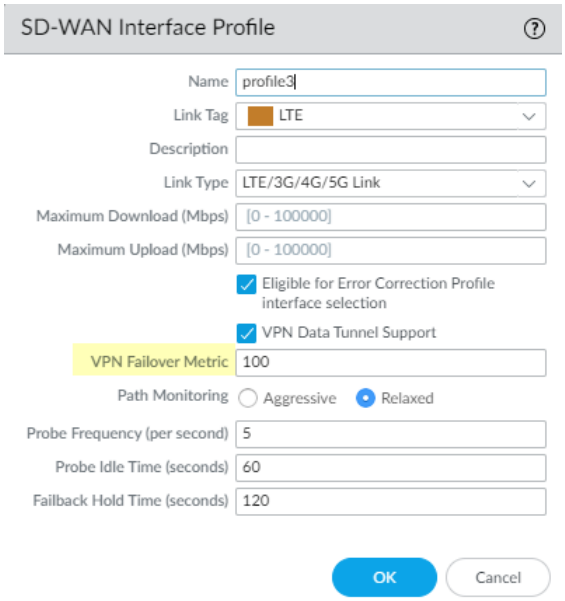
   La meilleure pratique consiste à configurer au moins une interface avec le type de liaison Ethernet, modem câble, ADSL, fibre, LTE ou WiFi.

2. Vous devez activer **VPN Data Tunnel Support (Assistance du tunnel de données VPN)**.
3. Indiquez la **VPN Failover Metric (Mesure de basculement VPN)** pour un tunnel VPN ; plage de 1 à 65 535 ; valeur par défaut 10. Plus la valeur de la mesure est faible, plus la priorité du tunnel VPN (liaison) auquel vous appliquez ce profil est élevée.

   Par exemple, réglez la mesure sur une valeur faible et appliquez le profil à une interface de bande passante ; ensuite créez un profil différent qui définit une mesure élevée à

appliquer à une interface LTE onéreuse afin de garantir qu'elle est utilisée uniquement après le basculement de bande passante.

*Si vous n'avez qu'un seul lien sur le hub, ce lien prend en charge toutes les interfaces virtuelles et le trafic DIA. Si vous souhaitez utiliser les types de liens dans un ordre spécifique, vous devez appliquer un profil de distribution du trafic au hub qui spécifie la **Top Down Priority (priorité descendante)** puis ordonner aux balises de lien de spécifier l'ordre préféré. Si vous appliquez un profil de distribution du trafic qui spécifie à la place **Best Available Path (meilleur chemin disponible)**, le pare-feu utilisera le lien, quel qu'en soit le coût, pour choisir le chemin d'accès le plus performant à la branche. En résumé, Lier des balises dans un profil de distribution du trafic. la balise link appliquée à une interface virtuelle hub (étape 6 de cette tâche) et une **VPN Failover Metric (métrique de basculement VPN)** fonctionnent uniquement lorsque le profil de distribution du trafic spécifie la**Top Down Priority (priorité descendante)**.*



4. Cliquez sur **OK**.

STEP 3 | Configurer une interface Ethernet physique pour SD-WANprofil et à l'onglet SD-WAN, appliquez le profil d'interface SD-WAN que vous avez créé à l'étape précédente.

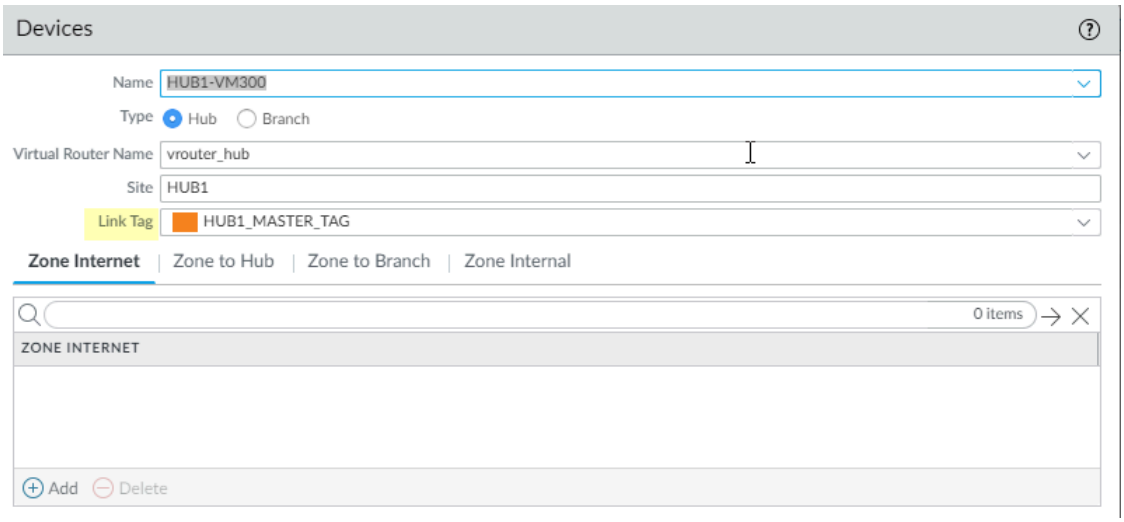
La meilleure pratique consiste à faire en place toutes les interfaces de l'interface virtuelle principale dans la même zone de sécurité.

STEP 4 | Répétez les étapes 2 et 3 pour configurer les profils d'interface SD-WAN supplémentaires possédant une mesure de basculement VPN différente et appliquer les profils à des interfaces Ethernet différentes pour déterminer l'ordre de basculement des liaisons.

STEP 5 | Créer une Link Tag (Étiquette de liens) pour une interface virtuelle de la plateforme.

STEP 6 | Ajoutez l'étiquette de liaison à une plateforme que vous souhaitez ajouter à DIA AnyPath.

1. Sous **Panorama** > **SD-WAN** > **Devices (Périphériques)**, Ajouter un Périphérique SD-WAN pour ajouter une plateforme à gérer par Panorama.
2. Sélectionnez la plateforme.
3. Sélectionnez la **Link Tag (Étiquette de liaison)** que vous avez créée à l'étape précédente, qu'Auto VPN applique à toute l'interface virtuelle de la plateforme, et non pas à une liaison individuelle. Vous pouvez donc référencer cette étiquette de liaison dans le Profil de distribution de trafic pour indiquer l'interface virtuelle de la plateforme pour l'ordre de basculement de DIA AnyPath. Sur le périphérique de branche, Auto VPN utilise cette étiquette pour remplir le champ de l'étiquette de lien dans l'interface virtuelle SD-WAN qui se termine sur le périphérique de la plateforme.



4. Cliquez sur **OK**.

STEP 7 | Répétez les étapes 5 et 6 pour créer une étiquette de liaison pour chaque interface virtuelle de la plateforme et ajouter l'étiquette à chaque plateforme qui participera à DIA AnyPath. Répétez pour chaque interface virtuelle de la branche.

STEP 8 | Créez un profil de distribution de trafic pour la mise en œuvre de DIA AnyPath.

1. Créer un Traffic Distribution Profile (profil de distribution du trafic).
2. Sélectionnez **Top Down Priority (Priorité descendante)**.
3. Ajoutez les étiquettes de liaison pour qu'elles apparaissent dans l'ordre que vous souhaitez que leurs liaisons connexes soient utilisées aux fins de basculement.

   Par exemple, si selon votre cas d'utilisation certaines applications doivent utiliser DIA en premier, indiquez l'étiquette DIA en premier, puis l'étiquette d'interface, puis une deuxième étiquette d'une interface virtuelle de la plateforme. Si, selon votre cas d'utilisation, certaines applications doivent d'abord passer par la plateforme avant d'être acheminées vers l'Internet, indiquez une interface virtuelle de la plateforme en premier, puis, éventuellement, une deuxième interface de la plateforme, et enfin une étiquette DIA. Si vous disposez d'un maillage complet sans plateforme, utilisez l'étiquette DIA et les étiquettes des interfaces virtuelles de la branche dans l'ordre de votre choix.

STEP 9 | Créez des profils de qualité SaaS pour des noms identiques pour les pare-feu de la plateforme et de la branche.

Deux profils de qualité SaaS portant le même nom doivent être configurés sur les pare-feu de la plateforme et de la branche pour exploiter avec succès le pare-feu de la plateforme comme solution de basculement de rechange.

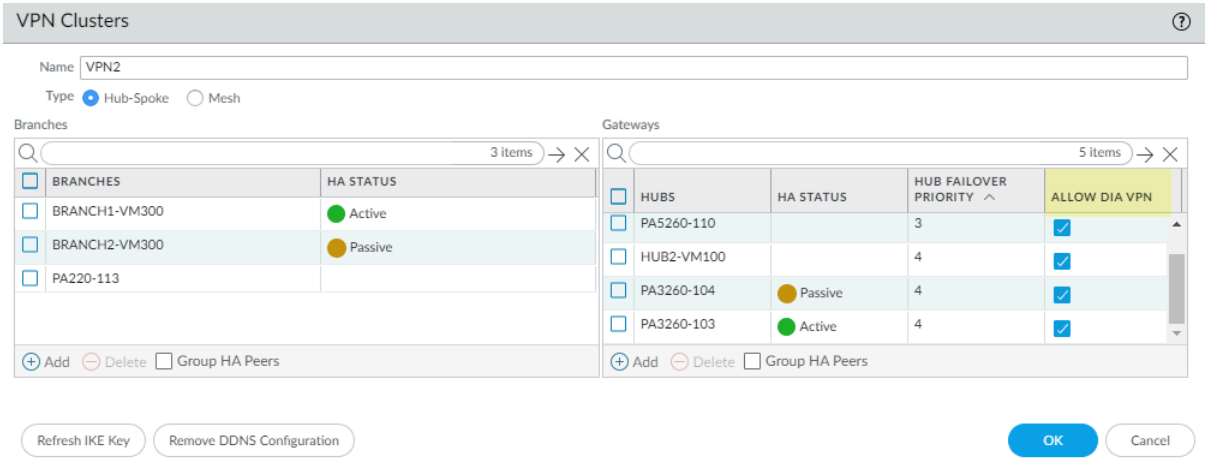
Pour configurer le basculement vers un pare-feu de la plateforme avec la même destination pour les applications SaaS, le plus simple consiste à créer un profil de qualité SaaS unique dans le groupe de périphériques partagés. Vous pouvez également créer deux profils de qualité SaaS ayant des noms identiques dans des groupes de périphériques différents et les appliquez à vos pare-feu de la plate-orme et de la branche.

Pour le basculement vers un pare-feu de la plateforme avec la même destination pour les applications SaaS, créez deux profils de qualité SaaS ayant des noms identiques, chacun pointant vers une destination pour les applications SaaS différente dans des groupes de périphériques différents et appliquez-les à vos pare-feu de la plateforme et de la branche.

Vous devez également créer une règle de politique SD-WAN référence ce profil de qualité SaaS pour permettre à la plateforme de publier des statistiques sur la qualité des liaisons du profil de qualité SaaS à la branche. Ce faisant, vous disposerez d'une surveillance SaaS de bout en bout jusqu'à la plateforme. Sans cette règle de politique SD-WAN, vous ne disposeriez que des mesures des liaisons de la branche à la plateforme, mais pas de la plateforme à l'application SaaS.

STEP 10 | Permettez aux plateformes de participer à DIA AnyPath.

1. Créer un cluster VPN et sélectionnez un hub.
2. Sélectionnez **Allow DIA VPN (Autoriser DIA VPN)** pour la plateforme. Un maximum de quatre hubs (toute combinaison de hubs PAN-OS participant aux hubs DIA AnyPath et Prisma Access) sont pris en charge. S'il y a des plateformes HA, huit plateformes sont prises en charge. Si vous **Allow DIA VPN (Autoriser DIA VPN)** pour un homologue HA d'une paire, vous devez également l'activer pour l'autre homologue HA.



STEP 11 | Créez une règle de politique SD-WAN pour que des applications spécifiques utilisent DIA AnyPath.

1. Configurer une Règle de politique SD-WAN.
2. À l'onglet **Application/Service**, spécifiez les applications et les services pour lesquels vous souhaitez mettre en œuvre DIA AnyPath.
3. Associez le **SaaS Quality Profile (Profil de qualité SaaS)**que vous avez créé à l'étape précédente.

   Si vous configurez un profil de qualité SaaS avec différentes destinations pour les applications SaaS, vous devez associer le profil de qualité SaaS avec la règle de politique SD-WAN dans chaque groupe de périphériques de la branche et de la plateforme.
4. Dans l'onglet **Path Selection** (sélection du chemin), sélectionnez le **Traffic Distribution Profile** (Profil de distribution du trafic) que vous avez créé pour les applications.

STEP 12 | Acheminez les nouvelles sessions qui ne correspondent pas à une règle de politique SD-WAN et aux sessions SD-WAN qui surviennent lors d'un changement de configuration du pare-feu ou de Panorama.

1. Créez un profil de qualité du chemin d'accès et un profil de distribution du trafic appropriés pour gérer de telles sessions.
2. Configurer une Règle de politique SD-WAN qui est une règle de récupération de la totalité pour ces sessions.
3. Placez la règle en dernier dans la liste.

STEP 13 | **Commit (validez)** et **Push to Devices (Appliquez aux périphériques)**.

STEP 14 | Créez une règle de politique de sécurité pour autoriser le trafic DIA vers les **zones de destination** nommées `zone-internet` et `zone-to-hub`, puis spécifiez le sujet **Applications** dans la règle. Validez, puis transmettez aux branches.

STEP 15 | Utilisez les commandes CLI suivantes pour surveiller l'information DIA :

1. **`afficher la connexion sdwan <dia-vif-name>`**
2. **`show sdwan path-monitor stats dia-vif all`**
3. **`show sdwan path-monitor dia-anypath`**
4. **`show sdwan path-monitor dia-anypath packet-buffer all`**
5. **`show sdwan path-monitor stats conn-idx <IDX>`**

Distribuer des sessions sans correspondance

Le pare-feu essaye de faire correspondre les sessions qui arrivent sur une interface virtuelle SD-WAN avec une règle de politique SD-WAN ; le pare-feu examine les règles de politique SD-WAN dans l'ordre descendant exactement comme pour les règles de politique de sécurité.

- Si une règle de politique SD-WAN correspond, le pare-feu exécute la surveillance des chemins et la distribution du trafic pour cette règle de politique SD-WAN.
- S'il n'y a pas de correspondance avec une règle de politique SD-WAN de la liste, la session correspond à une règle de politique SD-WAN implicite en fin de liste qui utilise la méthode à tour de rôle pour distribuer les sessions sans correspondance entre tous les liens d'une interface SD-WAN qui est basée sur la recherche d'itinéraire.

De plus, s'il n'y a aucune règle de politique SD-WAN pour une application spécifique, le pare-feu ne surveille pas la performance de cette application dans les outils de visibilité spécifiques à SD-WAN comme les journaux et les rapports du plug-in SD-WAN.

Pour illustrer la règle de politique implicite :

- Supposez que le pare-feu à trois règles de politique SD-WAN une règle spécifie cinq applications vocales, une règle spécifie six applications de vidéoconférence et une règle spécifie dix applications SaaS.
- Une session, par exemple, une session d'application vidéo, arrive au pare-feu et ne correspond pas à une des règles de politique SD-WAN. Comme la session ne correspondait à aucune règle, le pare-feu n'a pas de profil de qualité de chemin ni de profil de distribution de trafic à appliquer à la session.
- Par conséquent, le pare-feu fait correspondre l'application vidéo à la règle implicite et distribue chaque session vidéo entre toutes les étiquettes de lien SD-WAN disponibles et leurs liens associés sur le pare-feu qui peuvent être deux liens haut débit, un lien MPLS et un lien LTE. La session 1 va vers un membre de l'interface haut débit, la session 2 va vers une autre membre de l'interface haut débit, la session 3 va vers MPLS, la session 4 va vers LTE, la session 5 va au premier membre de l'interface haut débit, la session 6 va au deuxième membre de l'interface haut débit et la distribution à tour de rôle continue.

Mais peut-être que vous ne voulez pas que vos sessions sans correspondance aient recours à une correspondance avec une règle SD-WAN implicite parce que vous n'avez aucun contrôle sur la distribution de cette session. Dans ce cas, nous vous conseillons de créer une règle de politique SD-WAN de récupération de la totalité et de la placez en dernier dans la liste des règles de politique SD-WAN. Une règle de politique SD-WAN de récupération de la vous permet de:

- Contrôler quels liens les sessions sans correspondance utilisent.
- Afficher toutes les applications sur le pare-feu (y compris les sessions d'application sans correspondance) dans les journaux et les rapports du plug-in SD-WAN.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Créer un Path Quality Profile (Profil de qualité du chemin d'accès) qui définit des seuils de latence, gigue et perte de paquets très élevés qui ne seront jamais dépassés. Par exemple, latence de 2 000 ms, gigue de 1 000 ms et perte de paquets de 99 %.

STEP 3 | Créer un Traffic Distribution Profile (profil de distribution du trafic) qui spécifie les étiquettes de liens SD-WAN que vous voulez utiliser dans l'ordre dans lequel vous souhaitez que les liens associés avec ces étiquettes de liens soient utilisés par les sessions sans correspondance.

> *Si vous ne voulez pas du tout que les applications sans correspondance utilisent un chemin spécifique (interface physique), omettez l'étiquette qui inclut ce lien de la liste des étiquettes de liens du profil de distribution du trafic. Par exemple, si vous ne voulez pas qu'une application sans correspondance, comme la diffusion d'un film, utilise un lien LTE onéreux, omettez l'étiquette du lien pour le lien LTE dans la liste des étiquettes de liens du profil de distribution du trafic.*

STEP 4 | **Add** (ajoutez) une SD-WAN policy rule (règle de politique SD-WAN) de récupération de la totalité et dans l'onglet **Application/Service**, spécifiez le **Path Quality Profile** (Profil de qualité de chemin) que vous avez créé.

STEP 5 | Sélectionnez **Any** (n'importe lequel) pour **Applications** et **Service**.

STEP 6 | Dans l'onglet **Path Selection** (sélection du chemin), sélectionnez le **Traffic Distribution Profile** (Profil de distribution du trafic) que vous avez créé.

STEP 7 | **Move** (déplacez) la règle vers le bas jusqu'à la dernière position dans la liste des règles de politique SD-WAN.

STEP 8 | **Commit** (Validez) et **Commit and Push** (Validez et appliquez) les modifications de votre configuration.

STEP 9 | **Commit (Validez)** vos modifications.

Ajouter des Périphériques SD-WAN à Panorama

Ajoutez un seul pare-feu SD-WAN de hub ou de branche ou utilisez un fichier CSV pour importer en masse plusieurs pare-feu SD-WAN de hub et de branche avec clef pré-partagée ou type d'authentification de certificat.

- Configurer l'authentification basée sur le certificat pour les périphériques SD-WAN
- Ajouter un Périphérique SD-WAN
- Importer en masse plusieurs Périphériques SD-WAN
- Intégrer le pare-feu PAN-OS à Prisma Access

Configurer l'authentification basée sur le certificat pour les périphériques SD-WAN

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS • SD-WAN	❑ SD-WAN plugin license

Vous pouvez authentifier un périphérique SD-WAN à l'aide de l'un des deux types d'authentification suivants :

- Clef pré-partagée (type d'authentification par défaut)
- Certificat (plug-in SD-WAN 3.2.0 et versions ultérieures)

Lorsque vous créez un nouveau cluster SD-WAN ou actualisez la clef avec une version du plug-in SD-WAN antérieure à 3.2.0, le plug-in SD-WAN génère automatiquement la clef pré-partagée. En plus du type d'authentification par clef pré-partagée, nous proposons une authentification basée sur le certificat avec le plug-in SD-WAN 3.2.0 et les versions ultérieures pour les pare-feu nouvelle génération afin de répondre à vos besoins en matière de sécurité. Augmentez votre niveau de sécurité avec une authentification et une validation renforcées pour tous les sites SD-WAN avec une authentification basée sur le certificat.

Nous prenons en charge l'authentification basée sur le certificat sur tous les périphériques logiciels et matériels exécutant des moteurs de routage existants ou avancés prenant en charge SD-WAN.

Suivez les étapes mentionnées dans les Considérations de mise à niveau et de rétrogradation avant de mettre à niveau ou de rétrograder votre plug-in SD-WAN actuel.

Utilisez le flux de travail suivant pour configurer l'authentification basée sur le certificat pour votre périphérique SD-WAN :

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Générez un certificat pour les périphériques SD-WAN sur Panorama.

1. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)**.
2. Créez un certificat CA racine auto-signé ou importez un certificat de votre CA d'entreprise. En fonction de la CA racine, générez un certificat de périphérique pour un périphérique SD-WAN. Nous ne prenons pas en charge les certificats générés par SCEP.

   Le certificat généré doit être unique pour chaque périphérique SD-WAN. Autrement dit, vous ne pouvez pas générer un certificat et le partager entre plusieurs périphériques SD-WAN.

   Gardez les points suivants à l'esprit lors de la génération des certificats de pare-feu de branche et de hub utilisés pour l'authentification du tunnel SD-WAN :

   - Deux périphériques hub différents peuvent utiliser le même certificat hub.
   - Deux périphériques de branche différents peuvent utiliser les certificats de même branche si les conditions suivantes sont remplies :
     - Les périphériques de branche ne font pas partie du même cluster VPN.
     - Il n'existe pas de périphérique hub commun entre les clusters VPN dont ces périphériques de succursale feraient partie.
   - (Déploiements HA uniquement) Deux périphériques de branche différents peuvent également avoir les mêmes certificats de branche s'ils sont configurés en tant que membres HA.
   - Si le périphérique hub est commun entre les clusters VPN, les certificats des périphériques de branche faisant partie de ces clusters VPN doivent avoir des certificats uniques avec tous les attributs ayant des valeurs uniques. Si vous ne garantissez pas le caractère unique du certificat et ses valeurs, la validation échouera sur le périphérique hub (la validation n'échouera pas sur Panorama).

   Veillez également à ce que les certificats feuilles (certificats de pare-feu de branche et de hub) utilisés pour l'authentification du tunnel SD-WAN soient générés de manière à répondre aux critères suivants :

   - *L'utilisation de la clef doit être associée à des signatures numériques.*
   - *Tous les certificats doivent être signés par la même CA racine.*
   - *Le certificat de périphérique doit être directement signé par la CA racine.*
   - *Le certificat doit être au format PKCS12*

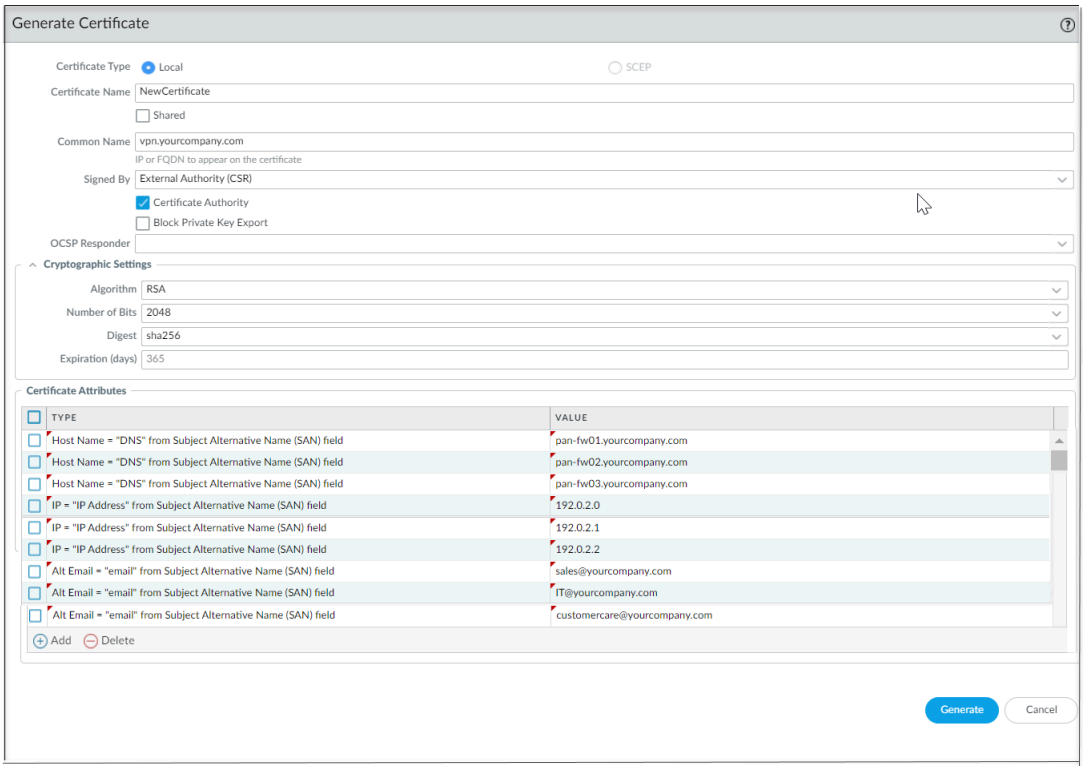
   Les attributs du certificat sont utilisés pour déterminer l'ID local et l'ID homologue des passerelles IKE. Par conséquent, les certificats feuilles, c'est-à-dire les certificats de pare-feu de branche et de hub utilisés pour l'authentification du tunnel SD-WAN doivent être générés avec les trois attributs de certificat suivants et chaque attribut de certificat doit

être attribué avec trois valeurs d'attribut uniques. Autrement, une erreur de validation sera générée.

- FQDN (**Host Name (Nom d'hôte)**)
- IP address (Adresse IP) (**IP**)
- FQDN de l'utilisateur (**Alt Email (Autre adresse e-mail)**)

*Il est obligatoire d'avoir des attributs de certificat **Host Name (Nom d'hôte)**, **IP**et **Alt Email (Autre adresse e-mail)** uniques entre tous les certificats. Autrement dit, aucun des certificats ne doit avoir ces valeurs d'attribut en commun.*

Dans l'exemple ci-dessous, NewCertificate est généré avec un total de neuf attributs de certificat obligatoires. L'attribut de certificat **Host Name (Nom d'hôte)** est configuré avec trois valeurs d'attribut uniques : pan-fw01.yourcompany.com, pan-fw02.yourcompany.com et pan-fw03.yourcompany.com. L'attribut du certificat **IP** est configuré avec trois valeurs d'attribut uniques : 192.0.2.0, 192.0.2.1 et 192.0.2.2 L'attribut de certificat **Alt Email (Autre adresse e-mail)** est configuré avec trois valeurs d'attribut uniques : sales@yourcompany.com, IT@yourcompany.com et customercare@yourcompany.com.



STEP 3 | (Facultatif) Configurez un profil de certificat qui inclut la CA racine et la CA intermédiaire pour la communication sécurisée avec le serveur.

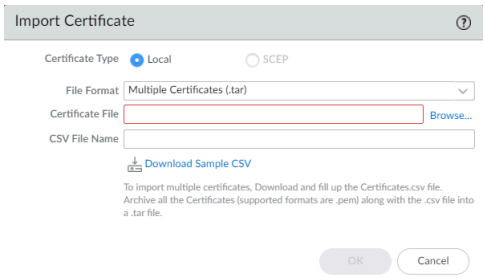
1. Sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificats)**.
2. Configurez un profil de certificat.

   Si vous configurez un CA intermédiaire dans le cadre du profil de certificat, vous devez également inclure la CA racine.

   Ce profil de certificat définit la manière dont les hubs SD-WAN et les branches s'authentifient mutuellement.

STEP 4 | Importez les certificats CA pour valider l'identité des périphériques SD-WAN.

1. **Panorama** > **Gestion des certificats** > **Certificats**
2. Importez le certificat CA et la paire de clefs sur Panorama pour chaque périphérique SD-WAN dans un cluster ou importez plusieurs certificats à l'aide de **Multiple Certificates (.tar) (Certificats multiples (.tar))**. Utilisez le fichier CSV pour importer en masse les certificats dans le serveur de gestion Panorama. Le fichier CSV vous permet d'importer plusieurs certificats à la fois, plutôt que de les ajouter un à un manuellement.



3. **Commit (Validez)** vos modifications. Il est important de valider après l'importation des certificats pour que les certificats importés soient disponibles pour une configuration ultérieure.

STEP 5 | Configurez un type d'authentification basé sur le certificat lors de l'ajout d'un hub SD-WAN ou d'un pare-feu de branche à gérer par le serveur de gestion Panorama. Lors de l'ajout de vos périphériques, vous spécifiez de quel type de périphérique il s'agit (branche ou hub), un type d'authentification pour le périphérique, et vous donnez à chaque périphérique son nom de site pour une identification facile.

1. Sélectionnez **Panorama** > **SD-WAN** > **Devices (Périphériques)** pour ajouter un périphérique SD-WAN (pare-feu de hub ou de branche SD-WAN) à gérer par le serveur de gestion Panorama.
2. Sélectionnez l'onglet **VPN Tunnel (Tunnel VPN)** et configurez le type **authentication (authentification)**. Pour l'authentification basée sur le certificat, sélectionnez **Certificate (Certificat)** et configurez les champs liés au certificat. Il est obligatoire de sélectionner un type d'authentification lors de l'ajout d'un périphérique SD-WAN.

STEP 6 | Configurez l'authentification basée sur le certificat lors de l'intégration des pare-feu PAN-OS à Prisma Access.

1. Sélectionnez **Panorama** > **SD-WAN** > **Devices (Périphériques)** pour sélectionner le pare-feu de branche SD-WAN à connecter au hub Prisma Access et configurez la connexion.
2. Sélectionnez **Prisma Access Onboarding (Intégration de Prisma Access)** et **Add (Ajouter)** un nœud de calcul à une **Region (Région)**. Dans le **VPN Tunnel (Tunnel VPN)**, il est obligatoire de sélectionner le type d'authentification pour authentifier le CN (hub Prisma Access). Pour l'authentification basée sur le certificat, sélectionnez **Certificate (Certificat)** comme le type **Authentication (Authentification)** et configurez les champs liés au certificat. Il est obligatoire de sélectionner un type d'authentification lors de l'intégration des pare-feu PAN-OS à Prisma Access.

   Assurez-vous de sélectionner le même type d'authentification pour tous les périphériques de succursale branche et le hub Prisma Access ajouté. Un échec de validation se produit sur Panorama si vous essayez d'utiliser différents types d'authentification pour la branche et le hub Prisma.

STEP 7 | Configurez l'authentification basée sur le certificat lors de la création d'un cluster VPN.

1. Sélectionnez **Panorama** > **SD-WAN** > **VPN Clusters (Clusters VPN)**.
2. Sélectionnez le **Type** de cluster VPN.
3. Sélectionnez le **Authentication Type (Type d'authentification)** comme **Certificate (Certificat)**. Il est obligatoire de spécifier le type d'authentification pour ajouter un périphérique dans un cluster VPN. Un cluster VPN doit avoir le même type d'authentification sélectionné pour tous ses périphériques. Vous ne pouvez pas modifier le type d'authentification d'un périphérique SD-WAN qui a déjà été ajouté à un cluster VPN. Si vous souhaitez le modifier, supprimez le cluster VPN et ses périphériques SD-WAN et reconfigurez-le avec le type d'authentification de votre choix. Par défaut, nous prenons en charge le type d'authentification par clef pré-partagée pour les périphériques d'un cluster VPN (si vous n'avez pas sélectionné le type de certificat manuellement).

STEP 8 | **Commit (validez)** vos modifications de configuration.

STEP 9 | Sélectionnez **Push to Devices** (Appliquer aux périphériques) pour appliquer vos modifications de configuration aux pare-feu que vous gérez.

Ajouter un Périphérique SD-WAN

Ajouter un pare-feu SD-WAN de hub ou de branche qui sera géré par le serveur de gestion Panorama™. Lorsque vous ajoutez vos périphériques, vous spécifiez de quel type de périphérique il s'agit (branche ou hub) et vous donnez à chaque périphérique son nom de site pour une identification facile. Avant d'ajouter vos périphériques, planifiez votre configuration SD-WAN pour vous assurer de disposer de toutes les adresses IP nécessaires et de comprendre la topologie SD-WAN. Cela aide à réduire les erreurs de configuration.

Si vous souhaitez qu'une HA active/passive fonctionne sur deux pare-feu de branche ou deux pare-feu de hub, n'ajoutez pas ces pare-feu en tant que périphériques SD-WAN lors de cette étape. Vous devez les ajouter séparément en tant qu'homologues HA lorsque vous Configurer les Périphérique HA pour SD-WAN.

Si vous utilisez un itinéraire BGP, vous devez ajouter une règle de politique de sécurité pour permettre à BGP d'aller de la zone interne à la zone du hub et de la zone du hub vers la zone interne. Si vous voulez utiliser des numéros de système autonome 4-bytes (ASN), vous devez tout d'abord activer les ASN 4-bytes pour le routeur virtuel.

Lorsque vous affichez des périphériques SD-WAN, si aucune donnée n'est présente ou si l'écran indique que SD-WAN n'est pas défini, vérifiez dans la matrice de compatibilité que la version Panorama que vous utilisez prend en charge la version du plug-in SD-WAN que vous essayez d'utiliser.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Sélectionnez **Panorama** > **SD-WAN** > **Devices (Périphériques)** et **Add (Ajouter)** un nouveau pare-feu SD-WAN.

STEP 3 | Sélectionnez le **Name** (Nom) du pare-feu géré pour l'ajouter en tant que Périphérique SD-WAN. Vous devez add your SD-WAN firewalls as managed devices (ajouter les pare-feux SD-WAN en tant que périphériques gérés) avant de les ajouter en tant que périphériques SD-WAN.

STEP 4 | Sélectionnez le **Type (Type)** de périphérique SD-WAN.

- **Hub** (Plateforme) — Un pare-feu centralisé déployé dans un bureau ou un emplacement principal auquel tous les périphériques de la branche se connectent à l'aide d'une connexion VPN. Le trafic entre les branches passe à travers le hub avant de continuer vers la branche cible et connecte les branches aux ressources centralisées à l'emplacement du hub. Le périphérique de hub traite le trafic, applique les règles de politique et gère les inversions de liens au bureau ou emplacement principal.
- **Branch** (Branche) — Un pare-feu déployé à l'emplacement physique de la branche qui connecte le hub à l'aide de la connexion VPN et qui offre une sécurité au niveau de la branche. Le périphérique de plateforme traite le trafic, applique les règles de politique et gère les inversions de liens à l'emplacement de la branche.

STEP 5 | (Facultatif) (PAN-OS 11.1.3 et versions ultérieures, et plug-in SD-WAN 3.2.1 et versions ultérieures) Configurez des routeurs virtuels multiples sur le hub SD-WAN.

Sélectionnez **Enable Multi-VR Support (Activer la prise en charge multi-VR)** pour configurer des routeurs virtuels multiples sur le hub SD-WAN.

Nous avons introduit la prise en charge des routeurs virtuels multiples sur le hub SD-WAN, ce qui vous permet d'avoir des adresses de sous-réseau IP qui se chevauchent sur les périphériques de branche qui se connectent au même hub SD-WAN. Lorsque vous sélectionnez le **Type** de SD-WAN comme hub, vous pourrez configurer des routeurs virtuels multiples en sélectionnant l'option **Enable Multi-VR Support (Activer la prise en charge multi-VR)**.

STEP 6 | Sélectionnez le **Router Name** (Nom du routeur) — à utiliser pour l'acheminement entre le hub et les branches SD-WAN. Par défaut, un routeur virtuel`sdwan-default` est créé et permet automatiquement à Panorama d'appliquer les configurations du routeur.

(**Routage avancé** activé) Si vous avez configuré le routage avancé et que les routeurs logiques sont créés avec succès, **Nom du routeur** affiche les noms des routeurs virtuels et logiques :

- Si les noms du routeur virtuel et du routeur logique sont identiques, le **Router Name (Nom du routeur)** affiche le même nom, car le routage avancé crée par défaut un routeur logique portant le même nom que le routeur virtuel. Il est important que le nom du routeur logique et le nom du routeur virtuel soient identiques pour le même modèle lors de l'utilisation du moteur de routage avancé.
- Si les noms du routeur virtuel et du routeur logique sont différents (ce qui se produit uniquement lorsque vous mettez à jour le nom du routeur logique manuellement), le nom du routeur affiche à la fois les noms du routeur virtuel et logique. Vous pouvez sélectionner un routeur virtuel (pour le moteur hérité) ou un routeur logique (pour le moteur de routage avancé) en fonction de vos besoins. Si vous n'avez pas activé **Advanced Routing (Routage avancé)**, vous n'aurez alors que des routeurs virtuels à sélectionner dans le **Router Name (Nom du routeur)** (pour l'ancien moteur).

(PAN-OS 11.1.3 et versions ultérieures, et le plug-in SD-WAN 3.2.1 et versions ultérieures) Lorsque l'option (**Enable Multi-VR Support (Activer la prise en charge multi-VR)**) d'un routeur virtuel multiple est activée, sélectionnez Routeur virtuel DIA pour le **Virtual Router Name (Nom du routeur virtuel)**.

STEP 7 | Saisissez le nom du**Site** SD-WAN afin d'identifier l'emplacement géographique ou le but du périphérique.

*Le nom du site SD-WAN supporte tous les caractère alphanumériques en minuscule et majuscule et les caractères spéciaux. Les espaces ne sont pas admis pour le nom du Site et ont pour conséquence que les données de surveillance (**Panorama** > **Monitoring (Surveillance)**) du site ne s'affichent pas.*

Tous les périphériques SD-WAN, y compris les périphériques SD-WAN dans une configuration haute disponibilité (HA), doivent avoir un nom de site unique.

STEP 8 | Sélectionnez la **Link Tag (Étiquette de liaisons)** que vous avez créée pour l'interface virtuelle de la plate-forme (ou l'interface virtuelle de la branche) ; Auto VPN l'affectera à l'interface virtuelle. Vous utiliserez cette étiquette de lien dans un profil de distribution de trafic pour permettre au hub (ou à la branche) de participer à DIA AnyPath.

STEP 9 | Si vous ajoutez un hub derrière un périphérique assurant le NAT pour le hub, vous devez spécifier l'adresse IP ou le FQDN de l'interface publique sur ce périphérique NAT en amont, afin que la configuration Auto VPN puisse utiliser cette adresse comme terminal du tunnel du hub. Il s'agit de l'adresse IP que l'IKE de la branche et les flux IPSec doivent pouvoir atteindre. (Vous devez avoir déjà configuré une interface Ethernet pour SD-WAN.)

1. Dans l'onglet **Upstream NAT** (NAT en amont), activez **Upstream NAT**.
2. **Add** (Ajoutez) une **SD-WAN interface** (interface SD-WAN) ; sélectionnez une interface que vous avez déjà configurée pour SD-WAN.

3. Sélectionnez **IP Address** (adresse IP) ou **FQDN** et saisissez l'adresse IPv4 sans masque de réseau secondaire (par exemple, 192.168.3.4) ou le FQDN du périphérique en amont, respectivement.
4. Cliquez sur **OK**.

De plus, sur le périphérique en amont qui effectue la NAT, vous devez aussi configurer la NAT de destination entrante avec une politique NAT un pour un et vous ne devez pas configurer la translation de port pour les flux de trafic IKE ou IPSec.

Si l'adresse IP du périphérique en amont change, vous devez configurer la nouvelle adresse IP et l'appliquer au cluster VPN. Vous devez aussi utiliser les commandes CLI ***clear vpn ipsec-sa (effacer vpn ipsec-sa)****,* ***clear vpn ike-sa (effacer vpn ike-sa)*** *et* ***clear session all (effacer toutes les sessions)*** *sur la branche et le hub. Vous devez aussi* ***clear session all*** *(effacer toutes les sessions) sur le routeur virtuel où vous avez configuré la politique NAT pour les adresses IP.*

Le NAT en amont n'est pas pris en charge sur les interfaces de couche 2.

STEP 10 | (Déploiements Full Mesh uniquement) Si vous ajoutez une branche derrière un périphérique effectuant la NAT pour la branche, vous devez spécifier l'adresse IP ou le FQDN de l'interface orientée public sur ce périphérique en amont effectuant la NAT ou sélectionner DDNS pour indiquer que l'adresse IP de l'interface installée sur le périphérique NAT est obtenue auprès du service DDNS de Palo Alto Networks. Par conséquent, la configuration Auto VPN utilise cette adresse IP publique comme point de terminaison du tunnel pour la branche. Il s'agit de l'adresse IP que l'IKE de la branche et les flux IPSec doivent pouvoir atteindre. (Vous devez avoir déjà configuré une interface Ethernet pour SD-WAN.)

1. Dans l'onglet **Upstream NAT** (NAT en amont), activez **Upstream NAT**.
2. **Add** (Ajoutez) une **SD-WAN interface** (interface SD-WAN) ; sélectionnez une interface que vous avez déjà configurée pour SD-WAN.
3. Sous **NAT IP Address Type (Type d'adresse IP NAT)**, si vous sélectionnez **Static IP (IP statique)**, sélectionnez **IP Address (Adresse IP)** ou **FQDN**, puis saisissez l'adresse IPv4 sans masque de réseau secondaire (par exemple, 192.168.3.4) ou le FQDN du périphérique en amont, respectivement.
4. Vous pouvez également sélectionner **DDNS** comme **NAT IP Address Type (Type d'adresse IP NAT)**.

5. Cliquez sur **OK**.

De plus, sur le périphérique en amont qui effectue la NAT, vous devez aussi configurer la NAT de destination entrante avec une politique NAT un pour un et vous ne devez pas configurer la translation de port pour les flux de trafic IKE ou IPSec.

Si l'adresse IP du périphérique en amont change, vous devez configurer la nouvelle adresse IP et l'appliquer au cluster VPN. Vous devez aussi utiliser les commandes CLI ***`clear ipsec`****(effacer ipsec),* ***`clear ike-sa`****(effacer ike-sa) et* ***`clear session all`*** *(effacer toutes les sessions) sur la branche et le hub. Vous devez aussi* ***`clear session all`*** *(effacer toutes les sessions) sur le routeur virtuel où vous avez configuré la politique NAT pour les adresses IP.*

Il y a un deuxième emplacement dans l'interface web où vous pouvez configurer la NAT en amont d'une branche. Cependant, l'emplacement suivant n'est pas souhaitable, et vous devriez éviter de configurer la NAT en amont d'une branche aux deux emplacements. Le deuxième emplacement (non recommandé) pour configurer la NAT en amont se trouve sur Panorama, sous ***Network (Réseau)*** *>* ***Interfaces*** *>* ***Ethernet****. Sélectionnez un modèle dans le champ* ***Template (Modèle)****, sélectionnez une interface Ethernet, puis sélectionnez l'onglet* ***SD-WAN****. À ce stade-ci, vous pouvez* ***Enable (Activer)*** *la NAT en amont et sélectionnez le* ***NAT IP Address Type (Type d'adresse IP NAT)****. Cette deuxième méthode a priorité. Si la NAT en amont est d'abord configurée pour l'interface Ethernet sur Panorama au moyen de la pile de modèles, le plug-in SD-WAN ne changera pas les paramètres, et ce, même si vous utilisez des paramètres différents à la page de configuration du périphérique sur lequel se trouve le plug-in. Pour que la configuration de la NAT sur le plugiciel prenne effet, la NAT en amont ne doit pas être configurée au moyen de la pile de modèles sur Panorama.*

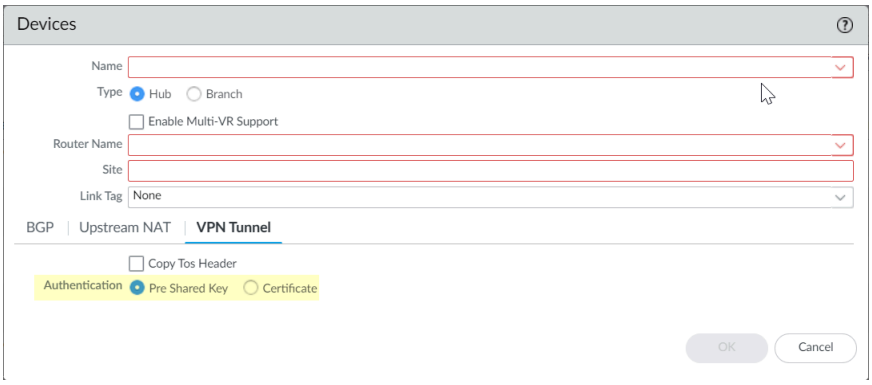
Le NAT en amont n'est pas pris en charge sur les interfaces de couche 2.

STEP 11 | Si le trafic de votre application est étiqueté avec des bits de type de service (ToS) ou des marquages Differentiated Services Code Point (DSCP), copiez le champ ToS de l'en-tête interne vers l'en-tête VPN externe des paquets encapsulés passant par le tunnel VPN afin de préserver les informations QoS.

1. Sélectionnez l'onglet **Tunnel VPN** .
2. Sélectionnez **Copier l'en-tête ToS**.
3. Cliquez sur **OK**.

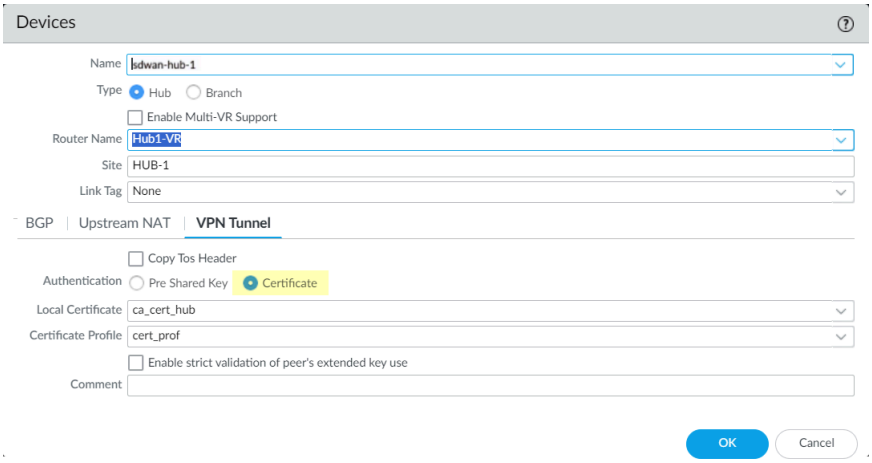
STEP 12 | (Obligatoire) (Plug-in SD-WAN 3.2.0 et versions ultérieures) Spécifiez comment authentifier l'homologue.

Sélectionner le type **Authentication (Authentification)** : **Pre-Shared Key (Clef pré-partagée)** ou **Certificate (Certificat)**. Si vous choisissez une clef pré-partagée, celle-ci sera automatiquement générée.



- *Vous devez utiliser un certificat unique pour chaque périphérique du cluster SD-WAN.*
- *Vous ne pouvez pas modifier le type d'authentification après l'ajout d'un périphérique SD-WAN au cluster VPN.*
- *(Déploiements HA uniquement) Si vous avez configuré une paire haute disponibilité (HA) dans Panorama, les pare-feu actif et passif doivent utiliser le même certificat. Pendant le processus RMA, vous devez configurer le pare-feu de remplacement avec le même certificat que le pare-feu actif. Si le certificat d'un pare-feu actif est révoqué et qu'un nouveau certificat est transmis, le pare-feu passif doit également être mis à jour avec le nouveau certificat. Autrement dit, les pare-feu actif et passif doivent avoir le même certificat configuré dans un déploiement haute disponibilité.*

STEP 13 | (Uniquement si vous activez le type d'authentification par certificat) Configurez l'authentification basée sur le certificat.



1. Sélectionnez un **Local Certificate (Certificat local)**, celui qui figure déjà sur Panorama, puis **Import (Importer)** un certificat ou **Generate (Générer)** un nouveau certificat.

   - Pour **Import (Importer)** un nouveau certificat, procédez d'abord à l'Importation d'un certificat pour l'authentification de passerelle IKEv2. Revenez ensuite à cette tâche. Nous ne prenons pas en charge les certificats générés par SCEP.
   - Si vous souhaitez **Generate (Générer)** un nouveau certificat, commencez par générer un certificat sur le Panorama, puis revenez à cette tâche. Le certificat généré doit être unique pour chaque périphérique SD-WAN. Autrement dit, vous ne pouvez pas générer un certificat et le partager entre plusieurs périphériques SD-WAN.

     Gardez les points suivants à l'esprit lors de la génération des certificats de pare-feu de branche et de hub utilisés pour l'authentification du tunnel SD-WAN :

     - Deux périphériques hub différents peuvent utiliser le même certificat hub.
     - Deux périphériques de branche différents peuvent utiliser le même certificat de branche si les conditions suivantes sont remplies :
       - Les périphériques de branche ne font pas partie du même cluster VPN.
       - Il n'y a pas de périphérique hub commun entre les clusters VPN dont ces périphériques de branche feraient partie.
     - (Déploiements HA uniquement) Deux périphériques de branche différents peuvent également avoir les mêmes certificats de branche s'ils sont configurés en tant que membres HA.
     - Si le périphérique hub est commun entre les clusters VPN, les certificats des périphériques de branche faisant partie de ces clusters VPN doivent avoir des certificats uniques avec tous les attributs ayant des valeurs uniques. Si vous

ne garantissez pas le caractère unique du certificat et ses valeurs, la validation échouera sur le périphérique hub (la validation n'échouera pas sur Panorama).

Veillez également à ce que les certificats feuilles (certificats de pare-feu de branche et de hub) utilisés pour l'authentification du tunnel SD-WAN soient générés de manière à répondre aux critères suivants :

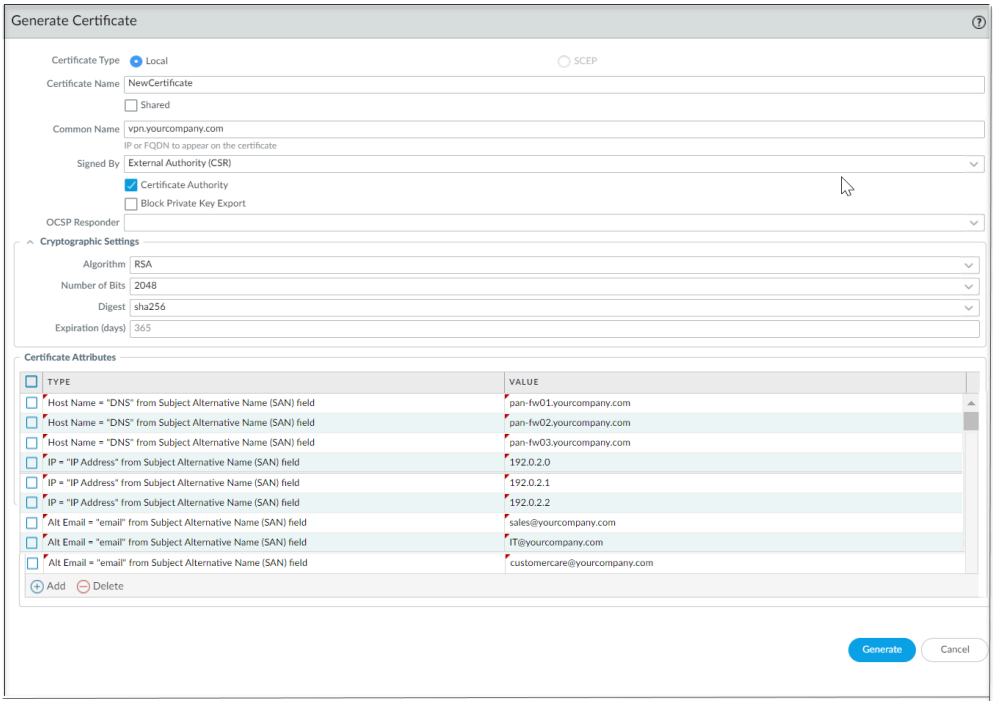
- *L'utilisation de la clef doit être associée à des signatures numériques.*
- *Tous les certificats doivent être signés par la même CA racine.*
- *Le certificat du périphérique doit être directement signé par la CA racine.*
- *Le certificat doit être au format PKCS12.*

- Les attributs du certificat sont utilisés pour déterminer l'ID local et l'ID homologue des passerelles IKE. Par conséquent, les certificats feuilles, c'est-à-dire les certificats de pare-feu de branche et de hub utilisés pour l'authentification du tunnel SD-WAN doivent être générés avec les trois attributs de certificat suivants et chaque attribut de certificat doit être attribué avec trois valeurs d'attribut uniques. Autrement, une erreur de validation sera générée.
  - FQDN (**Host Name (Nom d'hôte)**)
  - IP address (Adresse IP) (**IP**)
  - FQDN de l'utilisateur (**Alt Email (Autre adresse e-mail)**)

  *Il est obligatoire d'avoir des attributs de certificat **Host Name (Nom d'hôte)**, **IP**, et **Alt Email (Autre adresse e-mail)** uniques parmi tous les certificats. Autrement dit, aucun des certificats ne doit avoir ces valeurs d'attribut en commun.*

  Dans l'exemple ci-dessous, NewCertificate est généré avec un total de neuf attributs de certificat obligatoires. L'attribut de certificat **Host Name (Nom d'hôte)** est configuré avec trois valeurs d'attribut uniques : pan-fw01.yourcompany.com, pan-fw02.yourcompany.com et pan-fw03.yourcompany.com. Le certificat **IP** attribué est configuré avec trois valeurs d'attribut uniques : 192.0.2.0, 192.0.2.1 et 192.0.2.2 L'attribut de certificat **Alt Email (Autre adresse e-mail)** est configuré avec trois

valeurs d'attribut uniques : sales@yourcompany.com, IT@yourcompany.com et customercare@yourcompany.com.



2. (Facultatif) Choisissez un **Certificate Profile (Profil de certificat)**. Un profil de certificat contient des informations sur la manière d'authentifier la passerelle homologue.
3. (Facultatif) **Enable strict validation of peer's extended key use (Activer la validation stricte de l'utilisation de la clé étendue de l'homologue)** pour contrôler strictement l'utilisation de la clé.

STEP 14 | (Facultatif) Configurez le routage BGP.

Pour configurer automatiquement le routage BGP entre les membres du cluster VPN, saisissez les informations BGP ci-dessous. Si vous voulez configurer le routage BGP manuellement sur

chaque pare-feu ou utiliser un modèle Panorama séparé pour configurer le routage BGP pour plus de contrôle, laissez les informations BGP du plug-in vides.

Avant de mettre en œuvre SD-WAN avec routage BGP dans un environnement où BGP est déjà utilisé, assurez-vous que la configuration BGP générée par le plug-in SD-WAN n'entre pas en conflit avec votre configuration BGP pré-existante. Par exemple, vous devez utiliser le numéro BGP AS existant et les valeurs d'ID de routeur pour les valeurs de périphérique SD-WAN correspondantes. Si la configuration BGP générée par le plug-in entre en conflit avec votre configuration BGP préexistante, la configuration BGP préexistante. Si vous souhaitez que la configuration poussée soit prioritaire, vous devez activer la valeur du modèle de force lors d'une poussée panoramique.

1. Sélectionnez l'onglet **BGP** et activez **BGP** pour configurer le routage BGP pour le trafic SD-WAN.
2. Saisissez **Router ID**(l'ID du routeur) BGP, qui doit être unique parmi les autres routeurs.
3. Saisissez le **AS Number** (Numéro AS). Le numéro de système autonome spécifie une politique, règle, mesures d'itinéraire définie pour internet. Le numéro AS doit être unique pour chaque emplacement de hub et branche.

STEP 15 | Pour configurer BGP à utiliser IPv4, sélectionnez **IPv4 BGP**. Que votre environnement BGP soit uniquement IPv4 ou double pile (IPv4 et IPv6), vous devez activer IPv4 BGP.

1. **Activez la prise en charge BGP IPv4**.

   *Pour une configuration mise à niveau (une configuration SD-WAN IPv4 déjà existante), l'option **Enable IPv4 BGP support (Activer la prise en charge IPv4 BGP)** est sélectionnée par défaut. Sinon, vous devez **Enable IPv4 BGP support (Activer la prise en charge IPv4 BGP)** de manière explicite.*

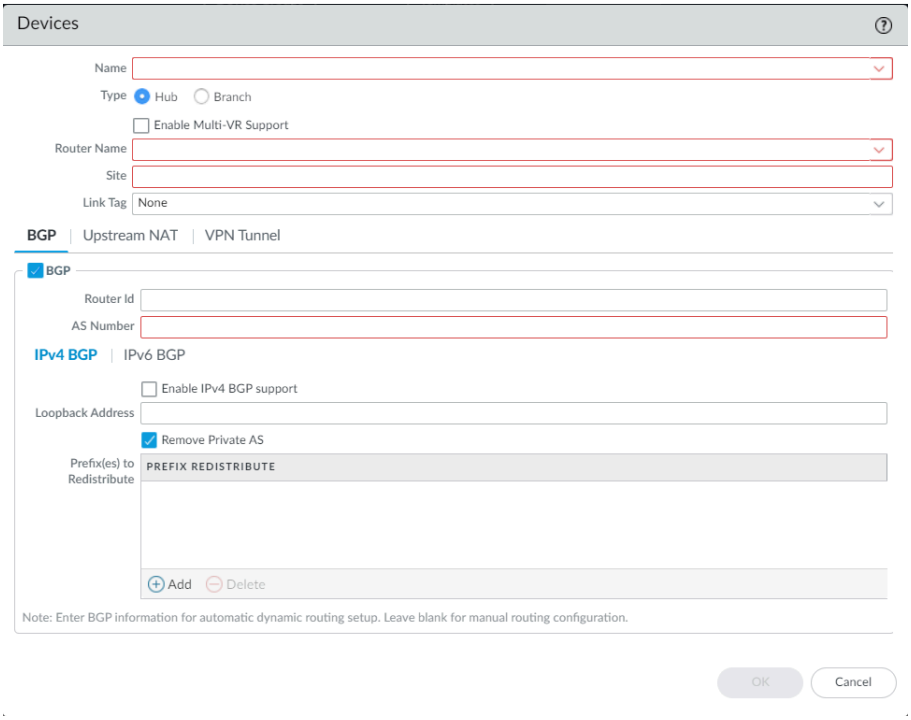
2. Spécifiez une **Loopback Adress** (adresse de bouclage) statique IPv4 pour les homologues BGP. La configuration Auto VPN crée automatiquement une interface de bouclage avec la même adresse IPv4 que vous spécifiez. Si vous spécifiez une adresse de bouclage existante, la validation échouera et vous devez donc spécifier une adresse IPv4 qui n'est pas déjà une adresse de bouclage.
3. Désactivez l'option **Remove Private AS (Supprimer l'AS privé)** (la valeur par défaut est activée) si vous avez des points de terminaison qui doivent échanger des routes avec un pare-feu de concentrateur ou de branche dans une topologie SD-WAN BGP et que vous ne souhaitez donc pas supprimer les numéros d'AS privés (64512 à 65534) à partir de

l'attribut AS_PATH dans les mises à jour BGP. Dans ce cas, vous souhaitez autoriser les numéros d'AS privés à quitter l'AS privé SD-WAN dans les mises à jour BGP.

*Le paramètre **Remove Private AS (Supprimer AS privé)** s'applique à tous les groupes d'homologues BGP sur le pare-feu de la succursale ou du concentrateur. Si vous avez besoin que ce paramètre diffère entre les groupes de pairs ou les pairs BGP, vous devez configurer le paramètre en dehors du plug-in SD-WAN.*

*Si vous modifiez le paramètre **Remove Private AS (Supprimer AS privé)**, que vous validez tous les nœuds du cluster SD-WAN, et que vous rétrogradez ultérieurement à une version du plug-in SD-WAN antérieure à 2.0.2, vous devrez alors effectuer toute la configuration liée à **Remove Private AS (Supprimer AS privé)** à l'extérieur du plug-in SD-WAN ou directement sur les pare-feu.*

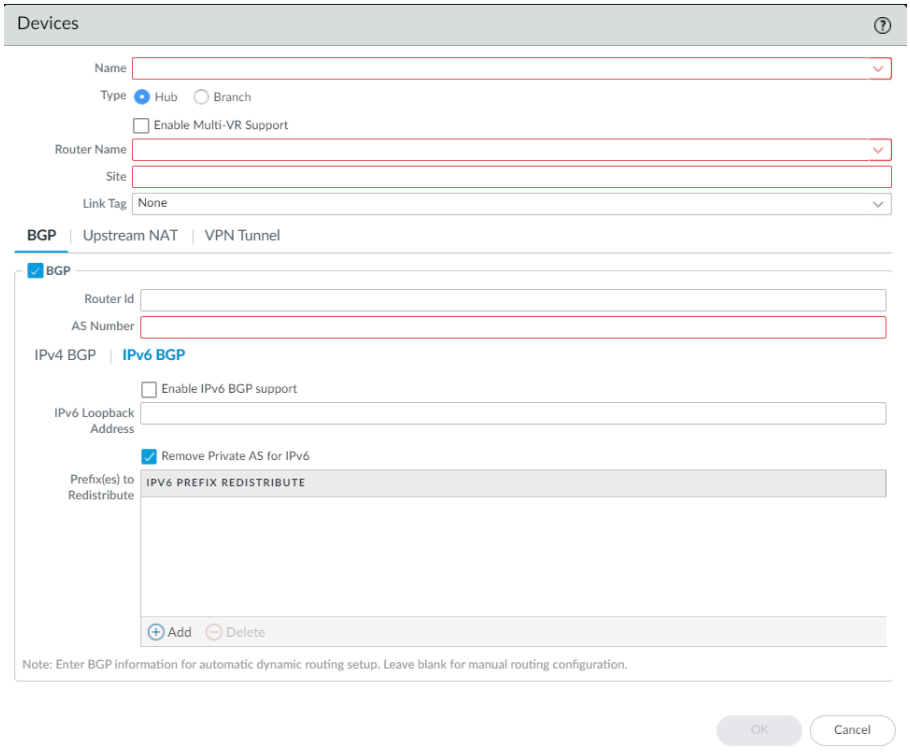
4. **Add (Ajouter)** l'option **Prefix(es) to Redistribute (Préfix(es) à redistribuer)**. Sur un périphérique hub, vous devez saisir au moins un préfixe à redistribuer sur le tunnel SD-WAN. Les périphériques de branche ne sont pas soumis à cette configuration obligatoire, car les sous-réseaux connectés aux emplacements des branches sont redistribués par défaut.



STEP 16 | Pour configurer BGP à utiliser IPv6, sélectionnez **IPv6 BGP**.

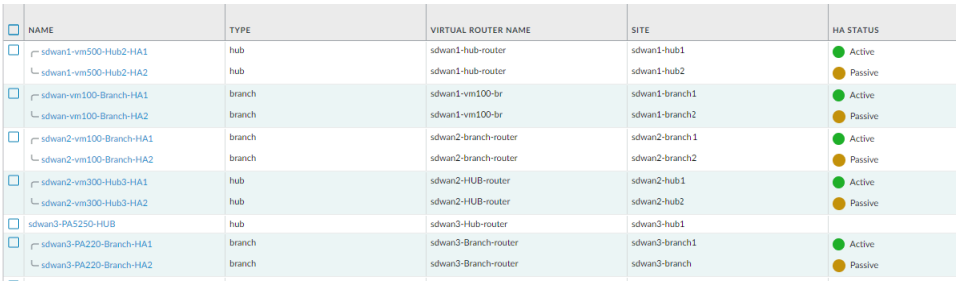
1. **Activez la prise en charge**BGP IPv6.
2. Spécifiez une **Loopback Adress** (adresse de bouclage) statique IPv6 pour les homologues BGP. La configuration Auto VPN crée automatiquement une interface de bouclage avec la même adresse IPv6 que vous spécifiez. Si vous spécifiez une adresse de bouclage existante, la validation échouera et vous devez donc spécifier une adresse IPv6 qui n'est pas déjà une adresse de bouclage.

3. **Add (Ajouter)** l'option **Prefix(es) to Redistribute (Préfix(es) à redistribuer)** sur le tunnel SD-WAN. Sur un périphérique hub, vous devez saisir au moins un préfixe à redistribuer sur le tunnel SD-WAN. Les périphériques de branche ne sont pas soumis à cette configuration obligatoire, car les sous-réseaux connectés aux emplacements des branches sont redistribués par défaut.



STEP 17 | Cliquez sur **OK**.

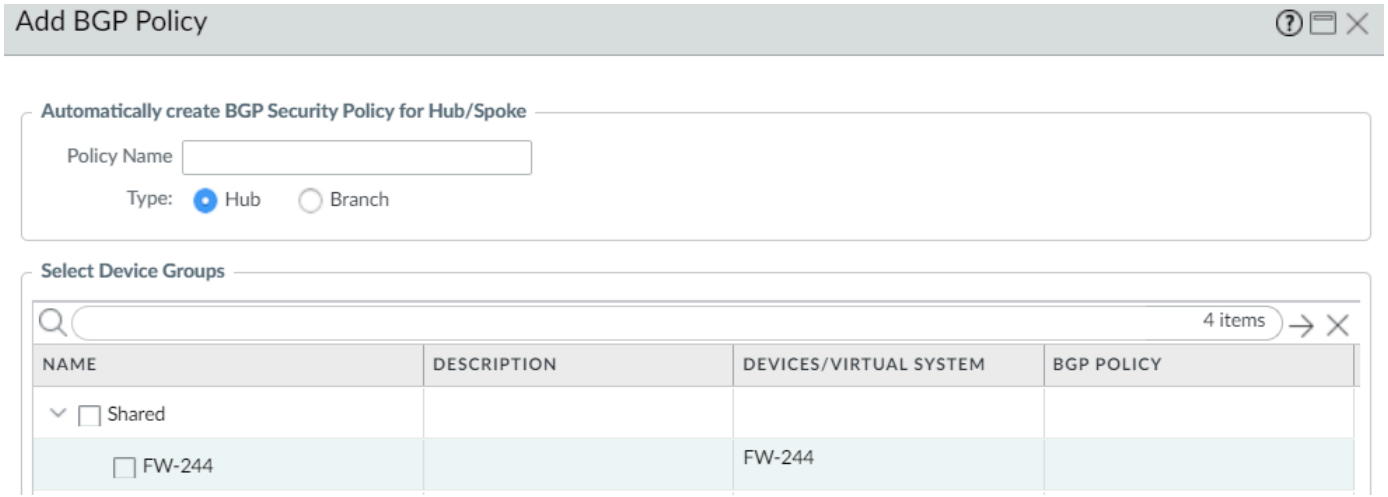
STEP 18 | Sélectionnez **Group HA Peers (Regrouper les homologues HA)** en bas de l'écran pour afficher les branches (ou hub) qui sont ses homologues entre elles.



NAME	TYPE	VIRTUAL ROUTER NAME	SITE	HA STATUS
sdwan1-vm500-Hub2-HA1	hub	sdwan1-hub-router	sdwan1-hub1	Active
sdwan1-vm500-Hub2-HA2	hub	sdwan1-hub-router	sdwan1-hub2	Passive
sdwan-vm100-Branch-HA1	branch	sdwan1-vm100-br	sdwan1-branch1	Active
sdwan-vm100-Branch-HA2	branch	sdwan1-vm100-br	sdwan1-branch2	Passive
sdwan2-vm100-Branch-HA1	branch	sdwan2-branch-router	sdwan2-branch 1	Active
sdwan2-vm100-Branch-HA2	branch	sdwan2-branch-router	sdwan2-branch2	Passive
sdwan2-vm300-Hub3-HA1	hub	sdwan2-HUB-router	sdwan2-hub1	Active
sdwan2-vm300-Hub3-HA2	hub	sdwan2-HUB-router	sdwan2-hub2	Passive
sdwan3-PA5250-HUB	hub	sdwan3-Hub-router	sdwan3-hub1	
sdwan3-PA220-Branch-HA1	branch	sdwan3-Branch-router	sdwan3-branch1	Active
sdwan3-PA220-Branch-HA2	branch	sdwan3-Branch-router	sdwan3-branch	Passive

STEP 19 | Faites en sorte que Panorama crée et applique aux pare-feu une règle de politique de sécurité qui permet à BGP de fonctionner entre les branches et les hubs.

1. Au bas de l'écran, sélectionnez **IPv4 BGP Policy (Politique BGP IPv4)** ou **IPv6 BGP Policy (Politique BGP IPv6)** et **Add (Ajouter)** une règle de politique.
2. Saisissez un **Policy Name** (Nom de politique) pour la règle de politique de sécurité que Panorama créera automatiquement.
3. Sélectionnez **Type** en tant que **hub** ou **branche**.
4. **Select Device Groups** (Sélectionnez ls groupes de périphériques) pour spécifier les groupes de périphériques auxquels Panorama applique les règles de politique de sécurité.
5. Cliquez sur **OK**.



STEP 20 | Sélectionnez **Push to Devices** (Appliquer aux périphériques) pour appliquer vos modifications de configuration aux pare-feu que vous gérez.

Importer en masse plusieurs Périphériques SD-WAN

Ajoutez plusieurs périphériques SD-WAN afin d'embarquer rapidement les pare-feux de branche et du hub plutôt que d'ajouter manuellement chaque périphérique à chaque fois. Lorsque vous ajoutez vos périphériques, vous spécifiez de quel type de périphérique il s'agit (branche ou hub) et vous donnez à chaque périphérique son nom de site pour une identification facile. Avant d'ajouter vos périphériques, planifiez votre configuration SD-WAN pour vous assurer de disposer de toutes les adresses IP nécessaires et de comprendre la topologie SD-WAN. Cela aide à réduire les erreurs de configuration.

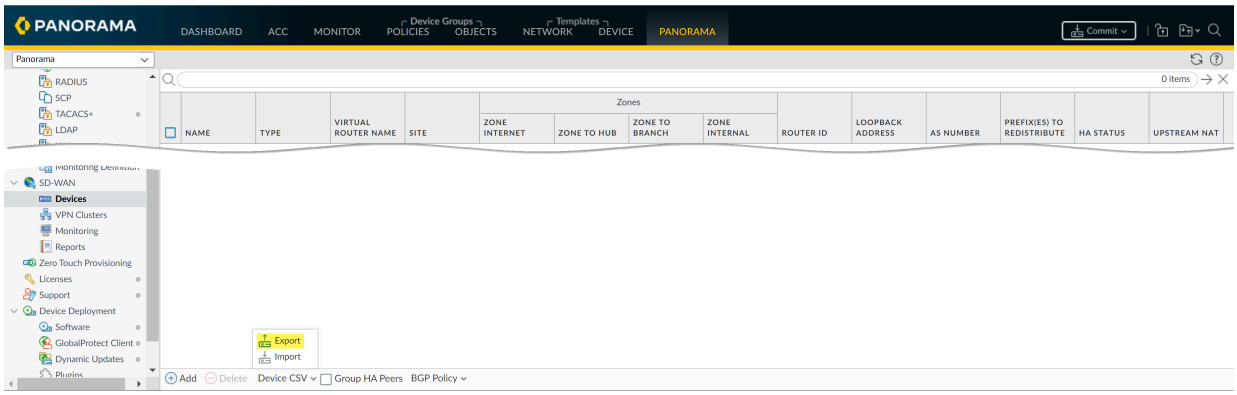
Si vous souhaitez qu'une HA active/passive fonctionne sur deux pare-feu de branche ou deux pare-feu de hub, n'ajoutez pas ces pare-feu en tant que périphériques SD-WAN dans votre fichier CSV. Vous devez les ajouter séparément en tant qu'homologues HA lorsque vous Configurer les Périphérique HA pour SD-WAN.

Si vous utilisez un itinéraire BGP, vous devez ajouter une règle de politique de sécurité pour permettre à BGP d'aller de la zone interne à la zone du hub et de la zone du hub vers la zone interne. Si vous voulez utiliser des numéros de système autonome 4-bytes (ASN), vous devez tout d'abord activer les ASN 4-bytes pour le routeur virtuel.

Si vous avez des zones préexistantes pour vos pare-feu de Palo Alto Networks, vous devrez les mapper selon les zones prédéfinies utilisées dans SD-WAN.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Sélectionnez **Panorama** > **SD-WAN** > **Devices** > **Device CSV** (Panorama SD-WAN Périphériques CSV des périphériques) et **Export** (Exportez un CSV vide de périphérique SD-WAN. Le fichier CSV vous permet d'importer plusieurs périphériques de branche et hub en une fois plutôt que d'ajouter chaque périphérique à la main.



STEP 3 | Remplissez le fichier CSV du périphérique SD-WAN avec les informations de la branche et du hub et enregistrez le CSV. Tous les champs sont obligatoires sauf autre indication. Saisissez ce qui suit pour chaque hub et branche :

- **device-serial** (numéro de série du périphérique) — Le numéro de série du pare-feu de la branche ou du hub.
- **type**— Spécifiez si un périphérique est une **`branch`** (branche) ou une **`hub`** (plateforme).
- **site**— Saisissez le nom du site du périphérique SD-WAN afin de vous aider à identifier l'emplacement géographique ou le but du périphérique.

  *Le nom du site SD-WAN supporte tous les caractère alphanumériques en minuscule et majuscule et les caractères spéciaux. Les espaces ne sont pas admis pour le nom du Site et ont pour conséquence que les données de surveillance (**Panorama** > **SD-WAN** > **Monitoring (Surveillance)**) du cluster ne s'affichent pas.*

  Tous les périphériques SD-WAN, y compris les périphériques SD-WAN dans une configuration haute disponibilité (HA), doivent avoir un nom de site unique.
- **router-name (nom du routeur)** – Saisissez le routeur virtuel à utiliser pour le routage entre le hub et les branches SD-WAN. Par défaut, Panorama crée un routeur virtuel `sdwan-`

`default` et permet à Panorama d'appliquer automatiquement les configurations du routeur.

- **vif-link-tag (balise de lien d'interface virtuelle)** – Spécifiez une balise de lien pour identifier le hub lorsque les applications et les services utilisent ce lien lors de la distribution et du basculement du trafic SD-WAN.
- (Facultatif) **router-id**— Spécifiez l'ID du routeur BGP, qui doit être unique parmi tous les routeurs virtuels.

  Saisissez l'adresse de bouclage en tant qu'ID du routeur.

  Avant de mettre en œuvre SD-WAN avec routage BGP dans un environnement où BGP est déjà utilisé, assurez-vous que la configuration BGP générée par le plug-in SD-WAN n'entre pas en conflit avec votre configuration BGP existante. Par exemple, vous devez utiliser le numéro BGP AS existant et les valeurs d'ID de routeur pour les valeurs de périphérique SD-WAN correspondantes.
- (Facultatif) **as-number**— Saisissez l'ASN de l'AS privé auquel le routeur virtuel sur le hub ou la branche appartient. Le plug-in SD-WAN n'est compatible qu'avec les systèmes autonomes privés. L'ASN doit être unique pour chaque hub et branche. La fourchette ASN 4-bytes est de 4 200 000 000 à 4 294 967 294 ou 64512.64512 à 65535.65534. La fourchette ASN 2-bytes est de 64512 à 65534.

  Utilisez un ASN privé 4-bytes.

  Avant de mettre en œuvre SD-WAN avec routage BGP dans un environnement où BGP est déjà utilisé, assurez-vous que la configuration BGP générée par le plug-in SD-WAN n'entre pas en conflit avec votre configuration BGP existante. Par exemple, vous devez utiliser le numéro BGP AS existant et les valeurs d'ID de routeur pour les valeurs de périphérique SD-WAN correspondantes.
- (Facultatif) **ipv4-bgp-enable** – Spécifiez oui ou non pour activer ou désactiver BGP pour les adresses IPv4.
- (Facultatif) **loopback-address (adresse de bouclage)** – Spécifiez une adresse de bouclage IPv4 statique pour l'appairage BGP. Le plug-in SD-WAN 3.1.1 et les versions ultérieures 3.1 prennent en charge une adresse de bouclage IPv6 pour l'appairage BGP.
- (Facultatif) **remove-private-as (supprimer l'as privé)** – Spécifiez non pour désactiver l'option Remove Private AS (Supprimer l'AS privé) (la valeur par défaut est activée) si vous avez des points de terminaison qui doivent échanger des itinéraires avec un pare-feu de hub ou de branche dans une topologie SD-WAN BGP et que vous ne souhaitez donc pas supprimer les numéros d'AS privés (64512 à 65534) à partir de l'attribut AS_PATH dans les mises à jour BGP.

  Ce paramètre s'applique à tous les groupes d'homologues BGP sur le pare-feu de branche ou de hub. Si vous avez besoin que ce paramètre diffère entre les groupes de pairs ou les pairs BGP, vous devez configurer le paramètre en dehors du plug-in SD-WAN.
- (Facultatif) **prefix-redistribute** (redistribution de préfixe)— Saisissez les préfixes IP dont la branche informe le hub qu'elle peut atteindre. Pour ajouter plus d'un préfixe, séparez les préfixes avec un espace, une esperluette (&), et un espace ; par exemple, 192.2.10.0/24 &

192.168.40.0/24. Par défaut, le pare-feu de la branche attribue tous les préfixes internet connectés en local au hub.

Palo Alto Networks ne redistribue pas les itinéraires par défaut des branches déduites de l'ISP.

- (Facultatif) **ipv6-bgp-enable (activer bgp pour ipv6)** – Spécifiez oui/non pour activer/désactiver BGP pour les adresses IPv6.
- (Facultatif) **ipv6-loopback-address (adresse de bouclage ipv6)** – Spécifiez une adresse de bouclage IPv6 statique pour l'appairage BGP.
- (Facultatif) **ipv6-prefix-redistribute (redistribuer des préfixes ipv6)** – Saisissez des préfixes IPv6 à redistribuer au routeur hub à partir de la branche. Par défaut, tous les préfixes Internet IPv6 i connectés en local sont publiés à l'emplacement du hub.
- (Facultatif) **copy-tos-header (copier l'en-tête tos)** – Spécifiez oui/non pour activer/désactiver cette option afin de copier l'en-tête Type of Service (type de service - ToS) de l'en-tête IP interne vers l'en-tête IP externe des paquets encapsulés afin de préserver les informations d'origine du TOS.
- **authentication-type (type d'authentification)** – Spécifiez le type d'authentification pris en charge par le périphérique (hub ou branche) : authentification par clef pré-partagée ou par certificat.
- (Uniquement pour le type d'authentification par **Certificate (Certificat)**) **certificate-name (nom du certificat)** – Saisissez un nom de certificat. Le nom est sensible à la casse et peut contenir jusqu'à 63 caractères sur le pare-feu et 31 caractères sur le Panorama. Il doit être unique et utiliser uniquement des lettres, des nombres, des traits d'union et des traits de soulignement.

  Ce champ doit rester vide pour le type d'authentification par clef pré-partagée.

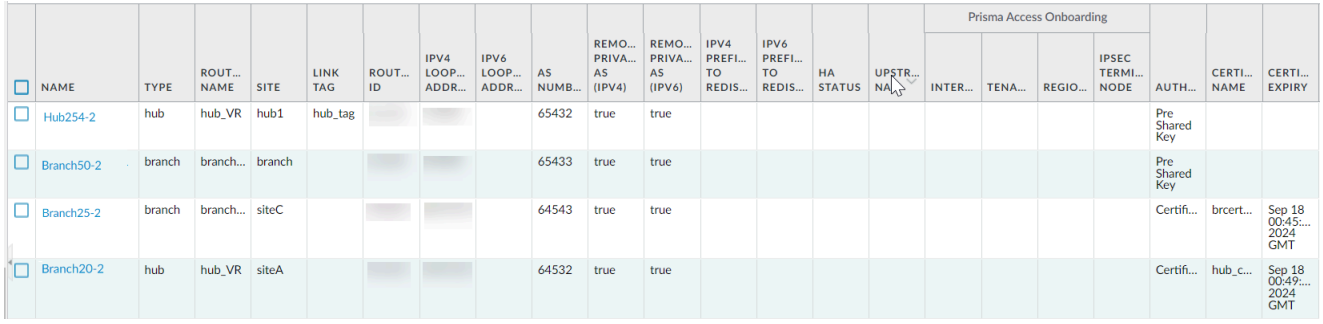
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	device-serial	type	site	router-name	vif-link-tag	router-id	as-number	ipv4-bgp-enable	loopback-addres	remove-private-a	prefix-redistribut	ipv6-bgp-enable	ipv6-loopback-a	ipv6-prefix-redis	copy-tos-he	authentication-ty	certificate-name
2		hub	hub1	hub_VR			65520			yes						pre-shared-key	
3		branch	branch	branch_VR			65501			yes						pre-shared-key	
4		branch	siteC	branch_VR			65502			yes						certificate	brcert1_cacert
5		hub	siteA	hub_VR			65525			yes						certificate	hub_cacert
6																	

STEP 4 | Importez le fichier CSV du périphérique SD-WAN dans Panorama.

Vérifiez qu'il n'y a pas de validations en attente dans Panorama ou l'importation échouera.

1. Dans Panorama, sélectionnez **Panorama** > **SD-WAN** > **Devices** > **Device CSV** (Panorama SD-WAN Périphériques CSV du périphérique) et **Import** (Importez) le CSV que vous avez modifié lors de l'étape précédente.
2. **Browse** (naviguez) et sélectionnez le CSV du périphérique SD-WAN.
3. Cliquez sur **OK** pour importer les périphériques SD-WAN.

STEP 5 | Vérifiez que vos périphériques SD-WAN ont été correctement ajoutés.



NAME	TYPE	ROUT... NAME	SITE	LINK TAG	ROUT... ID	IPV4 LOOP... ADDR...	IPV6 LOOP... ADDR...	AS NUMB...	REMO... PRIVA... AS (IPV4)	REMO... PRIVA... AS (IPV6)	IPV4 PREFI... TO REDIS...	IPV6 PREFI... TO REDIS...	HA STATUS	UPSTR... NA...	Prisma Access Onboarding				AUTH...	CERTI... NAME	CERTI... EXPIRY
															INTER...	TENA...	REGIO...	IPSEC TERMI... NODE			
Hub254-2	hub	hub_VR	hub1	hub_tag				65432	true	true									Pre Shared Key		
Branch50-2	branch	branch...	branch					65433	true	true									Pre Shared Key		
Branch25-2	branch	branch...	siteC					64543	true	true									Certifi...	brcert...	Sep 18 00:45:... 2024 GMT
Branch20-2	hub	hub_VR	siteA					64532	true	true									Certifi...	hub_c...	Sep 18 00:49:... 2024 GMT

STEP 6 | **Commit (validez)** vos modifications de configuration.

STEP 7 | Sélectionnez **Push to Devices** (Appliquer aux périphériques) pour appliquer vos modifications de configuration aux pare-feu que vous gérez.

Intégrer le pare-feu PAN-OS à Prisma Access

Le plug-in SD-WAN 2.2 assure une prise en charge du hub Prisma Access, dans lequel les pare-feu PAN-OS se connectant aux nœuds de calcul (CN) Prisma Access assurent une sécurité basée sur le cloud dans une topologie SD-WAN hub-and-spoke. Dans cette topologie, les hubs SD-WAN sont des CN Prisma Access (IPSec Termination Nodes) et les branches SD-WAN sont des pare-feu PAN-OS. Un maximum de quatre hubs (toute combinaison de hubs PAN-OS participant aux hubs DIA AnyPath et Prisma Access) sont pris en charge. Le SD-WAN crée automatiquement des tunnels IKE et IPSec qui connectent la branche au hub. Consultez la configuration système requise pour SD-WAN et Prisma Access.

Il est important de commencer par configurer Prisma Access, puis de configurer le SD-WAN.

- *Si vous démarrez une toute nouvelle configuration Prisma Access, lisez le Guide de l'administrateur de Prisma Access et suivez les étapes de configuration de la phase 1, puis de la phase 2.*
- *Si Prisma Access est déjà en cours d'exécution, assurez-vous que la phase 1 est terminée, puis terminez la phase 2.*

L'organigramme suivant montre l'ordre des deux phases de configuration et des étapes de base au sein de chaque phase. Les prérequis complets de Prisma Access avec des liens et les étapes de configuration pour SD-WAN suivent l'organigramme.

PHASE 1 – PRISMA ACCESS (TERMINEZ D'ABORD LA PHASE 1)	PHASE 2 : SD-WAN (NE COMMENCEZ QU'APRÈS AVOIR TERMINÉ LA PHASE 1)
1. Configurez le sous-réseau d'infrastructure, le BGP AS d'infrastructure, la pile de modèles et le groupe de périphériques pour un locataire.	1. Configurez un pare-feu de succursale avec une interface sur laquelle le SD-WAN est activé.

PHASE 1 – PRISMA ACCESS (TERMINEZ D'ABORD LA PHASE 1)	PHASE 2 : SD-WAN (NE COMMENCEZ QU'APRÈS AVOIR TERMINÉ LA PHASE 1)
2. Configurez des piles de modèles, des modèles, des groupes d'appareils, des zones de confiance et de non-approbation et une allocation de bande passante pour des régions spécifiques. 3. Assurez-vous que votre déploiement Prisma Access est sous licence pour les réseaux distants. 4. Assurez-vous que votre déploiement alloue de la bande passante par emplacement de calcul, plutôt que par emplacement. 5. Assurez-vous d'avoir affecté la bande passante à l'emplacement de calcul qui correspond à l'emplacement auquel vous souhaitez vous connecter. 6. Effectuez une validation locale et effectuez une poussée vers le cloud Prisma Access.	2. Connectez-vous à l'interface Web Panorama. 3. Spécifiez le pool d'adresses locales BGP pour les adresses de bouclage. 4. Sélectionnez le pare-feu de branche SD-WAN pour vous connecter au hub Prisma Access et configurez la connexion. 5. Validez et Lancez la configuration vers le cloud. 6. Vérifiez que l'intégration est terminée. 7. Synchronisez le pare-feu de succursale avec Prisma Access. 8. Validez sur Panorama). 9. Push to Devices (Appliquer aux périphériques). 10. Affichez la nouvelle interface qui a été créée. 11. Vérifiez que le tunnel IPSec est opérationnel. 12. Vérifiez que la passerelle IKE est active. 13. Créez une règle de stratégie SD-WAN pour générer des données de surveillance. 14. Validez et Validez et Appliquez aux pare-feux de branche. 15. Surveillez les performances de l'application et de la liaison du hub Prisma Access.

Avant de connecter le SD-WAN à Prisma Access, vous devez disposer d'un pare-feu de succursale avec une interface sur laquelle le SD-WAN est activé. En outre, assurez-vous d'avoir effectué les conditions préalables Prisma Access suivantes pour un ou plusieurs locataires ; voici les étapes de la phase 1 :

1. Pour **Panorama** > **Cloud Services** > **Configuration**,configurez le sous-réseau d'infrastructure, l'infrastructure BGP AS, la pile de modèles et le groupe de périphériques pour un locataire sur la page **Configuration du service**.
2. Dans la page **Réseaux distants**, configurez des piles de modèles, des modèles, des groupes de périphériques, des zones d'approbation et de non-approbation et l'allocation de bande passante pour des régions spécifiques.

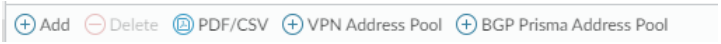
3. Assurez-vous que votre déploiement Prisma Access est sous licence pour les réseaux distants en sélectionnant **Licenses (Licences)** > **Panorama** et en vérifiant vos informations de licence.
   - Les licences disponibles après le 17 novembre 2020 indiquent la quantité de bande passante sous licence dont vous disposez pour les réseaux distants dans la zone **Net Capacity (Capacité nette)**.
   - Les licences disponibles avant le 17 novembre 2020 affichent la bande passante du réseau distant disponible dans la zone **GlobalProtect Cloud Service for Remote Networks (Service cloud GlobalProtect pour réseaux distants)** sous **Total Mbps (Total Mbits/s)**.
4. Assurez-vous que votre déploiement alloue de la bande passante par emplacement de calcul, plutôt que par emplacement.
5. Assurez-vous d'avoir affecté la bande passante à l'emplacement de calcul qui correspond à l'emplacement auquel vous souhaitez vous connecter. Prisma Access alloue un nœud de terminaison IPSec par 500 Mbit/s de bande passante que vous allouez à une région.
6. Effectuez une validation locale et effectuez une poussée vers le cloud Prisma Access.

Après avoir effectué les étapes précédentes pour la phase 1 avec Prisma Access, effectuez les étapes de phase 2 suivantes pour le SD-WAN.

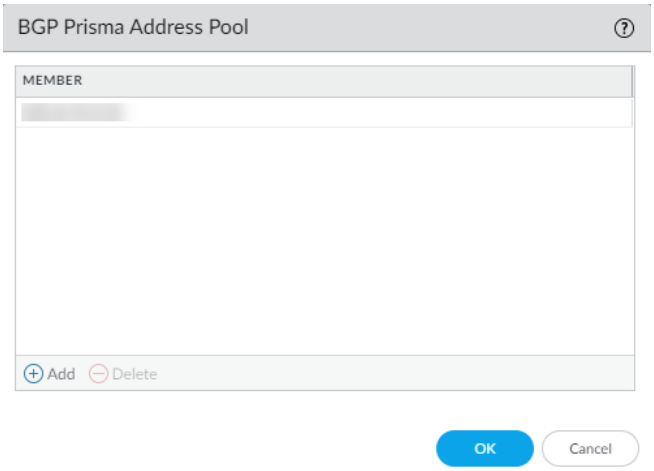
STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Spécifiez le pool d'adresses locales BGP pour les adresses de bouclage.

1. Sélectionnez **Panorama** > **SD-WAN** > **VPN Clusters** (Clusters VPN SD-WAN de Panorama).
2. En bas de l'écran, sélectionnez **BGP Prisma Address Pool (Pool d'adresses BGP Prisma)**.



3. **Ajoutez** un sous-réseau privé inutilisé (préfixe et masque de réseau) pour les adresses BGP locales pour Prisma Access.



4. Cliquez sur **OK**.
5. **Commit** (Valider).

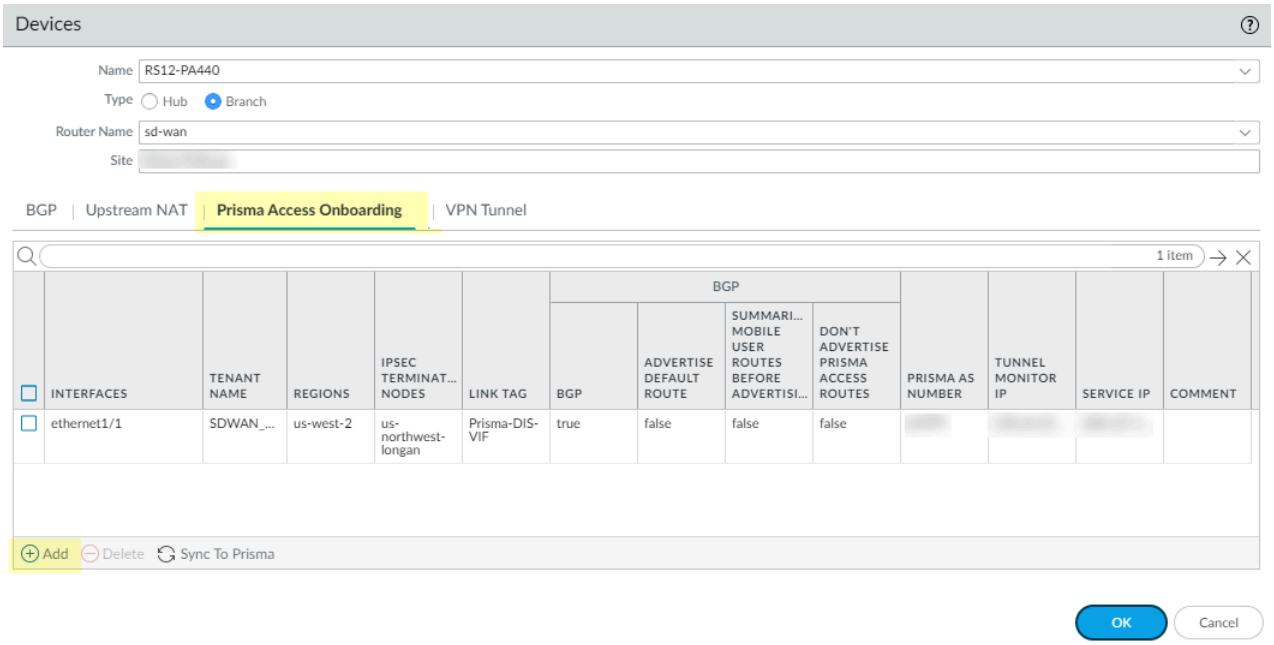
> *Ne modifiez pas simplement un pool d'adresses existant si Prisma Access est déjà intégré. Si vous devez modifier un pool d'adresses, procédez comme suit pendant une fenêtre de maintenance pour mettre à jour la branche SD-WAN et Prisma Access CN avec les modifications apportées à votre pool d'adresses :*
>
> 1. *Utilisez Panorama pour accéder à une branche SD-WAN et supprimez l'intégration existante sur laquelle le changement de pool d'adresses aura un impact ; puis faites un Commit local.*
> 2. *Mettez à jour le pool d'adresses VPN, puis effectuez une validation locale.*
> 3. *Effectuez à nouveau l'intégration de Prisma Access, puis effectuez une validation et une diffusion locales.*

STEP 3 | Sélectionnez le pare-feu de branche SD-WAN pour vous connecter au hub Prisma Access et configurez la connexion.

1. Sélectionnez **Panorama** > **SD-WAN** > **Devices (périphériques)**.
2. Sélectionnez le pare-feu de branche sur lequel vous avez activé le SD-WAN, dont le nom remplit ensuite le champ **Nom** .
3. Sélectionnez le **Type** de périphérique comme **Branche**.
4. Sélectionnez le **nom du routeur**.
5. Accédez au **Site**.

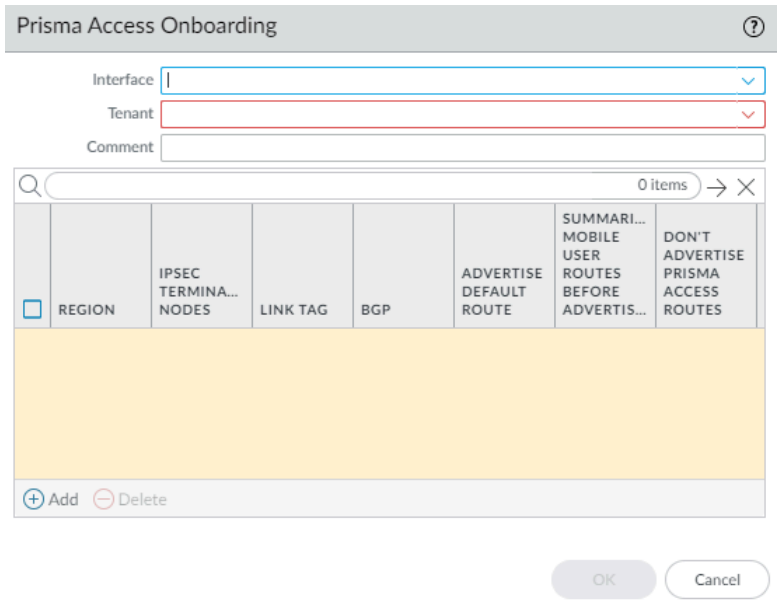
   Tous les périphériques SD-WAN doivent avoir un nom de site unique.

6. Sélectionnez **Prisma Access Onboarding (Intégration de Prisma Access)** et **Add (Ajouter)**.



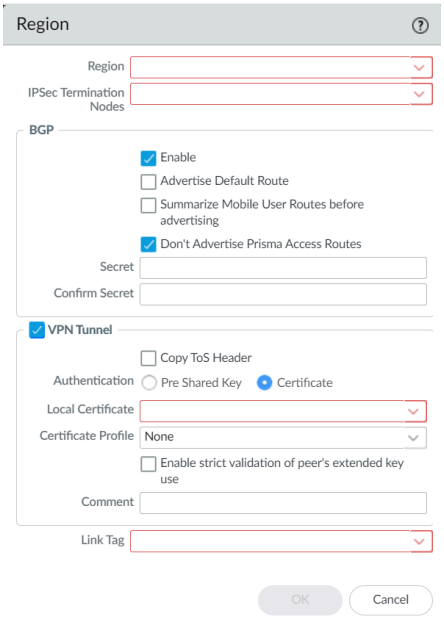
7. Sélectionnez une **Interface** SD-WAN locale sur le pare-feu pour vous connecter au hub Prisma Access.
8. Sélectionnez un **locataire** Prisma Access (sélectionnez par **défaut** pour un environnement à locataire unique).

   Toutes les interfaces SD-WAN d'un pare-feu de succursale doivent utiliser le même locataire Prisma Access.
9. Entrez un **Commentaire** utile.



10. **Ajoutez** un nœud de calcul à une **région en sélectionnant la région** où se trouve le CN (Prisma Access Hub).

    Il peut y avoir plusieurs régions par interface.



11. Sélectionnez un **nœud de terminaison IPSec (passerelle GP) dans la liste des nœuds** ; la liste est basée sur les nœuds que Prisma Access a créés pour la région précédemment.

Vous choisissez le hub auquel cette branche se connecte. La configuration SD-WAN Auto VPN établit des relations IKE et IPSec et des tunnels avec ce nœud.

12. **Activez** BGP pour la communication entre la branche et le concentrateur (Activer est la valeur par défaut).
13. **Annoncez l'itinéraire par défaut** pour autoriser la publication de l'itinéraire par défaut du hub Prisma Access sur le pare-feu de la succursale.
14. **Résumez les itinéraires des utilisateurs mobiles avant de faire de la publicité pour** que le hub Prisma Access annonce les itinéraires de sous-réseau IP des utilisateurs mobiles résumés, réduisant ainsi le nombre de publicités vers les succursales.
15. **Ne faites pas de publicité pour les routes d'accès Prisma** pour empêcher le nœud/hub de terminaison IPSec de faire la publicité de ses routes d'accès Prisma aux succursales SD-WAN.
16. Entrez le **Code secret** pour l'authentification des communications BGP et **Confirmer le secret**.
17. (Plug-in SD-WAN 3.2.0 et versions ultérieures) Configurez les paramètres du tunnel VPN et le type d'authentification pour authentifier le pare-feu PAN-OS et le hub Prisma Access.
    1. (Facultatif) Si vous souhaitez conserver les informations de type de service (ToS) dans les paquets encapsulés, sélectionnez **Copy TOS Header (Copier l'en-tête TOS)**.

       S'il y a plusieurs sessions à l'intérieur du tunnel (chacune avec une valeur ToS différente), la copie de l'en-tête ToS peut provoquer l'arrivée des paquets IPSec en désordre.
    2. Sélectionnez **Authentication (Authentification)** : **Pre-Shared Key (Clef pré-partagée)** ou **Certificate (Certificat)**.

       Assurez-vous de sélectionner le même type d'authentification pour tous les périphériques de branche et le périphérique Prisma Access ajouté.

       La clef pré-partagée est automatiquement générée si elle est sélectionnée comme type d'authentification pour une région.
18. Sélectionnez **Certificate (Certificat)** pour configurer l'authentification basée sur les certificats.
19. (Seulement si le type d'authentification **Certificate (Certificat)** est activé) Le certificat doit être présent sur Panorama avant d'effectuer l'intégration de Prisma Access du pare-feu de branche SD-WAN. Nous ne prenons pas en charge les certificats générés

par SCEP. Sélectionnez un **Local Certificate (Certificat local)**, celui qui figure déjà sur Panorama.

Vérifiez les éléments suivants pour le certificat que vous avez dans Panorama pour assurer la réussite du processus d'intégration de Prisma Access :

- Le certificat doit être unique pour chaque périphérique SD-WAN. C'est-à-dire que vous ne pouvez pas partager le certificat entre plusieurs périphériques SD-WAN.

  Gardez les points suivants à l'esprit lors de la génération des certificats de pare-feu de branche et de hub utilisés pour l'authentification du tunnel SD-WAN :

  - Deux périphériques hub différents peuvent utiliser le même certificat hub.
  - Deux périphériques de branche différents peuvent utiliser les certificats de même branche si les conditions suivantes sont remplies :
    - Les périphériques de branche ne font pas partie du même cluster VPN.
    - Il n'existe pas de périphérique hub commun entre les clusters VPN dont ces périphériques de branche feraient partie.
  - (Déploiements HA uniquement) Deux périphériques de branche différents peuvent également avoir les mêmes certificats de branche s'ils sont configurés en tant que membres HA.
  - Si le périphérique hub est commun entre les clusters VPN, les certificats des périphériques de branche faisant partie de ces clusters VPN doivent avoir des certificats uniques avec tous les attributs ayant des valeurs uniques. Si vous ne garantissez pas le caractère unique du certificat et ses valeurs, la validation échouera sur le périphérique hub (la validation n'échouera pas sur Panorama).

  Veillez également à ce que les certificats feuilles (certificats de pare-feu de branche et de hub) utilisés pour l'authentification du tunnel SD-WAN soient générés de manière à répondre aux critères suivants :

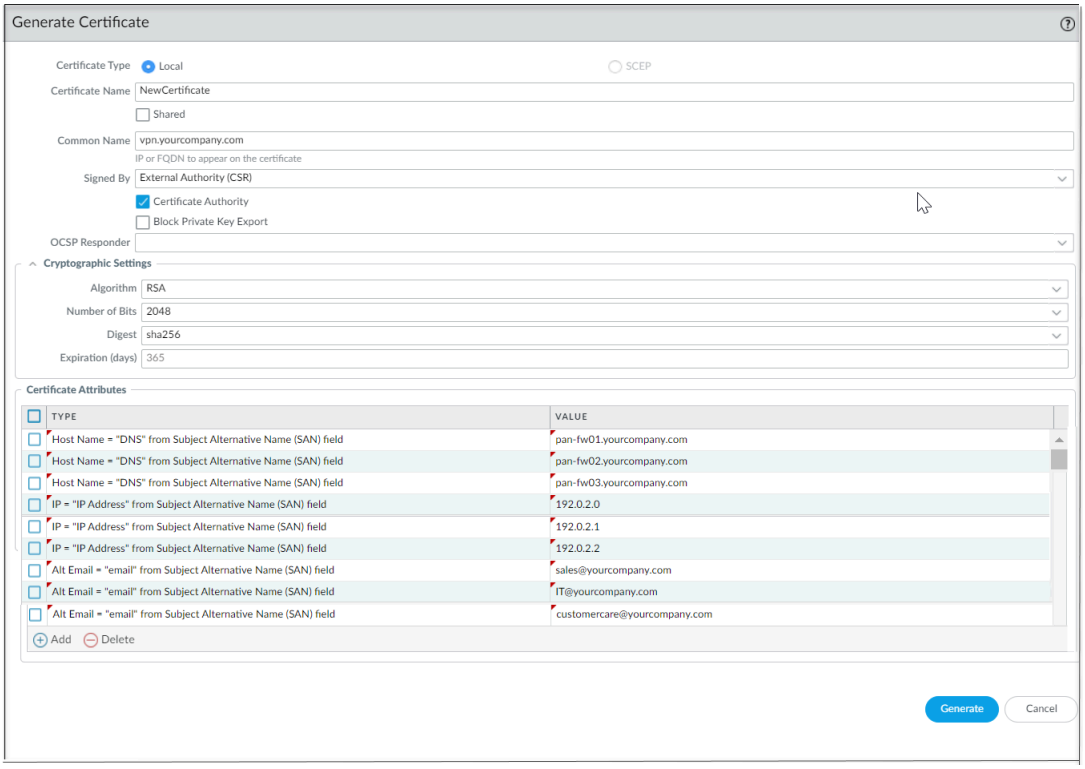
  - *L'utilisation de la clef doit être associée à des signatures numériques.*
  - *Tous les certificats doivent être signés par la même CA racine*
  - *Le certificatdu périphérique doit être directement signé par la CA racine*
  - *Le certificat doit être au format PKCS12*
- Les attributs du certificat sont utilisés pour déterminer l'ID local et l'ID homologue des passerelles IKE. Par conséquent, les certificats feuilles, c'est-à-dire les certificats de pare-feu de branche et de hub utilisés pour l'authentification du tunnel SD-WAN doivent être générés avec les trois attributs de certificat suivants et chaque attribut de certificat doit être attribué avec trois valeurs d'attribut uniques. Autrement, une erreur de validation sera générée.
  - FQDN (**Host Name (Nom d'hôte)**)
  - IP address (Adresse IP) (**IP**)

- FQDN de l'utilisateur (**Alt Email (Autre adresse e-mail)**)

> *Il est obligatoire d'avoir des attributs de certificat **Host Name (Nom d'hôte)**, **IP**, et **Alt Email (Autre adresse e-mail)** uniques parmi tous les certificats. Autrement dit, aucun des certificats ne doit avoir ces valeurs d'attribut en commun.*

Dans l'exemple ci-dessous, NewCertificate est généré avec un total de neuf attributs de certificat obligatoires. L'attribut de certificat **Host Name (Nom d'hôte)** est configuré avec trois valeurs d'attribut uniques : pan-fw01.yourcompany.com, pan-fw02.yourcompany.com et pan-fw03.yourcompany.com. L'attribut du certificat **IP** est configuré avec trois valeurs d'attribut uniques : 192.0.2.0, 192.0.2.1 et 192.0.2.2 L'attribut de certificat **Alt Email (Autre adresse e-mail)** est configuré avec trois

valeurs d'attribut uniques : sales@yourcompany.com, IT@yourcompany.com et customercare@yourcompany.com.

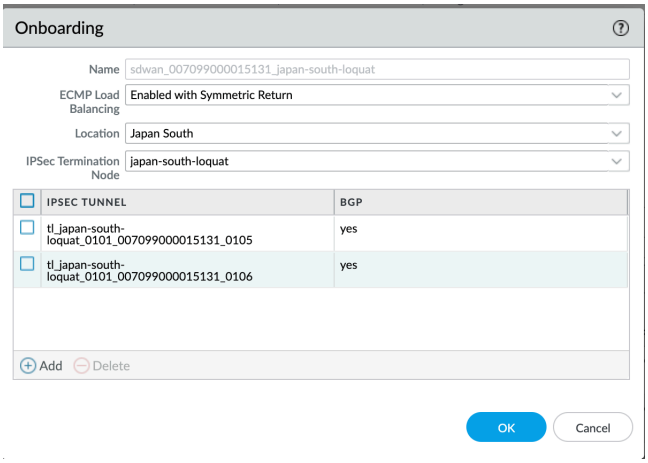


20. (Facultatif) (Uniquement si vous activez le type d'authentification par **Certificate (Certificat)**) Choisissez un **Certificate Profile (Profil de certificat)**. Un profil de certificat contient des informations sur la manière d'authentifier la passerelle homologue.
21. (Facultatif) **Enable strict validation of peer's extended key use (Activer la validation stricte de l'utilisation de la clé étendue de l'homologue)** pour contrôler strictement l'utilisation de la clé.
22. Sélectionnez une **balise de lien** pour le hub.

    Lorsque vous souhaitez activer ECMP pour un hub Prisma Access, intégrez plusieurs interfaces de branche au même nœud de calcul (CN) et utilisez la même balise Link sur ces interfaces de branche.
23. Cliquez sur **OK**. L'affichage comprendra un numéro Peer AS et l'adresse IP Tunnel Monitor fournie par Prisma Access.

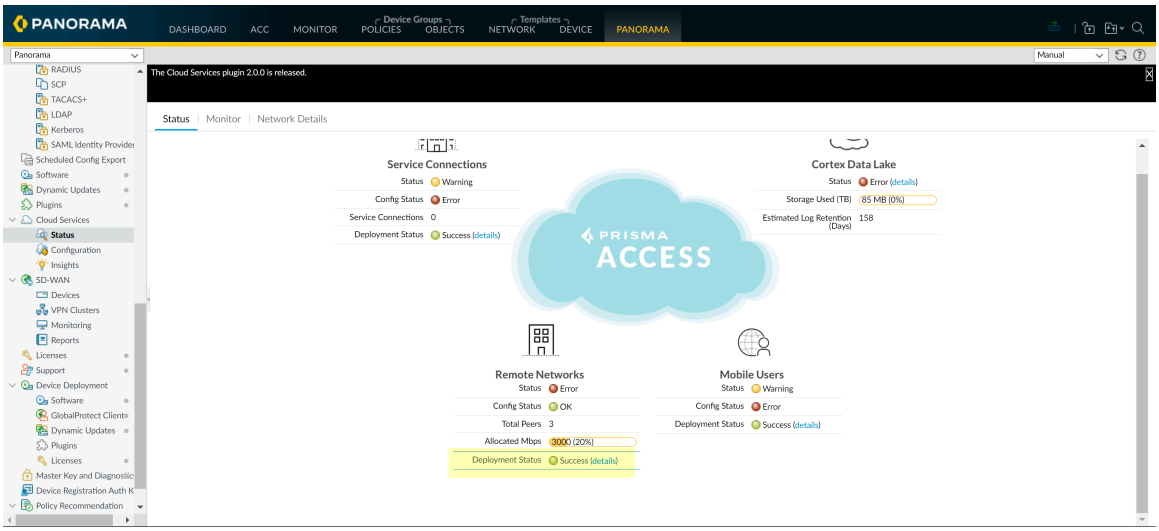
STEP 4 | **Validez et activez** la configuration vers le cloud, où Prisma Access fait tourner le nombre correct de nœuds de terminaison IPSec en fonction de la bande passante demandée.

Lorsque plusieurs tunnels IPSec vont au même CN, la configuration Prisma Access a activé ECMP avec retour symétrique, comme illustré dans cet exemple Prisma Access :

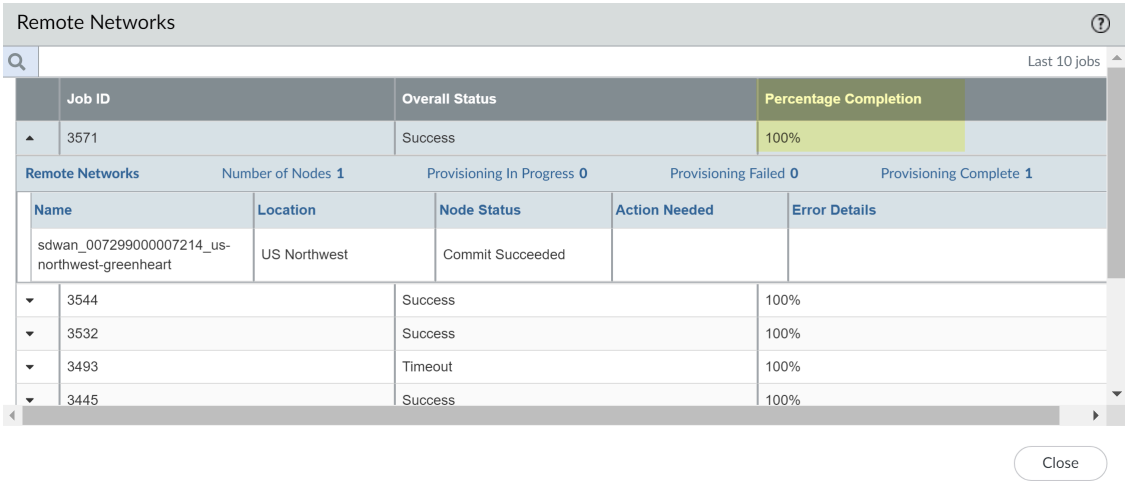


STEP 5 | Vérifiez que l'intégration est terminée.

1. Sélectionnez **Panorama** > **Cloud Services** > **Status** et vérifiez que l'état du déploiement des réseaux distants affiche `la réussite`.



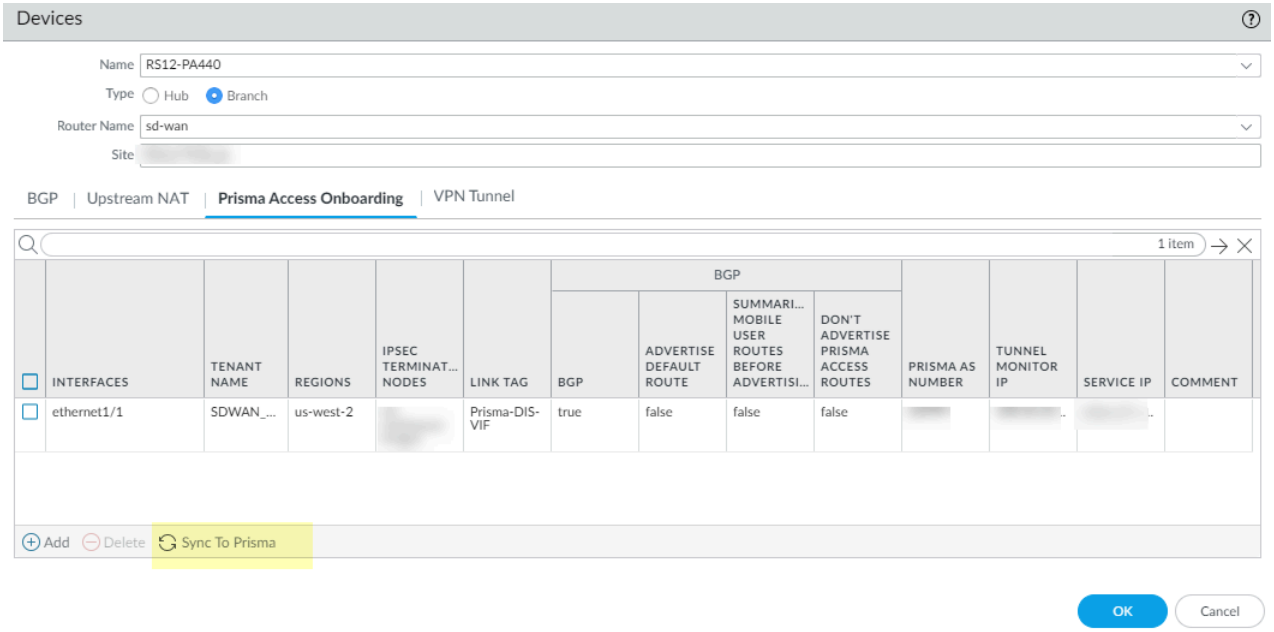
2. Sélectionnez les **détails** de l'état de déploiement des réseaux distant.
3. Vérifiez que l'achèvement du nœud Prisma Access affiche 100 %.



STEP 6 | Synchronisez le pare-feu de la succursale avec Prisma Access pour récupérer la ou les adresses IP de service des CN.

1. Sélectionnez **Panorama** > **SD-WAN** > **Devices (périphériques)**
2. Sélectionnez le périphérique de succursale SD-WAN.
3. Sélectionnez **Prisma Access Onboarding** and **Sync To Prisma** (et répondez au message pour continuer). Répétez l'opération pour chaque périphérique de branche.

> *Une fois la synchronisation avec Prisma réussie, vous verrez les paramètres de configuration de Prisma Access sur le pare-feu de la succursale SD-WAN. Si ce n'est pas le cas, attendez environ 15 minutes et répétez la synchronisation avec Prisma. Si nécessaire, rendez-vous sur le plugin Prisma Access et vérifiez que l'intégration CN est terminée (vous pouvez voir le CN avec la bande passante et les adresses IP attribuées). Après cette vérification, réessayez de synchroniser avec Prisma.*



STEP 7 | Cliquez sur **Commit (Valider)** pour valider sur Panorama.

STEP 8 | **Push to Devices (Poussez vers les périphériques**) pour effectuer une poussée vers le pare-feu de la succursale locale. **Modifiez les sélections** pour sélectionner la sélection de l'étendue Push. Sélectionnez le **modèle** et le **groupe d'appareils** appropriés.

STEP 9 | Sur le pare-feu de la succursale, sélectionnez **Network (Réseau)** > **Interfaces** > **SD-WAN** et affichez la nouvelle interface créée avec la balise Link que vous avez créée, affectée à la zone de sécurité nommée **zone-to-pa-hub** et avec le tunnel IPSec se connectant au CN.

STEP 10 | Sélectionnez **Network** > **Tunnels IPSec** réseau et vérifiez que le tunnel IPSec est actif.

STEP 11 | Sélectionnez **Network (Réseau)** > **Network Profiles (Profiles de réseau)** > **IKE Gateways (Passerelles IKE)** et vérifiez que la passerelle IKE est active.

STEP 12 | Créez une règle de stratégie SD-WAN pour générer des données de surveillance.

Cette étape est nécessaire pour établir les données de base de la latence, de la gigue et de la perte de paquets de Prisma Access Hub pour une distribution précise du trafic. Les données de surveillance SD-WAN sont générées à partir du trafic qui correspond à vos règles de stratégie SD-WAN.

1. Créer un Traffic Distribution Profile (profil de distribution du trafic).
2. Créer un Path Quality Profile (Profil de qualité du chemin d'accès) avec des seuils élevés de latence, de gigue et de perte de paquets.

   Un profil de qualité de chemin est nécessaire pour créer une règle de politique SD-WAN. La création d'un profil de qualité de chemin avec des seuils élevés vous permet de définir la latence, la gigue et la perte de paquets de base pour le hub Prisma Access sans que l'application passe à un autre lien.
3. Configurer une Règle de politique SD-WAN.

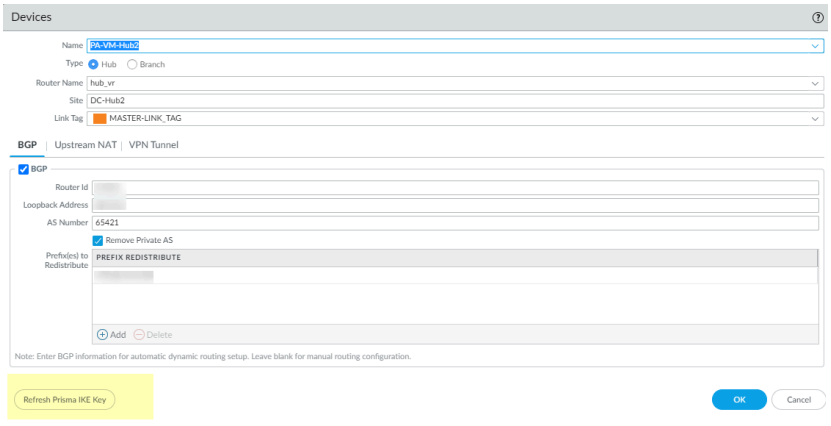
STEP 13 | **Commit (Validez)** et **Commit and Push (Validez et Appliquez)** vers les pare-feux de branche.

STEP 14 | (Uniquement si vous activez le type d'authentification par **Pre Shared Key (Clef pré-partagée)**) Actualisez la clef pré-partagée Prisma IKE.

Si vous devez modifier la clef Prisma IKE actuelle utilisée pour sécuriser la connexion IPSec entre la branche et le hub Prisma, effectuez cette étape pour générer de manière aléatoire une nouvelle clef pour le tunnel et mettre à jour les deux côtés du tunnel. Effectuez cette étape lorsque le hub et la branche ne sont pas occupés.

Ne créez pas manuellement une passerelle IKE avec un nom commençant par « gw_ », car ces noms sont réservés à la création IKE de Prisma lors de l'intégration. Cette étape d'actualisation de la clef prépartagée Prisma IKE actualise toutes les passerelles IKE nommées, s'il en existe en dehors de celles créées par Prisma Access.

1. Sélectionnez **Panorama** > **SD-WAN** > **Devices (Périphériques)** et sélectionnez un périphérique.
2. Au bas de l'écran, sélectionnez **Refresh IKE key** (Actualiser la clé IKE).



3. Un message s'affiche pour vous informer que `l'actualisation de la clé IKE mettra à jour tous les tunnels SD-WAN entre la succursale et le hub Prisma Access et nécessitera une poussée de configuration`

`simultanée vers tous les périphériques de la branche et du hub Prisma Access. Il est recommandé d'effectuer l'actualisation pendant une fenêtre de maintenance, car le trafic peut être affecté. Souhaitez-vous continuer?` Sélectionnez `Oui` si vous souhaitez continuer.

STEP 15 | **Commit (Validez)** et **Commit and Push (Validez et Appliquez)** vers les pare-feux de branche.

STEP 16 | Surveillez les performances des applications Prisma Access Hub et des liens pour comprendre la latence de base, la gigue et la perte de paquets pour les liens vers Prisma Access.

Cette étape est nécessaire pour collecter des données précises sur la latence, la gigue et la perte de paquets afin d'affiner vos profils de qualité du chemin d'accès du hub Prisma Access.

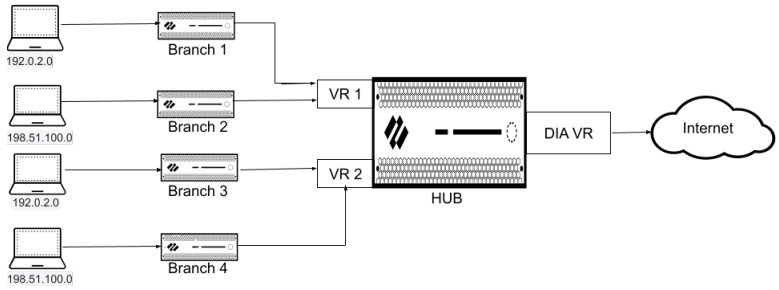
Configurer des routeurs virtuels multiples sur le hub SD-WAN

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS • SD-WAN	❑ SD-WAN plugin license

(PAN-OS 11.1.3 et versions ultérieures, et le plug-in SD-WAN 3.2.1 et versions ultérieures) Nous avons introduit une prise en charge pour les routeurs virtuels multiples sur le hub SD-WAN qui vous permettent d'avoir des adresses de sous-réseau IP qui se chevauchent sur les périphériques de branche qui se connectent au même hub SD-WAN. Cette fonctionnalité vous permet de disposer de plusieurs domaines de routage logique avec des sous-réseaux qui se chevauchent. Lorsque vous activez cette fonctionnalité, le hub SD-WAN prend en charge les sous-réseaux qui se chevauchent uniquement si ceux-ci se trouvent dans des routeurs virtuels différents.

Par défaut, les routeurs virtuels multiples d'un hub SD-WAN sont désactivés.

La figure suivante illustre un hub SD-WAN avec deux routeurs virtuels. En activant **la prise en charge de routeurs virtuels multiples** sur le hub SD-WAN, les quatre branches connectant au même hub SD-WAN peuvent avoir des sous-réseaux IP qui se chevauchent ou appartenir à des entités différentes et fonctionner de manière indépendante, car leur trafic est dirigé vers des routeurs virtuels différents.



La fonctionnalité de routeur virtuel multiple est prise en charge à la fois sur le pare-feu du hub SD-WAN ainsi que sur le hub Prisma Access. Vous pouvez intégrer Prisma Access en tant que hub depuis la branche, lorsque celle-ci est connectée à un hub sur site où la fonctionnalité de routeur virtuel multiple est activée.

Configurez des routeurs virtuels multiples tout en ajoutant un pare-feu de hub SD-WAN (**Panorama** > **SD-WAN** > **Devices (Périphériques)**).

L'importation de la configuration associée aux routeurs virtuels multiples à l'aide d'un fichier CSV lors de l'importation du périphérique SD-WAN n'est pas prise en charge.

Nous prenons en charge le routage avancé lorsque les routeurs virtuels multiples sur le hub SD-WAN sont activés.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Sélectionnez **Panorama** > **SD-WAN** > **Devices (Périphériques)** et **Add (Ajouter)** un nouveau pare-feu SD-WAN.

Lors de la création d'un modèle de hub, ajoutez tous les routeurs virtuels participant au hub SD-WAN dans lesquels le routeur virtuel multiple sera activé. Vous devez effectuer cette opération avant d'ajouter le périphérique SD-WAN à l'aide du plug-in SD-WAN. Lors de la création du modèle de hub, vérifiez que le nom du routeur virtuel de la branche correspond à l'un des routeurs virtuels du hub.

STEP 3 | Pour configurer des routeurs virtuels multiples sur le hub SD-WAN :

- Sélectionnez le **Type** de périphérique SD-WAN comme étant **Hub**.
- Sélectionnez **Enable Multi-VR Support (Activer la prise en charge multi-VR)**.

Le routeur virtuel sélectionné pour le **Virtual Router Name (Nom du routeur virtuel)** est utilisé comme routeur virtuel d'accès Internet direct (DIA) de hub et considéré comme le routeur virtuel par défaut. La configuration spécifiée sous l'onglet **BGP** doit être spécifique au routeur virtuel DIA.

- *Nous ne prenons pas en charge la FEC et la duplication de paquets lors de l'activation de la fonctionnalité de routeurs virtuels multiples sur le hub SD-WAN.*
- *La fonctionnalité de routeurs virtuels multiples sur le hub SD-WAN est prise en charge uniquement dans une topologie hub-spoke (et n'est pas prise en charge dans une topologie de maillage complet).*
- *Pour traiter le trafic Internet sur le hub SD-WAN, la politique SD-WAN doit s'assurer que la balise MPLS n'est sélectionnée que lorsque le lien MPLS dispose d'un accès Internet et d'un NAT.*
- *PAN-OS ne prend pas en charge le transfert du trafic de texte en clair (lorsque **VPN Data Tunnel Support (la prise en charge du tunnel de données VPN)** est désactivée sur le **SD-WAN Interface Profile (Profil d'interface SD-WAN)**) à l'extérieur du tunnel VPN SD-WAN lorsque la prise en charge des routeurs virtuels multiples sur la fonctionnalité du hub SD-WAN est activée.*

Le nombre de routeurs virtuels pris en charge sur les pare-feu Palo Alto Networks est comme suit :

Pare-feu Palo Alto Networks	Nombre maximal de routeurs virtuels pris en charge	Nombre maximal de routeurs virtuels de hub SD-WAN pris en charge
PA-3400	11	10
PA-5220 et PA-5410	20	20

Pare-feu Palo Alto Networks	Nombre maximal de routeurs virtuels pris en charge	Nombre maximal de routeurs virtuels de hub SD-WAN pris en charge
PA-5250 et PA-5430	125	50
PA-5420	50	20
PA-5260, PA-5280, PA-5400, PA-5440, PA-5445, et PA-7000.	225	50

STEP 4 | (Facultatif) Configurez les routeurs virtuels.

1. Sélectionnez l'onglet **Virtual Routers (Routeurs virtuels)** pour configurer plusieurs routeurs virtuels pour le hub SD-WAN.
2. Le routage BGP utilise IPv4 par défaut ; par conséquent, **Enable IPv4 BGP Support (Activer la prise en charge BGP pour IPv4)** est activé et vous ne pouvez pas modifier cette configuration.
3. Saisissez le nom du **Virtual Router (routeur virtuel)**.
4. Sélectionnez une **Zone** déjà créée dans le modèle de hub (**Network (Réseau)** > **Zones**) approprié au routeur virtuel que vous configurez.

   *Si vous configurez la même zone pour deux ou plusieurs routeurs virtuels dans la **Multi-VR Configuration (Configuration Multi-VR)**, vérifiez que les routeurs virtuels ne sont pas configurés avec des sous-réseaux qui se chevauchent.*
5. (Facultatif) Saisissez le **Router ID (ID de routeur)** virtuel qui doit être unique parmi les autres routeurs.
6. Spécifiez une **Loopback Adress** (adresse de bouclage) statique IPv4 pour les homologues BGP. La configuration Auto VPN crée automatiquement une interface de bouclage avec la même adresse IPv4 que vous spécifiez. Si vous spécifiez une adresse de bouclage existante, la validation échouera et vous devez donc spécifiez une adresse IPv4 qui n'est pas déjà une adresse de bouclage.
7. Saisissez le **AS Number** (Numéro AS). Le numéro de système autonome spécifie une politique, règle, mesures d'itinéraire définie pour internet. Le numéro AS doit être unique pour chaque emplacement de hub et branche.
8. Désactivez l'option **Remove Private AS (Supprimer l'AS privé)** (la valeur par défaut est activée) si vous avez des points de terminaison qui doivent échanger des routes avec un pare-feu de concentrateur ou de branche dans une topologie SD-WAN BGP et que vous ne souhaitez donc pas supprimer les numéros d'AS privés (64512 à 65534) à partir de

l'attribut AS_PATH dans les mises à jour BGP. Dans ce cas, vous souhaitez autoriser les numéros d'AS privés à quitter l'AS privé SD-WAN dans les mises à jour BGP.

*Le paramètre **Remove Private AS (Supprimer AS privé)** s'applique à tous les groupes d'homologues BGP sur le pare-feu de la succursale ou du concentrateur. Si vous avez besoin que ce paramètre diffère entre les groupes de pairs ou les pairs BGP, vous devez configurer le paramètre en dehors du plug-in SD-WAN.*

*Si vous modifiez le paramètre **Remove Private AS (Supprimer AS privé)**, que vous validez tous les nœuds du cluster SD-WAN, puis que vous rétrogradez à une version du plug-in SD-WAN antérieure à 2.0.2, toute la configuration liée à **Remove Private AS (Supprimer AS privé)** doit être effectuée à l'extérieur du plug-in SD-WAN ou directement sur les pare-feu.*

9. Saisissez **Prefix(es) to Redistribute** (Préfixes à redistribuer). Sur un périphérique de hub, vous devez saisir au moins un préfixe à redistribuer.
10. Cliquez sur **OK**.
11. Cliquez sur **Add (Ajouter)** en bas de l'onglet **Virtual Routers (Routeurs virtuels)** pour ajouter d'autres routeurs virtuels.

Configurer des routeurs virtuels multiples sur la branche SD-WAN

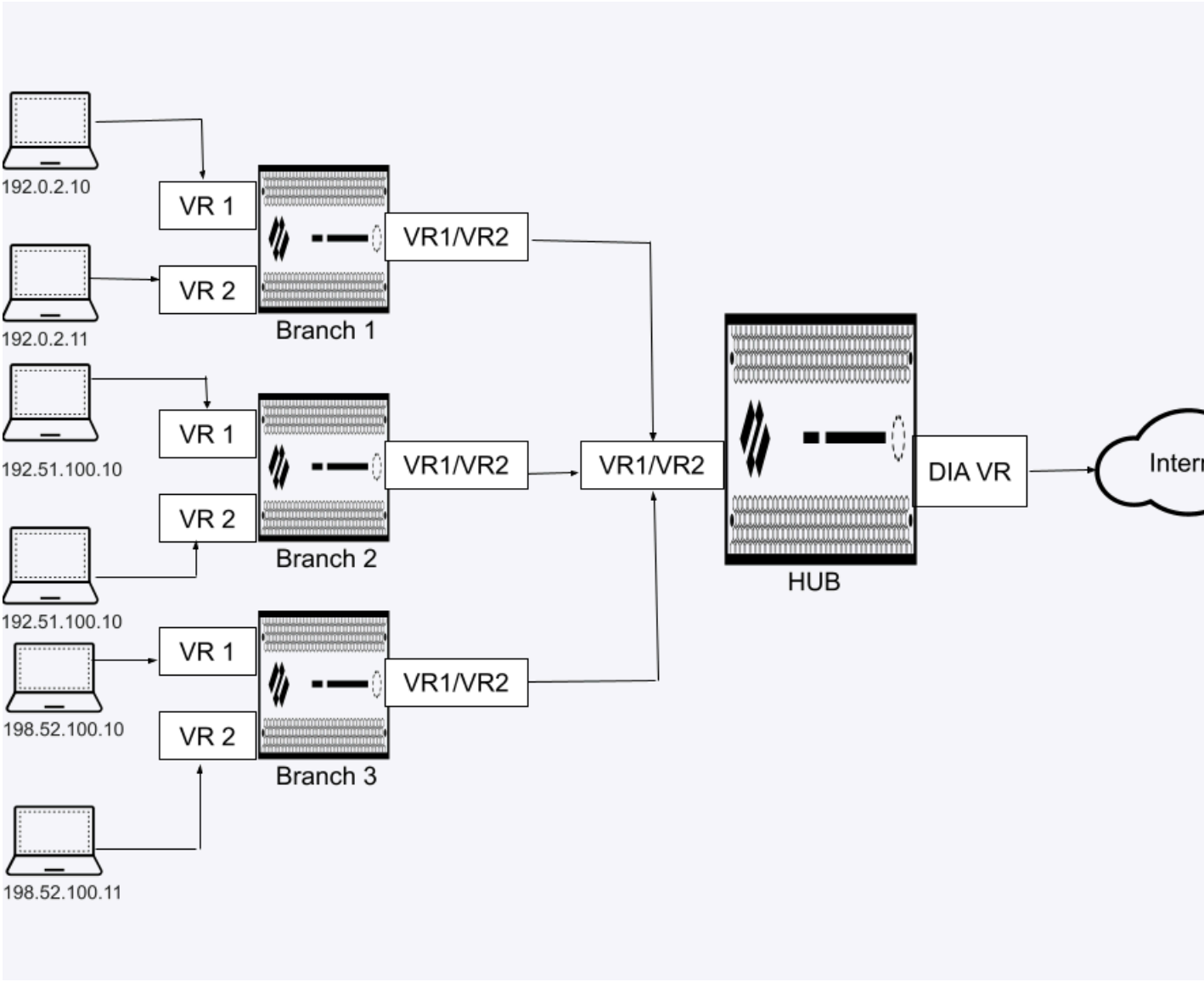
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS • SD-WAN	❑ SD-WAN plugin license

(PAN-OS 11.2.3 et version 11.2 ultérieure et le plug-in SD-WAN 3.3.1 et versions 3.3 ultérieures) Nous avons introduit une prise en charge des routeurs virtuels multiples sur les branches SD-WAN pour avoir des adresses de sous-réseau IP qui se chevauchent sur les périphériques du hub et de la branche. Cette fonctionnalité vous permet de disposer de plusieurs domaines de routage logique avec des sous-réseaux qui se chevauchent.

Vérifiez les points suivants avant d'activer les routeurs virtuels multiples sur les périphériques de branche SD-WAN :

- Le périphérique de hub auquel les branches sont connectées doit prendre en charge des routeurs virtuels multiples.
- Les périphériques de hub auxquels les branches sont connectées doivent disposer de tous les routeurs virtuels présents dans les périphériques de branche.
- Dans un cluster VPN, pour que les branches prennent en charge plusieurs routeurs virtuels, vous devez d'abord activer la prise en charge de routeurs virtuels multiples sur tous les hubs.

La figure suivante illustre trois branches SD-WAN, chacune étant configurée avec un ou plusieurs routeurs virtuels. En activant **la prise en charge de routeurs virtuels multiples** sur les branches SD-WAN, les trois branches connectant au même hub SD-WAN peuvent avoir des sous-réseaux IP qui se chevauchent ou appartenir à des entités différentes et fonctionner de manière indépendante, car leur trafic est dirigé vers des routeurs virtuels différents.



STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Sélectionnez **Panorama** > **SD-WAN** > **Devices (Périphériques)** et **Add (Ajouter)** un nouveau pare-feu SD-WAN.

STEP 3 | Pour configurer des routeurs virtuels multiples sur le périphérique de branche SD-WAN :

- Sélectionnez le **Type** de périphérique SD-WAN comme **Branch (Branche)**.
- Sélectionnez **Enable Multi-VR Support (Activer la prise en charge multi-VR)**.

Le routeur virtuel sélectionné pour le **Virtual Router Name (Nom du routeur virtuel)** est utilisé comme routeur virtuel d'accès Internet direct (DIA) de branche et considéré comme le routeur

virtuel par défaut. La configuration spécifiée sous l'onglet **BGP** doit être spécifique au routeur virtuel DIA.

- *Nous ne prenons pas en charge la FEC et la duplication de paquets lors de l'activation de la fonctionnalité de routeurs virtuels multiples sur la branche SD-WAN.*
- *La fonctionnalité de routeurs virtuels multiples sur la branche SD-WAN est prise en charge uniquement dans une topologie hub-spoke (et n'est pas prise en charge dans une topologie de maillage complet).*
- *Pour traiter le trafic Internet sur la branche SD-WAN, la politique SD-WAN doit s'assurer que la balise MPLS n'est sélectionnée que lorsque le lien MPLS dispose d'un accès Internet et d'un NAT.*
- *PAN-OS ne prend pas en charge le transfert du trafic de texte en clair (lorsque **VPN Data Tunnel Support (la prise en charge du tunnel de données VPN)** est désactivée sur le **SD-WAN Interface Profile (Profil d'interface SD-WAN)**) à l'extérieur du tunnel VPN SD-WAN lorsque la prise en charge des routeurs virtuels multiples sur la fonctionnalité de la branche SD-WAN est activée.*

Un maximum de 20 routeurs virtuels sont pris en charge sur le périphérique de la branche SD-WAN. Cependant, le nombre de routeurs virtuels pris en charge sur la branche SD-WAN varie selon la plateforme :

Pare-feu Palo Alto Networks	Nombre maximal de routeurs virtuels pris en charge	Nombre maximal de routeurs virtuels de branche SD-WAN pris en charge
PA-460	5	5
PA-450	5	5
PA-445	3	3
PA-440	3	3
PA-415	3	3
PA-1420	10	10
PA-1410	10	10
PA-850	5	5

Pare-feu Palo Alto Networks	Nombre maximal de routeurs virtuels pris en charge	Nombre maximal de routeurs virtuels de branche SD-WAN pris en charge
PA-820	5	5
PA-3200	10	10

STEP 4 | (Facultatif) Configurez les routeurs virtuels.

1. Sélectionnez l'onglet **Virtual Routers (Routeurs virtuels)** pour configurer plusieurs routeurs virtuels pour la branche SD-WAN.
2. Le routage BGP utilise IPv4 par défaut ; par conséquent, **Enable IPv4 BGP Support (Activer la prise en charge BGP pour IPv4)** est activé et vous ne pouvez pas modifier cette configuration.
3. Saisissez le nom du **Virtual Router (routeur virtuel)**.
4. Sélectionnez une zone unique pour le routeur virtuel.

   Dans un cluster VPN avec une configuration de routeurs virtuels multiples, chaque périphérique (branche ou hub) doté d'un routeur virtuel qui participe à la configuration de routeurs virtuels multiples doit avoir une zone unique.
5. (Facultatif) Saisissez le **Router ID (ID de routeur)** virtuel qui doit être unique parmi les autres routeurs.
6. Spécifiez une **Loopback Adress** (adresse de bouclage) statique IPv4 pour les homologues BGP. La configuration Auto VPN crée automatiquement une interface de bouclage avec la même adresse IPv4 que vous spécifiez. Si vous spécifiez une adresse de bouclage existante, la validation échouera et vous devez donc spécifiez une adresse IPv4 qui n'est pas déjà une adresse de bouclage.
7. Saisissez le **AS Number** (Numéro AS). Le numéro de système autonome spécifie une politique, règle, mesures d'itinéraire définie pour internet. Le numéro AS doit être unique pour chaque emplacement de hub et branche.
8. Désactivez l'option **Remove Private AS (Supprimer l'AS privé)** (la valeur par défaut est activée) si vous avez des points de terminaison qui doivent échanger des routes avec un pare-feu de concentrateur ou de branche dans une topologie SD-WAN BGP et que vous ne souhaitez donc pas supprimer les numéros d'AS privés (64512 à 65534) à partir de

l'attribut AS_PATH dans les mises à jour BGP. Dans ce cas, vous souhaitez autoriser les numéros d'AS privés à quitter l'AS privé SD-WAN dans les mises à jour BGP.

*Le paramètre **Remove Private AS (Supprimer AS privé)** s'applique à tous les groupes d'homologues BGP sur le pare-feu de la succursale ou du concentrateur. Si vous avez besoin que ce paramètre diffère entre les groupes de pairs ou les pairs BGP, vous devez configurer le paramètre en dehors du plug-in SD-WAN.*

*Si vous modifiez le paramètre **Remove Private AS (Supprimer AS privé)**, que vous validez tous les nœuds du cluster SD-WAN, puis que vous rétrogradez à une version du plug-in SD-WAN antérieure à 2.0.2, toute la configuration liée à **Remove Private AS (Supprimer AS privé)** doit être effectuée à l'extérieur du plug-in SD-WAN ou directement sur les pare-feu.*

9. Saisissez **Prefix(es) to Redistribute** (Préfixes à redistribuer). Sur un périphérique de hub, vous devez saisir au moins un préfixe à redistribuer.
10. Cliquez sur **OK**.
11. Cliquez sur **Add (Ajouter)** en bas de l'onglet **Virtual Routers (Routeurs virtuels)** pour ajouter d'autres routeurs virtuels.

Configurer les Périphérique HA pour SD-WAN

Vous pouvez configurer deux pare-feu en tant que branche en mode HA actif/passif (ou deux pare-feu en tant que hub en mode HA actif/passif) pour faire partie de votre environnement SD-WAN. Dans ce cas, Panorama™ a besoin d'appliquer la même configuration à l'homologue actif et à l'homologue passif, plutôt que de traiter deux pare-feux de façon individuelle. Pour faire cela, vous configurez la HA active/passive avant d'ajouter les périphériques pour SD-WAN afin que Panorama soit conscient que les périphériques sont des homologues HA et applique la même configuration à ceux-ci. (Seul le mode actif/passif HA est pris en charge.)

Lisez la procédure suivante avant de commencer afin de ne pas Valider après avoir ajouté les homologues HA en tant que périphériques SD-WAN.

Dans HA, le pare-feu ne synchronise pas les statistiques de distribution de session SD-WAN. Après un basculement HA, les statistiques de distribution de session affichent uniquement les statistiques des nouvelles sessions ; Les statistiques des sessions existantes sont perdues.

STEP 1 | Avant d'activer SD-WAN sur vos homologues HA, configure Active/Passive HA (configurez la HA active/passive) sur deux modèles de pare-feu compatibles SD-WAN.

STEP 2 | Ajoutez les homologues HA en tant que SD-WAN devices (périphériques SD-WAN), **mais n'effectuez pas la dernière étape pour Valider**.

STEP 3 | Sur Panorama, sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** > **Summary (Récapitulatif)**.

STEP 4 | Au bas de l'écran, sélectionnez **Group HA Peers** (Regrouper les homologues HA). Confirmez cela sous l'affichage de État, la colonne État HA inclut les deux pare-feux, un Actif et un Passif. Panorama connait l'état HA et appliquera la même configuration SD-WAN aux deux homologues HA lorsque vous validerez.

STEP 5 | Cliquez sur **OK** et sur **Commit and Push (Valider et appliquer)**.

Créer un cluster VPN

Dans votre configuration SD-WAN, vous devez configurer un ou plusieurs clusters VPN afin de déterminer quelles branches communiquent avec quelles hubs et créer une connexion sécurisée entre les périphériques de la branche et du hub. Les clusters VPN sont des regroupements logiques de périphériques et vous devez donc tenir compte de facteurs tels que l'emplacement géographique ou la fonction lorsque vous regroupez vos périphériques de façon logique.

PAN-OS® prend en charge les topologies VPN SD-WAN en étoile et en maillage complet. Dans la topologie Hub-Spoke, une plateforme de pare-feu centralisée dans un bureau ou un emplacement principal agit comme portail entre les périphériques de la branche. La connexion de hub à branche est un tunnel VPN. Dans cette configuration, le trafic entre les branches doit passer par le hub

La première fois que vous Configurer une Interface virtuelle SD-WAN avec des liens d'accès internet direct (DIA) pour un pare-feu de hub ou branche SD-WAN, un cluster VPN appelé `autogen_hubs_cluster` est automatiquement créé et le pare-feu SD-WAN est automatiquement ajouté au cluster VPN. Cela permet au serveur de gestion Panorama™ de Surveiller la Performance des applications et des liens SD-WAN pour les périphériques qui sont protégés par le pare-feu SD-WAN et qui accède à des ressources en dehors de votre réseau d'entreprise. De plus, tout pare-feu SD-WAN avec des liens DIA que vous configurerez à l'avenir est ajouté automatiquement au cluster VPN`autogen_hubs_cluster` contenant toutes les hubs et branches ayant des liens DIA pour permettre à Panorama de surveiller la performance des applications et des liens. Le `autogen_hubs_cluster` sert uniquement à la surveillance du bon état des applications et des liens, et non pour créer des tunnels VPN entre les hubs et les branches avec des liens DIA. Si vous avez besoin de connecter les hubs et les branches avec des tunnels VPN, vous devez créer un cluster VPN et ajouter toutes les hubs et branches nécessaires à ce cluster.

Lorsque vous sélectionnez **Pre-shared key (Clef pré-partagée)** comme **Authentication Type (Type d'authentification)**, une clef pré-partagée IKE aléatoire et solide est créée pour tous les hubs et toutes les branches du cluster VPN afin de sécuriser les tunnels VPN et chaque pare-feu a une clé principale qui crypte la clef pré-partagée. Le système sécurise la clé préalablement partagée, même de l'administrateur. Vous pouvez actualiser la clé préalablement partagée IKE que Panorama envoie à tous les membres du cluster.

Actualisez la clef pré-partagée lorsque les membres du cluster ne sont pas occupés.

Lorsque vous sélectionnez **Certificate (Certificat)** comme **Authentication Type (Type d'authentification)**, les hubs et branches du cluster VPN SD-WAN sont basés sur l'authentification basée sur le certificat.

Une fois le plug-in SD-WAN mis à niveau vers la version 2.1.0, les pare-feu de concentrateur et de succursale d'un même cluster VPN doivent tous exécuter PAN-OS 10.0.4 (ou une version 10.0) ou 10.1.0, et non une combinaison des deux versions.

Lors de l'affichage des clusters VPN, si aucune donnée n'est présente ou si l'écran indique que SD-WAN n'est pas défini, vérifiez dans la matrice de compatibilité que la version Panorama que vous utilisez prend en charge la version du plug-in SD-WAN que vous essayez d'utiliser.

Si un tunnel IPv4 ou IPv6 IPSec se forme entre deux ports Ethernet (ou sous-interface ou interface AE) (lien DIA) dépend si l'interface Ethernet (ou sous-interface ou interface AE) a une adresse IPv4 ou IPv6. Si les deux interfaces ont une adresse IPv4, un tunnel IPv4 apparaît. Si les deux interfaces ont une adresse IPv6, un tunnel IPv6 apparaît. Dans le cas d'une double pile, un tunnel IPv4 apparaît.

L'adresse IP de l'interface tunnel provient du pool VPN. Vous pouvez créer un pool d'adresses IPv6 indépendant d'un pool d'adresses IPv4. Si les adresses IPv4 et IPv6 sont configurées, l'interface tunnel se voit attribuer une adresse IPv4 uniquement, comme indiqué dans le tableau suivant. Si le pool d'adresses VPN IPv4 est épuisé et qu'un pool d'adresses IPv6 existe, l'interface tunnel se voit attribuer une adresse IPv6. Si seul IPv4 est configuré, le tunnel utilisera une adresse IPv4. Si seul IPv6 est configuré, le tunnel utilisera une adresse IPv6.

Pool VPN	Configuré		
IPv4	Oui	Oui	Non
IPv6	Oui	Non	Oui
IP de l'interface de tunnel	IPv4 uniquement	IPv4 uniquement	IPv6 uniquement

STEP 1 | Planifiez votre topologie VPN de hub et branche afin de déterminer quelles branches communiquent avec chacune de vos hubs. Pour plus d'informations, consultez Planifiez votre configuration SD-WAN.

STEP 2 | Connectez-vous à l'interface Web Panorama.

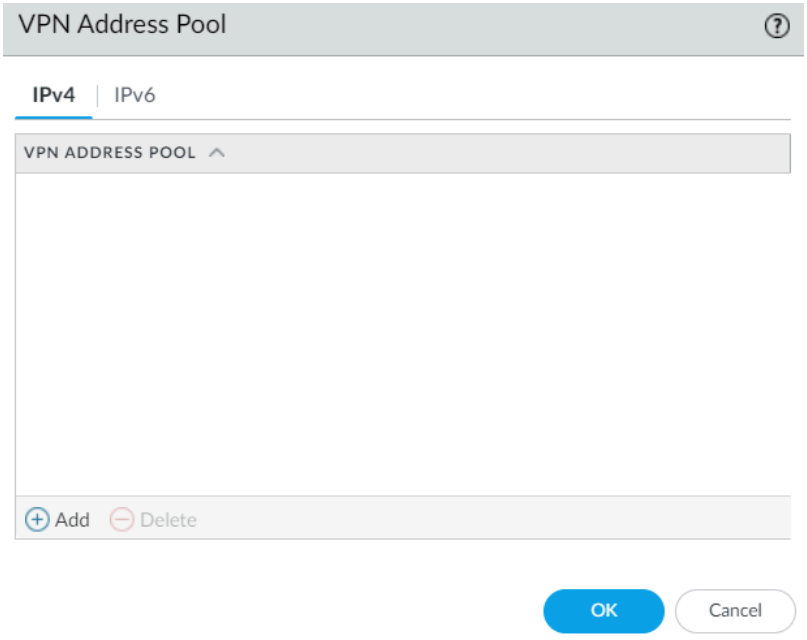
STEP 3 | Spécifiez les plages d'adresses IP pour les tunnels VPN IPSec que la configuration Auto VPN crée.

La configuration Auto VPN crée un tunnel VPN entre un hub et des branches et attribue les adresses IP aux terminaux du tunnel. Saisissez les plages de sous-réseaux que vous souhaitez que Auto VPN utilise comme adresses de tunnel VPN. Vous pouvez saisir jusqu'à 20 plages de préfixes/masques réseau IP. Auto VPN choisit dans ce pool des adresses de tunnel VPN, en choisissant en premier dans la première plus grande plage (pour la famille d'adresses), puis dans la deuxième plage la plus grande, si nécessaire. Vous devez configurer au moins une fourchette pour le réservoir. Si vous n'effectuez pas cette étape avant d'appliquer la configuration à un hub ou une branche, la Validation et l'Application échoueront.

Si vous améliorez depuis une version du plug-in SD-WAN antérieure, vous devez vérifier que vos fourchettes sont toujours correctes. Si elles ne le sont pas, saisissez de nouvelles plages. Après avoir cliqué sur ***Commit*** *(Valider), tous les tunnels sont abandonnés et de nouveaux tunnels sont utilisés, alors réalisez cette tâche à un moment où le trafic est faible.*

1. Sélectionnez **Panorama** > **SD-WAN** > **VPN Clusters (Clusters VPN)**.
2. Au bas de l'écran, sélectionnez **VPN Address Pool** (réservoir d'adresses VPN).

3. Sélectionnez **IPv4** ou **IPv6** et **Add (Ajouter)** un pool d'adresses avec une ou plusieurs (jusqu'à 20) plages d'adresses IP **Members (Membres)** et de masques réseau, par exemple, 192.168.0.0/16 ou 2001::/16, respectivement.
4. Cliquez sur **OK**.



Ne modifiez pas un pool d'adresses existant simplement si Prisma Access est intégré. Si vous devez modifier un pool d'adresses, procédez comme suit pendant une fenêtre de maintenance pour mettre à jour la succursale et le CN Prisma Access avec vos modifications de pool d'adresses :

1. *Utilisez Panorama pour accéder à une branche SD-WAN et supprimez l'intégration existante sur laquelle le changement de pool d'adresses aura un impact ; puis faites un Commit local.*
2. *Mettez à jour le pool d'adresses VPN, puis effectuez une validation locale.*
3. *Effectuez à nouveau l'intégration de Prisma Access, puis effectuez une validation et une diffusion locales.*

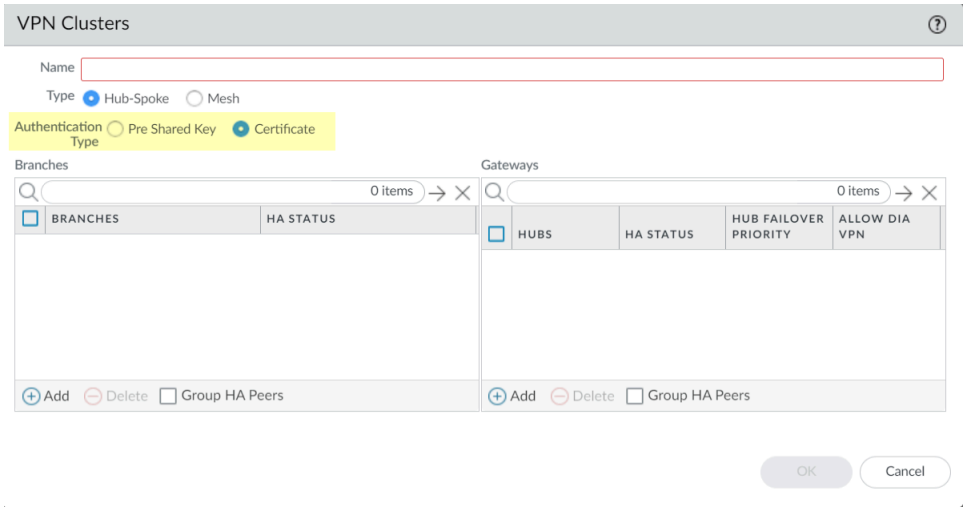
STEP 4 | Configurez le cluster VPN. Répétez cette étape pour créer des clusters VPN en fonction des besoins.

1. Sélectionnez **Panorama** > **SD-WAN** > **VPN Clusters (Clusters VPN)** et **Add (Ajouter)** un cluster VPN.
2. Saisissez un Name (Nom) descriptif pour le cluster VPN.

   *Les tirets bas et les espaces ne sont pas admis dans le nom du cluster VPN et ont pour conséquence que les données de surveillance (**Panorama** > **SD-WAN** > **Monitoring (Surveillance)**) du cluster ne s'affichent pas. Choisissez le nom du cluster VPN avec soin afin de ne pas avoir besoin de le modifier à l'avenir. Le monitoring (surveillance) SD-WAN des données est généré sur la base de l'ancien nom du cluster et ne peut pas être rapproché du nouveau nom du cluster et créera des problèmes avec le nombre de clusters indiqué lors de la surveillance de vos clusters VPN ou la génération de rapports.*
3. Sélectionnez le **Type** de cluster VPN.

   *Seul le type de cluster VPN **Hub-Spoke** est compatible avec PAN-OS 10.0.2 et les versions 11.0 antérieures. À partir de PAN-OS 10.0.3, vous pouvez* Création d'un cluster VPN Full Mesh avec le service DDNS.
4. (Plug-in SD-WAN 3.2.0 et versions ultérieures) Sélectionnez le **Authentification type (Type d'authentification) : Pre-Shared Key (Clef pré-partagée)** ou **Certificate (Certificat)**. Il est obligatoire de spécifier le type d'authentification pour ajouter un périphérique dans

un cluster VPN. Un cluster VPN doit avoir le même type d'authentification sélectionné pour tous ses périphériques.



Lorsque vous sélectionnez le type d'authentification d'un cluster VPN, vous ne pouvez ajouter au cluster VPN que les branches et hubs configurés avec le même type d'authentification (que le cluster VPN). Par exemple, lorsque vous sélectionnez certificat comme type d'authentification pour un cluster VPN, tous les hubs et branches ajoutés au cluster doivent être configurés avec certificat comme type d'authentification.

Vous ne pouvez pas modifier le type d'authentification ou le nom du cluster VPN d'un cluster VPN qui a déjà été configuré. Pour effectuer une modification, supprimez le cluster VPN et ses périphériques SD-WAN et reconfigurez-le à l'aide du nouveau type d'authentification ou du nouveau nom du cluster VPN. Par défaut, nous prenons en

charge le type d'authentification pré-partagée pour les périphériques d'un cluster VPN (si la méthode du certificat n'est pas sélectionnée manuellement).

- *Si vous avez configuré le cluster VPN, vous ne pouvez pas modifier le nom du cluster ou son type d'authentification (au niveau du cluster et du périphérique).*
- *Vous ne pouvez pas avoir différents types d'authentification au sein d'un seul cluster VPN. Autrement dit, un type d'authentification de cluster VPN doit correspondre à tous les périphériques SD-WAN du cluster VPN. Toute différence entraînerait un échec de la validation.*
- *Vous pouvez avoir différents clusters VPN avec différents types d'authentification configurés.*
- *Dans un cluster VPN, vous ne pouvez pas sélectionner de périphériques SD-WAN avec différents types d'authentification. Si un hub SD-WAN fait partie de deux clusters VPN, les deux clusters doivent être configurés avec le même type d'authentification.*

Si vous souhaitez changer le type d'authentification en **Certificate (Certificat)** pour un cluster VPN existant, supprimez le cluster VPN et créez-le à nouveau avec le type d'authentification de votre choix.

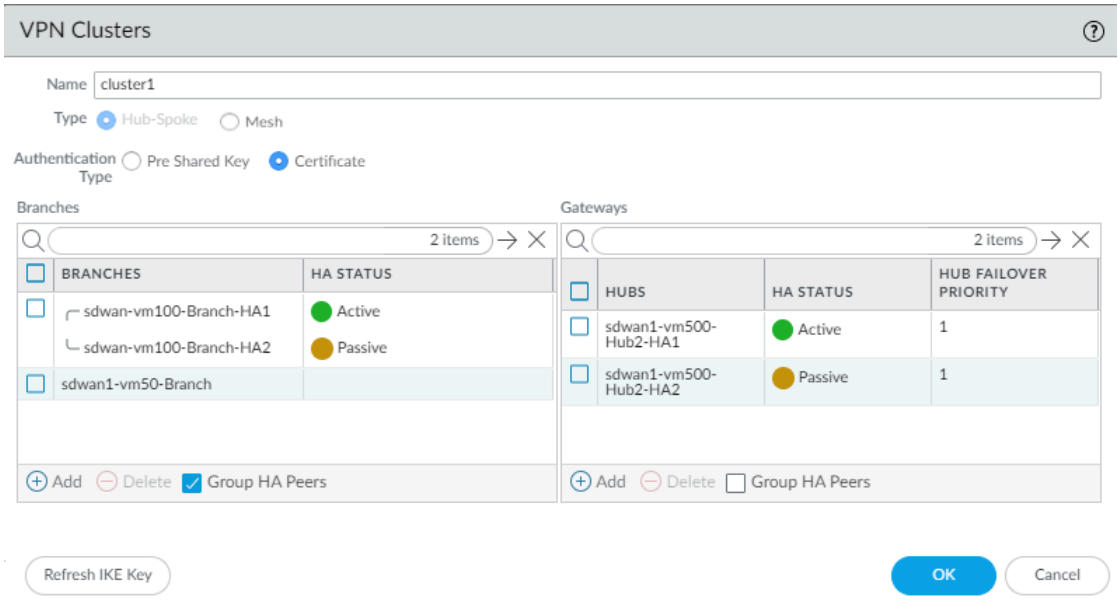
Après avoir créé un cluster VPN avec le type d'authentification de certificat, si vous souhaitez passer à une version de plug-in PAN-OS ou SD-WAN ne prenant pas en charge le type d'authentification de certificat, procédez comme suit :

- Supprimez le cluster VPN existant. L'authentification du périphérique SD-WAN passera automatiquement à la clef pré-partagée lors de la rétrogradation.
- Rétrogradez vers la version du plug-in PAN-OS ou SD-WAN de votre préférence. Consultez la configuration requise pour SD-WAN pour connaître les versions

minimales des plug-ins PAN-OS et SD-WAN requises pour la configuration du type d'authentification du certificat.

Suivez les étapes mentionnées dans les Considérations de mise à niveau et de rétrogradation avant de mettre à niveau ou de rétrograder votre plug-in SD-WAN actuel.

5. **Add** (Ajoutez) un ou plusieurs périphériques de branche dont vous déterminez qu'ils ont besoin de communiquer entre eux.
   - Sélectionnez **Group HA Peers (Regrouper les homologues HA)** pour afficher les périphériques de la branche qui sont regroupés en tant qu'homologues HA.



   - Sélectionnez les périphériques de la branche à ajouter au cluster.
   - Cliquez sur **OK**.
6. **Add** (Ajoutez) un ou plusieurs périphériques du hub dont vous déterminez qu'ils ont besoin de communiquer avec les périphériques de la branche.

   Les hubs SD-WAN d'une configuration HA sont considérés comme un seul pare-feu de hub SD-WAN.

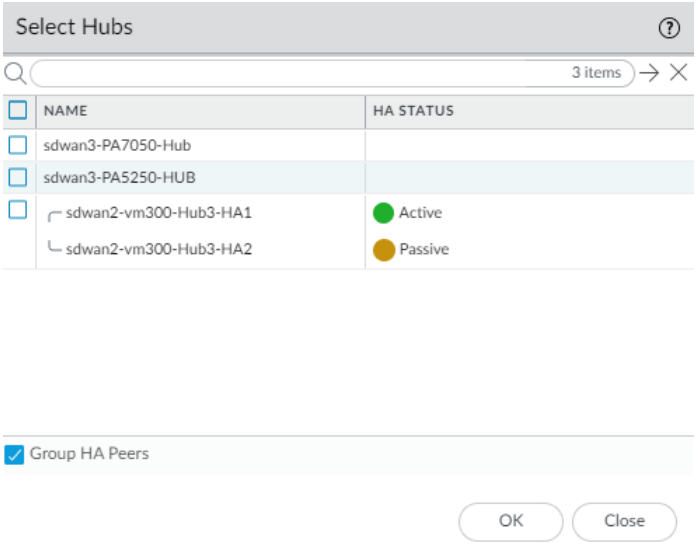
   Les types de liens MPLS et satellite formeront des tunnels avec uniquement le même type de liens ; par exemple, MPLS-to-MPLS et satellite-to-satellite. Les tunnels ne seront pas créés entre un lien MPLS et un lien Ethernet par exemple.

   Pour les versions SD-WAN antérieures à 3.1.3, vous pouvez ajouter jusqu'à quatre pare-feu SD-WAN hub à un cluster VPN.

   (Plug-in SD-WAN 3.2.1 et versions ultérieures) Vous pouvez ajouter jusqu'à 16 pare-feu SD-WAN hub à un cluster VPN. Seuls quatre des 16 hubs peuvent avoir la même priorité

au sein d'un cluster VPN à cause d'ECMP. Toute tentative de configurer la même priorité pour plus de quatre hubs SD-WAN entraînerait une erreur de validation.

- Sélectionnez **Group HA Peers (Regrouper les homologues HA)** pour afficher les périphériques de la plateforme qui sont regroupés en tant qu'homologues HA.
- Sélectionnez les plateformes à ajouter au cluster, puis cliquez sur **OK**.



- Pour tout cluster VPN, nouveau ou existant, qui possède plus d'une plateforme, vous devez prioriser les plateformes pour déterminer a) que le trafic doit être envoyé à une plateforme donnée et b) l'ordre du basculement des plateformes subséquent. La plage de priorité du basculement des plateformes est de 1 à 4. Si vous procédez à la mise à niveau, la priorité par défaut est définie sur 4. Le plugin interne traduit la priorité de basculement des plateformes en un numéro de préférence local BGP, comme l'illustre la table suivante. Plus la valeur de priorité est faible, plus la priorité et la préférence locale sont élevées. Un cluster prend en charge un maximum de quatre hubs pour les versions SD-WAN antérieures à la version 3.1.3. Avec le plug-in SD-WAN 3.2.1 et versions ultérieures, vous pouvez ajouter jusqu'à 16 pare-feu SD-WAN hub à un cluster VPN. Une paire HA active/passive vaut un hub. Plusieurs plateformes peuvent avoir la même priorité ; une paire HA doit avoir la même priorité. Panorama utilise le modèle BGP de la branche pour appliquer la préférence locale des plateformes par rapport aux branches au sein du cluster.

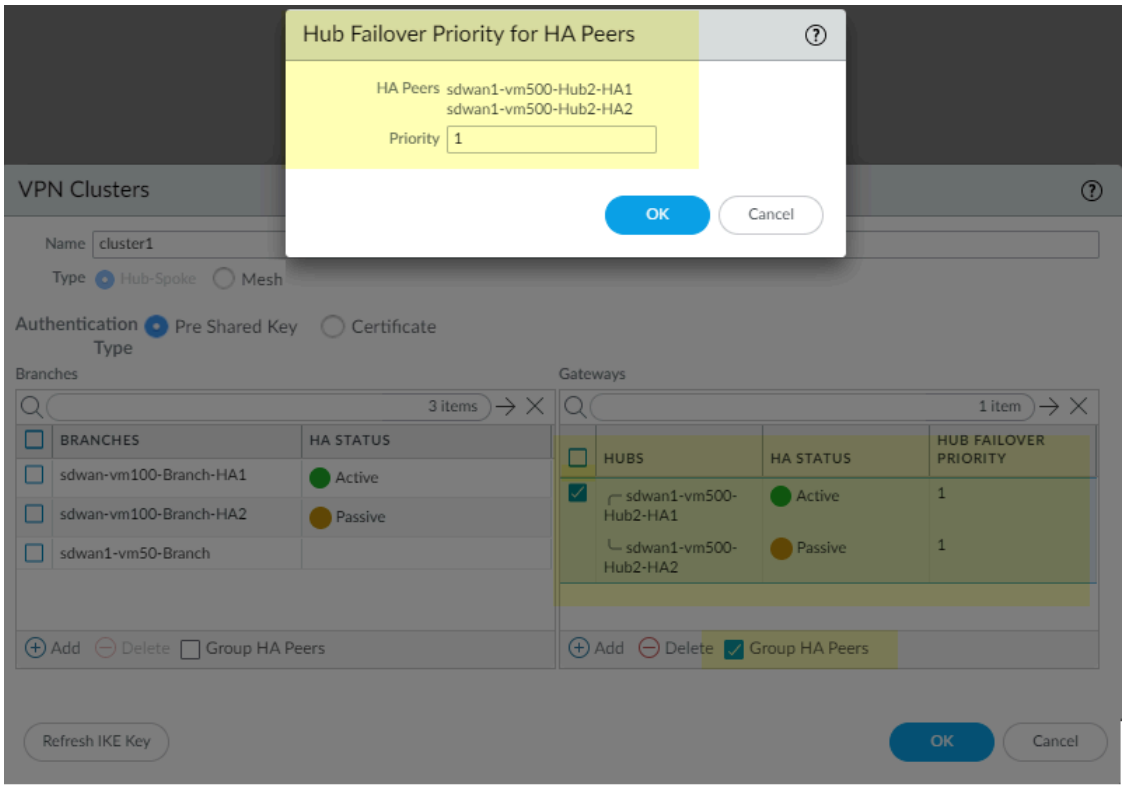
Priorité de basculement de hub	Préférence locale
1	250
2	200
3	150

Priorité de basculement de hub	Préférence locale
4	100

*Si plusieurs hubs ont la même priorité, Panorama active ECMP en deux emplacements sur chaque pare-feu de la branche pour déterminer la façon dont les branches sélectionnent le chemin. ECMP est activé pour le routeur virtuel (**Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** > **ECMP**) et **ECMP Multiple AS Support (Support de multiples AS dans ECMP)** est activé pour BGP (**Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** > **BGP** > **Advanced (Avancé)**). Si toutes les plateformes du cluster possèdent une priorité unique, ECMP est désactivé sur les branches. Si une configuration de priorité de hub est modifiée, Panorama réévalue si ECMP doit être activé ou désactivé.*

- Si vous avez sélectionné **Group HA Peers (Regrouper les homologues HA)**, sélectionnez la paire, puis cliquez dans le champ **Hub Failover Priority (Priorité de**

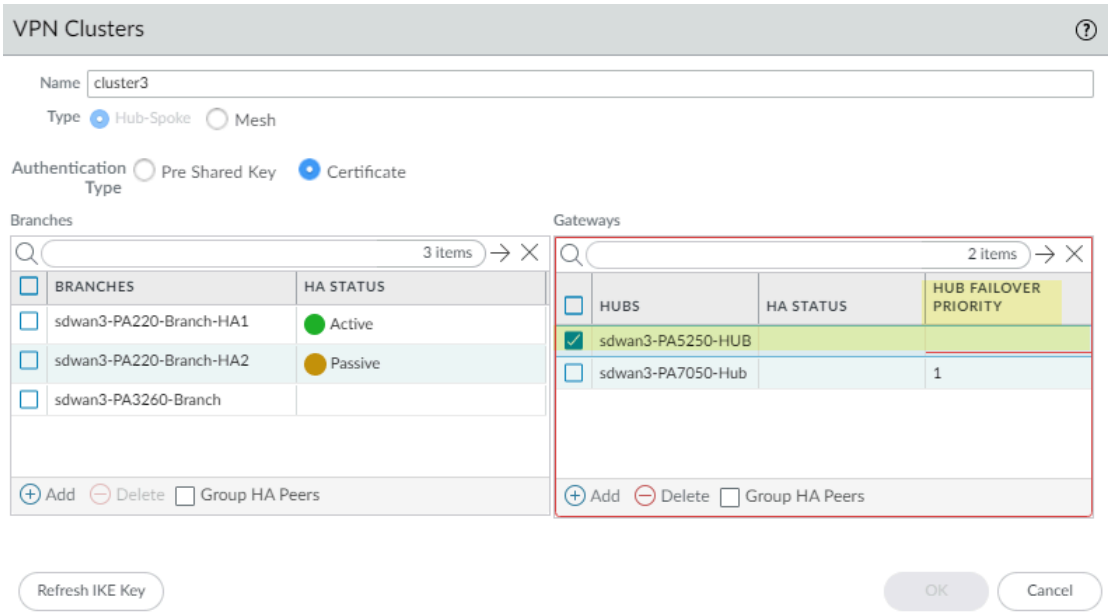
basculement des hubs); saisissez une seule **Priority (Priorité)** (plage entre 1 et 4), qui s'applique aux deux hubs de la paire HA, puis cliquez sur **OK**.



La priorité de basculement des plateformes pour la fenêtre des homologues HA apparaît uniquement pour les paires HA configurées. Si vous ajoutez une nouvelle paire HA, vous devez configurer la priorité de basculement du hub pour chacun des deux nouveaux homologues indépendamment.

Vous obtiendrez un message d'erreur si vous affectez des priorités différentes aux hubs qui sont des homologues HA non groupés, puis que vous sélectionnez ***Group HA Peers (Regrouper les homologues HA)*** *et* ***Submit (Envoyer)****.*

- Pour les plateformes qui ne sont pas des paires HA, sélectionnez un hub et cliquez dans le champ **Hub Failover Priority (Priorité de basculement des hubs)**, saisissez une priorité (plage comprise entre 1 et 4).



7. Cliquez sur **OK** pour enregistrer le cluster VPN.

STEP 5 | Publiez les préfixes supplémentaires de la branche sur la plateforme.

*Le pare-feu redistribue (annonce) tous les itinéraires non publics connectés de la branche au hub. Vous pouvez aussi redistribuer des préfixes supplémentaires depuis la branche vers le hub. Le champ **Prefix(es) to Redistribute** (préfixes à redistribuer) accepte une liste de préfixes plutôt qu'un préfixe unique.*

1. Sélectionnez **Panorama** > **SD-WAN** > **Devices (Périphériques)** et sélectionnez un pare-feu de branche.
2. Sélectionnez **BGP** et **Add** (Ajoutez) une ou plusieurs adresses IP avec un masque réseau à **Prefix(es) to Redistribute** (préfixes à redistribuer).
3. Cliquez sur **OK**.

STEP 6 | Cliquez sur **Commit (Valider)** et **Commit to Panorama (Validez sur Panorama)**.

STEP 7 | (SD-WAN Plugin 2.0.1 et versions 2.0 ultérieures) Si votre pare-feu de la plateforme dans un cluster VPN Hub-Spoke possède des interfaces DHCP ou PPPoE, vous devez utiliser DDNS. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet** puis, dans le champ **Template (Modèle)**. sélectionnez la pile de modèles d'un hub.

STEP 8 | (SD-WAN Plugin 2.0.1 et versions 2.0 ultérieures) Sélectionnez les interfaces dont l'adresse IP indique `Dynamic-DHCP Client (Client DHCP dynamique)` ou PPPOE, cliquez sur **Override (Remplacer)** au bas de l'écran, puis cliquez sur **OK** pour fermer.

STEP 9 | (SD-WAN Plugin 2.0.1 et versions 2.0 ultérieures) Sur Panorama, vérifiez que les paramètres DDNS ont été configurés.

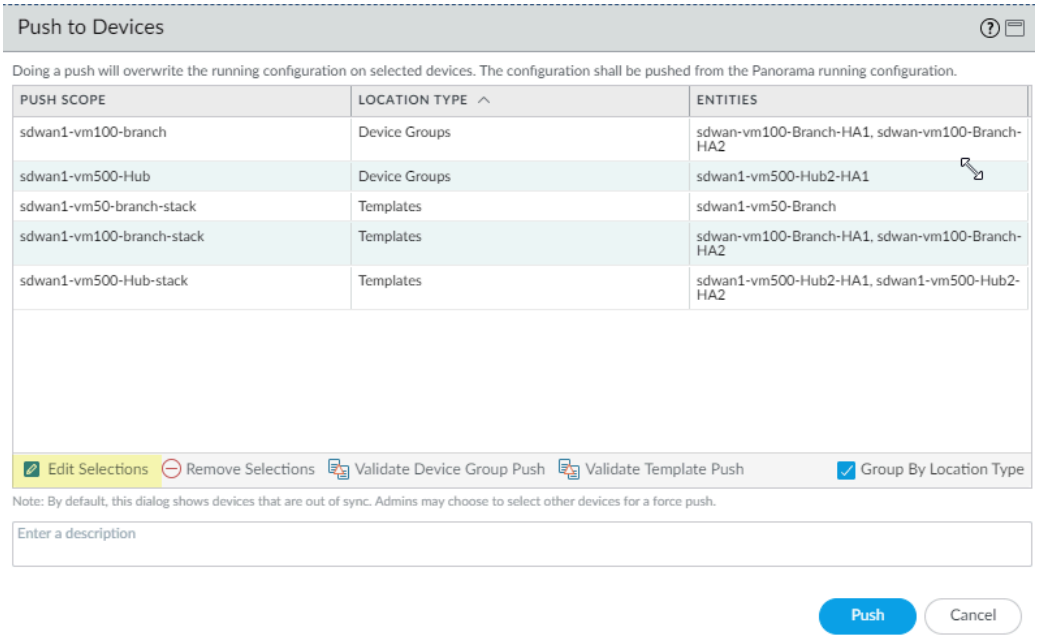
1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet** et sélectionnez la même interface de nouveau.
2. Sélectionnez **Advanced (Avancé)** > **DDNS**.
3. Vérifiez que les paramètres DDNS ont été automatiquement configurés avec un **Hostname (nom d'hôte)** et le **Vendor (fournisseur)** défini sur `Palo Alto Networks DDNS`.
4. Cliquez sur **OK**.

STEP 10 | (SD-WAN Plugin 2.0.1 et versions 2.0 ultérieures) **Commit (Validez)**, puis **Commit to Panorama (Appliquez à Panorama)**.

STEP 11 | Appliquez la configuration aux hubs.

Lorsque Panorama crée des interfaces virtuelles SD-WAN pour les hubs, Panorama ne crée pas nécessairement les interfaces en utilisant des numéros d'interface contigus. Il peut sauter un numéro d'interface au hasard , par exemple, sdwan.921, sdwan.922, sdwan.924, sdwan.925. Malgré la numérotation discontinue, Panorama crée le nombre correct d'interfaces SD-WAN. Utilisez la commande CLI opérationnelle ***`show interface sdwan?`*** *(afficher l'interface sdwan?) pour afficher les interfaces SD-WAN.*

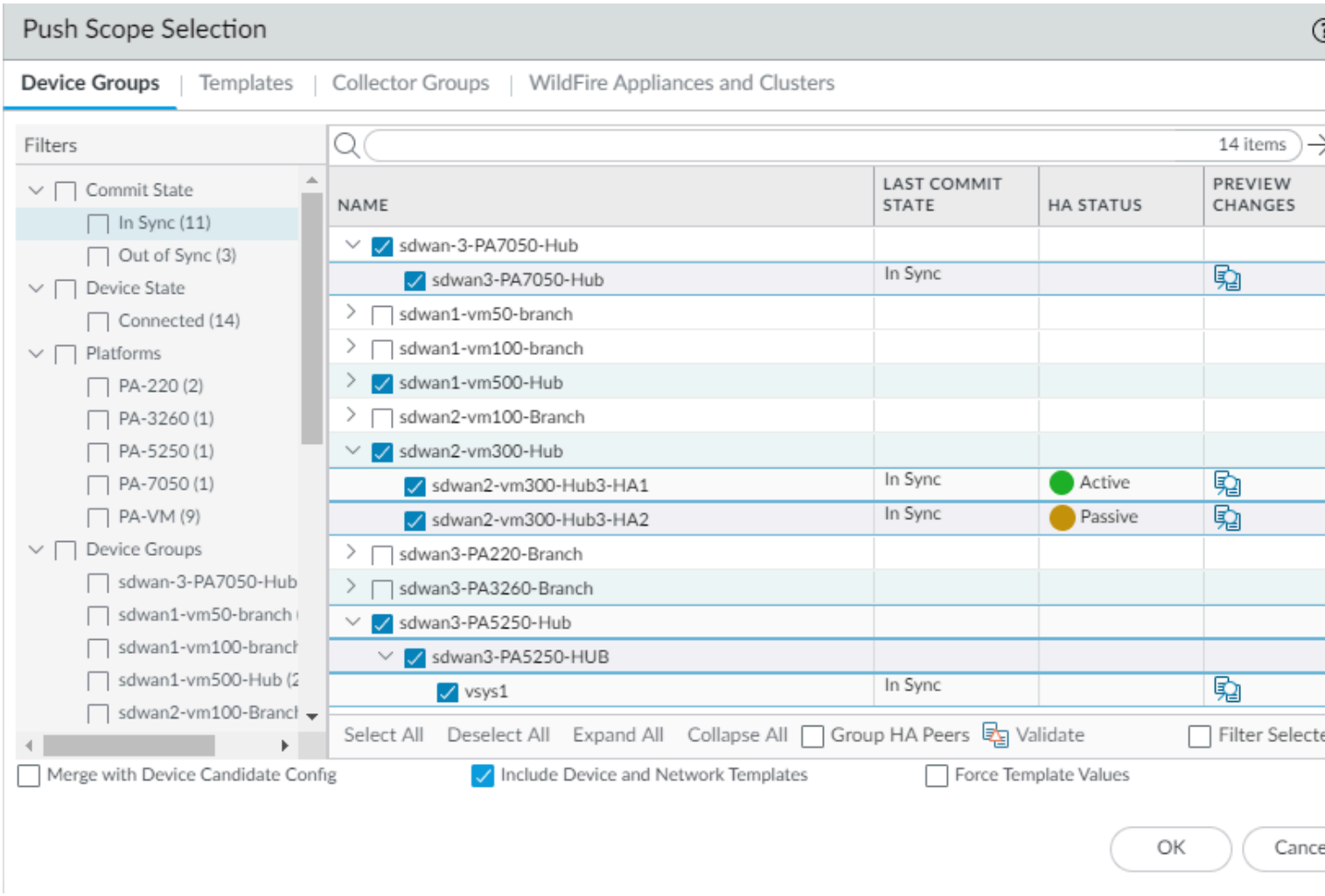
1. Sélectionnez **Commit (valider) Push to Devices (Appliquer aux périphériques)**.
2. **Edit Selections** (Modifier les sélections) en bas à gauche de l'écran.



3. Désélectionnez **Filter Selected** (Filtre sélectionné).
4. Cliquez sur **Deselect All** (Tout désélectionner).
5. Sélectionnez le groupe de périphériques de votre hub. Sélectionnez **Include Device and Network Templates** (Inclure le périphérique et les modèles de réseau) en bas de l'écran. Vous devez appliquer aux hubs avant d'appliquer aux branches.

   La plupart des branches ont des adresses IP dynamiques par l'intermédiaire de leurs fournisseurs de services et les branches doivent donc lancer la connexion IKE/IPSec car le hub ne possède pas les adresses IP des branches. Pour s'assurer que le hub est prête à recevoir les connexions IKE/IPSec, la configuration du hub doit être validée et appliquée

avant la configuration de la branche. Ainsi, lorsque les configurations de branche sont appliquées et que les branches lancent la connexion vers le hub, le hub est prêt.



6. Sélectionnez l'onglet **Templates** (modèles) et **Deselect All** (Tout désélectionner).
7. **Push Scope**(Etendue de la transmission) est le Groupe de périphériques. **Push** (Appliquez) la configuration aux hubs.

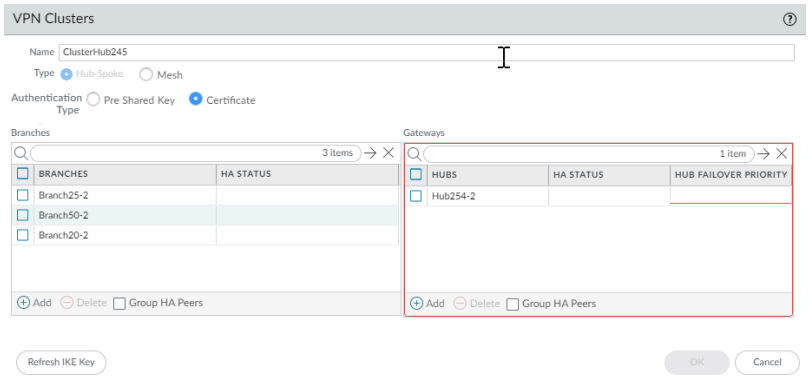
STEP 12 | Appliquez la configuration aux branches en répétant l'étape antérieure mais en sélectionnant le Groupe de périphériques de votre branche.

STEP 13 | Réactualisez la clé prépartagée IKE.

Si vous avez besoin de modifier la clé IKE actuelle qui est utilisée pour sécuriser les connexions IPSec entre les périphériques du cluster VPN, réalisez cette étape afin de générer de façon aléatoire une nouvelle clé pour le cluster.

Réalisez cette étape lorsque les membres du cluster ne sont pas occupés.

1. Sélectionnez **Panorama** > **SD-WAN** > **VPN Clusters (Clusters VPN)** et sélectionnez un cluster.
2. Au bas de l'écran, sélectionnez **Refresh IKE key** (Actualiser la clé IKE).



3. Un message s'affiche pour vous informer que `l'actualisation de la clé IKE générera une nouvelle association de sécurité (SA) pour chaque pare-feu SD-WAN du cluster VPN. Cela peut entraîner une interruption de service. Souhaitez-vous continuer? Oui | Non` Sélectionnez `Yes (Oui)` si vous souhaitez continuer.
4. **Commit** (Valider).

   *Après **Refresh IKE Key (actualiser la clé IKE)**, vous devez vous engager sur l'ensemble du cluster ; un commit partiel fera tomber les tunnels.*
5. **Push to Devices** (Appliquer aux périphériques).

Création d'un cluster VPN Full Mesh avec le service DDNS

À partir de la version 10.0.3 de PAN-OS, SD-WAN prend en charge une topologie Full Mesh en plus de la topologie Hub-Spoke. Le maillage peut comprendre des branches avec ou sans plateformes. Utilisez Full Mesh lorsque les branches doivent communiquer directement entre elles. Parmi les exemples de cas d'utilisation de Full Mesh, notons les commerçants qui possèdent des branches et des plateformes et les entreprises qui fonctionnent avec ou sans plateformes.

Certaines interfaces de pare-feu utilisent DHCP pour obtenir leur adresse IP. Souvent, les bureaux des branches utilisent un service Internet destiné aux particuliers et reçoivent une adresse IP dynamique, qui, évidemment, peut changer. C'est pourquoi les pare-feu exigent DNS dynamique (DDNS) pour qu'un service DDNS puisse détecter l'adresse IP orientée public de l'interface du pare-feu qui exécute SD-WAN. Lorsque vous appliquez le paramètre DDNS à tous les pare-feu, chaque pare-feu est avisé d'enregistrer son adresse IP d'interface externe auprès du service de cloud DDNS de Palo Alto Networks pour que l'adresse IP soit convertie en un FQDN.

DDNS est également requis parce que le périphérique CPI du ISP peut exécuter la NAT source. (L'adresse IP dynamique peut être une traduction NAT source). Le service DDNS permet au pare-feu d'enregistrer l'adresse IP orientée publique auprès du serveur DDNS. Lorsque vous avez des périphériques se connecter pour un maillage branche à branche, Auto VPN contacte le service DDNS pour que ces pare-feu puissent extraire leurs adresses IP publiques qui sont enregistrées dans le cloud DDNS et utiliser ces adresses IP publiques pour créer l'appairage IKE et les tunnels VPN. Si le périphérique CPE effectue la NAT source, lorsque vous ajouter un périphérique de branche SD-WAN à être géré par Panorama, vous activerez la **Upstream NAT (NAT en amont)**, et le type d'adresse IP NAT sera **DDNS**.

Pour le périphérique CPE ou le périphérique de routage en amont qui utilise la NAT source, vous êtes responsable de la création de la règle de la NAT de destination un-à-un (sans traduction de port) sur ce périphérique pour traduire l'adresse IP externe en l'adresse IP privée affectée à l'interface du pare-feu. Cette traduction permet aux protocoles IKE et IPSec de revenir dans le pare-feu. (Palo Alto Networks n'a pas de droits d'accès au CPE en amont ou au routeur en amont qui effectue la NAT source.)

La SD-WAN Full Mesh avec service DDNS exige ce qui suit :

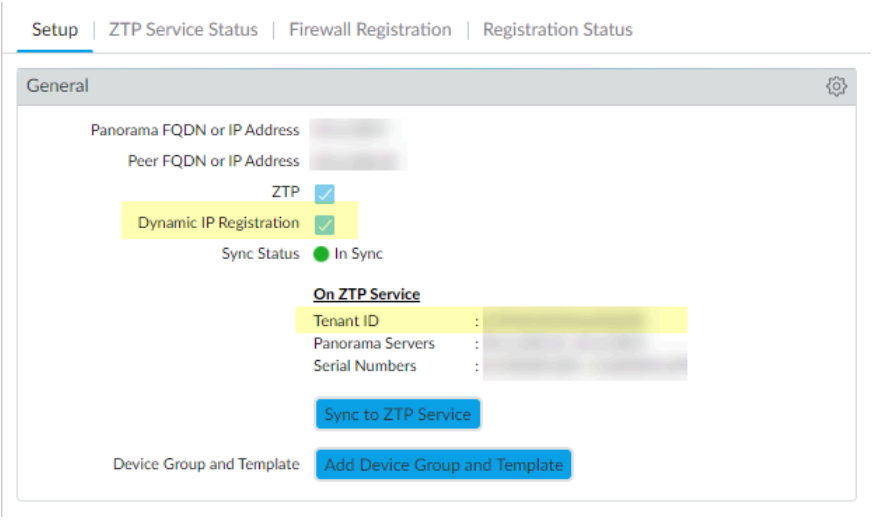
- PAN-OS 10.0.3 ou version 11.1 ultérieure
- SD-WAN Plugin 2.0.1 ou version 2.0 ultérieure
- ZTP Plugin 1.0.1 ou une version 1.0 ultérieure qui est téléchargée, installée et configurée pour utiliser le DDNS qui est associé à ZTP. Panorama doit être enregistré auprès de ZTP et communiquer avec le service ZTP.
- Version de publication du contenu des applications et des menaces 8354 ou une version ultérieure
- Tous les pare-feu qui participent au DDNS Full Mesh doivent être enregistrés sous le même compte du portail de support client (CSP).

- Le dernier certificat doit être installé sur tous les pare-feu qui participent au DDNS Full Mesh. La bonne authentification des pare-feu, de Panorama et des services de cloud est une procédure de sécurité importante qui dépend du certificat et des services CSP et ZTP.
- Si vous disposez d'un pare-feu ou d'un autre périphérique réseau qui contrôle le trafic sortant positionné devant le pare-feu Palo Alto Networks, vous devez modifier la configuration de ce périphérique pour autoriser le trafic des interfaces compatibles DDNS vers les noms de domaine complets suivants :
  - https://myip.ngfw-ztp.paloaltonetworks.com/ (pour accéder au service whatsmyIP)
  - https://ngfw-ztp.paloaltonetworks.com/ (pour accéder au service d'enregistrement DDNS)

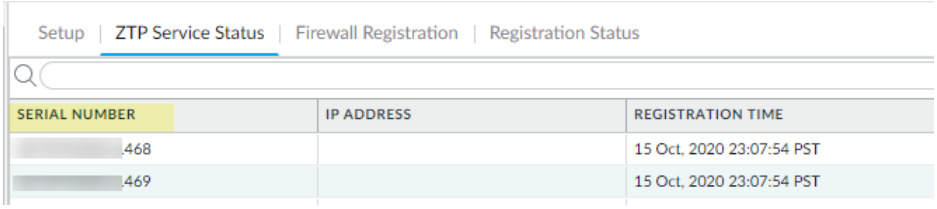
STEP 1 | Installez le dernier certificat périphérique pour Panorama et pour tous les pare-feu gérés qui sont des plateformes ou des branches.

STEP 2 | Installez le ZTP Plugin 1.0.1 pour configurer Zero Touch Provisioning.

1. Dans le guide de l'administrateur de Panorama, lisez la Présentation de ZTP.
2. Installez le plug-in ZTP.
3. Configurez le compte administrateur de l'installateur ZTP.
4. Sélectionnez **Panorama** > **Zero Touch Provisioning** > **Setup (Configuration)** et modifiez les paramètres généraux pour activer **Dynamic IP Registration (Enregistrement de l'adresse IP dynamique)**.
5. Cliquez sur **OK**. Les paramètres généraux indiquent Service ZTP activé et un ID de locataire.



6. Sélectionnez **ZTP Service Status (État du service ZTP)**, puis confirmez que le numéro de série du pare-feu est indiqué.



STEP 3 | Si vous ne l'avez pas encore fait, installez le Plugin SD-WAN 2.0.1 ou une version 2.0 ultérieure.

STEP 4 | **Commit (Validez)** sur Panorama.

STEP 5 | Connectez-vous à l'interface Web Panorama.

STEP 6 | Créez le pool d'adresses VPN, comme illustré à la section Créer un cluster VPN.

STEP 7 | Créez le cluster VPN Full Mesh.

1. Sélectionnez **Panorama** > **SD-WAN** > **VPN Clusters** (Clusters VPN SD-WAN de Panorama).
2. Sous **Type**, sélectionnez **Mesh**.
3. **Add (Ajoutez)** les **Branches** qui doivent communiquer entre elles.
4. (Facultatif) **Add (Ajoutez)** une ou plusieurs **Hubs (Plateformes)** si vous voulez également qu'il y ait une plateforme dans le maillage.
5. Cliquez sur **OK**.

STEP 8 | Cliquez sur **Commit (Valider)** et **Commit to Panorama (Validez sur Panorama)**. Si vos pare-feu ont des adresses IP statiques, vous avez terminé. Si vos pare-feu de branche ou de plateforme dans un maillage VPN possèdent des interfaces DHCP ou PPPoE, vous devez utiliser DDNS. Vous devez donc poursuivre cette procédure comme suit.

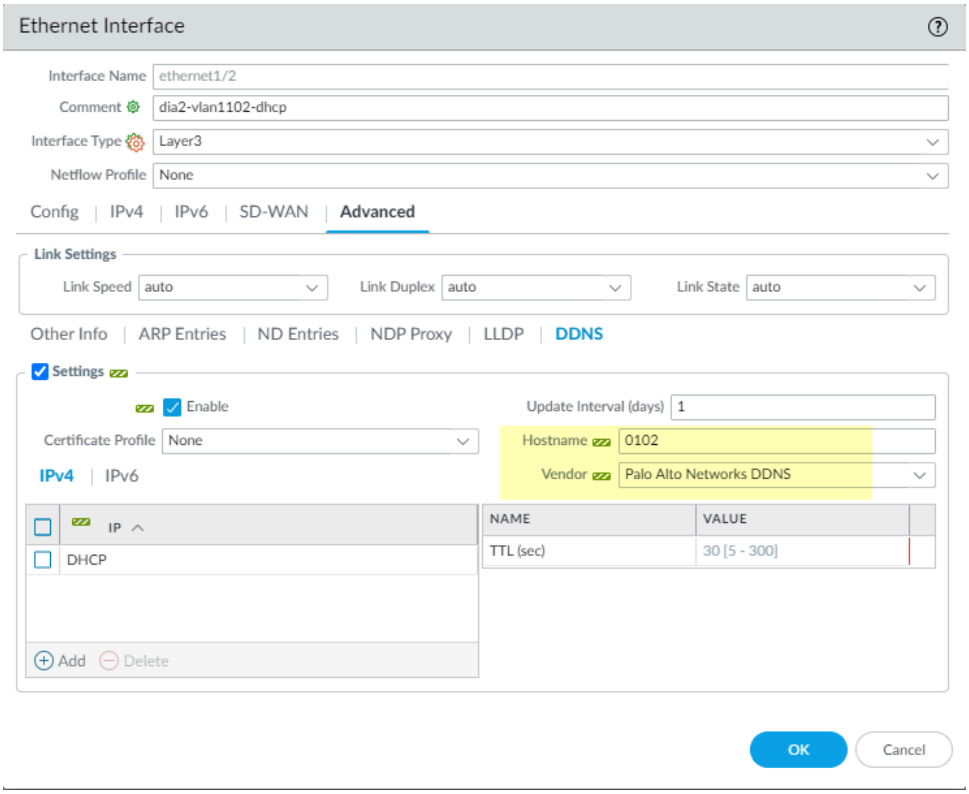
STEP 9 | Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet** puis, dans le champ **Template (Modèle)**. sélectionnez la pile de modèles d'une branche donnée.

STEP 10 | Sélectionnez les interfaces dont l'adresse IP indique `Dynamic-DHCP Client (Client DHCP dynamique)` ou PPPOE, cliquez sur **Override (Remplacer)** au bas de l'écran, puis cliquez sur **OK** pour fermer.

STEP 11 | Sur Panorama, vérifiez que les paramètres DDNS ont été configurés.

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet (Ethernet)** et sélectionnez la même interface de nouveau.
2. Sélectionnez **Advanced (Avancé)** > **DDNS**.
3. Vérifiez que les paramètres DDNS ont été automatiquement configurés avec un **Hostname (nom d'hôte)** fondé sur le nom de l'interface et le **Vendor (fournisseur)** défini

sur `Palo Alto Networks DDNS`. Par exemple, sur l'interface Ethernet1/2, le nom d'hôte est 0102.



4. Cliquez sur **OK**.

STEP 12 | Si le cluster VPN comprend des plateformes qui possèdent une interface DHCP ou PPPoE, répétez les étapes 9 à 11, mais, dans le champ **Template (Modèle)**, sélectionnez la pile de modèles pour une plateforme donnée.

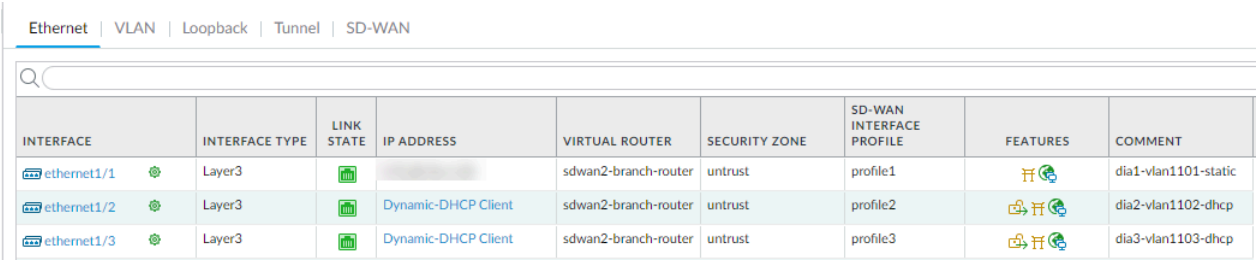
Même si votre plateforme n'est pas dans un cluster Full Mesh, mais dans un cluster Hub-Spoke, si la plateforme utilise DHCP ou PPPoE pour obtenir son adresse IP pour une interface SD-WAN, vous devez effectuer les étapes de contrôle prioritaire pour activer DDNS.

STEP 13 | **Commit (Validez)** sur Panorama et **Push to Devices (Appliquez aux périphériques)**.

STEP 14 | Sur le pare-feu de la branche, vérifiez que la branche est configurée avec DDNS.

1. Connectez-vous au pare-feu de la branche.
2. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet** et, pour l'interface Ethernet que vous avez configurée, faites défiles l'icône d'info DDNS dans la colonne Features

(Caractéristiques) pour voir le fournisseur, le nom d'hôte, l'adresse IP et les autres informations DDNS.



STEP 15 | Sur une autre branche du cluster, vérifiez que l'adresse de l'homologue de l'interface est un FQDN généré par le système pour l'enregistrement DDNS.

1. Connectez-vous à une autre branche et sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Gateways (Passerelles IKE)**.
2. Vérifiez que l'adresse de l'homologue est un nom sécurisé, difficilement référencé et qui ne contient pas d'informations sur l'entreprise; par exemple 0101.8ced8460fcc5177cd3665ce41b6345323a15a612b8e52ec1d9ec057a582cb4.t13855f6c9a92c

STEP 16 | Affichez les FQDN des branches et des plateformes et mettez à jour les informations DDNS.

1. Accédez à la CLI.
2. Affichez les FQDN (générés par DDNS) des autres branches et plateformes : **`show dns-proxy fqdn all`**
3. Mettez à jour les adresses DDNS :**`request system fqdn refresh`**

Créer une route statique pour SD-WAN

En plus du (ou comme une alternative au) routage BGP, vous pouvez créer des itinéraires statiques afin d'acheminer votre trafic SD-WAN.

Vous pouvez configurer des itinéraires statiques à l'aide de Panorama™ ou directement sur le pare-feu du hub ou de la branche. Si vous allez utiliser Panorama, vous devez vous familiariser avec la procédure de Configure a Template or Template Stack Variable (Configurer une variable de modèle ou de pile de modèles). Vous allez créer une variable à utiliser comme destination de votre itinéraire statique, tel que cela est indiqué dans la procédure suivante. (Vous pouvez aussi créer une variable pour le saut suivant.) Vous allez appliquer un itinéraire statique (qui va jusqu'au hub) à la branche. Vous allez appliquer un itinéraire statique (qui va jusqu'à la branche) au hub.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Configure a Template or Template Stack Variable(Configurer une variable de modèle ou de pile de modèles) et saisissez le **Name** (Nom) de la variable format suivant : $*peerhostname_clustername.customname*. Par exemple, $branchsanjose_clusterca.10 or $DIA_cluster2.location3. Après le symbole du dollar ($), les éléments de la variable sont :

- *peerhostname* (Nom d'hôte homologue)— Nom d'hôte du hub ou de la branche de destination vers laquelle va l'itinéraire statique. Pour un itinéraire statique vers internet, le nom d'hôte homologue doit être **DIA**. Une alternative au nom d'hôte homologue consiste à utiliser le numéro de série homologue. Si l'homologue fait partie d'une paire HA, vous pouvez utiliser le nom d'hôte ou le numéro de série d'un des deux pare-feux HA.
- *clustername* (nom du cluster) — Nom du cluster VPN auquel le hub ou la branche de destination appartient.
- *customname* (nom personnalisé) — Texte de votre choix ; vous ne pouvez pas utiliser le point (.) dans le nom personnalisé.

Vous pouvez avoir plus d'un itinéraire statique vers le même homologue, ce qui signifie que les variables auront le même nom d'hôte homologue et le même nom de cluster ; vous différenciez les variables en utilisant un nom personnalisé différent.

STEP 3 | Sous **Type**, sélectionnez **IP Netmask (Masque réseau IP)**, puis saisissez l'adresse IP de destination, suivie d'une barre oblique et de la longueur du masque réseau, par exemple : 192.168.2.1/24. Pour IPv6, saisissez l'adresse IPv6 avec une barre oblique et une longueur de préfixe, par exemple 2001:DB8 ::/32.

STEP 4 | Cliquez sur **OK** pour enregistrer la variable.

STEP 5 | Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et sélectionnez un routeur virtuel.

STEP 6 | Sélectionnez **Static Routes (Itinéraires statiques)**.

STEP 7 | Sélectionnez **IPv4** ou **IPv6** et **Add (Ajoutez)** un **Name (Nom)** pour l'itinéraire statique.

STEP 8 | Pour **Destination**, sélectionnez la variable que vous avez créée.

STEP 9 | Sous **Interface**, faites un choix dans la liste déroulante, qui ne comprend que les interfaces tirées du modèle, par exemple, Ethernet1/1, Tunnel.x ou sdwan.xx.

STEP 10 | Pour **Next Hop (Saut suivant)**, sélectionnez **IP Address (Adresse IP)** ou **IPv6 Address (Adresse IPv6)** et saisissez l'adresse IP ou la variable du saut suivant de l'itinéraire statique (le hub ou la branche de destination de l'itinéraire statique).

STEP 11 | Cliquez sur **OK**.

STEP 12 | **Commit** (Validez) et **Commit and Push** (Validez et appliquez) les modifications de votre configuration.Validez et appliquez vos modifications.

La configuration Auto VPN remplace le mot clé **sdwan** dans le champ d'interface de l'itinéraire statique avec l'interface virtuelle de sortie SD-WAN qu'il détermine sur la base de la variable de Destination. Ainsi, l'itinéraire statique dans le tableau d'acheminement indique que le trafic qui va vers l'hôte homologue dans le cluster VPN identifié sortira de l'interface virtuelle SD-WAN pour atteindre le saut suivant spécifié.

STEP 13 | Configurer un itinéraire statique pour le trafic de retour.

Configurer le routage avancé pour SD-WAN

Un moteur de routage avancé permet au pare-feu d'évoluer et de fournir des fonctions de routage stables, hautement performantes et hautement disponibles aux grands centres de données, aux FAI, aux entreprises et aux utilisateurs du cloud. Le moteur de routage avancé s'appuie sur une méthodologie de configuration standard de l'industrie, ce qui facilite les tâches de l'administrateur. Il permet la création de profils qui sont utilisés pour différentes fonctions (telles que le filtrage, la redistribution et les modifications de métriques), qui peuvent toutes être utilisées sur des routeurs logiques. Ces profils fournissent une granularité plus fine pour filtrer les routes pour chaque protocole de routage dynamique et améliorent la redistribution des routes sur plusieurs protocoles.

Bien que conceptuellement équivalent, le moteur de routage avancé utilise des routeurs logiques plutôt que des routeurs virtuels pour instancier les domaines de routage.

Contrairement aux routeurs virtuels, les routeurs logiques ne sont pas créés par défaut ; vous devez en créer un avant de configurer les fonctions de routage.

Vous pouvez utiliser un moteur de routage avancé ou un ancien moteur en fonction des exigences de votre réseau :

- Lorsque vous activez le Routage avancé, des routeurs logiques sont créés et le moteur de routage avancé est utilisé pour le routage.
- Lorsque vous désactivez le**Routage avancé**, des routeurs virtuels sont créés et le moteur hérité est utilisé pour le routage.

Le moteur de routage avancé prend en charge plusieurs routeurs logiques (appelés routeurs virtuels sur le moteur de routage hérité). Le moteur de routage avancé dispose d'options de menu plus pratiques et il existe de nombreux paramètres BGP que vous pouvez facilement configurer dans un profil (authentification, minuteurs, famille d'adresses ou profil de redistribution) que vous appliquez à un groupe d'homologues ou à un homologue BGP, par exemple.

Le moteur de routage avancé prend en charge les routes statiques, MP-BGP, OSPFv2, OSPFv3, RIPv2, Protocol Independent Multicast Sparse Mode (PIM-SM), PIM Source-Specific Multicast (SSM), BFD, la redistribution, le filtrage des routes dans le RIB, les listes d'accès , des listes de préfixes et des cartes de route.

Vous aurez besoin des éléments suivants pour configurer le moteur de routage avancé sur SD-WAN :

Platform (Plateforme)	Pare-feu exécutant la version PAN-OS	Plug-in SD-WAN
Panorama^{MC}	11.1 et versions ultérieures	3.1.0 et versions ultérieures

Le plug-in SD-WAN crée un routeur logique ou un routeur virtuel en fonction de la valeur de l'option de routage avancé. Lorsque le routage avancé est activé, un routeur logique est créé ; Sinon, un routeur virtuel est créé.

Lorsque vous activez le routage avancé dans la pile de modèles et que vous effectuez une validation Panorama et une poussée vers le pare-feu, le plug-in SD-WAN exécute le script de migration pour créer les objets liés au SD-WAN (statiques, interfaces, profil de redistribution, BGP) dans le routeur logique. Le script de migration crée le même nom de routeur logique que le nom de routeur virtuel pour le même modèle. Par conséquent, les hubs et les branches ont toujours le même nom de routeur.

Après la migration, Panorama ne vous permet pas de supprimer les routeurs virtuels migrés.

Le plug-in Panorama SD-WAN 3.1.0 peut gérer simultanément les pare-feu à l'aide du moteur de routage avancé et les pare-feu à l'aide du moteur de routage hérité. L'avantage est que vous pouvez migrer certains pare-feux gérés vers le nouveau moteur de routage avancé tout en conservant la configuration actuelle de votre moteur de routage hérité sur les autres.

Alors que le plug-in SD-WAN 3.1.0 gère un pare-feu quel que soit le moteur de routage, une seule configuration de moteur de routage peut être effective à la fois sur un pare-feu géré. Vous pouvez utiliser l'option **de routage avancé** pour activer ou désactiver le moteur de routage avancé. Chaque fois que vous modifiez le moteur que le pare-feu utilise (vous activez ou désactivez le routage avancé pour accéder au moteur avancé ou au moteur hérité, respectivement), vous devez valider la configuration et redémarrer le pare-feu pour que la modification prenne effet.

Avant de passer au moteur de routage avancé, effectuez une sauvegarde de votre configuration actuelle. De même, si vous configurez Panorama avec une pile de modèles qui active ou désactive le routage avancé, après avoir validé et poussé la pile de modèles vers les périphériques, vous devez redémarrer les périphériques dans la pile de modèles pour que la modification prenne effet.

Lors de la configuration de Panorama, créez des groupes de périphériques et des piles de modèles pour les appareils qui utilisent tous le même paramètre de routage avancé (tous activés ou tous désactivés). Panorama ne transmettra pas les configurations avec le routage avancé activé vers les pare-feu plus petits qui ne prennent pas en charge le routage avancé. Pour ces pare-feu, Panorama transmettra une configuration héritée si elle est présente.

Assurez-vous de rétrograder vers un plug-in SD-WAN et une version PAN-OS appropriés, et désactivez le **Routage avancé** si vous prévoyez d'utiliser un routeur virtuel. Utilisez un modèle distinct dans lequel le **Routage avancé** est désactivé (dans ce cas, des routeurs virtuels sont créés) lors de la rétrogradation du plug-in SD-WAN.

Si vous avez configuré le**Routage avancé** et que vous souhaitez basculer vers un routeur virtuel, désactivez le routage avancé pour revenir à la configuration du routeur virtuel précédemment enregistrée. Validez et transférez toutes les modifications apportées au pare-feu après avoir désactivé le routage avancé avant de tenter une procédure de rétrogradation, telle que la rétrogradation des versions du plug-in PAN-OS et SD-WAN.

Si vous activez le routage avancé, les interfaces SD-WAN doivent être configurées dans le même routeur logique ; ils ne peuvent pas être répartis entre les routeurs logiques.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Mettez à niveau Panorama vers la version 11.1 et installez le plug-in SD-WAN 3.1.0.

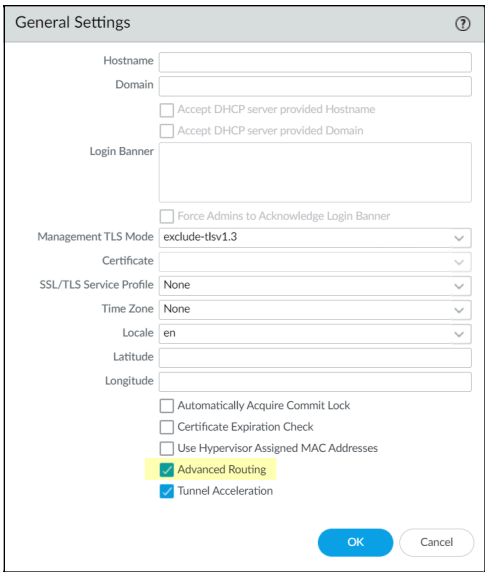
STEP 3 | Ajoutez vos pare-feux de concentrateur et de succursale en tant que périphériques gérés au serveur de gestion Panorama™ .

STEP 4 | Effectuez une sauvegarde de votre configuration actuelle avant d'activer le routage avancé.

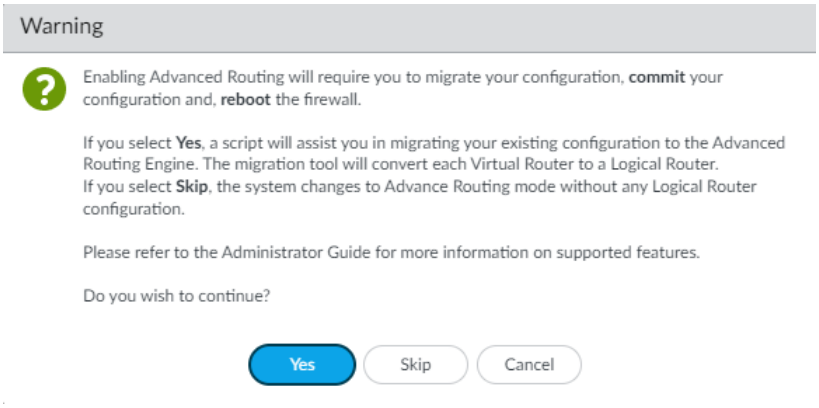
STEP 5 | Dans la section **Périphérique** , sélectionnez la pile de modèles appropriée dans la liste déroulante Contexte **du modèle** .

STEP 6 | Activer le moteur de routage avancé.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les paramètres généraux.
2. Activer le module de routage avancé Le plug-in SD-WAN créera un routeur logique ou un routeur virtuel en fonction de la valeur de l'option de routage avancé. Lorsque le routage avancé est activé, un routeur logique est créé. Sinon, un routeur virtuel est créé.

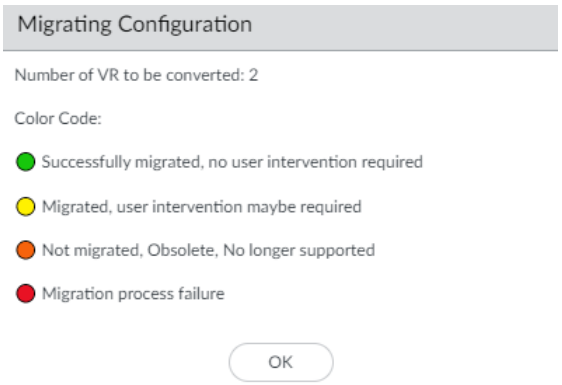


3. Cliquez sur **OK**.
4. Un message d'avertissement concernant la migration s'affiche ; cliquez sur **Oui** pour continuer.

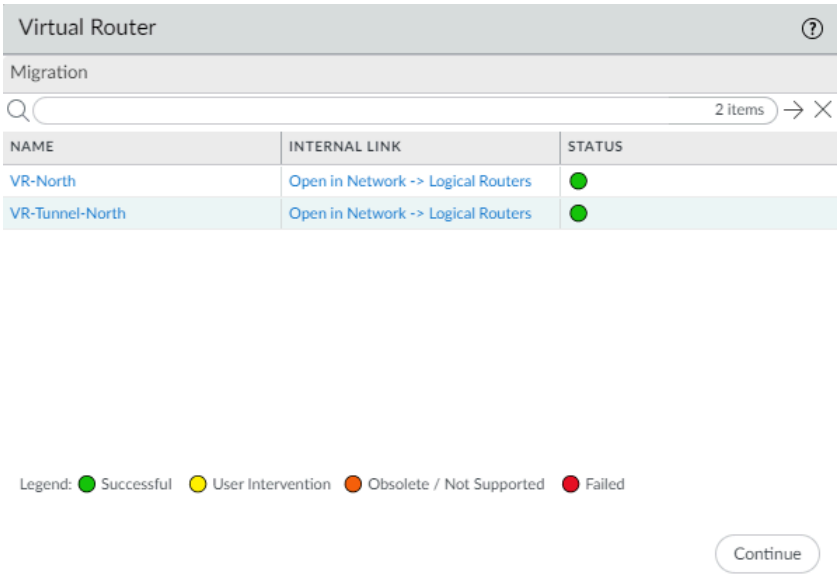


En cliquant sur **Oui**, un script de migration intégré migrera votre configuration existante vers le moteur de routage avancé. Si vous sélectionnez **Ignorer**, une configuration vide est créée pour le moteur de routage avancé.

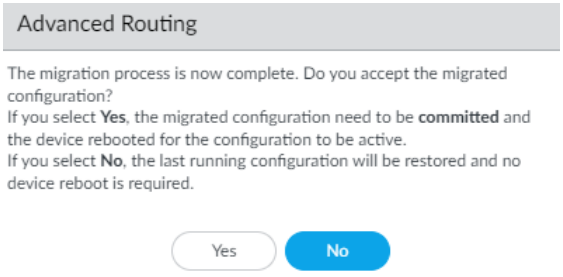
La **Configuration de la migration** affiche les codes de couleur qui indiquent l'état de la migration.



Dans le **Routeur virtuel**, vérifiez le**STATUT** des modèles dans les piles de modèles. Le **STATUT** doit être vert pour une migration réussie. Sinon, prenez les mesures nécessaires pour tous les modèles qui n'ont pas réussi la migration.



La migration réussie convertit automatiquement chaque routeur virtuel en un routeur logique correspondant. Il est obligatoire de valider la configuration et de redémarrer le pare-feu pour que les modifications prennent effet.



5. **Commit** (Valider).
6. Sélectionnez **Device (Appareil)** > **Setup (Configuration)** > **Operations (Opérations)** et **Reboot Device (Réamorcer l'appareil)**.

STEP 7 | Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

STEP 8 | Commit and Push (Validez et appliquez) les modifications de votre configuration à vos pare-feux gérés. **Appuyez sur Appareils** pour afficher les routeurs logiques ajoutés dans les pare-feux SD-WAN sélectionnés.

1. Sélectionnez **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** et **Edit Selections (Modifier les sélections)**.
2. Sélectionnez **Modèles** et choisissez la pile de modèles et le modèle dans la liste.
3. Activez **Forcer les valeurs de modèle** pour remplacer la configuration locale par les valeurs de modèle mises à jour. Avant d'utiliser cette option, vérifiez les valeurs forcées des pare-feu pour garantir que votre validation ne donne pas lieu à des pannes réseau imprévus ou à des problèmes causés par le remplacement de ces valeurs forcées.
4. Cliquez sur **OK** et **Appliquez** aux appareils.

STEP 9 | Reconnectez-vous au pare-feu.

STEP 10 | Sélectionnez **Réseau**.

Notez les éléments de menu, qui sont plus standard de l'industrie et plus détaillés que l'élément unique (routeurs virtuels) du menu hérité. Le **Routage** inclut les **Routeurs logiques** et les **Profils de routage**, qui incluent**BGP**, **BFD**, **OSPF**, **OSPFv3**, **RIPv2**, les **Filtres**, et la **Multidiffusion**.

STEP 11 | Vous devez activer le **Routage avancé** pour chaque pile de modèles individuellement lorsque vous avez plusieurs piles de modèles dans votre configuration. Répétez les étapes 5 à 10 pour les autres piles de modèles sur les pare-feux que vous avez l'intention de mettre à jour pour le routage avancé.

Selon nos exigences de conception, le nom du routeur logique doit être le même que le nom du routeur virtuel pour le même modèle lors de l'utilisation du moteur de routage avancé. Cela signifie que les hubs et les branches ont toujours le même nom de routeur. Lorsque vous créez manuellement des routeurs logiques plutôt que d'utiliser un script de migration, vous devez vous assurer que le nom du routeur logique et le nom du routeur virtuel sont identiques.

STEP 12 | Sélectionnez un routeur virtuel ou logique dans votre déploiement SD-WAN.

Sélectionnez **Panorama** > **SD-WAN** > **Périphériques**pour ajouter un périphérique SD-WAN (concentrateur SD-WAN ou pare-feu de branche) à gérer par le serveur de gestion Panorama.

Outre les options de configuration existantes pour l'ajout d'un périphérique SD-WAN, vous pouvez désormais sélectionner un routeur logique (pour le moteur de routage avancé) ou un routeur virtuel (pour le moteur hérité) pour un **Nom de routeur**. Il est important que le nom du

routeur logique et le nom du routeur virtuel soient identiques pour le même modèle lors de l'utilisation du moteur de routage avancé.

Sélectionnez le **Nom du routeur** (routeur logique ou virtuel) à utiliser pour le routage entre le concentrateur SD-WAN et les branches :

- Si les noms du routeur virtuel et du routeur logique sont identiques, le **Nom du routeur** affiche un seul nom.
- Si les noms de routeur virtuel et de routeur logique sont différents, le **Nom du routeur** affiche à la fois le nom du routeur virtuel et le nom du routeur logique. Vous pouvez sélectionner un routeur virtuel (pour le moteur hérité) ou un routeur logique (pour le moteur de routage avancé) en fonction de vos besoins.

Surveillance et Création de rapports

Surveillez et générez des rapports sur l'état de santé des applications et des liens dans vos clusters VPN afin d'identifier et de résoudre les problèmes. Afin que le serveur de gestion Panorama™ affiche les informations d'état de santé des applications et liens SD-WAN, vous devez activer les pare-feux SD-WAN afin de mettre en avant les données de surveillance des périphériques dans Panorama et de Configurer le transfert des journaux vers Panorama lorsque vous Ajouter vos pare-feux SD-WAN en tant que Périphériques gérés. Si vous n'avez pas configuré vos pare-feux SD-WAN pour transférer les journaux vers Panorama, le **Monitoring** (surveillance) SD-WAN n'affiche aucune information sur la santé des applications ou des liens.

Pour que Panorama recueille des données de surveillance SD-WAN, vous devez appliquer la configuration SD-WAN de Panorama à vos pare-feu SD-WAN. Si aucune donnée de surveillance SD-WAN ne s'affiche, vérifiez que vous avez appliqué avec succès la configuration SD-WAN.

- Surveiller les Tâches SD-WAN
- Surveiller la Performance des applications et des liens SD-WAN
- Surveiller les hubs d'accès Prisma
- Générer un rapport SD-WAN

Surveiller les Tâches SD-WAN

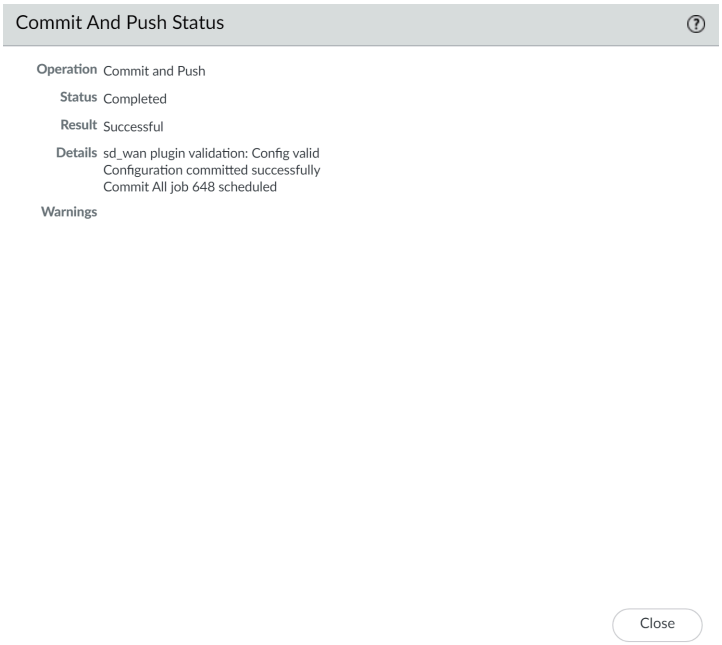
La surveillance valide, met en avant d'autres tâches SD-WAN exécutées depuis le serveur de gestion Panorama™ afin d'obtenir un aperçu et des informations détaillées sur une tâche spécifique.

Si une tâche réussit avec des avertissements ou échoue, vous pouvez afficher les informations des avertissements et la description afin de mieux comprendre comment résoudre l'erreur de configuration. De plus, vous pouvez afficher les informations du dernier état de mise en avant pour savoir ce qui a causé les avertissements ou les erreurs de la tâche.

STEP 1 | Connectez-vous à l'interface Web Panorama.

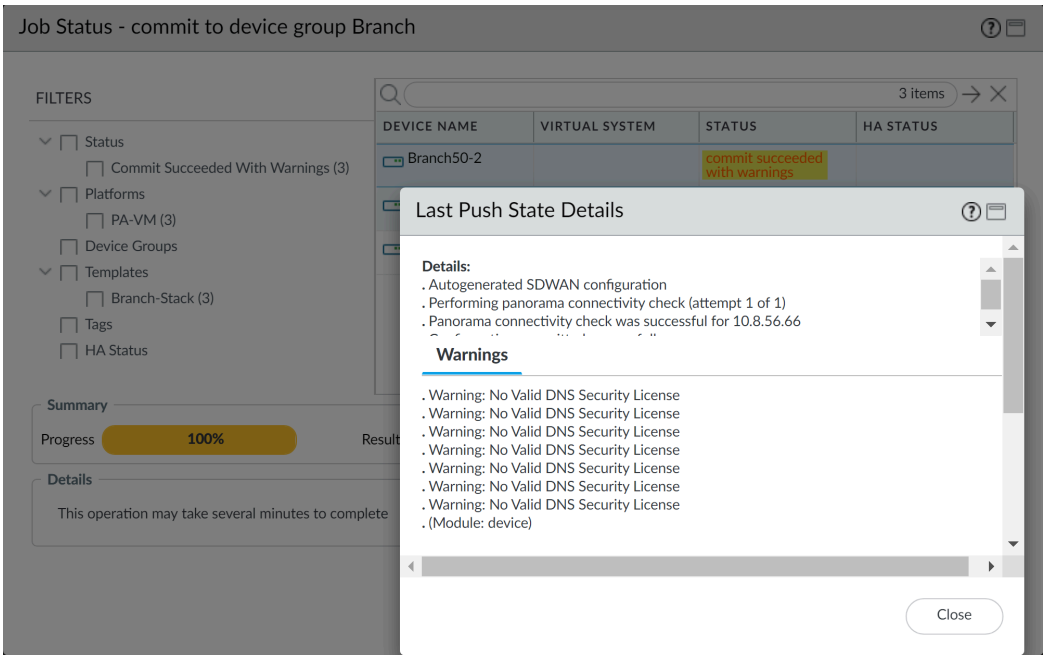
STEP 2 | Après avoir modifié la configuration SD-WAN, **Commit** (validez) vos modifications pour afficher l'état de la tâche.

La fenêtre d'état de la tâche affiche l'opération réalisée, le résultat et les informations et avertissements en lien avec l'état de la tâche.



STEP 3 | Affichez les dernières informations de la mise en avant des tâches qui réussissent avec des avertissement ou qui ont échoué.

1. Cliquez sur **Tasks** (tâches) (Tasks) au bas de l'interface web pour ouvrir le Task Manager (Gestionnaires de tâches).
2. Cliquez sur le **Type** de tâche pour la tâche SD-WAN.
3. Cliquez sur **Status** (état) de la tâche pour afficher les informations du dernier état de mise en avant de la tâche.
4. Examinez les informations du dernier état de mise en avant afin d'identifier et résoudre les problèmes de configuration.



Surveiller la Performance des applications et des liens SD-WAN

Surveillez l'application et la performance des liens dans vos clusters VPN afin de régler les problèmes en affichant un résumé des informations des tous les clusters VPN puis en procédant par élimination afin d'isoler les problèmes des sites, applications et liens affectés. La visibilité du trafic SD-WAN est affichée sur le pare-feu SD-WAN qui reçoit le trafic. Par exemple, pour le trafic qui circule du pare-feu de la plate-forme vers le pare-feu de la branche, les données de surveillance SD-WAN s'affichent sur le pare-feu de la branche. Le tableau de bord d'accueil s'affiche :

- Performance des applications
  - **Impacted** (impactée) — une ou plusieurs applications du cluster VPN pour lequel aucun des chemins ne présente de performance suffisante, de gigue, latence ou perte de paquets, qui atteint les seuils indiqués dans le Profil de Qualité de chemin de la liste des chemins entre lesquels le pare-feu peut choisir.
  - **OK** — Nombre de clusters VPN, plateformes et branches qui ne subissent aucun problème de gigue, latence ou perte de paquets.
- Performance des liens
  - **Error** (erreur) — Un ou plusieurs sites du cluster VPN ont des problèmes de connectivité comme lorsqu'un tunnel ou une interface virtuelle (VIF) est en panne.
  - **Avertissement** — Nombre de clusters, hubs et branches VPN ayant des liens avec la bande passante (prise en charge dans PAN-OS 11.2.0 avec le plug-in SD-WAN 3.3.0 et versions ultérieures) la bande passante (prise en charge dans PAN-OS 11.1.5 et versions ultérieures avec le plug-in SD-WAN 3.2.2 et versions ultérieures), les mesures de performance de gigue, latence ou perte de paquets qui dépassent la valeur moyenne mobile sur sept jours de la métrique.
  - **OK** — Nombre de clusters, hubs et branches VPN n'ayant aucun problème de bande passante (prise en charge dans PAN-OS 11.2.0 avec le plug-in SD-WAN 3.3.0 et versions ultérieures), de bande passante (prise en charge dans PAN-OS 11.1.5 et versions ultérieures avec le plug-in SD-WAN 3.2.2 et versions ultérieures) gigue, latence ou perte de paquets.

  À partir de PAN-OS 11.2.0, le plug-in SD-WAN 3.3.0 et les versions ultérieures prennent en charge la « bande passante », qui est la principale mesure de la performance des liens.À partir de PAN-OS 11.1.5, le plug-in SD-WAN 3.2.2 et les versions ultérieures prennent en charge la « bande passante », qui est la principale mesure de la performance des liens.

Si une règle de politique SD-WAN est configurée avec un transfert de correction des erreurs pour un pare-feu de la plateforme ou de la branche, un message `Error Correction Initiated (Initié par la correction d'erreurs)` s'affiche pour vous aviser que le pare-feu de la plateforme ou de la branche a détecté et corrigé des erreurs dans les données transmises pour une application.

Les plateformes SD-WAN affichent `Error Correction Initiated (Initié par la correction des erreurs)` uniquement si le trafic provenait de la plateforme SD-WAN vers la branche SD-WAN et qu'il correspondait à une règle de politique SD-WAN avec un profil de correction des erreurs associé.

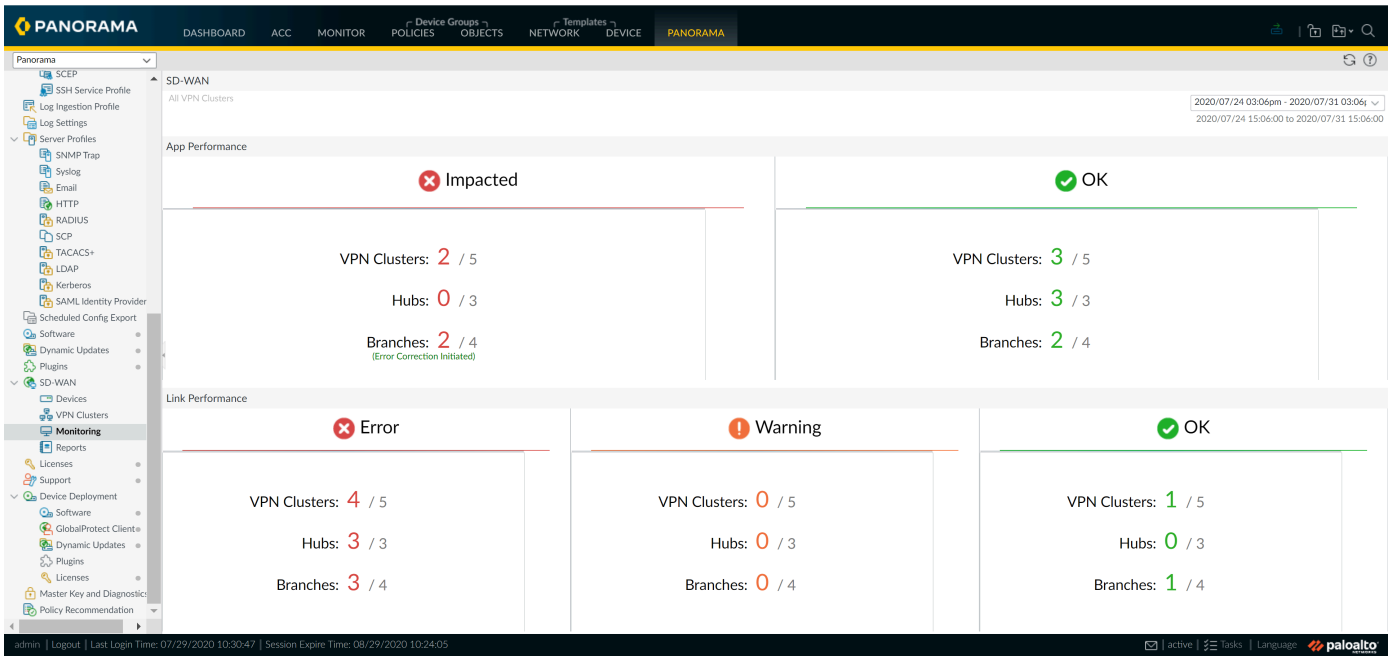
Depuis le tableau de bord d'accueil, procédez par élimination pour afficher les applications impactées ou les liens qui présentent un état d'Erreur ou d'Avertissement. Puis sélectionnez un site affecté afin d'afficher les informations au niveau du site. Depuis le site, affichez les informations au niveau des applications ou des liens.

Voir Surveillez les performances des applications Prisma Access Hub et des lienspour surveiller les performances des applications et des liens pour les hubs Prisma Access.

Si aucune donnée n'est présente ou si l'écran indique que SD-WAN n'est pas défini, vérifiez dans Compatibility Matrix (matrice de compatibilité) que la version Panorama que vous utilisez prend en charge la version du plug-in SD-WAN que vous essayez d'utiliser.

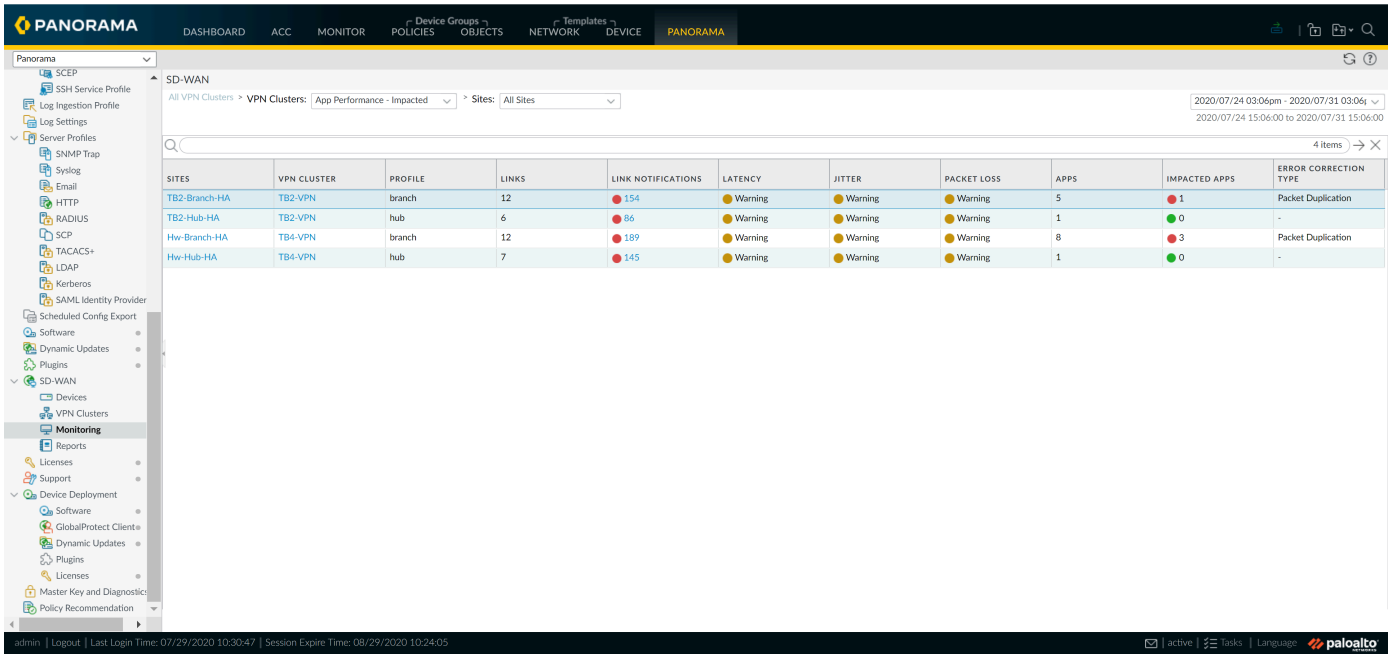
STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Sélectionnez **Panorama** > **SD-WAN** > **Monitoring** (surveillance) afin d'afficher les résumés d'état de santé de vos clusters VPN, hubs et branches.



STEP 3 | Cliquez sur un résumé des Performances de l'application ou des Performances des liens qui indique le nombre des Impacts, Erreurs ou Avertissements pour afficher une liste détaillée des sites et de leur état en fonction de la bande passante (prise en charge dans PAN-OS 11.2.0 avec le plug-in SD-WAN 3.3.0 et versions ultérieures pour les performances des

liens), la bande passante (prise en charge dans PAN-OS 11.1.5 et versions ultérieures avec le plug-in SD-WAN 3.2.2 et versions ultérieures)la latence, la gigue et la perte de paquets.



STEP 4 | Cliquez sur un site qui affiche Warning (avertissement) ou Error (erreur) pour afficher un cluster VPN. Les données du site affichent la Performance des applications et la Performance des liens, y compris les applications impactées. De plus, utilisez le filtre de sites pour afficher les clusters VPN sur la base des notifications de liens, déviations de latence, déviations de gigue, déviations de perte de paquets ou applications impactées.

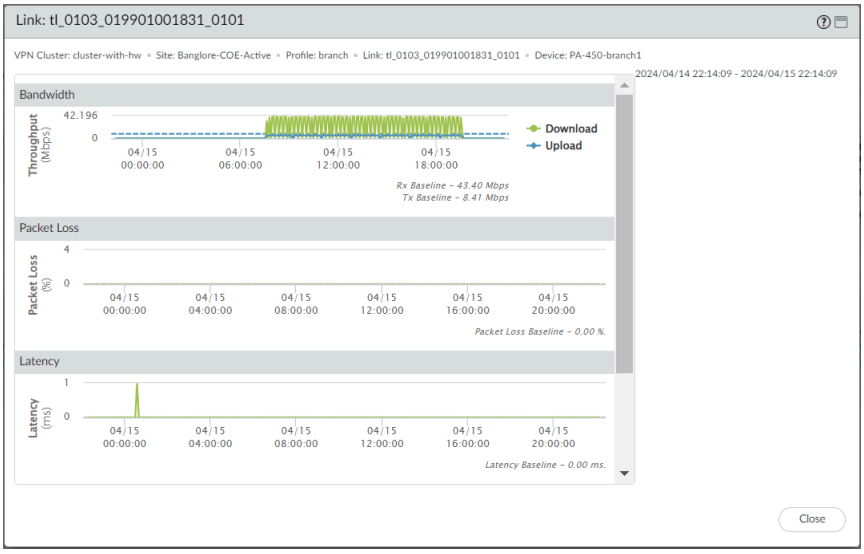
(PAN-OS 11.2.0 avec le plug-in SD-WAN 3.3.0 et versions ultérieures) (PAN-OS 11.1.5 et versions ultérieures avec le plug-in SD-WAN 3.2.2 et versions ultérieures) Vous pouvez maintenant afficher le nouveau paramètre de performance des liens, la **maximum upload/ download speed (vitesse maximale de chargement/téléchargement)** pour le site sélectionné dans un cluster VPN.

Cliquez sur chaque **Link (Lien)** pour afficher la bande passante de base (prise en charge dans PAN-OS 11.2.0 avec le plug-in SD-WAN 3.3.0 et versions ultérieures) la bande passante (prise en charge dans PAN-OS 11.1.5 et versions ultérieures avec le plug-in SD-WAN 3.2.2 et versions ultérieures), la gigue, la perte de paquets et la latence mesurées pour le tunnel.

(PAN-OS 11.2.0 avec le plug-in SD-WAN 3.3.0 et versions ultérieures) (PAN-OS 11.1.5 et versions ultérieures avec le plug-in SD-WAN 3.2.2 et versions ultérieures) Le graphique **Bandwidth (Bande passante)** affiche les vitesses maximales mobiles de chargement et de téléchargement pour les liens physiques et tunnel.

- Pour le lien physique, le graphique affiche la configuration du profil de l'interface SD-WAN (si configuré) comme valeur maximale. Sinon, le graphique affiche les valeurs maximales Tx et Rx considérées jusqu'à présent par le lien physique comme valeur maximale.

- Pour les liens tunnel, le graphique affiche les valeurs maximales Tx et Rx considérées jusqu'à présent par le tunnel comme valeur maximale.



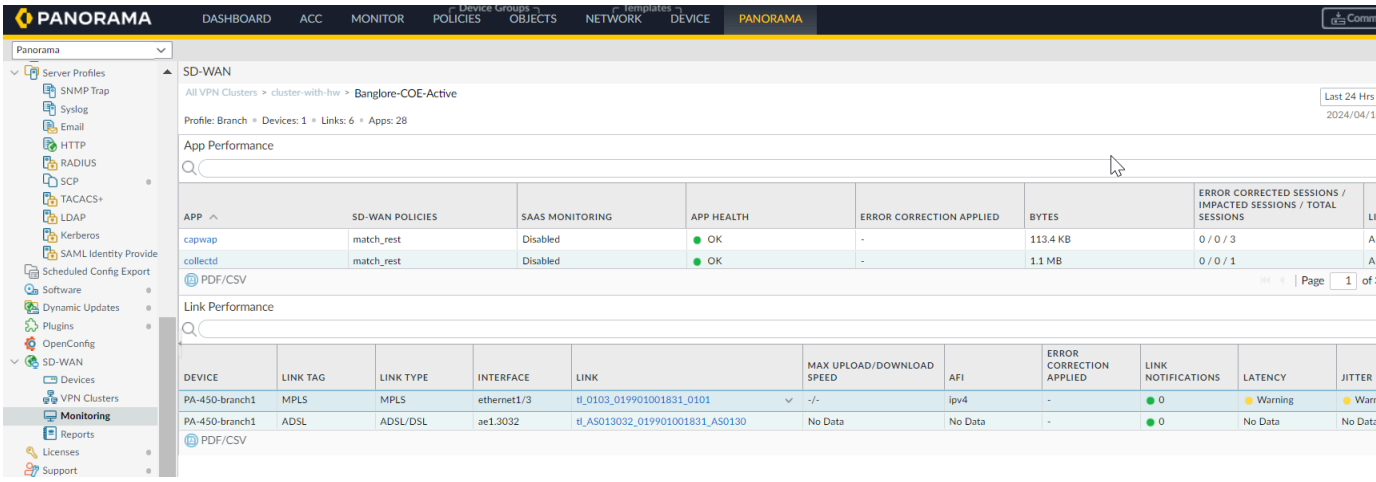
Pour les applications SaaS sur une liaison Direct Internet Access (Accès Internet direct ; DIA), la colonne **SaaS Monitoring (Surveillance SaaS)** indique si l'application est créée dans un profil de qualité SaaS et associée à une ou plusieursrègles de politique SD-WAN.

- `Disabled` : l'application n'est pas une application SaaS configurée dans un profil de qualité SaaS.
- `Enabled` : l'application est une application SaaS configurée dans un profil de qualité SaaS et est associée à une ou plusieurs politiques SD-WAN.

Si vous associez un profil de correction des erreurs avec une règle de politique SD-WAN pour une application, les colonnes **Error Correction Applied (Correction des erreurs appliquée)** s'affichent si des types de corrections d'erreurs ont été appliqués et, le cas échéant, lesquels. De plus, vous pouvez consulter **Error Corrected Sessions/Impacted Sessions/Total Sessions (Sessions au cours desquelles des erreurs ont été corrigées/Sessions impactées/Sessions totales)** pour comprendre, du nombre total de sessions sur la période spécifiée, combien de

sessions comportaient des erreurs qui ont été corrigées par le pare-feu de la branche ou de la plateforme.

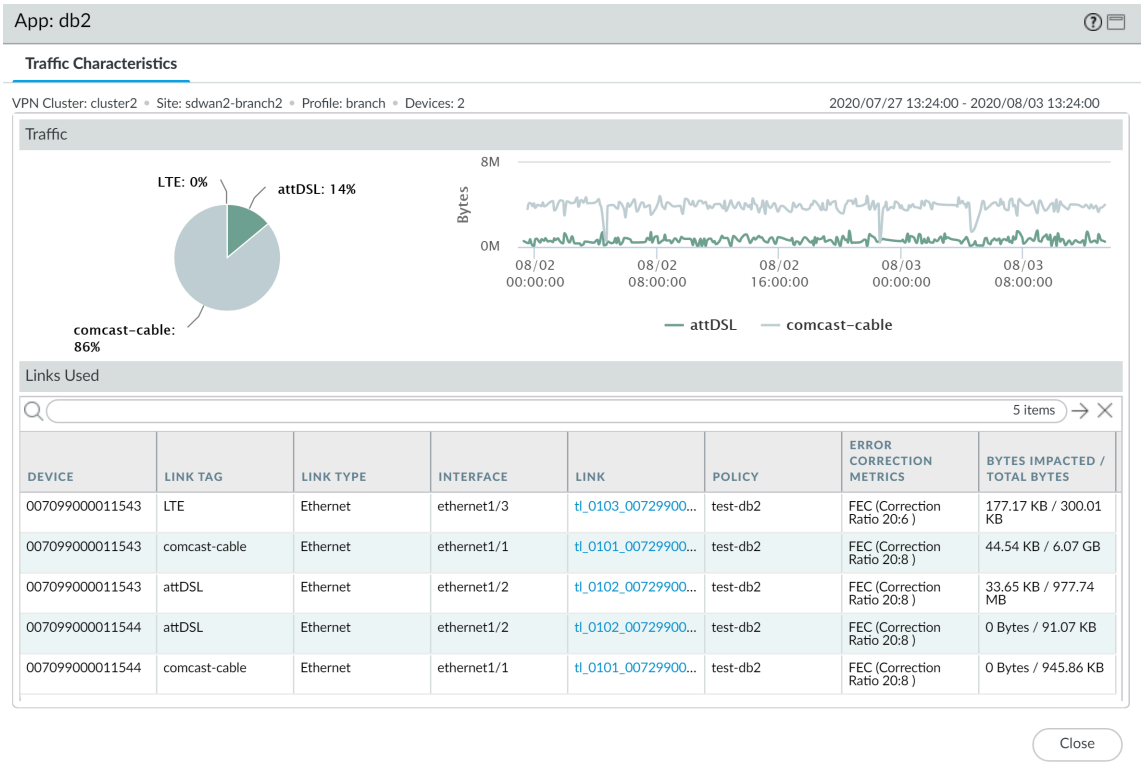
Cliquez sur **PDF/CSV** pour exporter les informations détaillées des applications et des liens du Site au format PDF ou CSV.

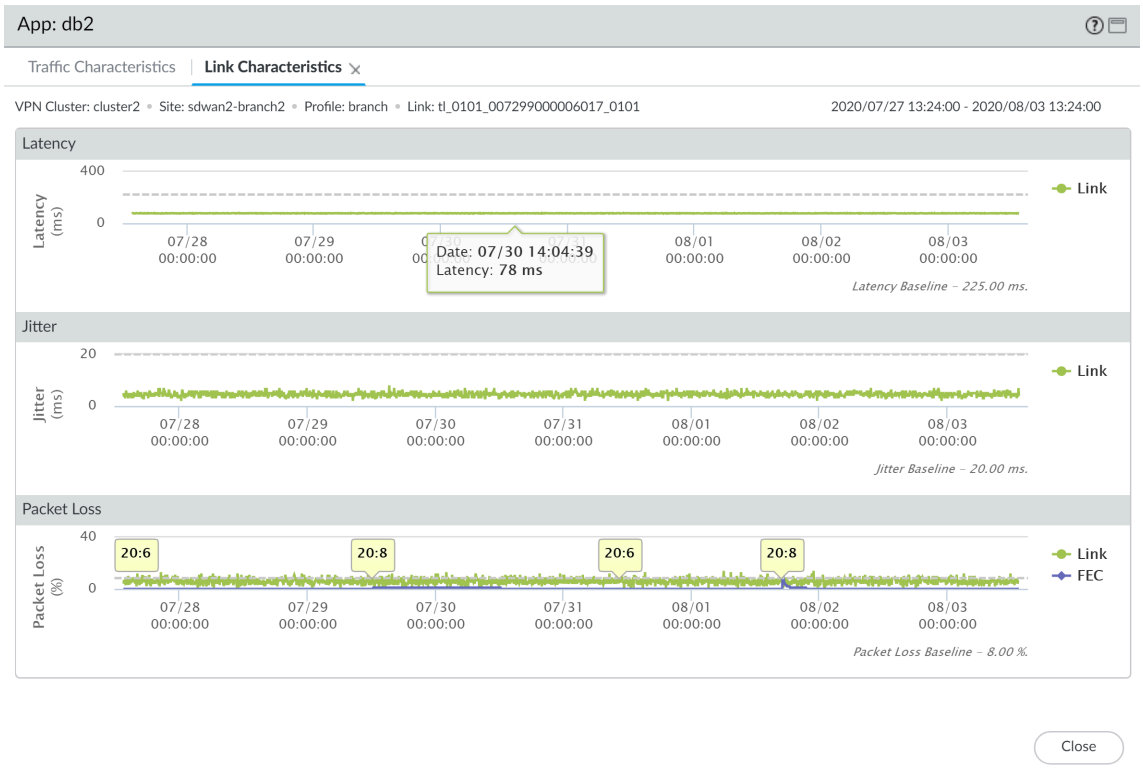


STEP 5 | Cliquez sur la branche ou le hub dont une application a besoin de votre attention.

STEP 6 | Cliquez sur une application impactée pour afficher les informations au niveau des applications ou des liens.

Par exemple, consultez les caractéristiques des liaisons d'une application pour comprendre la latence, la gigue et la perte des paquets de l'application sur la liaison spécifiée. De plus, vous pouvez consulter le moment où la correction des erreurs a été appliquée pour la liaison.





Surveiller les hubs d'accès Prisma

Établissez une base de référence et surveillez les performances de votre application Prisma Access Hub et des liens pour comprendre comment configurer et modifier vos profils de gestion de liens SD-WAN.

- Référencez les performances de votre application Prisma Access Hub et de vos liens
- Surveillez les performances des applications Prisma Access Hub et des liens

Référencez les performances de votre application Prisma Access Hub et de vos liens

Avant de Configurez les Profils de gestion des liaisons SD-WAN, Palo Alto Networks vous recommande de définir les performances de votre application Prisma Access Hub et de lier pour mieux comprendre l'activité de charge utile normale de votre Prisma Access Hub afin d'éviter l'échange de liens inutile pour les applications et le trafic qui n'en ont pas besoin.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Intégrer le pare-feu PAN-OS à Prisma Access.

STEP 3 | Sélectionnez **Panorama** > **SD-WAN** > **Surveillance** et modifiez la plage de temps de surveillance SD-WAN.

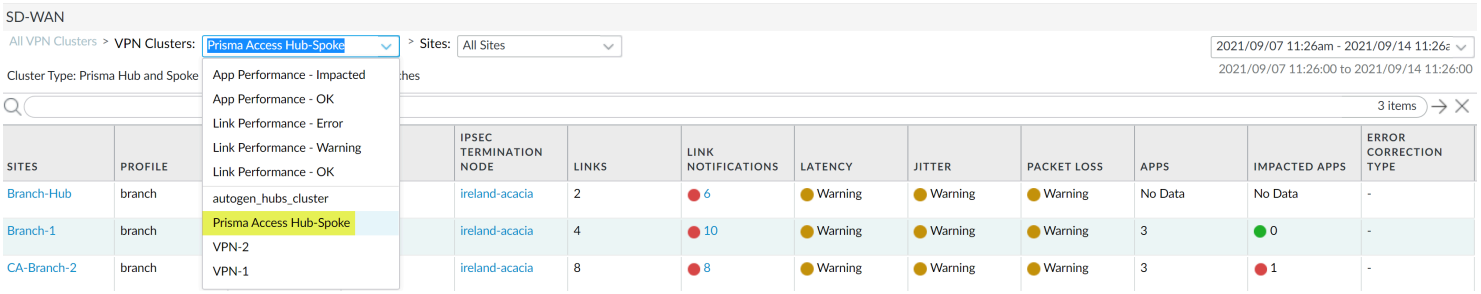
Plus la période que vous utilisez pour établir le niveau de référence de votre application Prisma Access Hub et les performances des liens est longue, plus la ligne de base sera précise. Au minimum, utilisez trois jours de performances d'application et de lien pour établir la base de référence des données de latence, de gigue et de perte de paquets que vous utilisez pour créer vos profils de gestion de liens SD-WAN.

Palo Alto Networks recommande d'évaluer sept jours de données de performances d'application et de liaison pour établir une base de référence de la latence, de la gigue et de la perte de paquets pour le Prisma Access Hub.

STEP 4 | Filtrez la surveillance SD-WAN pour afficher uniquement vos clusters VPN Prisma Access Hub-Spoke.

1. Cliquez sur un résumé de Performance des applications ou Performance des liens qui indique un nombre de Impacted (impacté), Error (erreur) ou Warning (avertissement) pour afficher une liste détailler des sites et de leur état en fonction de la latence, de la gigue et de la perte de paquets.
2. Dans le filtre de cluster VPN, sélectionnez **Prisma Access Hub-Spoke**.

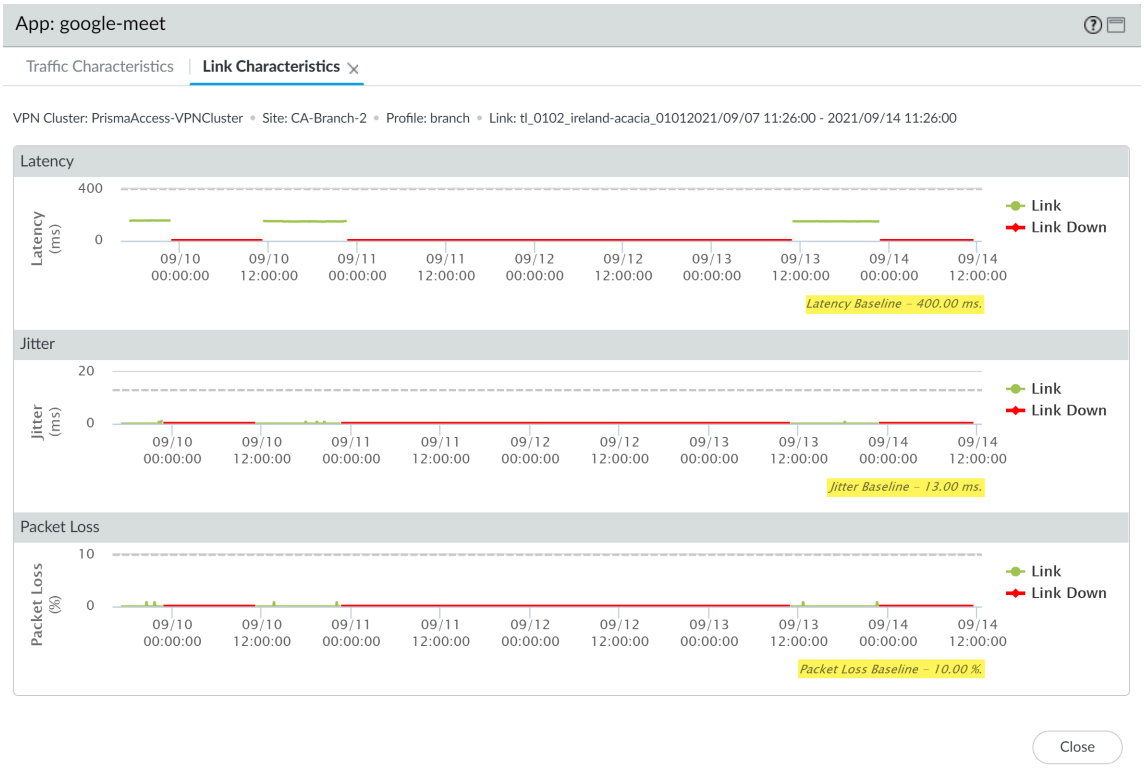
3. Cliquez sur un site pour afficher des détails détaillés sur l'état de santé de Prisma Access Hub.



STEP 5 | Passez en revue les caractéristiques de liaison d'une application Prisma Access Hub.

1. Cliquez sur une application dans la section Performances de l'application pour afficher les caractéristiques du trafic et les liens utilisés pour le trafic des applications.
2. Cliquez sur chaque lien pour afficher la latence de base, la gigue et la perte de paquets mesurées pour l'application sur le lien.

   Répétez cette opération pour tous les liens jusqu'à ce que vous rassembliez suffisamment de données de référence pour modifier votre profil de qualité de chemin Prisma Access Hub.



STEP 6 | Modifiez votre profil de qualité du chemin d'accès Prisma en fonction des lignes de base de latence, de gigue et de perte de paquets que vous avez collectées.

STEP 7 | Continuez à configurer le SD-WAN si nécessaire.

STEP 8 | Surveillez les performances des applications Prisma Access Hub et des liens pour affiner davantage vos profils de gestion des liens SD-WAN.

Surveillez les performances des applications Prisma Access Hub et des liens

Surveillez l'application et la performance des liens de votre Hub Prisma Access afin de régler les problèmes en affichant un résumé des informations des tous les clusters VPN puis en procédant par élimination afin d'isoler les problèmes des sites, applications et liens affectés. La visibilité sur le trafic SD-WAN est affichée sur le déploiement Prisma Access ou le pare-feu SD-WAN recevant le trafic. Par exemple, pour le trafic qui circule du pare-feu de la plate-forme vers le pare-feu de la branche, les données de surveillance SD-WAN s'affichent sur le pare-feu de la branche. Le tableau de bord d'accueil s'affiche :

- Performance des applications
  - **Impacted** (impactée) — une ou plusieurs applications du cluster VPN pour lequel aucun des chemins ne présente de performance suffisante, de gigue, latence ou perte de paquets, qui atteint les seuils indiqués dans le Profil de Qualité de chemin de la liste des chemins entre lesquels le pare-feu peut choisir.
  - **OK** — Nombre de clusters VPN, plateformes et branches qui ne subissent aucun problème de gigue, latence ou perte de paquets.
- Performance des liens
  - **Error** (erreur) — Un ou plusieurs sites du cluster VPN ont des problèmes de connectivité comme lorsqu'un tunnel ou une interface virtuelle (VIF) est en panne.
  - **Warning** (avertissement) — Nombre de clusters VPN, hubs et branches qui ont des liens présentant des mesures de performance de gigue, latence ou perte de paquets qui dépassent la valeur de la moyenne flottante sur sept jours de la mesure.
  - **OK** — Nombre de clusters VPN, plateformes et branches qui ne subissent aucun problème de gigue, latence ou perte de paquets.

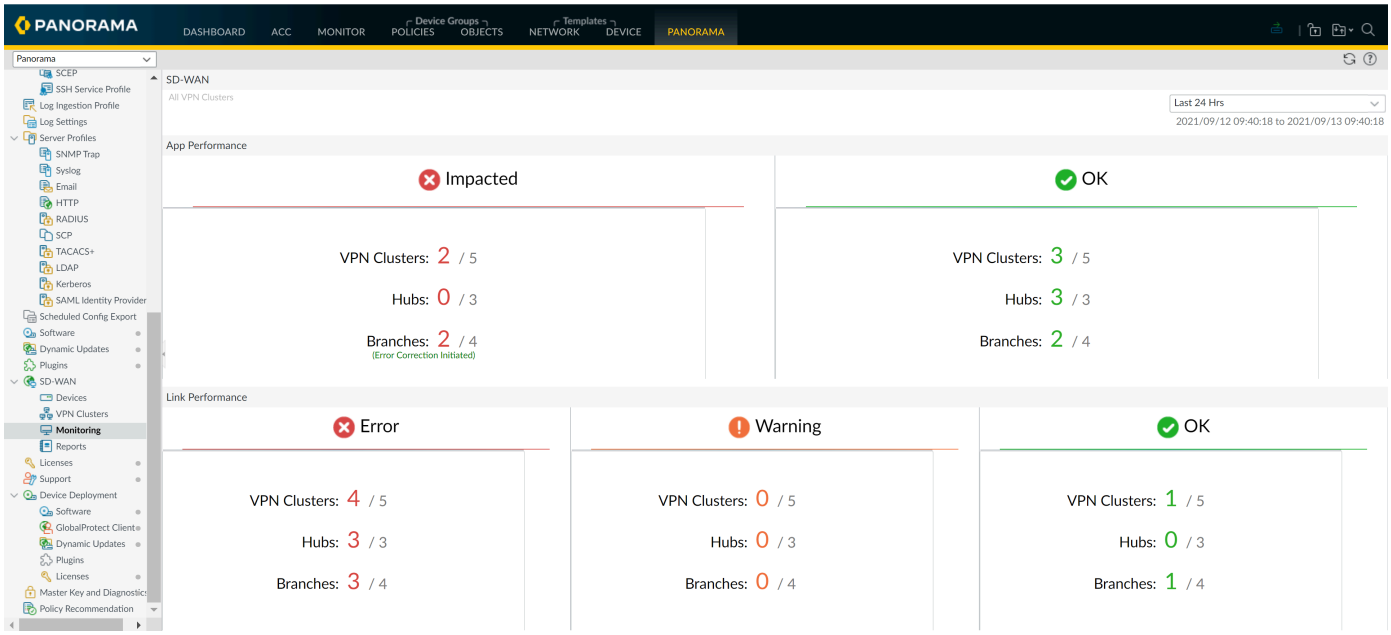
Depuis le tableau de bord d'accueil, procédez par élimination pour afficher les applications impactées ou les liens qui présentent un état d'Erreur ou d'Avertissement. Puis sélectionnez un site affecté afin d'afficher les informations au niveau du site. Depuis le site, affichez les informations au niveau des applications ou des liens.

Consultez Surveiller la Performance des applications et des liens SD-WAN pour surveiller les performances des applications et des liens entre tous vos sites SD-WAN.

Si aucune donnée n'est présente ou si l'écran indique que SD-WAN n'est pas défini, vérifiez dans Compatibility Matrix (matrice de compatibilité) que la version Panorama que vous utilisez prend en charge la version du plug-in SD-WAN que vous essayez d'utiliser.

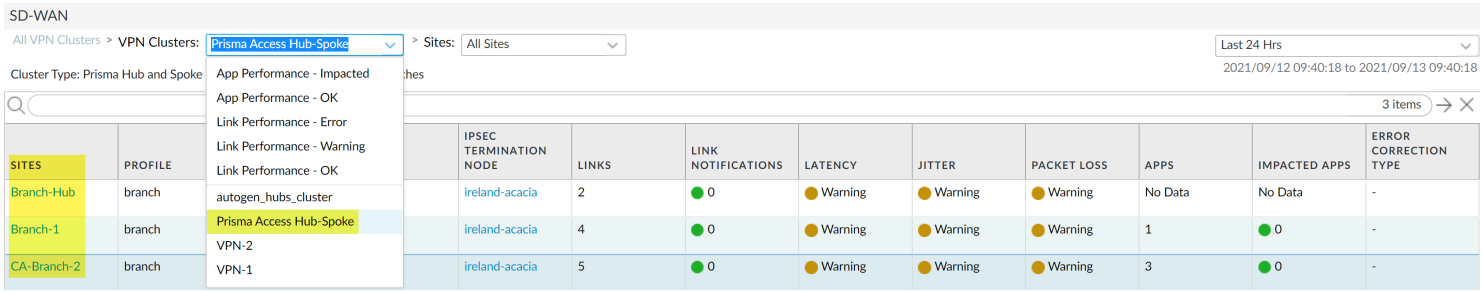
STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Sélectionnez **Panorama** > **SD-WAN** > **Monitoring** (surveillance) afin d'afficher les résumés d'état de santé de vos clusters VPN, hubs et branches.



STEP 3 | Filtrez la surveillance SD-WAN pour afficher uniquement vos clusters VPN Prisma Access Hub-Spoke.

1. Cliquez sur un résumé de Performance des applications ou Performance des liens qui indique un nombre de Impacted (impacté), Error (erreur) ou Warning (avertissement) pour afficher une liste détailler des sites et de leur état en fonction de la latence, de la gigue et de la perte de paquets.
2. Dans le filtre de cluster VPN, sélectionnez **Prisma Access Hub-Spoke**.
3. Cliquez sur un site pour consulter les détails de santé détaillés du Prisma Access Hub.



STEP 4 | Examinez les détails de santé détaillés du Prisma Access Hub.

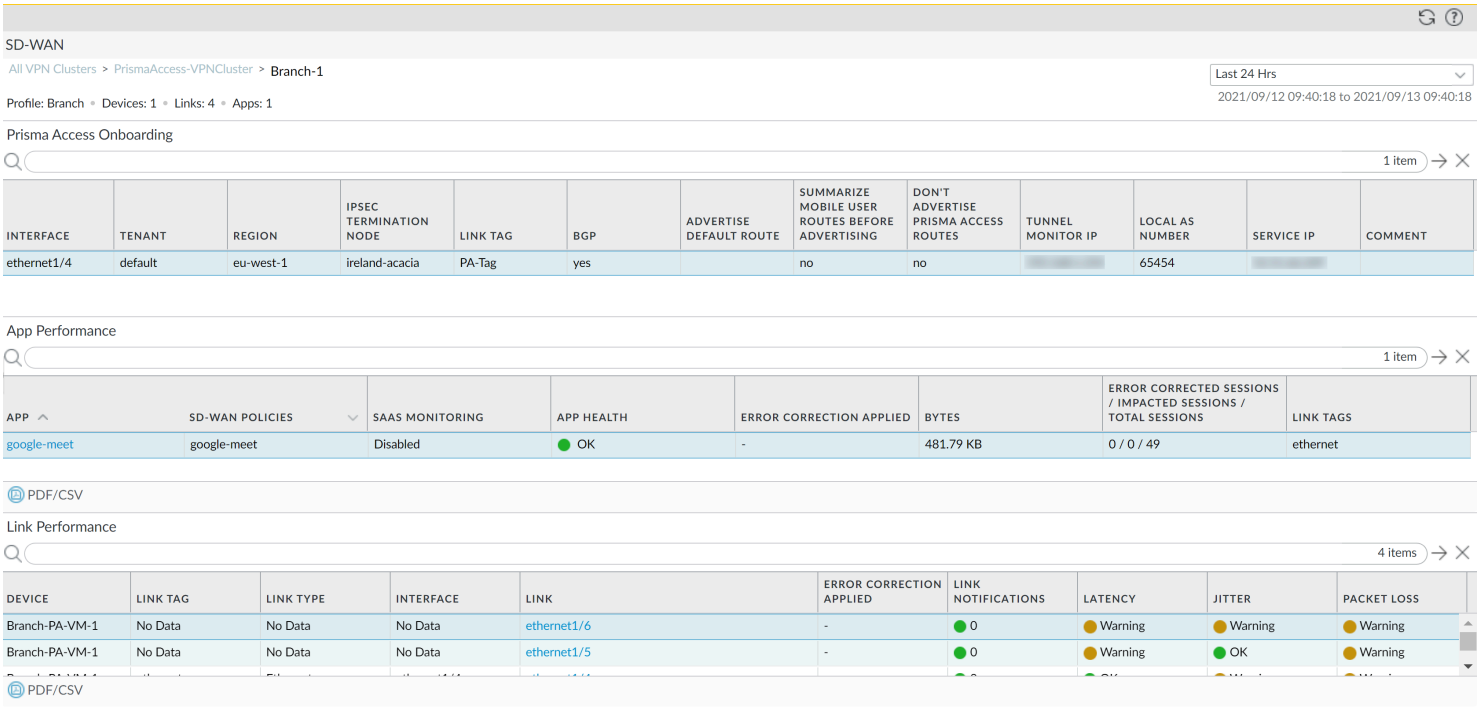
Les données du site affichent les détails de Prisma Access Onboarding, ainsi que les performances des applications et des liens, y compris les applications impactées.

Pour les applications SaaS sur une liaison Direct Internet Access (Accès Internet direct ; DIA), la colonne **SaaS Monitoring (Surveillance SaaS)** indique si l'application est créée dans un profil de qualité SaaS et associée à une ou plusieursrègles de politique SD-WAN.

- `Disabled` : l'application n'est pas une application SaaS configurée dans un profil de qualité SaaS.
- `Enabled` : l'application est une application SaaS configurée dans un profil de qualité SaaS et est associée à une ou plusieurs politiques SD-WAN.

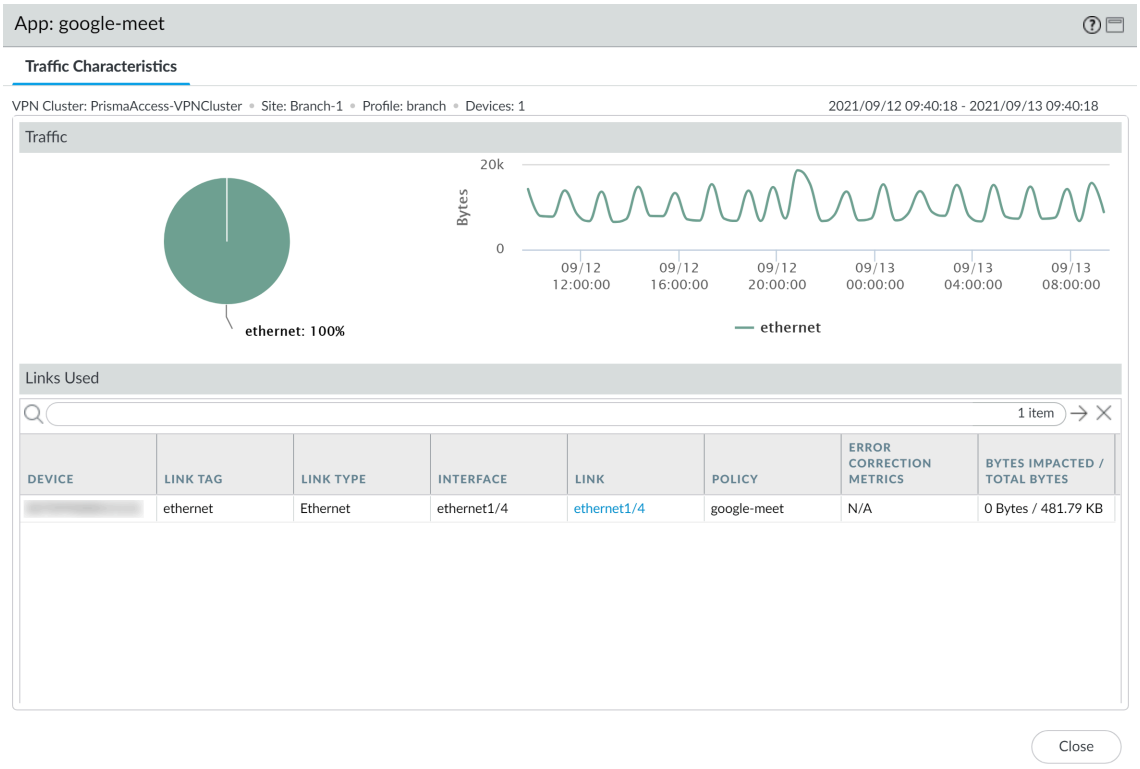
Si vous associez un profil de correction des erreurs avec une règle de politique SD-WAN pour une application, les colonnes **Error Correction Applied (Correction des erreurs appliquée)** s'affichent si des types de corrections d'erreurs ont été appliqués et, le cas échéant, lesquels. De plus, vous pouvez consulter **Error Corrected Sessions/Impacted Sessions/Total Sessions (Sessions au cours desquelles des erreurs ont été corrigées/Sessions impactées/Sessions totales)** pour comprendre, du nombre total de sessions sur la période spécifiée, combien de sessions comportaient des erreurs qui ont été corrigées par le pare-feu de la branche ou de la plateforme.

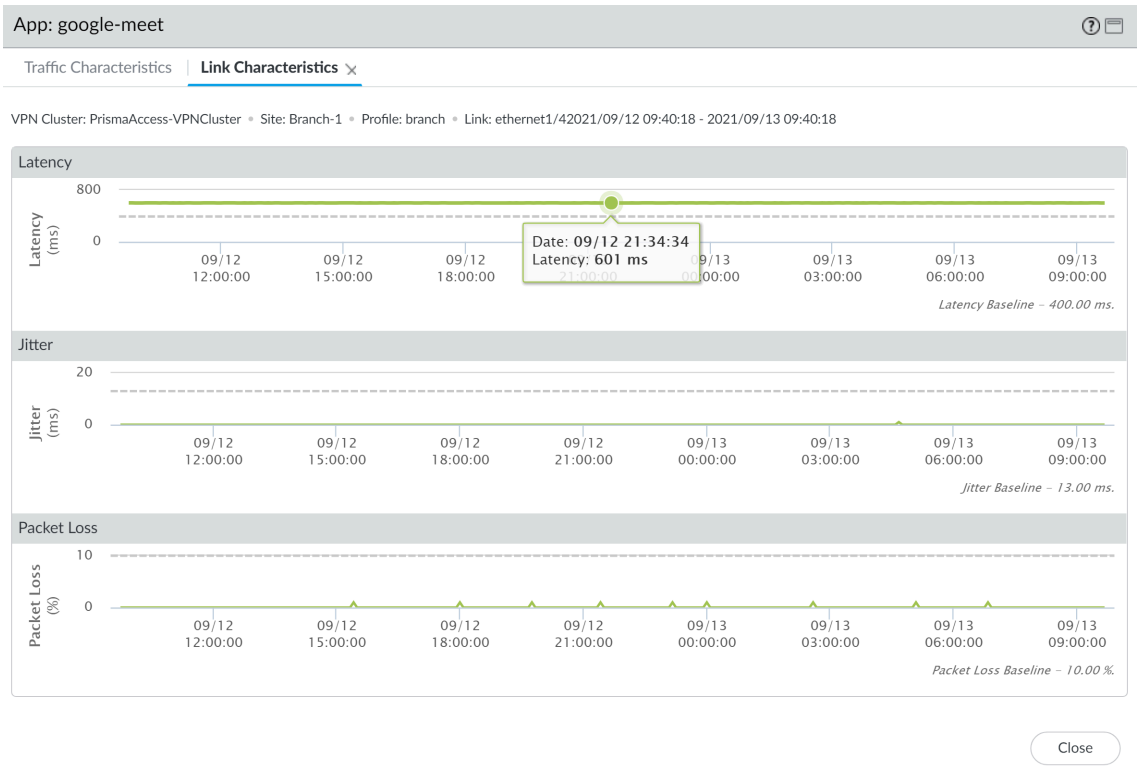
Cliquez sur **PDF/CSV** pour exporter les informations détaillées des applications et des liens du Site au format PDF ou CSV.



STEP 5 | Cliquez sur une application impactée pour afficher les informations au niveau des applications ou des liens.

Par exemple, consultez les caractéristiques des liaisons d'une application pour comprendre la latence, la gigue et la perte des paquets de l'application sur la liaison spécifiée. De plus, vous pouvez consulter le moment où la correction des erreurs a été appliquée pour la liaison.





Générer un rapport SD-WAN

Configurez et générez un rapport SD-WAN donnant des informations sur les applications et les liens présentant la plus grande fréquence de dégradation de qualité du chemin. L'ordre dans lequel les applications et les liens apparaissent dans un rapport se base sur la quantité de données impactées ; plus il y a de données impactées, plus l'application ou le lien apparaît dans le rapport. Les rapports SD-WAN sont générés le cas échéant et ne peuvent être programmés. Utilisez les rapports SD-WAN pour vérifier la bande-passante correcte de l'application ou du lien ou pour vous assurer que l'impact sur l'application ou le lien n'a pas été ressenti par les utilisateurs. Par exemple, si votre ISP a garanti une certaine capacité de bande-passante pour un lien, générez un rapport de Performance des liens pour ce lien afin de vérifier que la bande passante garantie est respectée.

Depuis le serveur de gestion Panorama™, vous ne pouvez générer que des rapports pour les applications ou les liens sur tous vos pare-feux activés SD-WAN. Pour générer un rapport pour des applications ou des liens traités par un pare-feu individuel, vous devez créer et générer le rapport localement sur le pare-feu.

Si aucune donnée n'est présente ou si l'écran indique que SD-WAN n'est pas défini, vérifiez dans Compatibility Matrix (matrice de compatibilité) que la version Panorama que vous utilisez prend en charge la version du plug-in SD-WAN que vous essayez d'utiliser.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Sélectionnez **Panorama** > **SD-WAN** > **Reports** (rapports SD-WAN de Panorama) et **Add** (ajoutez) un nouveau rapport.

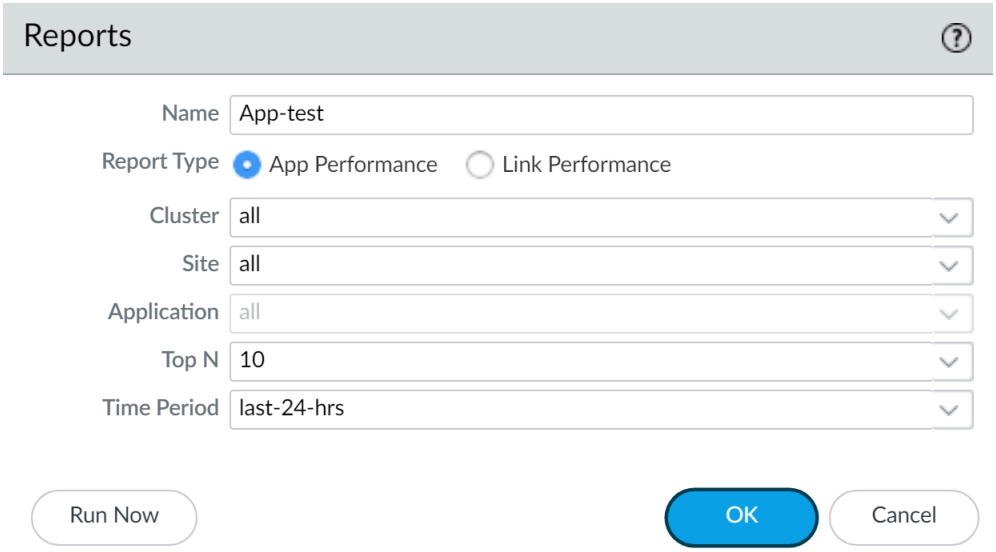
STEP 3 | Configurez les paramètres du rapport SD-WAN.

1. Saisissez un **Name** (Nom) descriptif pour le rapport.
2. Choisissez le **Report Type (Type de rapport)** à générer :
   - Sélectionnez**App Performance** (Performance des applications) pour générer un rapport donnant des informations uniquement sur la bonne performance des applications.
   - Sélectionnez**Link Performance** (Performance des liens) pour générer un rapport donnant des informations sur la bonne performance des liens.
3. Sélectionnez le **Cluster** VPN pour lequel générer le rapport. Par défaut, **all** (tous) est sélectionné.
4. Sélectionnez un **Site** dans le cluster VPN sélectionné pour lequel générer le rapport. Par défaut, **all** (tous) est sélectionné.

   Si vous avez sélectionné **all** (tous) les Clusters, alors ce champ est grisé et aucun Site ne peut être sélectionné.
5. (Performance des applications uniquement) Sélectionnez l'**Application** pour laquelle générer le rapport.

   Si vous avez sélectionné **all** (tous) les Clusters et Sites, alors ce champ est grisé et aucune Application individuelle ne peut être sélectionnée.
6. (Performance des liens uniquement) Sélectionnez le**Link tag** (étiquette de lien) pour laquelle générer le rapport. La sélection d'une étiquette de lien génère un rapport pour tous les liens regroupés utilisant cette étiquette dans le cluster ou le site. Par défaut, **all** (tous) est sélectionné.
7. (Performance des liens uniquement) Sélectionnez le**Link Type** (type de lien) pour lequel générer le rapport. La sélection d'un type de lien génère un rapport pour tous les liens de ce type dans le cluster ou le site. Par défaut, **all** (tous) est sélectionné.
8. Sélectionnez les applications ou les liens **Top N** pour les inclure dans le rapport. Ce paramètre détermine le nombre d'applications ou liens qui subissent une dégradation de leur état à inclure dans le rapport. Par défaut, le rapport inclut les **5** premiers applications ou liens qui subissent une dégradation de leur état.
9. Indiquez la**Time Period** (Période de temps) selon laquelle générer le rapport. Par défaut, **None** (Aucune) est sélectionné et la demande se fait sur tout l'historique de l'état des applications ou liens.

STEP 4 | Cliquez sur **Run Now** (Exécuter maintenant)pour générer le rapport sur demande.



STEP 5 | Affichez le rapport généré et cliquez sur **Export XML** (Exporter XML) pour exporter le rapport au format XML sur votre périphérique local. Lorsqu vous êtes prêt, cliquez sur **Close** (Fermer).

App Performance Report by application - top 10 apps across all clusters and all sites

Time period 2020-09-15 14:14:24 to 2020-09-16 14:14:24

CLUSTER	SITE	APP	SAAS MONITORING	AVG FLAP/SESSION	IMPACTED/TOT... BYTES PER APP	ERROR CORRECTED/IM... SESSIONS PER APP	POLICIES	Link Info			
								LINK TAG	LINK TYPE	ERROR CORRECTED METRICS	IMPACTED/... BYTES PER LINK TAG
ClusterHub245	Branch20	ssh	Disabled	175	9.08GB/339.08...	0/4/12	Tunnel_SCP	BroadBand2	ADSL/DSL		4.45GB/23....
							Tunnel_SCP	BroadBand1	Cablemodem		4.62GB/51....
ClusterHub245	Hub254	bgp	Disabled	16	904.35KB/19.4...	0/1/1		BroadBand2			904.24KB/9...
								BroadBand1	Ethernet		117.00b/11...
ClusterHub245	Branch50	ftp	Disabled	0	900.00b/1.64KB	0/1/2	Tunnel_FTP	BroadBand1	Cablemodem		900.00b/1.6...
ClusterHub245	Branch20	bgp	Disabled	15	380.00b/18.68...	0/1/1		BroadBand2	ADSL/DSL		170.00b/17...
								BroadBand1	Cablemodem		210.00b/21...
autogen_hubs_cl...	Hub254	dropbox-base	Disabled	0	0/38.41KB	0/0/33	DIA	BroadBand1	Ethernet		0/27.47KB
							DIA	BroadBand2	Ethernet		0/10.94KB
ClusterHub245	Branch20	taobao	Disabled	0	0/1.65MB	0/0/1.4k	DIA	BroadBand2	ADSL/DSL		0/729.81KB
							DIA,test-rule	BroadBand1	Cablemodem		0/962.53KB
ClusterHub245	Branch25	netbios-dg	Disabled	0	0/3.56KB	0/0/15	test-rule	BroadBand1	Cablemodem		0/3.56KB
ClusterHub245	Branch25	youku-base	Disabled	0	0/167.28KB	0/0/115	DIA	BroadBand2	ADSL/DSL		0/20.36KB
							DIA,test-rule	BroadBand1	Cablemodem		0/146.92KB
ClusterHub245	Hub254	insufficient-data	Disabled	0	0/24.92KB	0/0/105	BranchToBranch...	BroadBand1	Ethernet		0/13.05KB
							BranchToBranch...	BroadBand2	Ethernet		0/11.87KB
autogen_hubs_cl...	Hub254	apt-get	Disabled	0	0/62.36KB	0/0/2	DIA	BroadBand1	Ethernet		0/62.36KB

Export XML Close

STEP 6 | Dans la fenêtre des Rapports, cliquez sur **OK** pour enregistrer votre rapport configuré.

STEP 7 | Cliquez sur **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

Dépannage

Utilisez la Command Line Interface (interface de ligne de commande - CLI) du serveur de gestion Panorama™ pour afficher les informations SD-WAN et effectuer des opérations.

Utiliser les Commandes CLI pour les Tâches SD-WAN

Utilisez les Commandes CLI suivantes pour afficher et effacer les informations SD-WAN et afficher les compteurs généraux SD-WAN. Vous pouvez aussi afficher les informations du tunnel VPN, les informations BGP et les informations de l'interface SD-WAN.

Si vous souhaitez...	Utilisez ...
Afficher ou Effacer des informations SD-WAN	
• Afficher les noms des chemins d'accès et les ID d'une interface SD-WAN, leur état, les adresses IP locales et des pairs et le numéro de l'interface tunnel.	`> afficher toutes les connexions SDWAN | <sdwan-interface>`
• Afficher le nombre et le pourcentage de sessions distribuées vers chaque membre du tunnel d'une interface SD-WAN virtuelle.	`> afficher nom de la politique de distribution de session sdwan <sdwan-policy-name>`
• Afficher les noms des règles de politique SD-WAN qui dirige le trafic vers l'interface SD-WAN virtuelle spécifiée, ainsi que la méthode de distribution du trafic, la latence configurée, la gigue et les seuils de perte de paquets, les étiquettes de liens identifiées pour la règle et les interfaces de tunnel du membre.	`> afficher la règle sdwan vif sdwan.x`
• Afficher les événements SD-WAN tels que la sélection du chemin d'accès et les mesures de la qualité du chemin d'accès. *Pour PAN-OS 10.0.0 et 10.0.1, lorsque vous apportez une modification à la configuration SD-WAN (comme un changement au profil de qualité du chemin) qui entraîne la sélection d'un autre chemin SD-WAN, le journal du trafic ne calcule pas le changement de chemin ou ne le journalise pas.*	`> afficher événement SDWAN`
• Effacer les événements SD-WAN.	`> effacer événement sdwan`

Si vous souhaitez...	Utilisez ...
• Afficher la latence, la gigue et la perte de paquets d'une interface SD-WAN virtuelle (précisez le numéro ou le nom de l'interface). Les mesures de latence, gigue et perte de paquets sont prises et leur moyenne est calculée selon trois délais. Chaque délai a une version saine, qui augmente lorsque la valeur du paramètre sain (qui dépasse le seuil) change. En plus de la mesure en temps réel, il existe une mesure de l'usage courant qui affiche la valeur du paramètre lorsque la modification de valeur en temps réel a dépassé le seuil pour la dernière fois.	`afficher toutes les stats de surveillance de chemin sdwan dia-vif` `afficher toutes les stats de surveillance de chemin sdwan dia-vif`
• Afficher le nom de la règle de politique SD-WAN à laquelle correspond la session, les interfaces des tunnels source et destination, la latence configurée, la gigue et le pourcentage de perte de paquets pour la règle et la méthode de distribution du trafic. *Pour PAN-OS 10.0.0 et 10.0.1, lorsque vous apportez une modification à la configuration SD-WAN (comme un changement au profil de qualité du chemin) qui entraîne la sélection d'un autre chemin SD-WAN, le journal du trafic ne calcule pas le changement de chemin ou ne le journalise pas.*	`> afficher chemin session sdwan sélectionner id session <session-id>`
• Afficher le mode de surveillance pour le lien SD-WAN virtuel (Agressif ou Souple) et les intervalles de mise à jour.	`> afficher le nom du chemin du paramètre de surveillance du chemin sdwan <sdwan-path-name>`
• Afficher le mode de surveillance pour l'interface SD-WAN virtuelle (Agressif ou Souple), les intervalles de mise à jour et les statistiques de sondage.	`> afficher le paramètre de surveillance de chemin sdwan vif <sdwan.x>`
Afficher les Compteurs généraux afin de diagnostiquer les problèmes SD-WAN	

Si vous souhaitez...	Utilisez ...

• Sur une branche, vérifie que le nombre de paquets de requêtes de sonde SD-WAN transmis correspond au nombre de paquets de requêtes de sonde reçus.
Sur le pare-feu d'une branche, la plupart des tunnels SD-WAN sont l'initiateur, ce qui signifie que le tunnel aura un sondage de contrôle du chemin SD-WAN activé.
	> afficher le delta du filtre global du compteur oui
	`flow_sdwan_prob_req_tx`
	`flow_sdwan_prob_reply_rx`

• Sur un hub, vérifie que le nombre de paquets de requêtes de sonde SD-WAN reçus correspond au nombre de paquets de requêtes de sonde transmis.
Sur le pare-feu d'un hub, la plupart des tunnels SD-WAN sont le répondeur, ce qui signifie que le tunnel aura un sondage de contrôle du chemin SD-WAN désactivé.
	> afficher le delta du filtre global du compteur oui
	`flow_sdwan_prob_req_rx`
	`flow_sdwan_prob_reply_tx`

Afficher les informations du tunnel VPN	
• Afficher tous les tunnels créés sur le pare-feu.	**> afficher le flux vpn**
• Afficher les détails des tunnels individuels identifiés par leur nom.	**> afficher le nom du flux vpn <name>**
• Afficher les détails des tunnels individuels identifiés par leur ID.	**> afficher id du tunnel de flux VPN <tunnel-id>**
• Afficher les détails de Internet Key Exchange (échange de clés Internet - IKE) Phase 1 et Phase 2 pour tous les tunnels.	**> afficher VPN ike-sa**
• Afficher Security Association (association de sécurité - SA) IKEv2 et les SA child IPSec IKEv2 d'une passerelle spécifique.	**>afficher passerelle vpn ike-sa <gateway>**
• Afficher les détails du tunnel.	**> afficher le tunnel vpn**
Afficher les informations BGP	

Si vous souhaitez...	Utilisez ...
• Afficher le résumé BGP pour Virtual Router (routeur virtuel - VR).	`> afficher le résumé du protocole de routage BGP routeur virtuel <virtual-router>`
• Afficher le résumé des pairs BGP.	`> afficher le protocole de routage bgp nom du pair routeur virtuel<virtual-router>`
• Affichez le résumé de Routing Information Base (base d'informations de routage - RIB).	`> afficher le protocole de routage BGP LOC-RIB`
Afficher les informations de l'interface SD-WAN parmi RIB et FIB	
• Afficher la nouvelle interface de sortie SD-WAN.	`>Afficher itinéraire de routage`
• Afficher les interfaces SD-WAN dans Forwarding Information Base (base d'informations de transfert - FIB).	`afficher fib de routage`

Remplacer un périphérique SD-WAN

Le processus d'authentification de retour de marchandise (RMA) vous permet de remplacer les périphériques SD-WAN défaillants ou défectueux par des périphériques SD-WAN fonctionnels neufs ou réutilisés dans une branche ou un site de centre de données. Un périphérique SD-WAN peut présenter des pannes ou des dysfonctionnements pour un certain nombre de raisons, telles qu'une défaillance de la puce du périphérique, une mauvaise configuration du périphérique ou l'usure quotidienne. Si le périphérique SD-WAN est inutilisable en raison d'un dysfonctionnement ou d'une panne globale, remplacez le périphérique défaillant ou défectueux à l'aide du processus RMA.

Un échec de validation se produit sur Panorama™ et les appareils gérés si vous essayez de remplacer un pare-feu SD-WAN à partir d'un déploiement existant sans suivre un processus RMA approprié.

Avant de lancer le processus RMA :

- Passer en revue Before Starting RMA Firewall Replacement (Avant de commencer le remplacement d'un pare-feu RMA).
- Le SD-WAN génère des configurations, telles que des passerelles IPSec et des ID de clé, en fonction du numéro de série du périphérique. Par conséquent, vous devez mettre à jour le numéro de série du pare-feu de remplacement pour que SD-WAN puisse reconnaître le nouveau pare-feu et éviter les échecs de validation. Découvrez si votre configuration SD-WAN comporte des références d'objets IPSec ou VPN à l'ancien pare-feu :
  - Pour remplacer un pare-feu de branche dans un déploiement haute disponibilité (HA), connectez-vous au pare-feu du hub et sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Gateways (Passerelles IKE)**. Recherchez le numéro de série (sans espaces) de l'ancien pare-feu. Si vous obtenez un ou plusieurs résultats de recherche, cela indique que le SD-WAN fait référence à l'ancien numéro de série du pare-feu dans la configuration de passerelle. Dans ce cas, nous vous recommandons de déconnecter l'ancien pare-feu de branche de Panorama et du déploiement HA.
  - Pour remplacer un pare-feu dans un déploiement Full Mesh sans hubs, recherchez les numéros de série de l'ancien pare-feu sur l'un des pare-feu de branche. Si vous obtenez un ou plusieurs résultats de recherche, cela indique que le SD-WAN fait référence à l'ancien numéro de série du pare-feu dans la configuration de passerelle. Dans ce cas, nous vous recommandons de déconnecter l'ancien pare-feu de branche de Panorama et du déploiement Mesh.
  - Pour remplacer un pare-feu autonome, il n'est pas nécessaire de rechercher le numéro de série.

Utilisez le flux de travail suivant pour restaurer la configuration d'un pare-feu géré en cas de RMA.

STEP 1 | Sélectionnez **Panorama** > **SD-WAN** > **VPN Clusters (Clusters VPN)** et supprimez l'ancien pare-feu.

STEP 2 | Sélectionnez **Panorama** > **SD-WAN** > **Devices (Périphériques)** et supprimez l'ancien pare-feu.

STEP 3 | Validez les modifications sur Panorama.

STEP 4 | (Déploiements HA uniquement) Transmettez les modifications à tous les hubs et aux autres homologues HA (à l'exception de l'ancien pare-feu qui doit être remplacé). Avant de continuer, vérifiez le succès de la validation sur les hubs et les pare-feu autonomes. Si la recherche de l'ancien numéro de série du pare-feu ne renvoie aucune configuration de passerelle, vous pouvez ignorer cette étape.

STEP 5 | Configurez un pare-feu de remplacement RMA.

STEP 6 | (Déploiements HA uniquement) Établissez une connexion HA entre le pare-feu de remplacement et le pare-feu autonome. Le pare-feu ayant une valeur numérique plus basse et, par conséquent, une priorité plus élevée, est désigné comme étant actif. Pour éviter que votre pare-feu de remplacement ne devienne un homologue HA actif, assurez-vous qu'une priorité de périphérique plus élevée ne lui est pas attribuée.

STEP 7 | Sélectionnez **Panorama** > **SD-WAN** > **Devices (Périphériques)** et ajoutez le nouveau pare-feu de branche.

STEP 8 | Sélectionnez **Panorama** > **SD-WAN** > **VPN Clusters (Clusters VPN)** et ajoutez le nouveau pare-feu de branche.

STEP 9 | Validez les modifications sur Panorama.

STEP 10 | Sélectionnez **Commit (Valider)** > **Push to Devices (Transmettre aux périphériques)** et transmettez l'intégralité de la configuration gérée par Panorama aux hubs et aux deux homologues HA de la branche.

*Lorsque vous effectuez l'opération **Push to Devices (Transmettre aux périphériques)**, Panorama tente de transmettre les modifications à tous les périphériques du cluster pour les déploiements HA et hub-and-spoke. Pour éviter de transmettre les modifications à tous les périphériques, sélectionnez **Edit Selections (Modifier les sélections)** dans l'étendue de la transmission et désactivez tous les autres périphériques dans les périphériques **Device Groups (Groupe d'appareils)**et les **Templates (Modèles)**.*

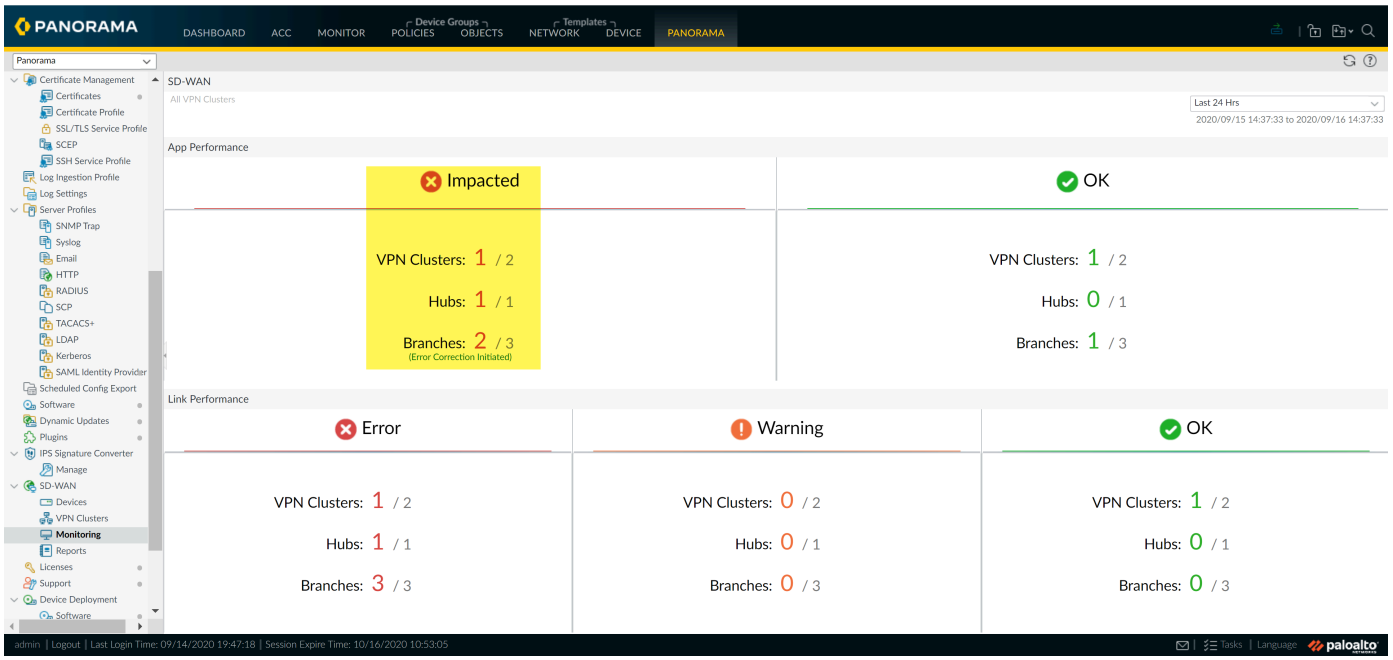
- *Dans les déploiements hub-and-spoke, sélectionnez les pare-feu de hub et la pile de modèles HA du système de branche vers lequel vous souhaitez transmettre la configuration. Par conséquent, les sites non sélectionnés peuvent devenir désynchronisés.*
- *Dans les déploiements Full Mesh, il est obligatoire de transmettre les modifications à tous les périphériques du cluster.*

Résoudre les problèmes de performance des applications

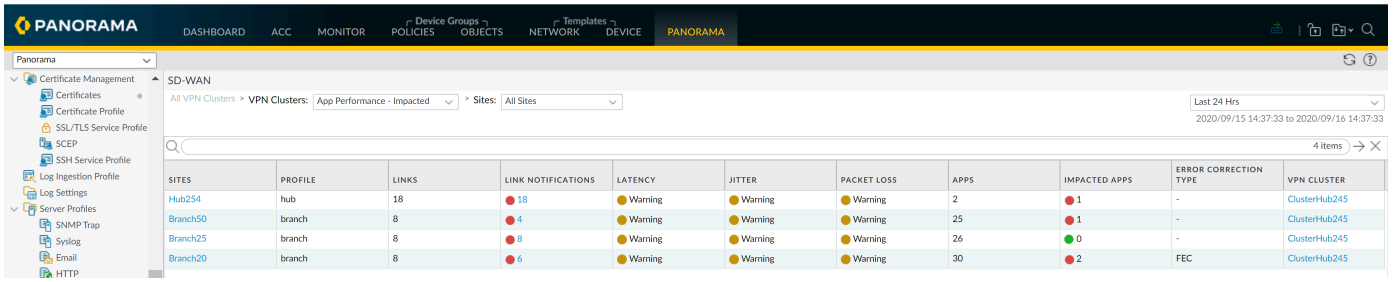
Comprendre ce qui provoque une dégradation de la performance de vos applications est crucial pour garantir que l'expérience de l'utilisateur ne soit pas impactée. Comprendre pourquoi vos clusters de VPN sont impactés et pourquoi le trafic de l'application a basculé vers différents liens aide à ajuster votre configuration SD-WAN.

STEP 1 | Connectez-vous à l'interface Web Panorama.

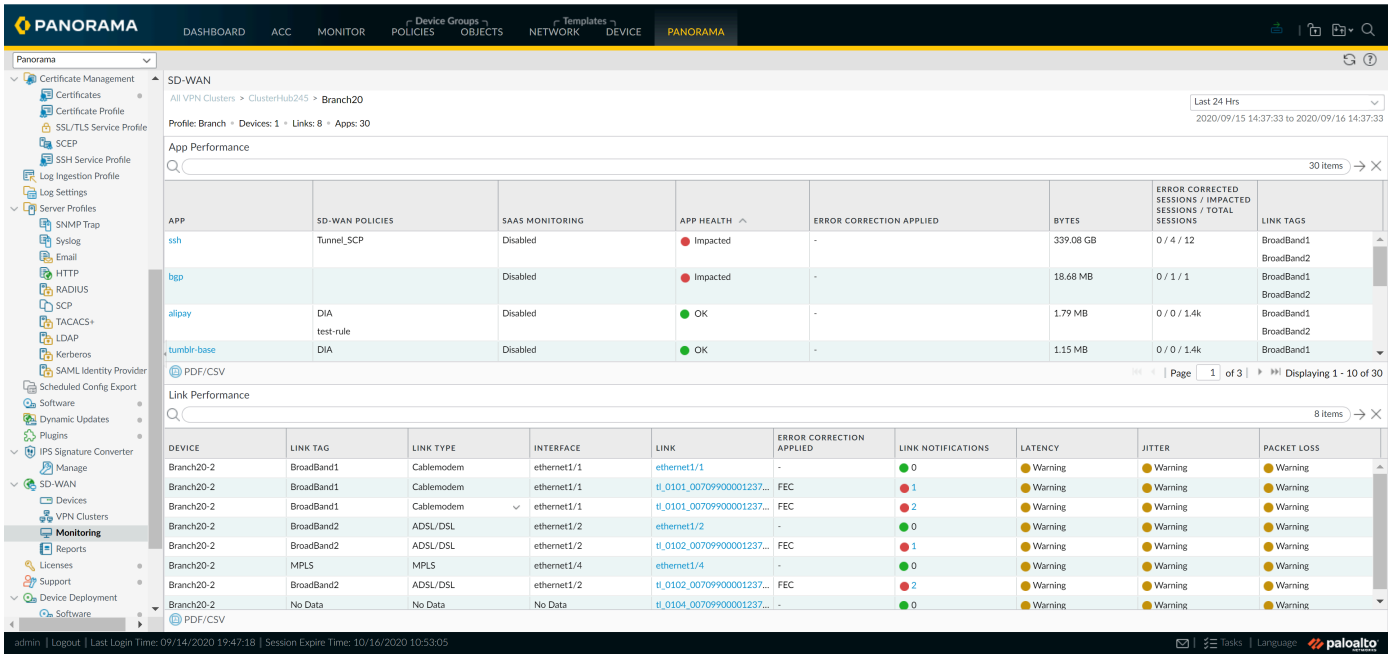
STEP 2 | Sélectionnez **Panorama** > **SD-WAN** > **Monitoring** (Surveillance SD-WAN Panorama) et affichez les clusters de VPN **Impacted** (impactés).



STEP 3 | Filtrez les clusters de VPN sur la base de votre mesure préférée dans la liste déroulante du **Site** et sélectionnez le délai. Dans cet exemple, nous affichons **All Sites** (tous les sites) contenant des clusters de VPN impactés au cours des 12 dernières heures.

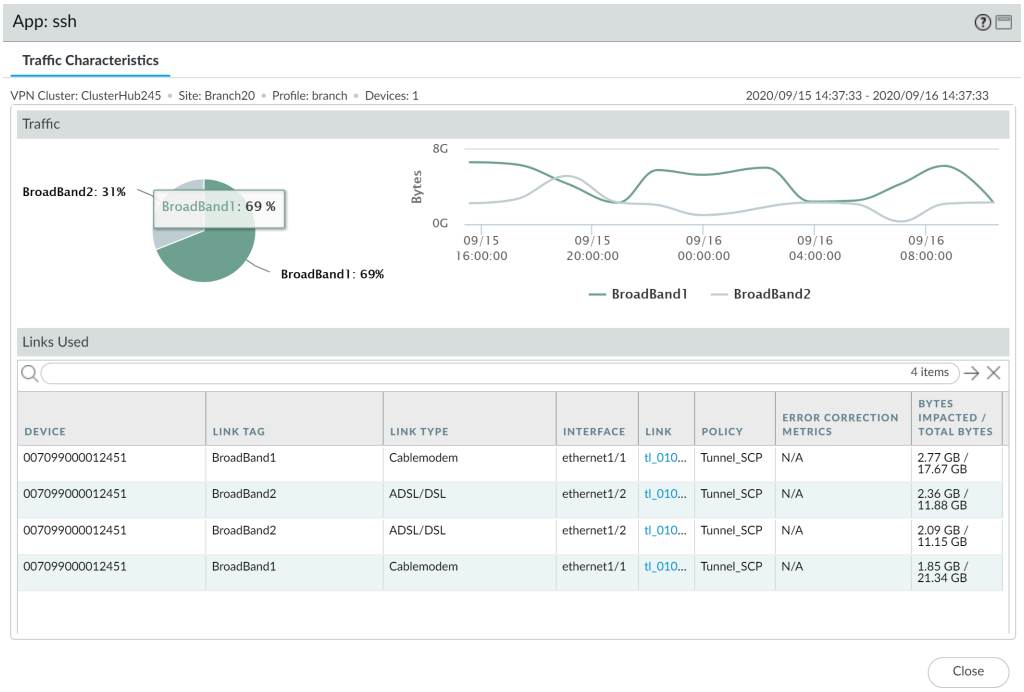


STEP 4 | Dans les colonnes des Sites, sélectionnez le pare-feu du hub ou de la branche impacté afin d'afficher les applications impactées et la performance du lien correspondant.



STEP 5 | Dans la partie App Performance (Performance des appli), cliquez sur une appli afin d'afficher les informations détaillées de Traffic Characteristic (caractéristiques du trafic) relatives au trafic de l'application comme le(s) service(s) internet et les liens utilisés :

- Passez en revue le diagramme en camembert afin de comprendre le détail du trafic de l'application sur vos services internet.
- Passez en revue le graphique linéaire afin de comprendre combien de bytes (octets) de données ont été transférés sur chaque service internet dans le temps.
- Passez en revue la partie Links Used (liens utilisés) afin de comprendre quels sont les liens que le trafic de l'application a utilisés et comprendre combien de bytes (octets) ont été impactés sur le nombre total de bytes (octets) dans le délai sélectionné.

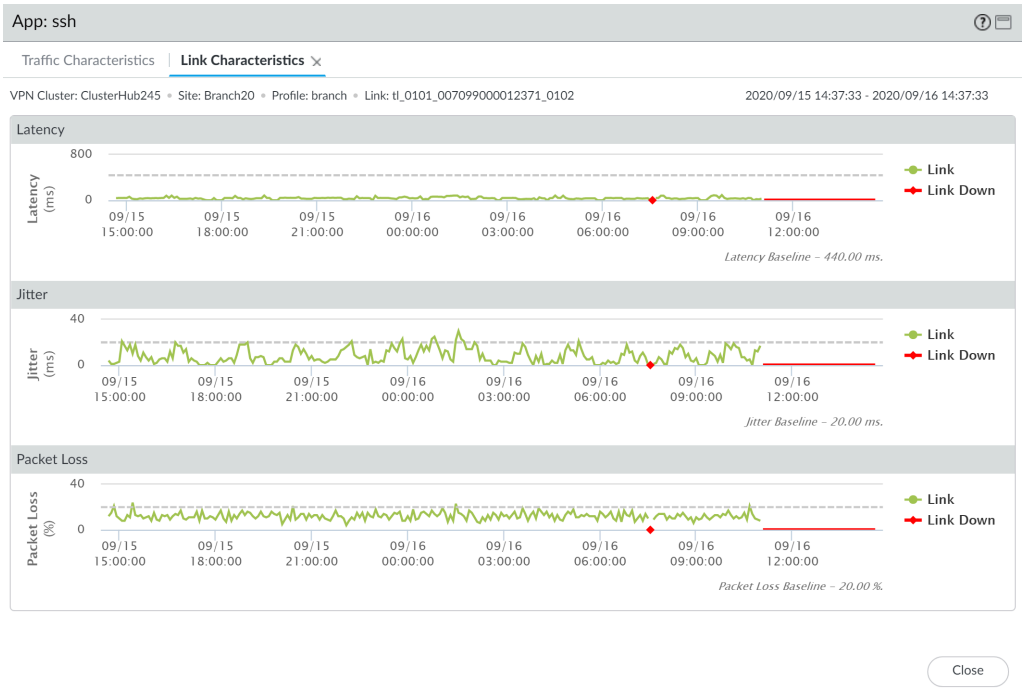


STEP 6 | Recherchez quelle mesure de l'état a fait que l'application a inversé des liens.

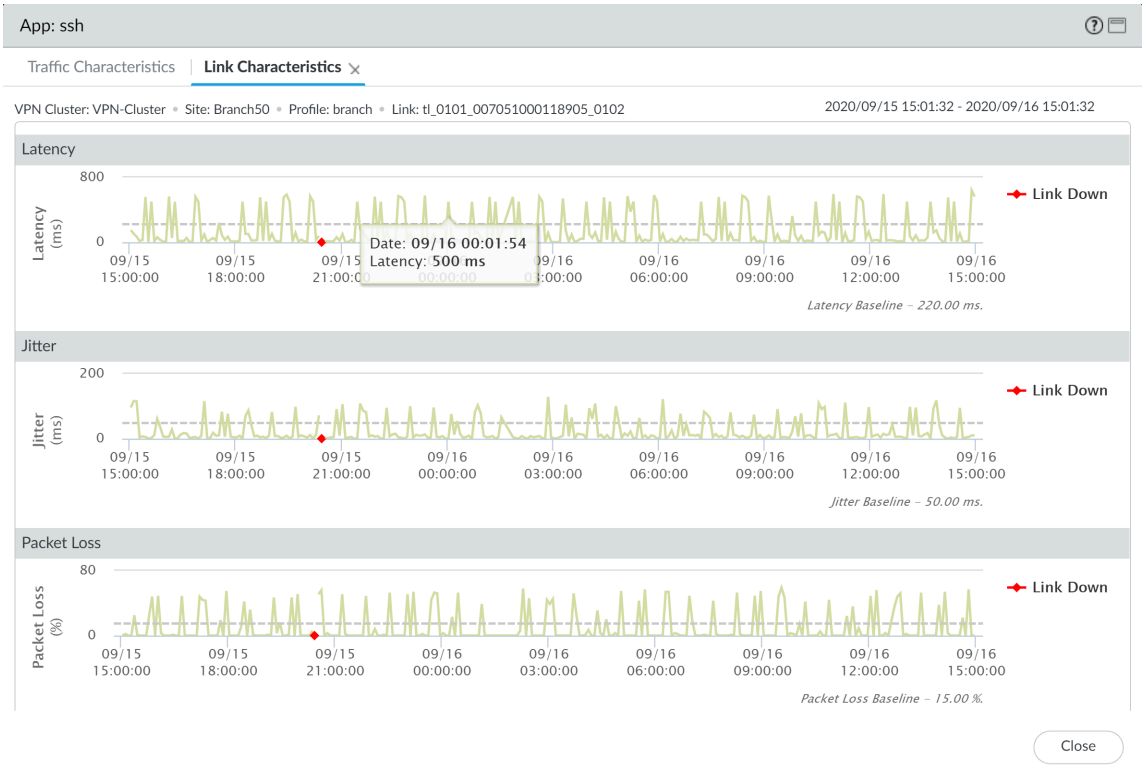
La ligne en pointillé indique la moyenne de sept jours de la mesure de l'état.

1. Dans la partie Links Used (liens utilisés) de l'onglet Traffic Characteristics (caractéristiques du trafic), cliquez sur un lien Ethernet afin d'afficher les Link Characteristics (caractéristiques des liens) détaillées (latence, instabilité et perte de

paquets) dans le délai indiqué dans l'Étape 2 afin de rechercher quelle est la mesure de l'état qui a fait que l'application a inversé des liens.



2. À l'onglet **Traffic Characteristics (Caractéristiques du trafic)**, sélectionnez une autre liaison pour afficher les caractéristiques de la liaison secondaire afin de mieux comprendre pourquoi le cluster VPN a été impacté.



STEP 7 | Une fois que vous avez identifié le trafic de l'application qui est impacté, envisagez ce qui suit afin de résoudre le problème :

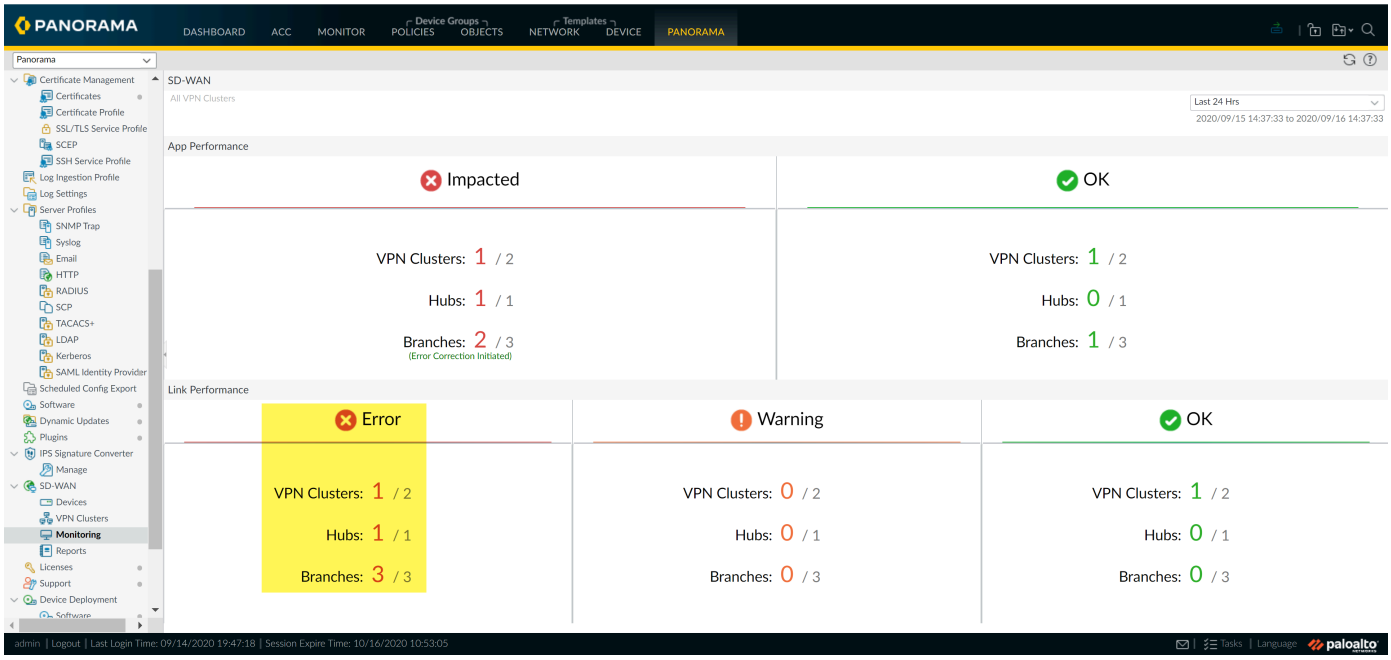
- Envisagez d'ajouter des liens supplémentaires au Traffic Distribution Profile (profil de distribution du trafic). En ajoutant des liens supplémentaires pour que le trafic de l'application bascule dessus, vous vous assurez que le trafic de l'application et l'expérience de l'utilisateur ne sont pas impactés par les liens dégradés.
- Reconfigurez les seuils de bon état de votre Path Quality Profile (profil de qualité des chemins d'accès). Il est possible que les seuils de bon état soient trop stricts, ce qui a pour conséquence un basculement de lien inutile. Par exemple, si vous avez une appli qui peut subir jusqu'à 18 % de perte de paquets avant que l'expérience de l'utilisateur ne soit impactée, en ayant un seuil de perte de paquets de 10 %, l'application basculera sur un lien différent sans que cela soit nécessaire.
- Consultez votre fournisseur de service internet (ISP) afin de déterminer s'il y a des impacts sur votre réseau hors de votre contrôle qu'il peut résoudre.

Résoudre les problèmes de performance des liens

Comprendre ce qui provoque une dégradation de la performance des liens est crucial pour garantir que l'expérience de l'utilisateur lorsqu'il utilise des applications et des services n'est pas impactée. Comprendre pourquoi des liens de clusters de votre VPN sont impactés aide à ajuster la configuration de votre SD-WAN afin de vous assurer que les expériences de l'utilisateur lorsqu'il utilise des applications et des services ne soient pas affectées par des liens dégradés.

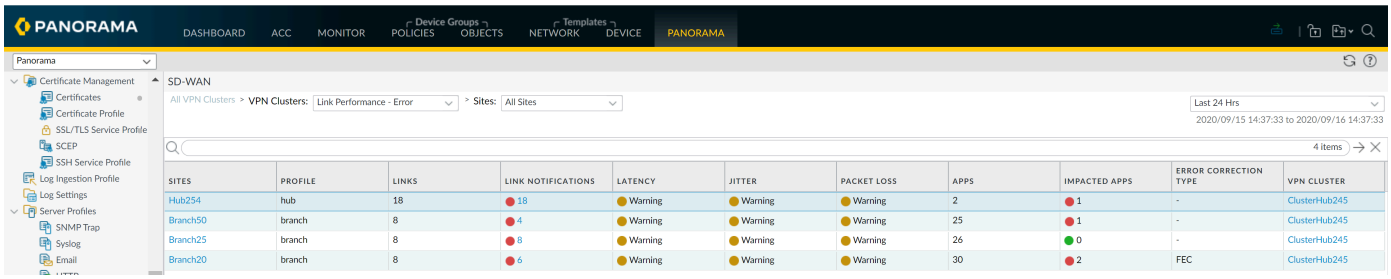
STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Sélectionnez **Panorama** > **SD-WAN** > **Monitoring** (Surveillance SD-WAN Panorama) et affichez les clusters de VPN **Impacted** (impactés).

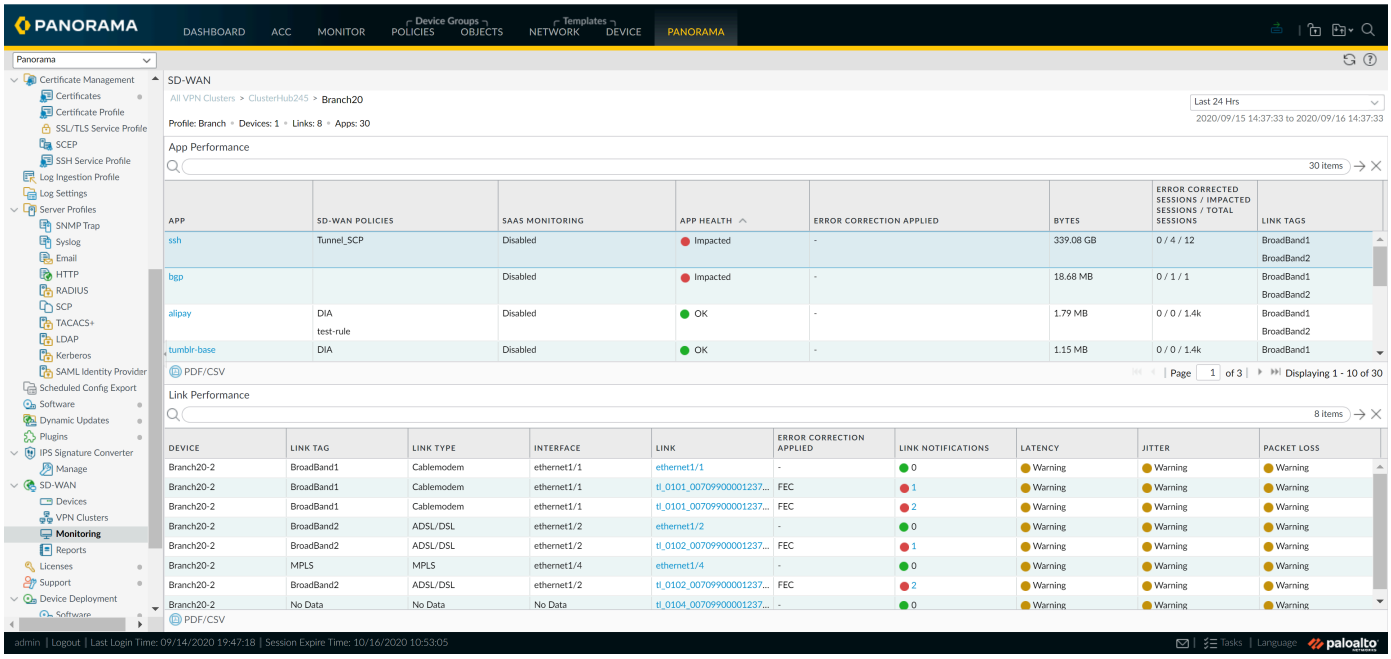


STEP 3 | Filtrez les clusters de VPN sur la base de votre mesure préférée dans la liste déroulante du **Site** et sélectionnez le délai. Dans les colonnes des Sites, sélectionnez le pare-feu du hub ou de la branche impacté afin d'afficher les applications impactées et la performance du lien correspondant.

Dans cet exemple, nous affichons **All Sites** (tous les sites) contenant des clusters de VPN impactés au cours des dernières 24 heures.

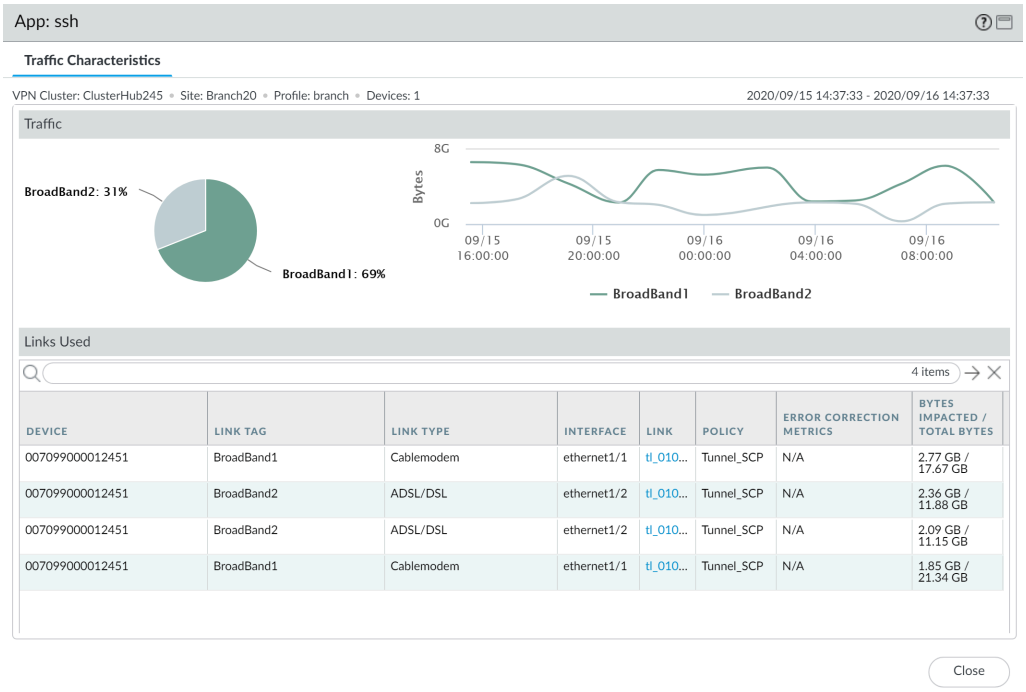


STEP 4 | Dans les colonnes des Sites, sélectionnez le pare-feu du hub ou de la branche impacté afin d'afficher les applications impactées et la performance du lien correspondant.



STEP 5 | Dans la partie App Performance (Performance des appli), cliquez sur une appli afin d'afficher les informations détaillées de Traffic Characteristic (caractéristiques du trafic) relatives au trafic de l'application comme le(s) service(s) internet et les liens utilisés :

- Passez en revue le diagramme en camembert afin de comprendre le détail du trafic de l'application sur vos services internet.
- Passez en revue le graphique linéaire afin de comprendre combien de bytes (octets) de données ont été transférés sur chaque service internet dans le temps.
- Passez en revue la partie Links Used (liens utilisés) afin de comprendre quels sont les liens que le trafic de l'application a utilisés et comprendre combien de bytes (octets) ont été impactés sur le nombre total de bytes (octets) dans le délai sélectionné.

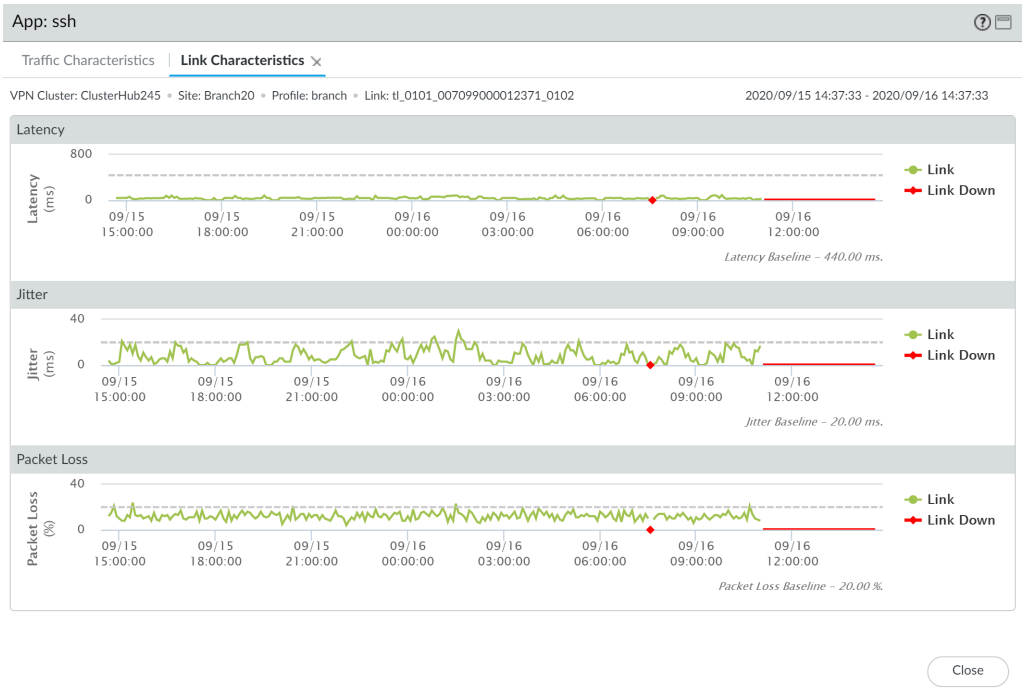


STEP 6 | Recherchez quelle mesure de l'état a fait que l'application a inversé des liens.

La ligne en pointillé indique le seuil que vous configurez lorsque Créer un Path Quality Profile (Profil de qualité du chemin d'accès).

1. Dans la partie Links Used (liens utilisés) de l'onglet Traffic Characteristics (caractéristiques du trafic), cliquez sur un lien Ethernet afin d'afficher les Link Characteristics (caractéristiques des liens) détaillées (latence, instabilité et perte de paquets) dans le délai indiqué dans l'Étape 2 afin de rechercher quelle est la mesure de l'état qui a fait que l'application a inversé des liens. Dans cet exemple, nous affichons Ethernet 1/1 et nous pouvons voir que le pourcentage de paquets perdus a régulièrement dépassé le seuil configuré pour le Path Quality Profile (profil de qualité

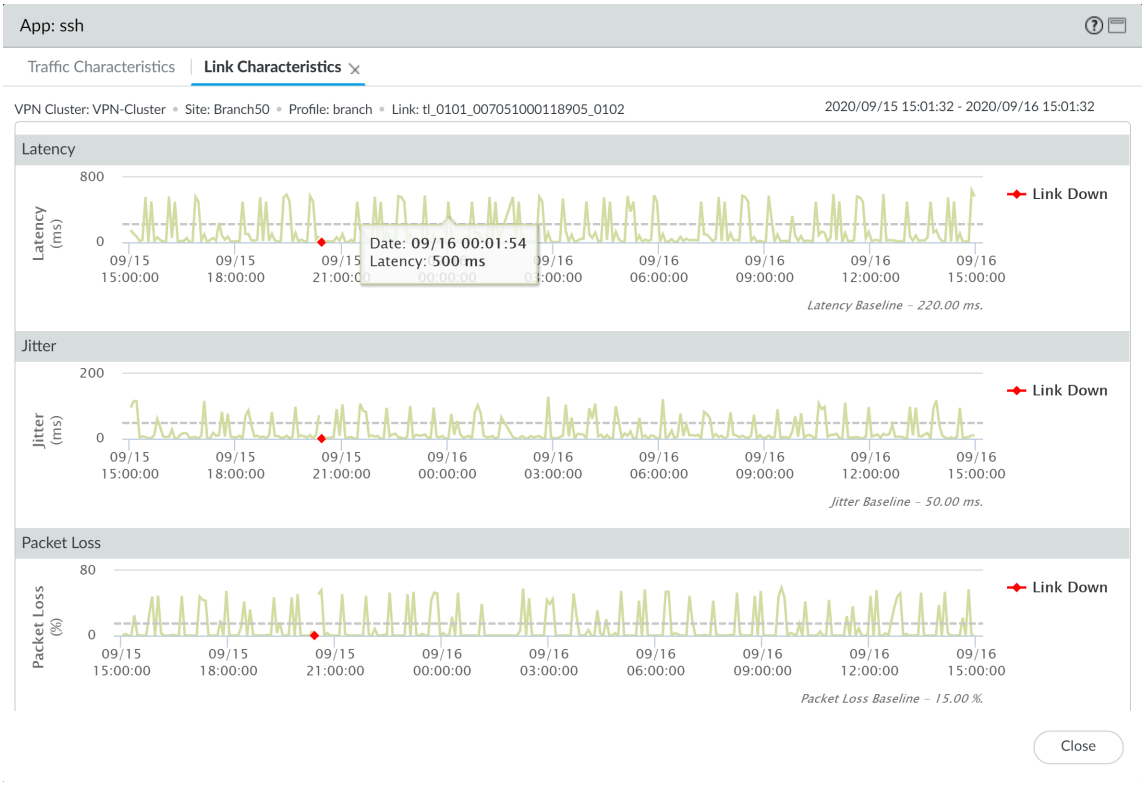
du chemin d'accès) de l'application et nous pouvons conclure que c'est la raison pour laquelle le trafic de l'application a basculé sur le meilleur lien suivant.



2. Dans l'onglet **Traffic Characteristics** (caractéristiques du trafic), sélectionnez un autre lien pour afficher Link Characteristics (caractéristiques des liens). Dans cet exemple, nous affichons l'Ethernet 1/4 et nous pouvons voir qu'après le basculement du trafic

de l'application, l'Ethernet 1/4 a subi une gigue de l'application qui a dépassé le seuil configuré. Cela a forcé le trafic de l'application à rebasculer sur l'Ethernet 1/1.

Comme les deux liens avaient des mesures de l'état qui ont été dépassées, le trafic de l'application ne pouvait pas basculer sur un lien sain, ce qui a eu pour conséquence un impact du cluster du VPN.



STEP 7 | Une fois que vous avez identifié le trafic de l'application qui est impacté, envisagez ce qui suit afin de résoudre le problème :

- Envisagez d'ajouter des liens supplémentaires au Traffic Distribution Profile (profil de distribution du trafic). En ajoutant des liens supplémentaires pour que le trafic de l'application bascule dessus, vous vous assurez que le trafic de l'application et l'expérience de l'utilisateur ne sont pas impactés par les liens dégradés.
- Reconfigurez les seuils de bon état de votre Path Quality Profile (profil de qualité des chemins d'accès). Il est possible que les seuils de bon état soient trop stricts, ce qui a pour conséquence un basculement de lien inutile. Par exemple, si vous avez une appli qui peut subir jusqu'à 18 % de perte de paquets avant que l'expérience de l'utilisateur ne soit impactée, en ayant un seuil de perte de paquets de 10 %, l'application basculera sur un lien différent sans que cela soit nécessaire.
- Consultez votre fournisseur de service internet (ISP) afin de déterminer s'il y a des impacts sur votre réseau hors de votre contrôle qu'il peut résoudre.

Mise à niveau de vos pare-feu SD-WAN

Passez en revue les Panorama Plugin for SD-WAN 2.1 Release Notes (Notes de version 2.1 sur le plugin Panorama pour SD-WAN), puis utilisez les procédures suivantes pour mettre à niveau votre Panorama et vos pare-feu SD-WAN gérés.

STEP 1 | Installer les mises à jour de contenu et logicielles pour Panorama.

STEP 2 | Mettre à niveau vos collecteurs de journaux.

- Mettre à niveau les collecteurs de journaux lorsque Panorama est connecté à Internet.
- Mettre à niveau les collecteurs de journaux lorsque Panorama n'est pas connecté à Internet.

STEP 3 | Mettre à niveau vos pare-feu de la plate-forme SD-WAN.

*Vous devez mettre à jour les pare-feux de votre plate-forme depuis PAN-OS 10.0.0 vers PAN-OS 10.0.1 ou une version ultérieure avant de pouvoir mettre à jour les pare-feux de votre branche. La mise à jour des pare-feux de branche avant les pare-feux de plate-forme peut entraîner une mauvaise surveillance des données (**Panorama** > **SD-WAN** > **Monitoring**) et les liens SD-WAN peuvent être affichés comme étant en panne de façon erronée.*

- Mettre à niveau les pare-feu lorsque Panorama est connecté à Internet.
- Mettre à niveau les pare-feu lorsque Panorama n'est pas connecté à Internet.

STEP 4 | Mettre à niveau vos pare-feu de la branche SD-WAN.

- Mettre à niveau les pare-feu lorsque Panorama est connecté à Internet.
- Mettre à niveau les pare-feu lorsque Panorama n'est pas connecté à Internet.

Installer le plug-in SD-WAN

Installez la version du plug-in SD-WAN sur votre serveur de gestion Panorama™ et sur vos pare-feu qui utilisent SD-WAN.

Consultez la matrice de compatibilité des plug-ins Panorama de Palo Alto Networks et passez en revue la version minimale de PAN-OS requise pour votre version de plug-in SD-WAN cible. Reportez-vous à la mise à niveau du plug-in SD-WAN avec la version PAN-OS compatible pour mettre à niveau le serveur de gestion Panorama et les pare-feu Palo Alto Networks compatibles avec la version du plug-in SD-WAN.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Installez la version du plug-in SD-WAN sur Panorama.

Si Panorama est en configuration High Availability (haute disponibilité - HA), répétez cette étape sur l'homologue HA de Panorama.

1. Sélectionnez **Panorama** > **Plugins** et **Check Now (Vérifier maintenant)** pour passer à la version la plus récente du plugin **`sd_wan`**.
2. **Download (Téléchargez)** et **Install (Installez)** la dernière version du plugin SD-WAN.
3. Après avoir réussi l'installation du plug-in SD-WAN, sélectionnez **Commit** (Validez) puis **Commit to Panorama** (Validez sur Panorama).

   Cette étape est nécessaire avant que vous puissiez valider des modifications de la configuration de Panorama.

STEP 3 | Une fois la nouvelle version du plug-in installée avec succès, consultez le **Dashboard (Tableau de bord)** Panorama et dans le widget Informations générales, vérifiez que le `plug-in SD-WAN` affiche la version de plug-in SD-WAN que vous avez installée.

Désinstaller le plug-in SD-WAN

Pour désinstaller le plug-in SD-WAN du serveur de gestion Panorama, vous devez supprimer votre configuration d'extension SD-WAN de Panorama avant de pouvoir réussir à désinstaller le plug-in SD-WAN.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Supprimez toutes les règles de politique qui permettent à BGP de fonctionner entre les hubs et les branches de votre SD-WAN.

1. Sélectionnez **Panorama** > **SD-WAN** > **Devices** > **BGP Policy** (Politique BGP des périphérique SD-WAN de Panorama) et **Remove** (Supprimez) les règles de politique de sécurité.
2. Cliquez sur **OK** pour enregistrer les modifications de votre configuration.

STEP 3 | Sélectionnez **Panorama** > **Plugins** (Plug-ins de Panorama) puis sélectionnez**Remove Config (Supprimer Config.)** pour le plug-in SD-WAN.

STEP 4 | Cliquez sur **Commit (Valider)** et **Commit and Push (Validez et appliquez)** vos modifications aux pare-feu que vous gérez.

STEP 5 | **Désinstaller** le plug-in SD-WAN.

Cliquez sur **OK** lorsqu'on vous le demande afin de poursuivre la désinstallation du plug-in SD-WAN.

