Guide de l'administrateur SD-WAN

1.0

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

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

About the Documentation

- To ensure you are viewing the most current version of this document, or to access 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

July 2, 2020

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
> Éléments de configuration SD-WAN
> Planifiez votre configuration SD-WAN

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.

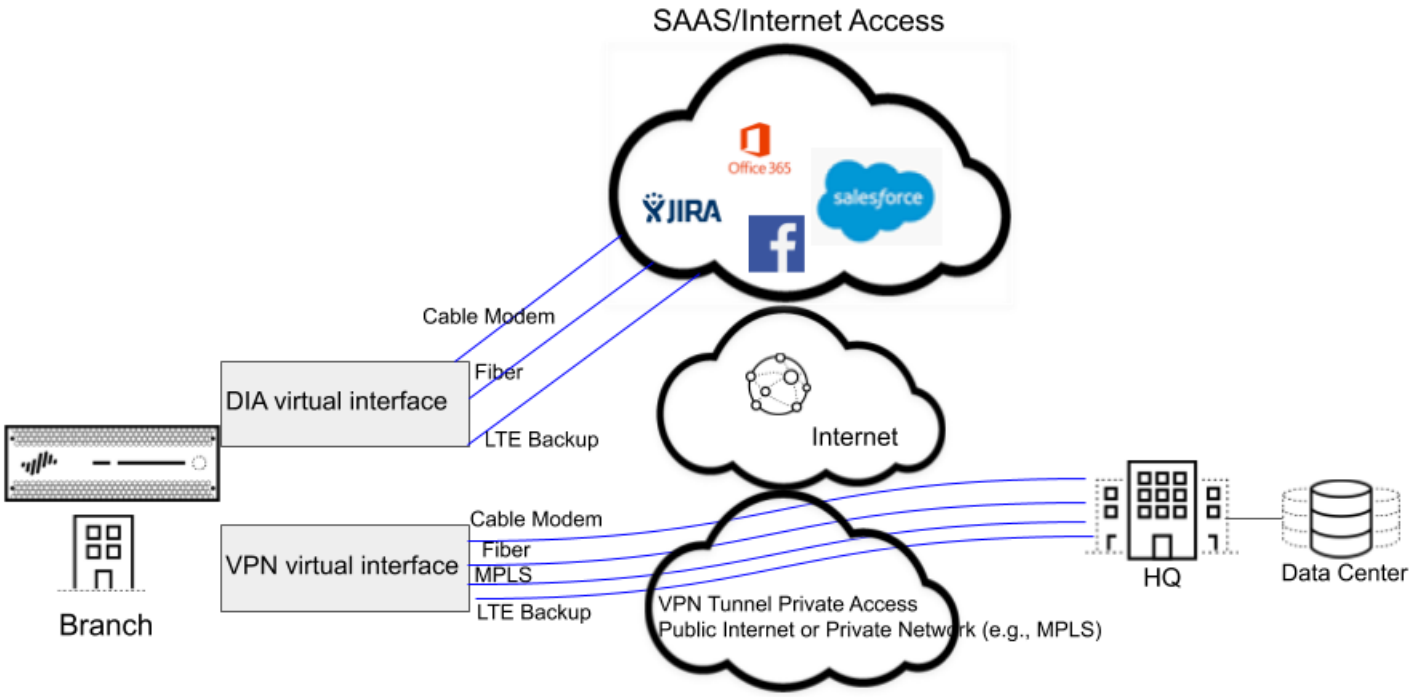
- Sécurité PAN-OS avec fonctionnalité SD-WAN
- Lien SD-WAN et Assistance pare-feu
- Gestion centralisée

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 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.

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

- PA-220
- PA-220R
- PA-820
- PA-850
- PA-3200 Series
- PA-5200 Series

- VM-300
- VM-500
- VM-700

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.

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.

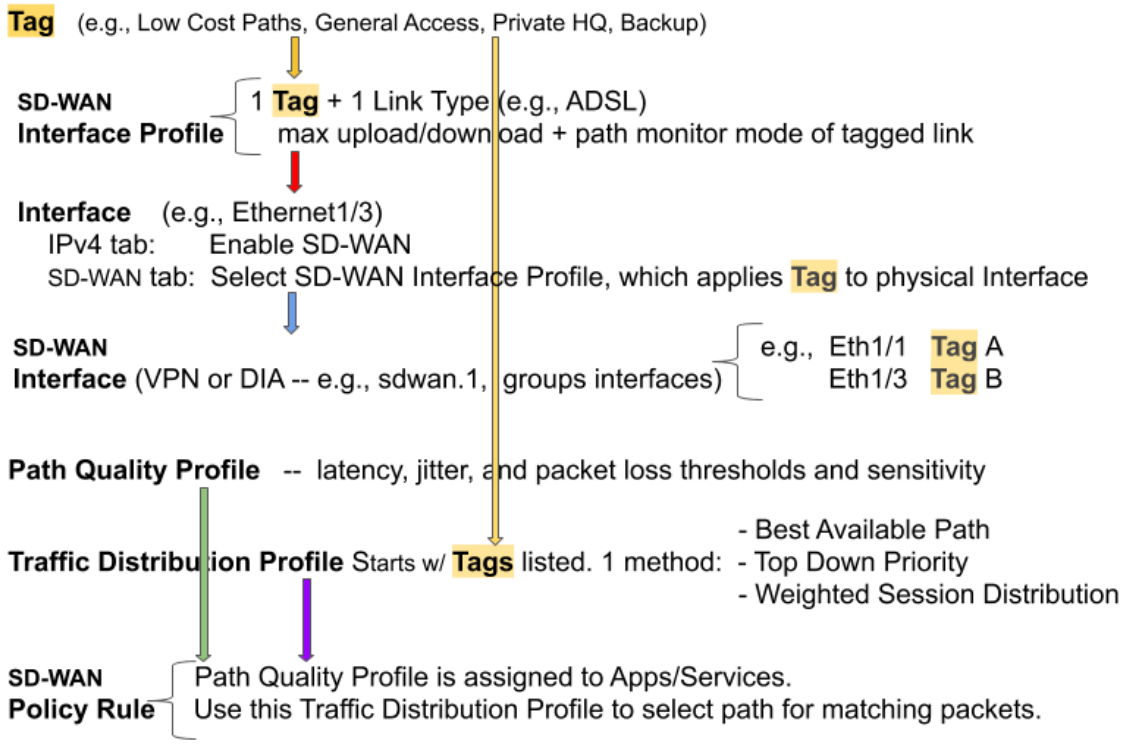
Commencez par comprendre votre utilisation de SD-WAN, puis examinez les éléments de la configuration SD-WAN, les méthodes de distribution de trafic et planifiez votre configuration SD-WAN. Afin de grandement accélérer la configuration, une bonne pratique consiste à exporter un fichier CSV de périphérique 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.

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 est compatible avec les fonctionnalités SD-WAN. Vous appliquez un Profile d'Interface SD-WAN à cette interface (flèche rouge) pour indiquer les caractéristique de l'interface. La flèche bleu 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.

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 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 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. 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 avezPlanifiez 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.

- 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
- Configurer une Interface virtuelle SD-WAN
- Créer un itinéraire par défaut vers l'interface SD-WAN
- Créer un Path Quality Profile (Profil de qualité du chemin d'accès)
- Traffic Distribution Profiles (profils de distribution du trafic) SD-WAN
- Créer un Traffic Distribution Profile (profil de distribution du trafic)
- Configurer une Règle de politique SD-WAN
- (PAN-OS 9.1.2 et version 9.1 ultérieures)Autoriser le basculement du trafic de l'accès direct à internet vers un lien MPLS
- Distribuer des sessions sans correspondance
- Ajouter des Périphériques SD-WAN à Panorama
- (Facultatif) Configurer les Périphérique HA pour SD-WAN
- Créer un cluster VPN
- (Facultatif) Créer une route statique pour 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 | Continuez versConfigurer 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 (mises à jour)** > **Software Updates (mises à jour des logiciels)**, 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 (plug-ins de Panorama)** 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 | Continuez versConfigurer 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.

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.

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.

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**, et **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 allez créer les zones prédéfinies nécessaires dans Panorama appelées **`zone-internet`**, **`zone-internal`**, **`zone-to-hub`**, et **`zone-to-branch`**. 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.

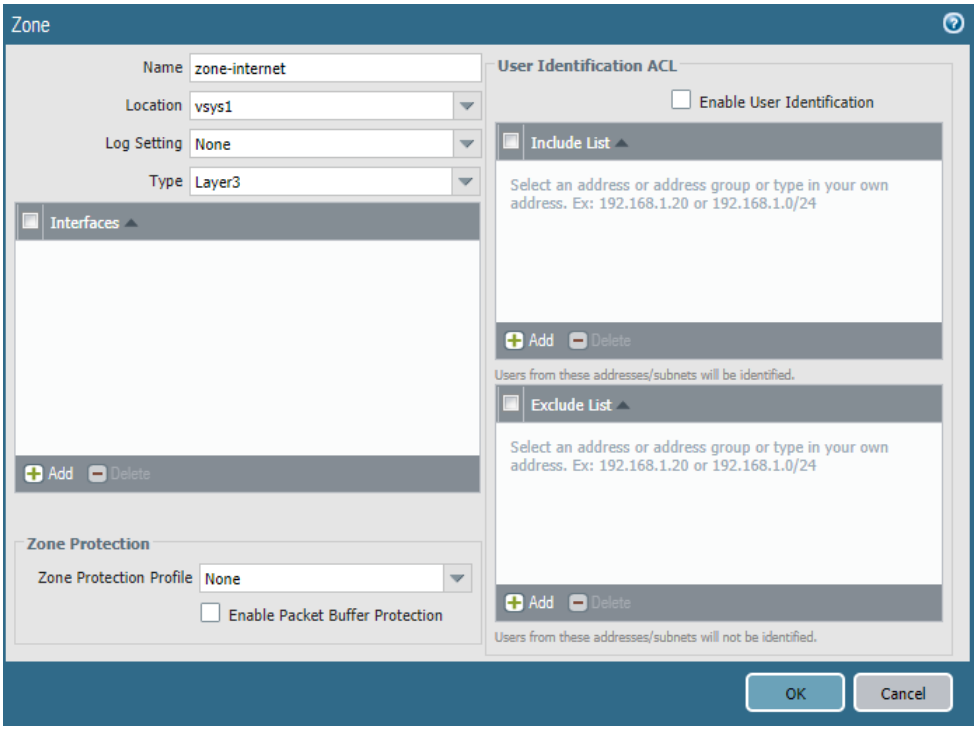
STEP 2 | Sélectionnez **Network** > **Zones** (Réseau Zones) et dans la liste déroulante du **Template** (Modèle), sélectionnez le network template (modèle de réseau) que vous avez créé au préalable.

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`**

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 **Source** > **Source Zone** (Source Zone de la source) 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.

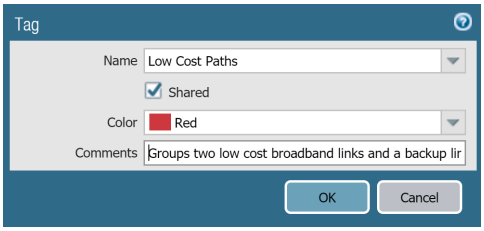
STEP 4 | Donnez un **Name (Nom)** descriptif à l'étiquette. par exemples ; Chemins à faible coût, Chemins onéreux, Accès général, HQ privé ou Sauvegarde.

STEP 5 | Activez (cochez) **Shared** (Partagé) afin que l'Étiquette de liens soit disponible pour tous les groupes de périphériques sur le serveur de gestion Panorama™ et chaque système virtuel (vsys) d'une plateforme ou d'une branche multi-vsys à laquelle vous l'appliquez.

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-onde/radio)**, **Satellite**, **WiFi**, ou **Other (Autre)**). 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 de point à point privés (MPLS, satellite, micro-onde et autres) 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.

STEP 9 | (PAN-OS 9.1.2 et versions 9.1 ultérieures) **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 **VPN Data Tunnel Support** (Assistance du tunnel de données VPN) pour les types de liens privés comme MPLS, satellite, ou micro-onde qui n'ont pas de capacité d'interruption d'internet. 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.
- 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 privés n'utilise pas). Le pare-feu utilise des zones pour segmenter le trafic qui a bascule en DIA depuis le trafic MPLS privé.

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). 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 | 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). 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 12 | (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 charge 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.

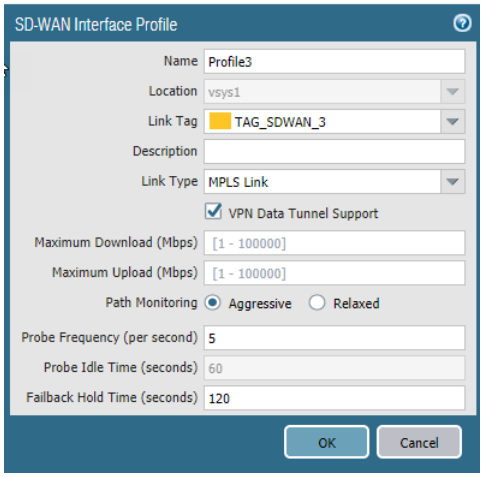
STEP 13 | Réglez la **Probe Frequency (per second)** (Fréquence de sondage (par seconde), qui correspond au nombre de fois par seconde où le pare-feu envoie un paquets de sondage à l'extrémité opposée du lien SD-WAN (la fourchette est de 1 à 5 ; la valeur par défaut est de 5). Les paramètres par défaut 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 14 | 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 15 | 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 16 | Cliquez sur **OK** pour enregistrer le profil.



STEP 17 | **Commit** (Validez) et **Commit and Push** (Validez et appliquez) les modifications de votre configuration.

STEP 18 | 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, reportez-vous à la section 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 et une passerelle et attribuer un SD-WAN Interface Profile (Profil d'interface SD-WAN) à l'interface.

Après avoir utilisé Panorama pour créer un cluster VPN et exporté les informations de votre branche et de votre hub dans le fichier CSV, la configuration Auto VPN du plug-in SD-WAN utilise ces informations pour générer une configuration pour les branches et les hubs associées qu 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** > **Interfaces** > **Ethernet**(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 | Sélectionnez un **Virtual Router** (routeur virtuel) ou créez un nouveau Routeur virtuel.

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

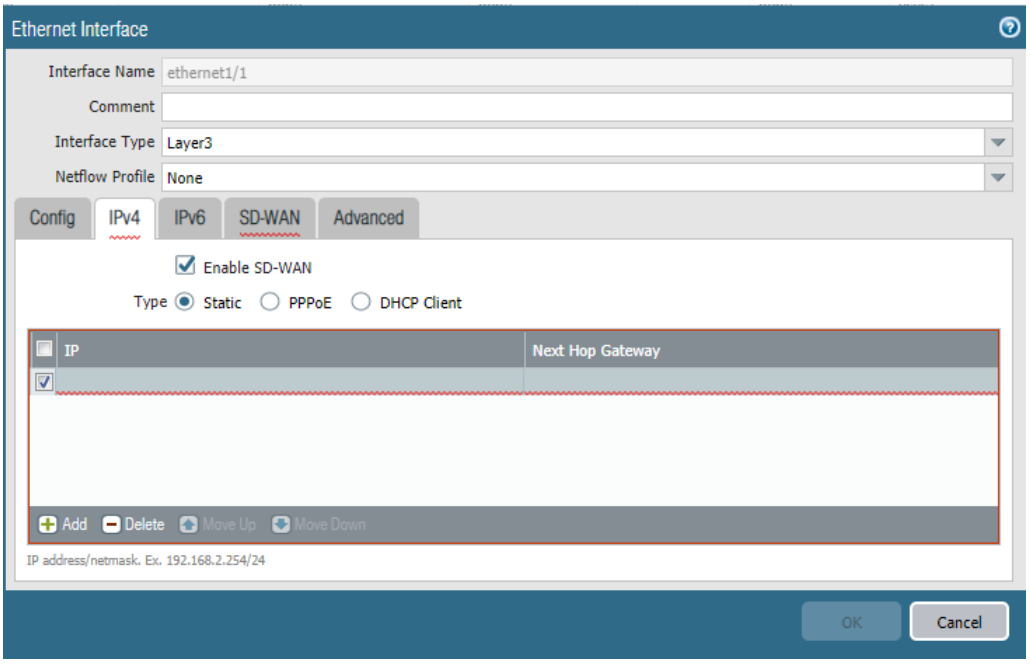
Par exemple, si vous créez une liaison montante vers un ISP, vous devez savoir que l'interface Ethernet que vous choisissez va vers une zone non approuvée.

STEP 6 | Dans l'onglet **IPv4**, **Enable SD-WAN** (Activez SD-WAN).

STEP 7 | Sélectionnez **Type** d'adresse :

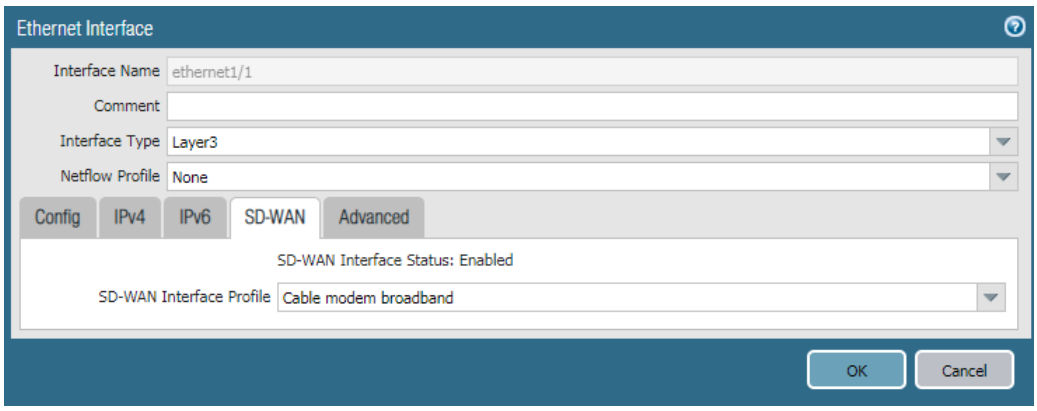
- **Static** (statique) — Dans le champ**IP**, **Add** (Ajoutez) une adresse IPv4 et une longueur de préfixe pour l'interface. Vous pouvez utiliser une variable définie comme $uplink avec une fourchette d'adresses. Saisissez l'adresse IPv4 du **Next Hop Gateway** (le saut suivant de votre adresse IPv4 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.
- (PAN-OS 9.1.2 et versions 9.1 ultérieures, et plug-in SD-WAN 1.0.2 et versions 1.0 ultérieures) **PPPoE**—**Enable** (Activé) authentification PPPoE pour les liens DSL, saisissez **Username** (nom d'utilisateur) et **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.

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 | 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 9 | Cliquez sur **OK (OK)** pour enregistrer l'interface ethernet.



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

STEP 11 | (Configuration SD-WAN manuelle uniquement) Configurer une Interface virtuelle SD-WAN. La configuration Auto VPN effectuera cette tâche si vous utilisez Auto VPN.

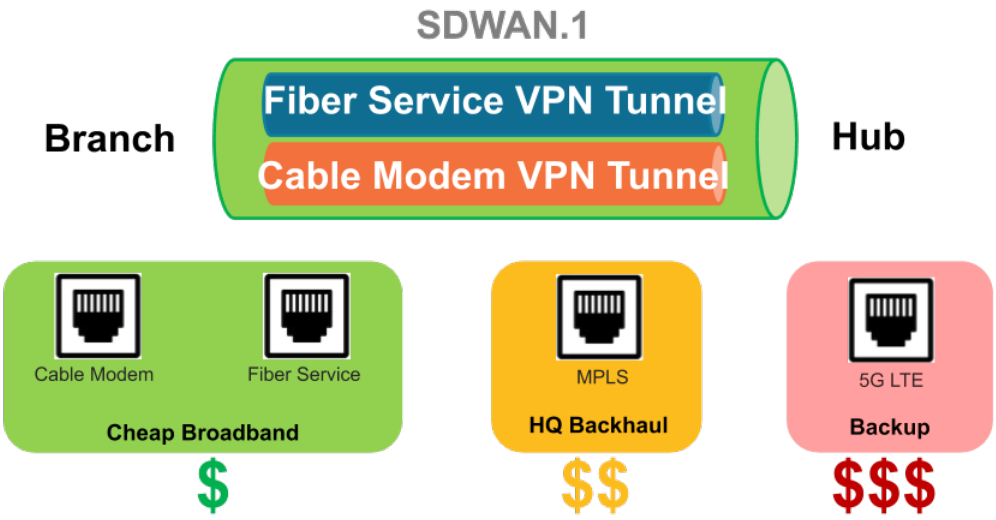
Configurer une Interface virtuelle SD-WAN

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.

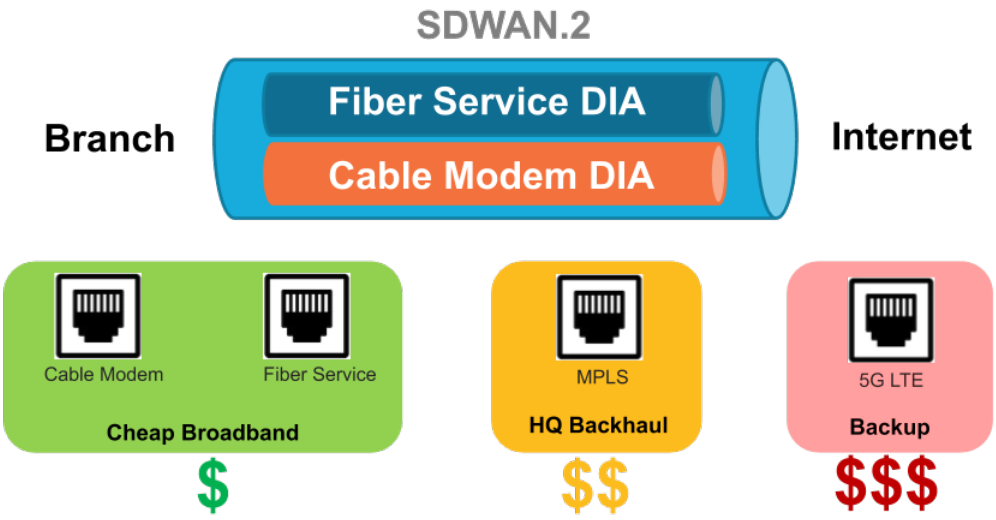
Si vous n'utilisez pas la configuration Auto VPN par le biais de Panorama, créez et configurez une interface virtuelle SD-WAN pour spécifier une ou plusieurs ethernet interfaces (interfaces ethernet) physiques compatibles SD-WAN qui vont vers la même destination, comme une plateforme spécifique ou internet. 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.1 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.2 rassemble les liens Ethernet 1/1 et Ethernet 1/2, qui sont tous les deux des liens DIA de la branche jusqu'à 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. alors n'utilisez pas ces chiffres.

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

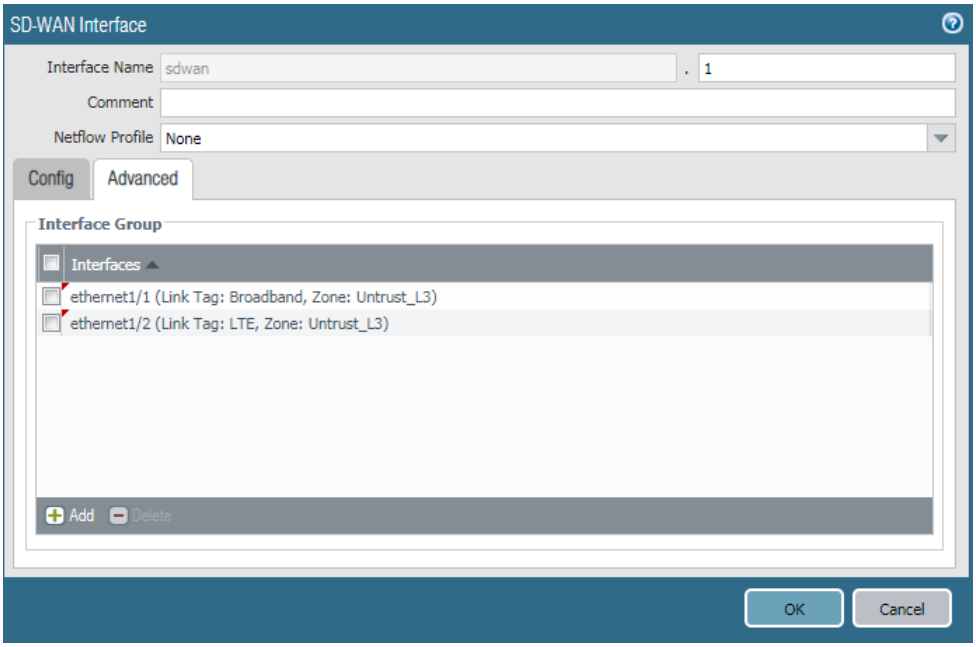
STEP 6 | Affectez l'interface SD-WAN à une **Security Zone (Zone de sécurité)**.

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 7 | 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 8 | Cliquez sur **OK** pour enregistrer la modification de votre configuration.



STEP 9 | **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 et crée une interface virtuelle SD-WAN appelée sdwan.902 pour les tunnels VPN. Auto VPN crée aussi son propre itinéraire par défaut qui utilise l'interface sdwan.901 en tant qu'interface de sortie et utilise des métriques faibles afin que l'interface sdwan.901 soit préférée par rapport à l'itinéraire par défaut que vous avez créé.

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

STEP 2 | Sélectionnez le **Template** (Modèle) sur le quel 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) et **Add** (Ajoutez) un itinéraire statique par son **Name** (Nom).

STEP 5 | Pour la**Destination**, saisissez 0.0.0.0/0.

STEP 6 | Pour l'**Interface** de sortie, sélectionnez une des interfaces logiques SD-WAN que vous avez créées pour afficher le pare-feu, comme sdwan.1.

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

STEP 7 | Pour **Next Hop** (saut suivant), sélectionnez **None** (Aucun).

STEP 8 | 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 9 | Cliquez sur **OK**.

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

STEP 11 | **Commit (Validez)** vos modifications.

STEP 12 | Répétez cette tâches pour les autres modèles sur les pare-feux qui utilisent un itinéraire de service pour accéder à Panorama™.

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 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 bas 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 nécessaire 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.

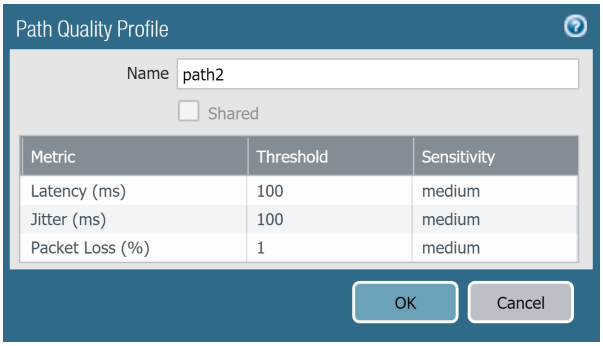
Créer un profil de qualité du chemin d'accès dans une SD-WAN policy rule (règle de politique SD-WAN) pour contrôler le seuil auquel le pare-feu remplace un chemin d'accès détérioré par un nouveau chemin pour les paquets de l'application correspondante.

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 caractère 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 2 000 ; 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 ; par défaut on a 1).

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 | Pour **Packet Loss** (perte de paquets), sélectionnez **Sensitivity** (Sensibilité) (**low**, **medium**, or **high**) (faible, moyenne ou élevée). Le réglage par défaut est **medium** (moyenne).

STEP 11 | Cliquez sur **OK**.

STEP 12 | **Commit** (Validez) et **Commit and Push** (Validez et appliquez) les modifications de votre configuration.

STEP 13 | **Commit (Validez)** vos modifications.

STEP 14 | Répétez cette tâche pour chaque Groupe de périphériques.

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 ont besoin d'une grande capacité de bande passante du lien, comme des sauvegardes importantes de branche et des transferts de gros fichiers.

Si le lien subit une défaillance, 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 :

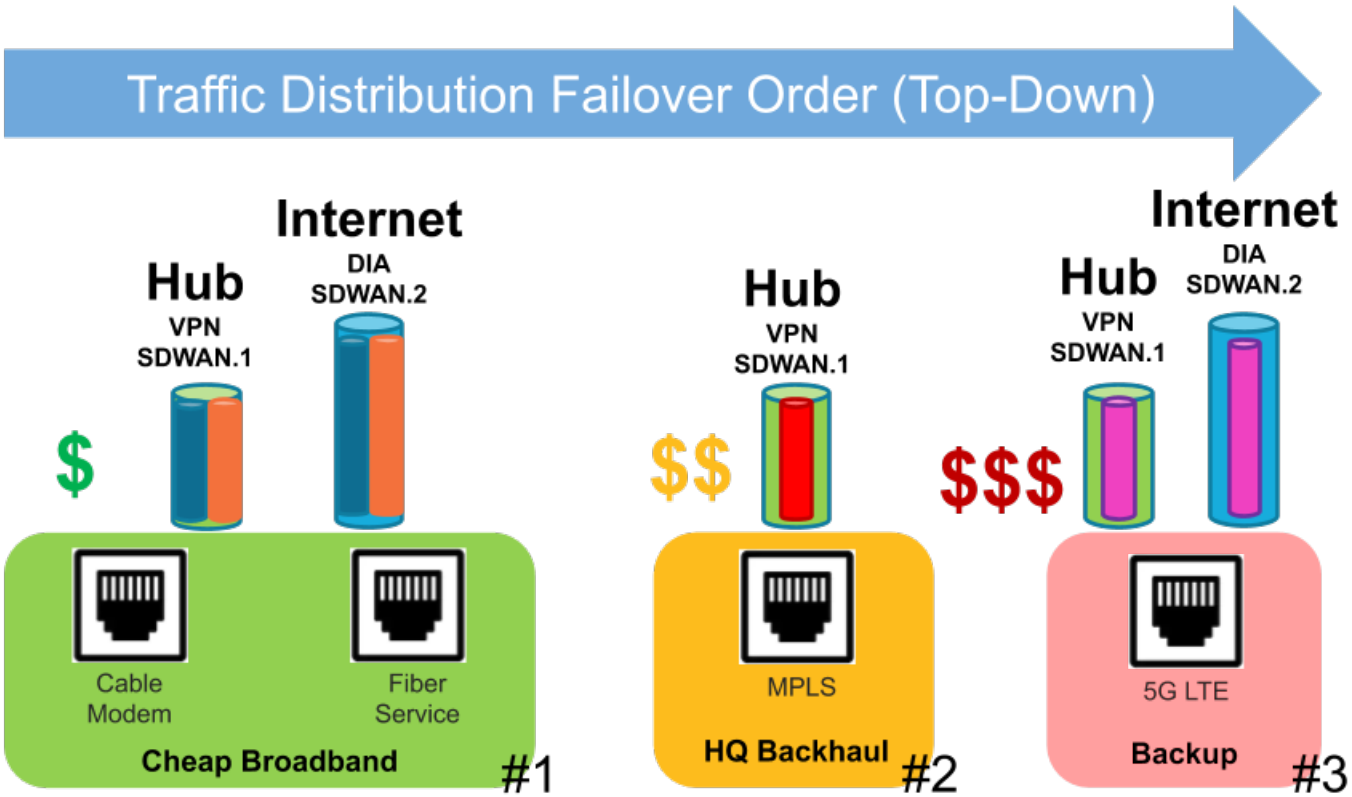
Condition du chemin d'accès	Top-Down Priority (Priorité descendante)	Best Available Path (Meilleur chemin disponible)	Weighted Session Distribution (Distribution pondérée de sessions)
La session sur un chemin d'accès existant a basculé à un seuil de bon état du chemin d'accès (restriction d'alimentation)	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
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 sur la liste	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	Partage de la charge de la session sur la base du	Partage de la charge de la session sur la base du % de pondération

Condition du chemin d'accès	Top-Down Priority (Priorité descendante)	Best Available Path (Meilleur chemin disponible)	Weighted Session Distribution (Distribution pondérée de sessions)
	la même Étiquette SD-WAN	meilleur chemin dans une Étiquette SD-WAN	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.

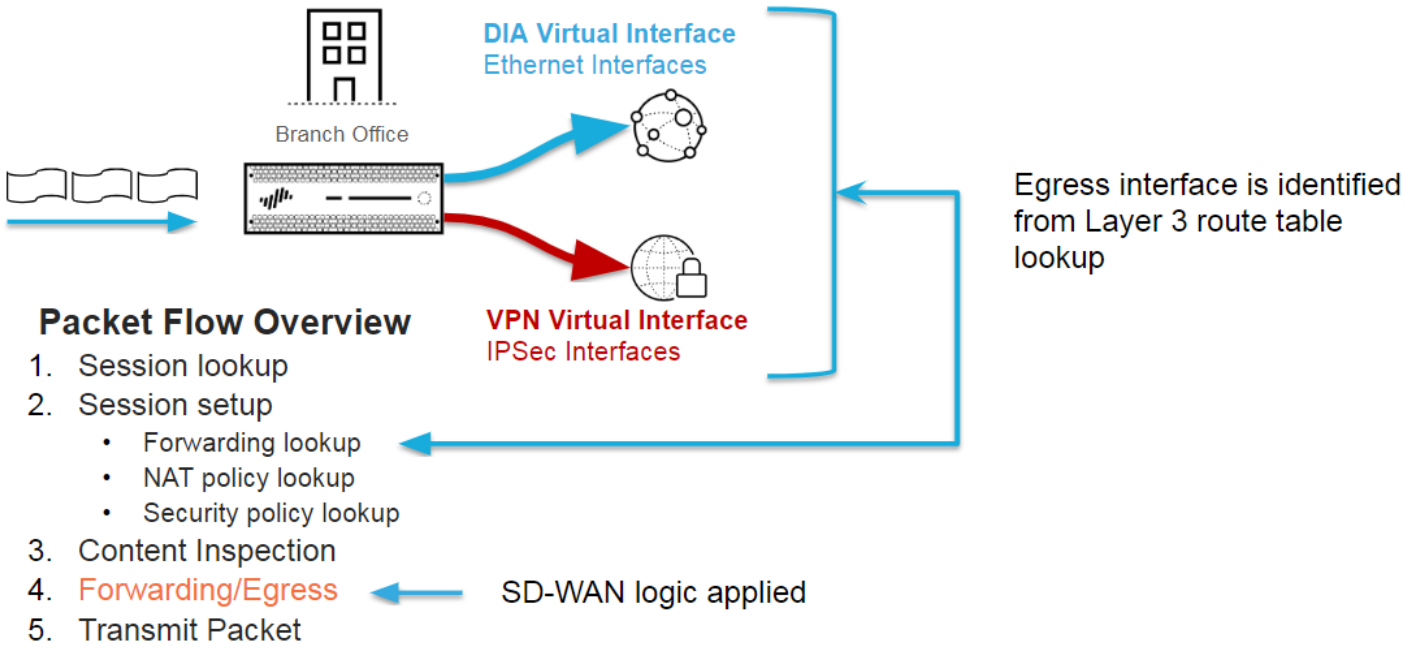


1. Dans cet exemple de Priorité descendante, les paquets d'une branche supportant une application spécifique (par exemple, office365-enterprise-access) arrivent au pare-feu. Le pare-feu utilise le tableau d'acheminement afin de déterminer le saut suivant vers la destination et l'interface sortante qui est le tunnel d'interface SD-WAN intitulé sdwan.1. 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.1 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.1 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 lin MPLS 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.



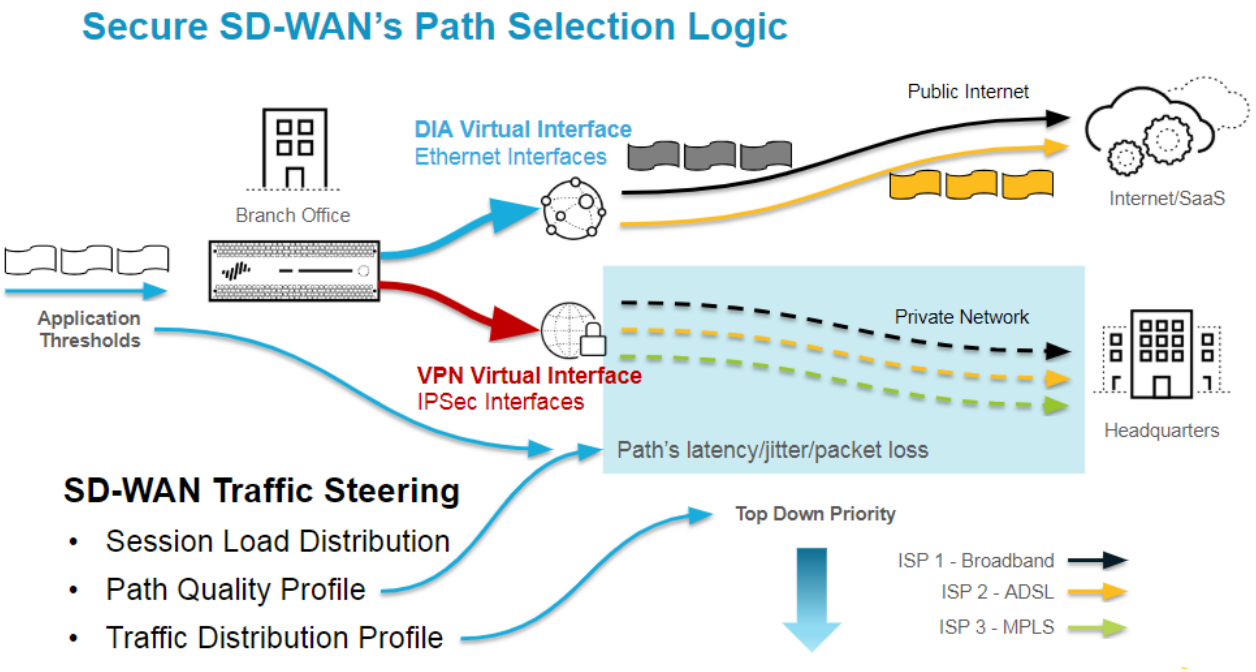
Les détails du flux de paquets de la figure sont les suivants :

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.

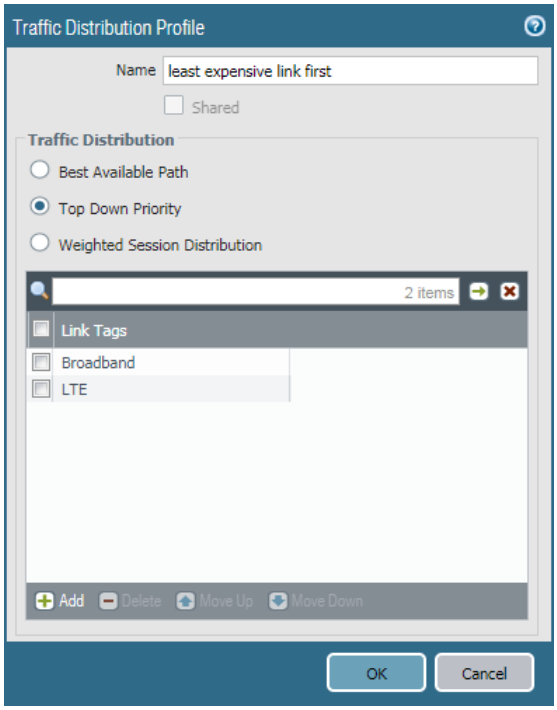
STEP 1 | Connectez-vous à l'interface Web Panorama.

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 que le pare-feu sélectionne lorsqu'un paquet qui répond aux critères arrive.

  Lorsqu'un lien n'est pas qualifié et doit basculer vers le meilleur chemin suivant, le pare-feu peut migrer un maximum de 1 000 sessions par minute depuis le 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 les seuils de Qualité du chemin de ce chemin soient dépassés, stade auquel le pare-feu recommence en haut de la liste des Étiquettes de liens pour trouver le nouveau chemin préféré.
- **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.

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 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 | Dans l'onglet **Application/Service**, sélectionnez un profil de **Path Quality** (Qualité de chemin) ou Créer un Path Quality Profile (Profil de qualité du chemin d'accès).

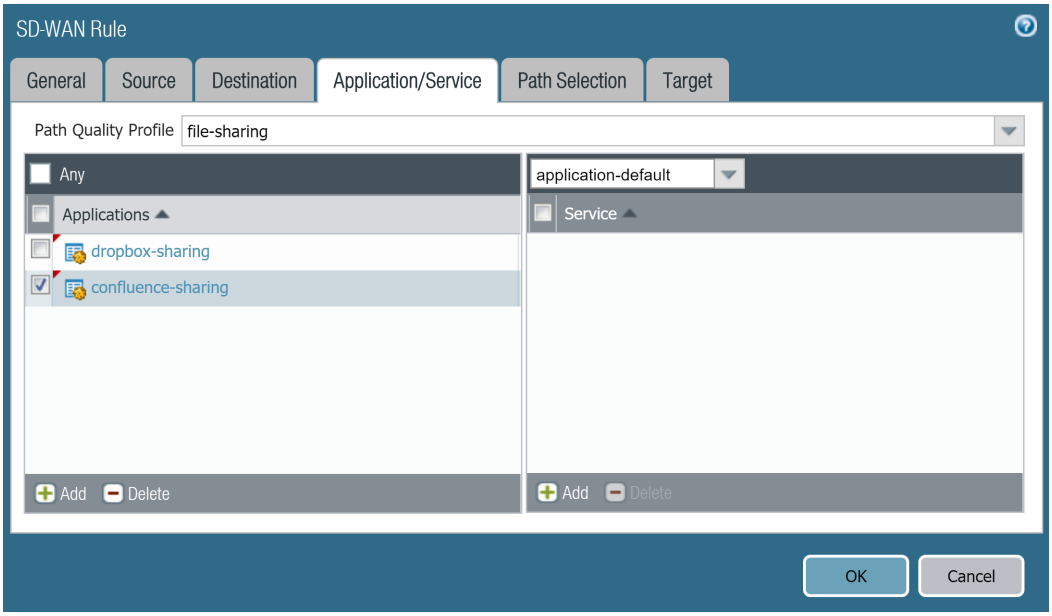
STEP 8 | **Add Applications**(Ajoutez des applications) et sélectionnez une ou plusieurs applications dans la liste ou sélectionnez **Any** (n'importe quelles) applications. Toutes les applications que vous sélectionnez sont soumises à des seuils d'état dans le profil de Qualité du chemin que

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.

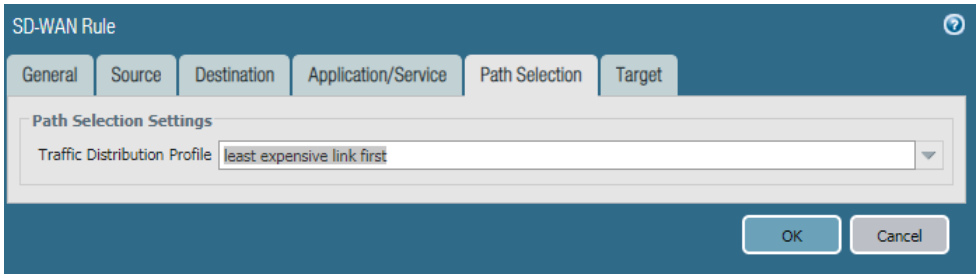
Ajoutez uniquement les applications critiques à l'entreprise et les applications qui sont sensibles aux conditions du chemin pour leur utilisation.

STEP 9 | **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.

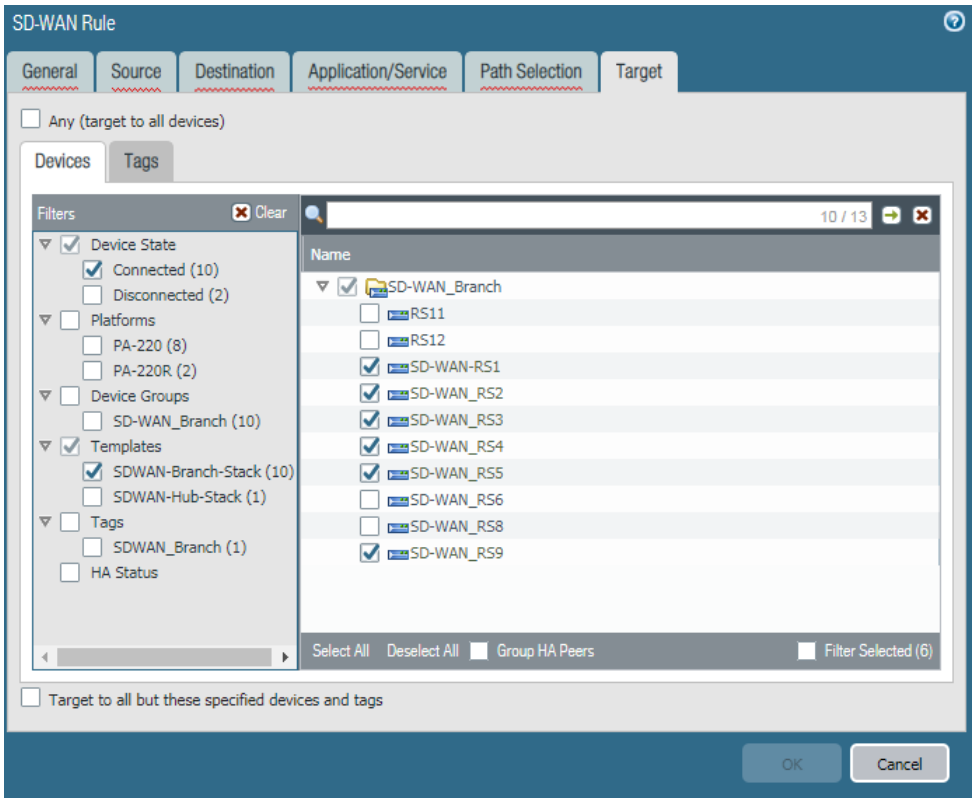


STEP 10 | Dans l'onglet **Path Selection** (sélection du chemin), sélectionnez le **Traffic Distribution Profile** (Profil de distribution du trafic) ou Créer un Traffic Distribution Profile (profil de distribution du trafic). Quand un paquet entrant (non associé avec une session) correspond à tous les critères de correspondance de la règle, le pare-feu utilise ce profil de Distribution de trafic pour sélectionner un nouveau chemin préféré.

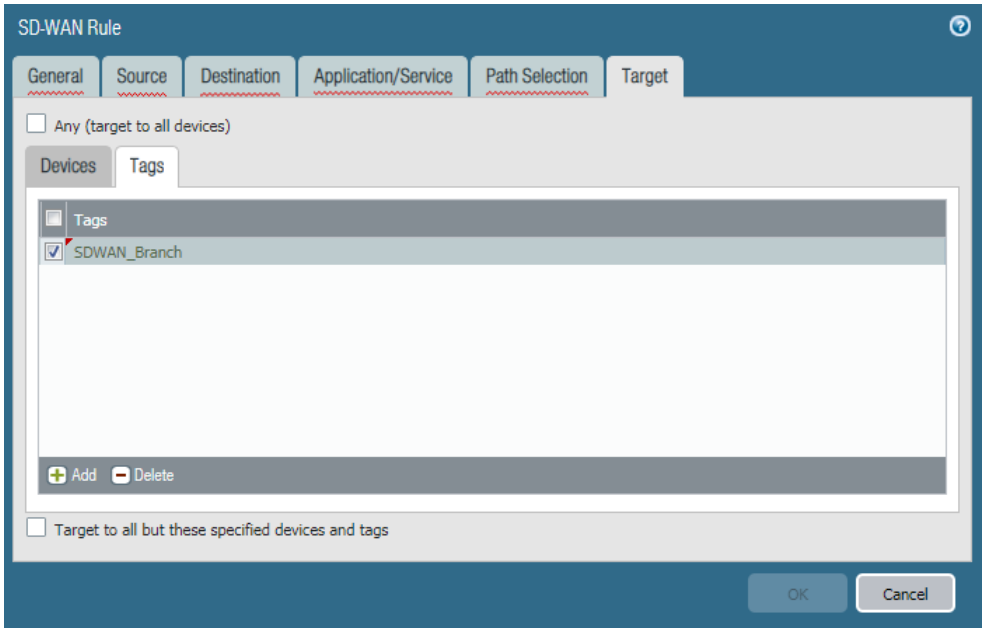


STEP 11 | Dans l'onglet **Target** (cible), utilisez une ou plusieurs des méthodes suivantes pour spécifier les pare-feux cibles dans le groupe de périphériques auxquels Panorama applique la règle de politique SD-WAN :

- 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 12 | Cliquez sur **OK**.

STEP 13 | **Commit** (Validez) et **Commit and Push** (Validez et appliquez) les modifications de votre configuration.

STEP 14 | (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 15 | 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 16 | (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 17 | 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 18 | 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. En commençant avec PAN-OS 9.1.2, 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 | (PAN-OS 9.1.2 et versions 9.1 ultérieures) 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.

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

Ajouter un seul pare-feu de hub ou de branche ou utilisez un fichier CSV pour importer en masse plusieurs pare-feux SD-WAN de branche et de hub.

- Ajouter un Périphérique SD-WAN
- Importer en masse plusieurs Périphériques SD-WAN

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, plan your SD-WAN configuration(planifiez votre configuration SD-WAN) afin de vous assurer que vous avez toutes les adresses IP nécessaires et que la topologie SD-WAN est bien comprise. Cela aide à réduire les erreurs de configuration.

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

Si vous souhaitez qu'un HA active/passive fonctionne sur deux pare-feux de branche ou deux pare-feux de hub, n'ajoutez pas ces pare-feux en tant que périphériques SD-WAN lors de cette étape. Vous les ajouterez en tant qu'homologues HA séparément 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.

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

STEP 2 | Sélectionnez **Panorama** > **SD-WAN** > **Devices** (Panorama SD-WAN Périphériques) et **sélectionnez** 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** (Platforme) — 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 | Sélectionnez le **Virtual Router Name** (Nom du routeur virtuel) — 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.

STEP 6 | 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 > SD-WAN > Monitoring) du cluster ne s'affichent pas.

STEP 7 | (PAN-OS 9.1.3 et versions 9.1 ultérieures et plug-in SD-WAN 1.0.3 et versions 1.0 ultérieures) Si vous ajoutez un hub derrière un périphérique assurant le NAT pour le hub, vous devez spécifiez 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**.

Vous devez aussi configurer le NAT de destination entrant 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 reconfigurer la nouvelle adresse IP et l'appliquer aux membres du 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.*

STEP 8 | (Nécessaire pour les clients préexistants) Mappez vos zones préexistantes selon les zones prédéfinies utilisées pour SD-WAN.

Lorsque vous mappez vos zones existantes selon une zone SD-WAN, vous devez modifier vos security policy rules (règles de politique de sécurité) et ajouter les zones SD-WAN en fonctions des zones Source et Destination correctes.

1. Sélectionnez **Zone Internet** et **Add** (Ajoutez) les zones préexistantes qui feront sortir le trafic SD-WAN vers internet.
2. Sélectionnez **Zone to Hub** (zone vers plateforme) et **Add** (Ajoutez) les zones préexistantes qui feront sortir le trafic SD-WAN vers le hub.
3. Sélectionnez **Zone to Branch** (zone vers branche) et **Add** (Ajoutez) les zones préexistantes qui feront sortir le trafic SD-WAN vers la branche.

4. Sélectionnez **Zone Internal** (zone interne) et **Add** (Ajoutez) les zones préexistantes qui feront sortir le trafic SD-WAN vers la zone interne.

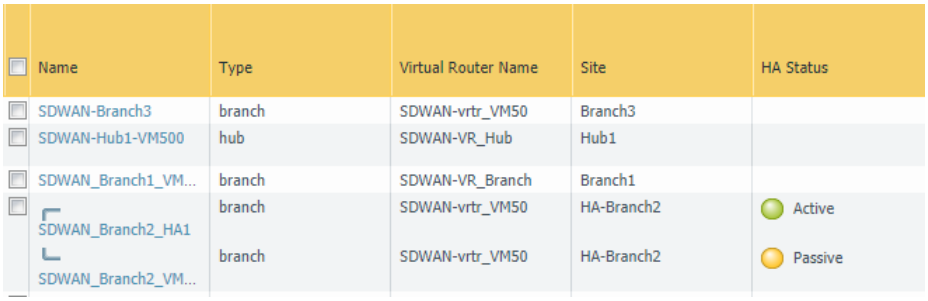
STEP 9 | (Facultatif) Configurer le protocole BGP (Border Gateway Protocol).

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.

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. 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.
4. 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.
5. Saisissez **Prefix(es) to Redistribute** (Préfixes à redistribuer). Sur un périphérique de hub, vous devez saisir au moins un préfixe à redistribuer. Les périphériques de branche n'ont pas cette option ; les réseaux secondaires connectés aux emplacements des branches sont redistribués par défaut.

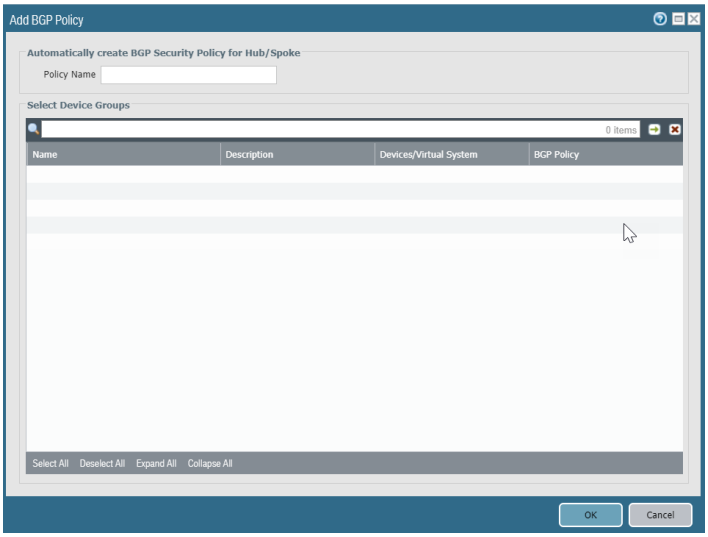
STEP 10 | Cliquez sur **OK**.

STEP 11 | (Plug-in SD-WAN 1.0.1 et versions ultérieures) 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.



STEP 12 | (PAN-OS 9.1.2 et versions 9.1 ultérieures et plug-in SD-WAN 1.0.2 et versions 1.0 ultérieures) Faites en sorte que Panorama crée et applique aux pare-feux une règle de politique de sécurité qui permettent à BGP de fonctionner entre les branches et les hubs.

1. Sélectionnez **BGP Policy** (politique BGP) en bas de l'écran et **Add** (Ajouter).
2. Saisissez un **Policy Name** (Nom de politique) pour la règle de politique de sécurité que Panorama créera automatiquement.
3. **Select Device Groups** (Sélectionnez ls groupes de périphériques) pour spécifier les groupes de périphériques auxquels Panorama applique les règles de politique de sécurité.
4. Cliquez sur **OK**.



STEP 13 | 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, plan your SD-WAN configuration(planifiez votre configuration SD-WAN) afin de vous assurer que vous avez toutes les adresses IP nécessaires et que la topologie SD-WAN est bien comprise. Cela aide à réduire les erreurs de configuration.

Si vous souhaitez qu'un HA active/passive fonctionne sur deux pare-feux de branche ou deux pare-feux de hub, n'ajoutez pas ces pare-feux en tant que périphériques SD-WAN dans votre fichier CSV. Vous les ajouterez en tant qu'homologues HA séparément 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-feux 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. Vous devez saisir 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) du cluster ne s'affichent pas.
- (Nécessaire pour les clients préexistants) Mappez vos zones préexistantes selon les zones prédéfinies utilisées pour SD-WAN.

  Lorsque vous mappez vos zones existantes selon une zone SD-WAN, vous devez modifier vos security policy rules (règles de politique de sécurité) et ajouter les zones SD-WAN en fonctions des zones Source et Destination correctes.

  - **zone-internet**— Saisissez les noms des zones préexistantes par lesquelles le trafic SD-WAN sortira pour atteindre internet.
  - **zone-internet**— Saisissez les noms des zones préexistantes par lesquelles le trafic SD-WAN sortira pour atteindre une branche
  - **zone-to-hub**— Saisissez les noms des zones préexistantes par lesquelles le trafic SD-WAN sortira pour atteindre un hub.
  - **zone-internal**—Saisissez les noms des zones préexistantes par lesquelles le trafic SD-WAN sortira pour atteindre une zone interne.
- (Facultatif) **loopback-address** (adresse de bouclage) — Spécifiez une adresse IPv4 statique de bouclage pour les homologie du protocole BGP (Border Gateway Protocol).
- (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) **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.

- (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.

- **vr-name**— Saisissez le nom du routeur virtuel à utiliser pour l'acheminement entre le hub et les branches SD-WAN. Par défaut, Panorama crée un routeur virtuel`sdwan-default` et peut automatiquement appliquer les configurations du routeur.

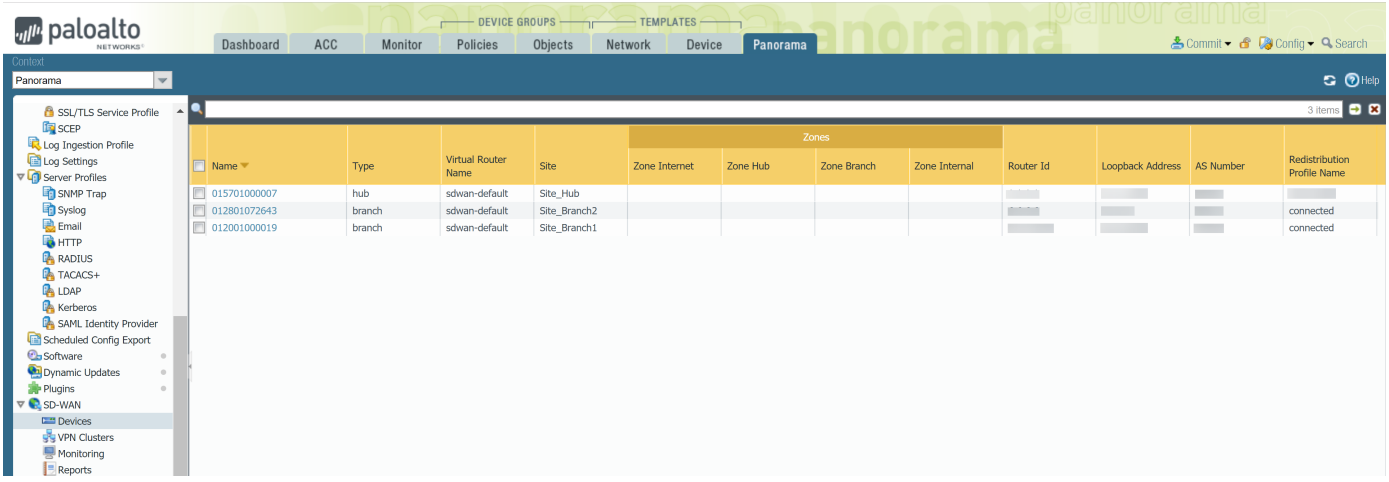
	A	B	C	D	E	F	G	H	I	J	K
1	device-serial	type	site	zone-internet	zone-branch	zone-hub	zone-internal	loopback-address	prefixes redist	as-number	router-id
2	12001000019	branch	Site_Branch1					2.2.2.2/32		65420	5.5.5.5/32
3	12801072643	branch	Site_Branch2					3.3.3.3		65413	6.6.6.6
4	15710000007	hub	Site_Hub					1.1.1.1/32	10.0.0.0/8	65432	1.1.1.1

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.



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.

Configurer les Périphérique HA pour SD-WAN

Vous pouvez configurer deux branches ou deux hubs en mode HA active/passive pour qu'elles fassent 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.

Lisez la procédure suivante avant de commencer afin de ne pas Valider après avoir ajouté les homologues HA en tant que périphériques SD-WAN.

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® 9.1.0 est compatible uniquement avec la topologie VPN SD-WAN Hub-Spoke. 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 topologie VPN SD-WAN Full Mesh n'est pas compatible avec PAN-OS 9.1.0.

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.

Une clé préalablement partagé IKE aléatoire et forte est créée pour tous les hubs et les branches du cluster VPN afin de sécuriser les tunnels VPN et chaque pare-feu a une clé principale qui crypte la clé préalablement partagée. Le système sécurise la clé préalablement partagée, même de l'administrateur. En commençant avec PAN-OS 9.1.2, vous pouvez actualiser la clé préalablement partagée IKE que Panorama envoie à tous les membres du cluster.

Actualisez la clé préalablement partagée lorsque les membres du cluster ne sont pas occupés.

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, reportez-vous à la section Planifiez votre configuration SD-WAN.

STEP 2 | Connectez-vous à l'interface Web Panorama.

STEP 3 | (PAN-OS 9.1.2 et les versions 9.1 ultérieures, et le plug-in SD-WAN 1.0.2 et versions 1.0 ultérieures) Spécifiez les fourchettes d'adresses IP pour les tunnels VPN IPSec que la configuration Auto VPN crée.

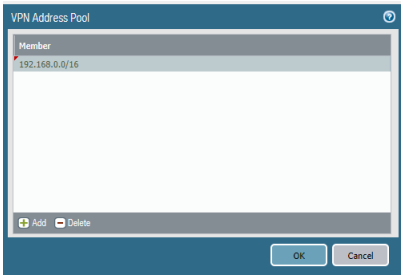
La configuration Auto VPN crée un tunnel VPN entre un hub et des branches et attribue les adresses IP aux terminaux du tunnel. Saisissez les fourchettes de sous-réseau que vous souhaitez que Auto VPN utilise comme adresses de tunnel VPN. Vous pouvez saisir

jusqu'à 20 fourchettes de prefixes/masques réseau. Auto VPN choisit dans ce réservoir des adresses de tunnel VPN, en choisissant fans la première plus grande fourchette en premier (puis dans la deuxième fourchette 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 ce n'est pas le cas, saisissez de nouvelles fourchettes. 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 SD-WAN de Panorama).
2. Au bas de l'écran, sélectionnez **VPN Address Pool** (réservoir d'adresses VPN).

3. **Add** (Ajoutez) une ou plusieurs fourchettes d'adresse IP et masques réseau (jusqu'à 20) de **Member** (Membre), par exemple, 192.168.0.0/16.
4. Cliquez sur **OK**.



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 SD-WAN de Panorama) et **Add** (Ajoutez) 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) 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.

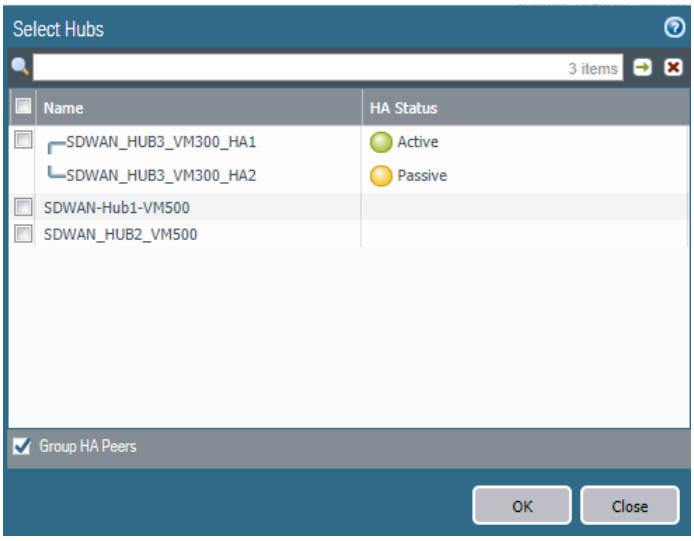
   Seul le type de cluster VPN Hub-Spoke est compatible avec PAN-OS 9.1.0.
4. **Add** (Ajoutez) un ou plusieurs périphériques de branche dont vous déterminez qu'ils ont besoin de communiquer entre eux.
   - (Plug-in SD-WAN 1.0.1 et versions 1.0 ultérieures) Sélectionnez**Group HA Peers** (Grouper les homologues HA) pour afficher les homologues ensemble.
   - Sélectionnez les périphériques de la branche à ajouter au cluster.

- Cliquez sur **OK**.

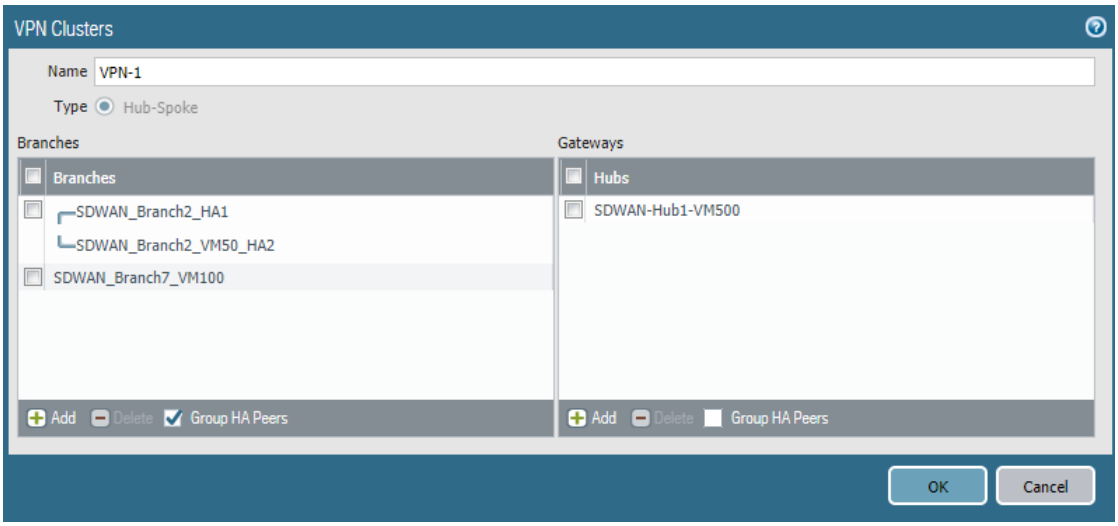
5. **Add** (Ajoutez) un ou plusieurs périphériques du hub dont vous déterminez qu'ils ont besoin de communiquer avec les périphériques de la branche. Si plus d'un périphérique de hub est ajouté, vous devez utiliser les métriques d'itinéraire pour contrôle quel hub est le principal et lequel est secondaire.

   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.

   - (Plug-in SD-WAN 1.0.1 et versions 1.0 ultérieures) Sélectionnez**Group HA Peers** (Grouper les homologues HA) pour afficher les homologues ensemble.
   - Sélectionnez les plateformes à ajouter au cluster.
   - Cliquez sur **OK**.



6. (Plug-in SD-WAN 1.0.1 et versions 1.0 ultérieures) Sélectionnez**Group HA Peers** (Grouper les homologues HA) des branches ou des zones des portails pour afficher les homologues ensemble.



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

STEP 5 | (PAN-OS 9.1.2 et versions 9.1 ultérieures, et plug-in SD-WAN 1.0.2 et versions ultérieures 1.0) Annonce des préfixes supplémentaires de la branche vers le hub.

Dans PAN-OS 9.1.0, le pare-feu redistribue (annonce) tous les itinéraires non publics connectés de la branche au hub. En commençant avec PAN-OS 9.1.2, vous pouvez aussi redistribuer des préfixes supplémentaires depuis la branche vers le hub. Le champs Prefix(es) to Redistribute (préfixes à redistribuer) accepte une liste de préfixes plutôt qu'un préfixe unique.

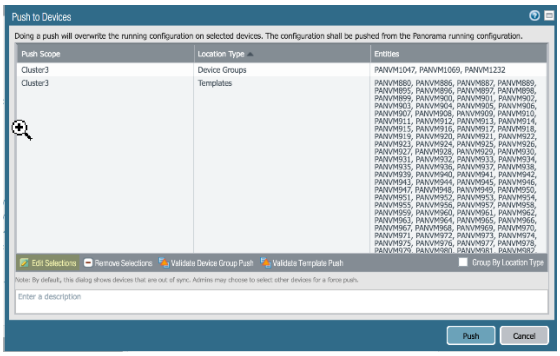
1. Sélectionnez **Panorama** > **SD-WAN** > **Devices** (Panorama SD-WAN Périphériques) et sélectionnez un pare-feu de branche.
2. Sélectionnez **BGP** et **Add** (Ajoutez) une ou plusieurs adresses IP avec un masque réseau à **Prefix(es) to Redistribute** (préfixes à redistribuer).
3. Cliquez sur **OK**.

STEP 6 | Cliquez sur **Commit (Valider)** et **Commit to Panorama (Validez sur Panorama)**.

STEP 7 | Appliquez la configuration aux hubs.

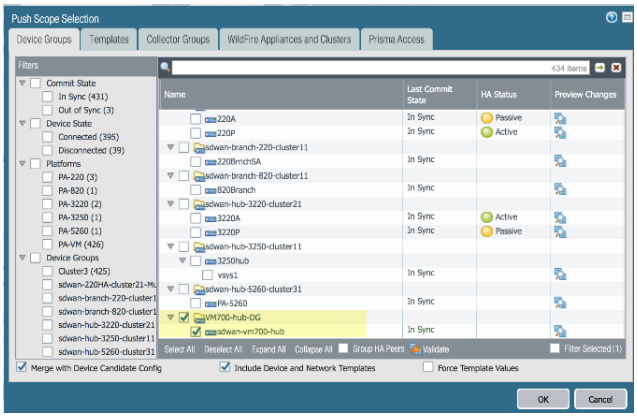
Lorsque Panorama crée des interfaces virtuelles SD-WAN pour les hubs, Panorama ne crée pas nécessairement les interfaces en utilisant des numéros d'interface contigus. Il peut sauter un numéro d'interface au hasard , par exemple, sdwan.921, sdwan.922, sdwan.924, sdwan.925. Malgré la numérotation discontinue, 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.

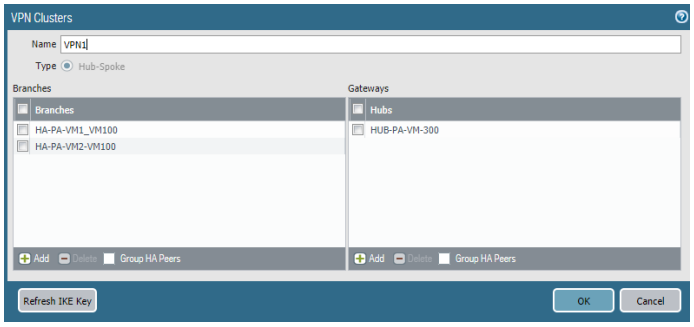
STEP 8 | Appliquez la configuration aux branches en répétant l'étape antérieure mais en sélectionnant le Groupe de périphériques de votre branche.

STEP 9 | (PAN-OS 9.1.2 et versions 9.1 ultérieures, et plug-in SD-WAN 1.0.2 et versions ultérieures 1.0) Actualisez la clés préalablement partagée 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 SD-WAN de Panorama) et sélectionnez un cluster.
2. Au bas de l'écran, sélectionnez **Refresh IKE key** (Actualiser la clé IKE).



3. **Commit** (Valider).
4. **Push to Devices** (Appliquer aux périphériques).

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 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 | Sélectionnez le **Type** de variable comme étant **Interface**.

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)** > **IPv4 (IPv4)**, puis **Add (Ajoutez)** un **Name (Nom)** à donner à l'itinéraire.

STEP 7 | Pour **Destination**, sélectionnez la variable que vous avez créée.

STEP 8 | Pour **Interface**, sélectionnez **sd_wan**.

STEP 9 | Pour **Next Hop** (Saut suivant), sélectionnez **IP Address** (Adresse IP) et saisissez l'adresse IP du saut suivant pour l'itinéraire statique (le hub ou la branche vers laquelle va l'itinéraire statique).

STEP 10 | Cliquez sur **OK**.

STEP 11 | **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 **sd_wan** 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 12 | Configurer un itinéraire statique pour le trafic de retour.

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 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 deConfigurer 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.

- Surveiller les Tâches SD-WAN
- Surveiller la Performance des applications et des liens SD-WAN
- Résoudre les problèmes de performance des applications
- Résoudre les problèmes de performance des liens
- Générer un rapport SD-WAN.

Surveiller les Tâches SD-WAN

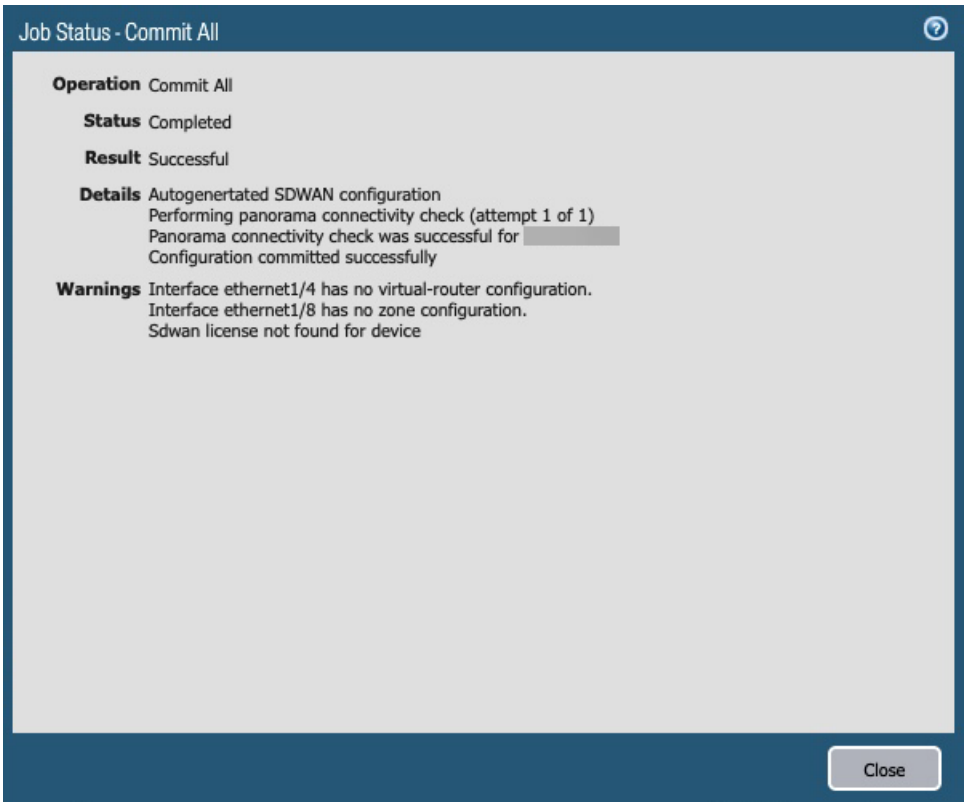
La surveillance valide, met en avant d'autres tâches SD-WAN exécutées depuis le serveur de gestion Panorama™ afin d'obtenir un aperçu et des informations détaillées sur une tâche spécifique.

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.

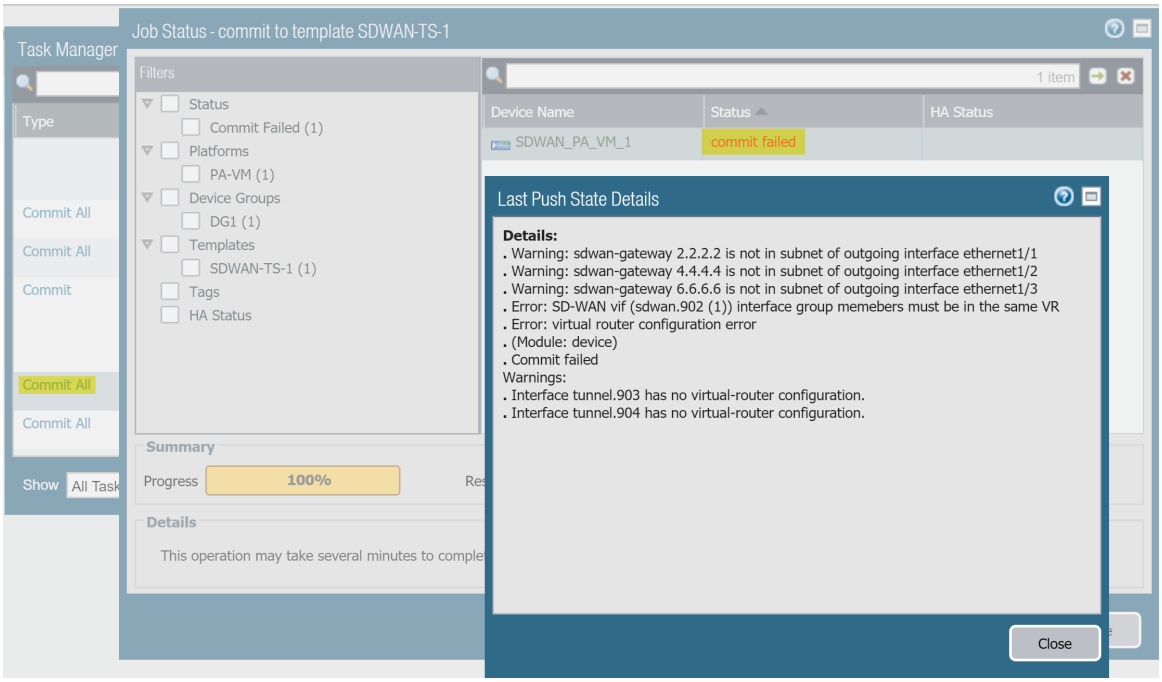
STEP 2 | Après avoir modifié la configuration SD-WAN, **Commit** (validez) vos modifications pour afficher l'état de la tâche.

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

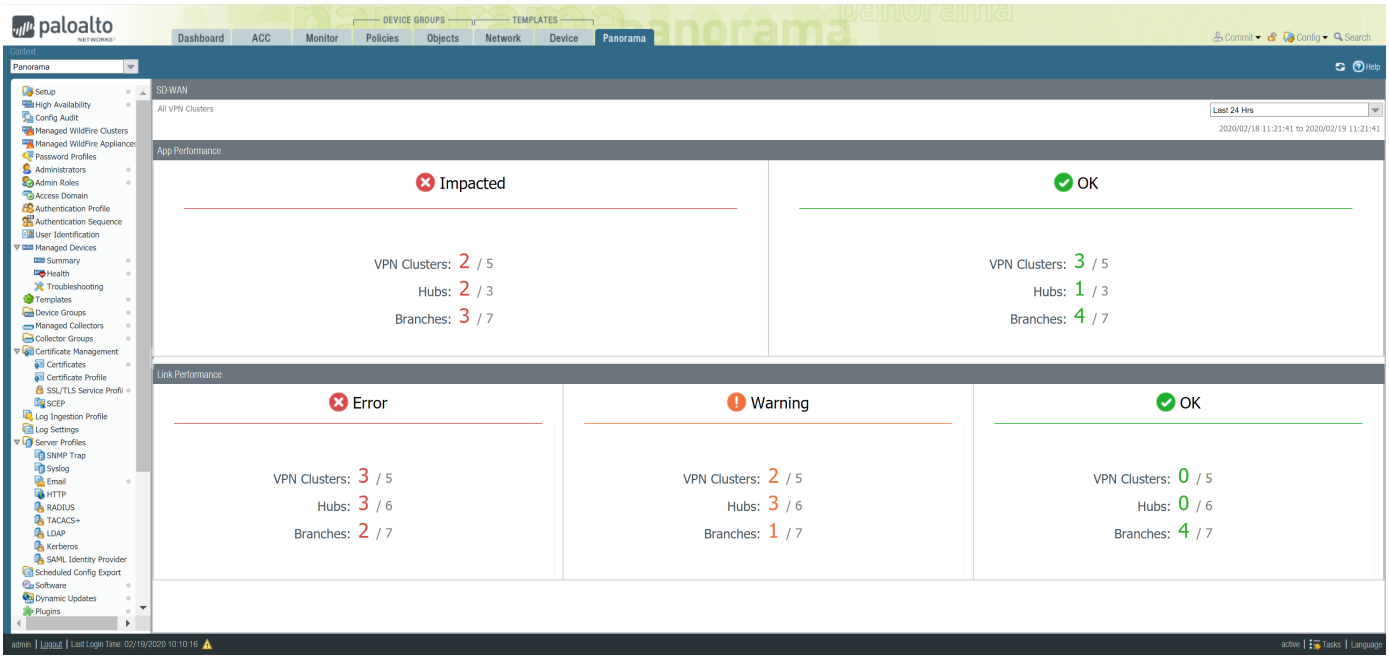
Surveillez l'application et la performance des liens dans vos clusters VPN afin de régler les problèmes en affichant un résumé des informations des tous les clusters VPN puis en procédant par élimination afin d'isoler les problèmes des sites, applications et liens affectés. Le tableau de bord d'accueil 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.

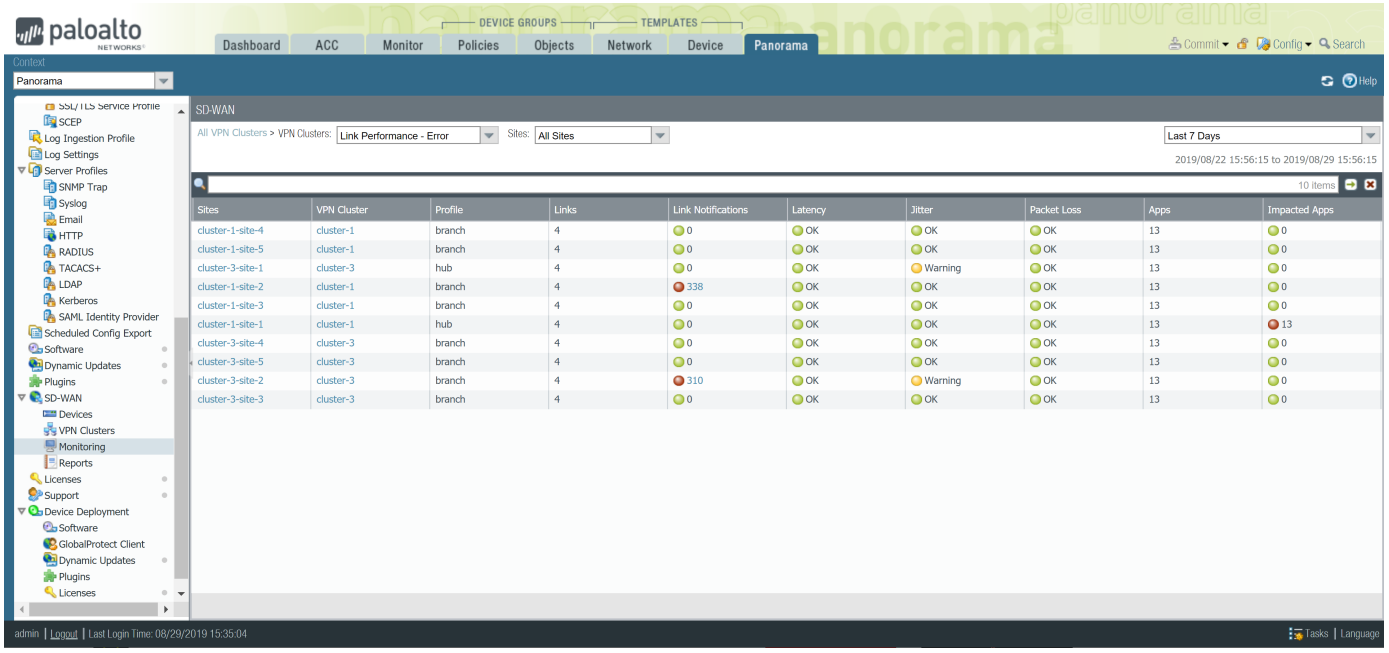
Depuis le tableau de bord d'accueil, procédez par élimination pour afficher les applications impactées ou les liens qui présentent un état d'Erreur ou d'Avertissement. Puis sélectionnez un site affecté afin d'afficher les informations au niveau du site. Depuis le site, affichez les informations au niveau des applications ou des liens.

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 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.



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.

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.

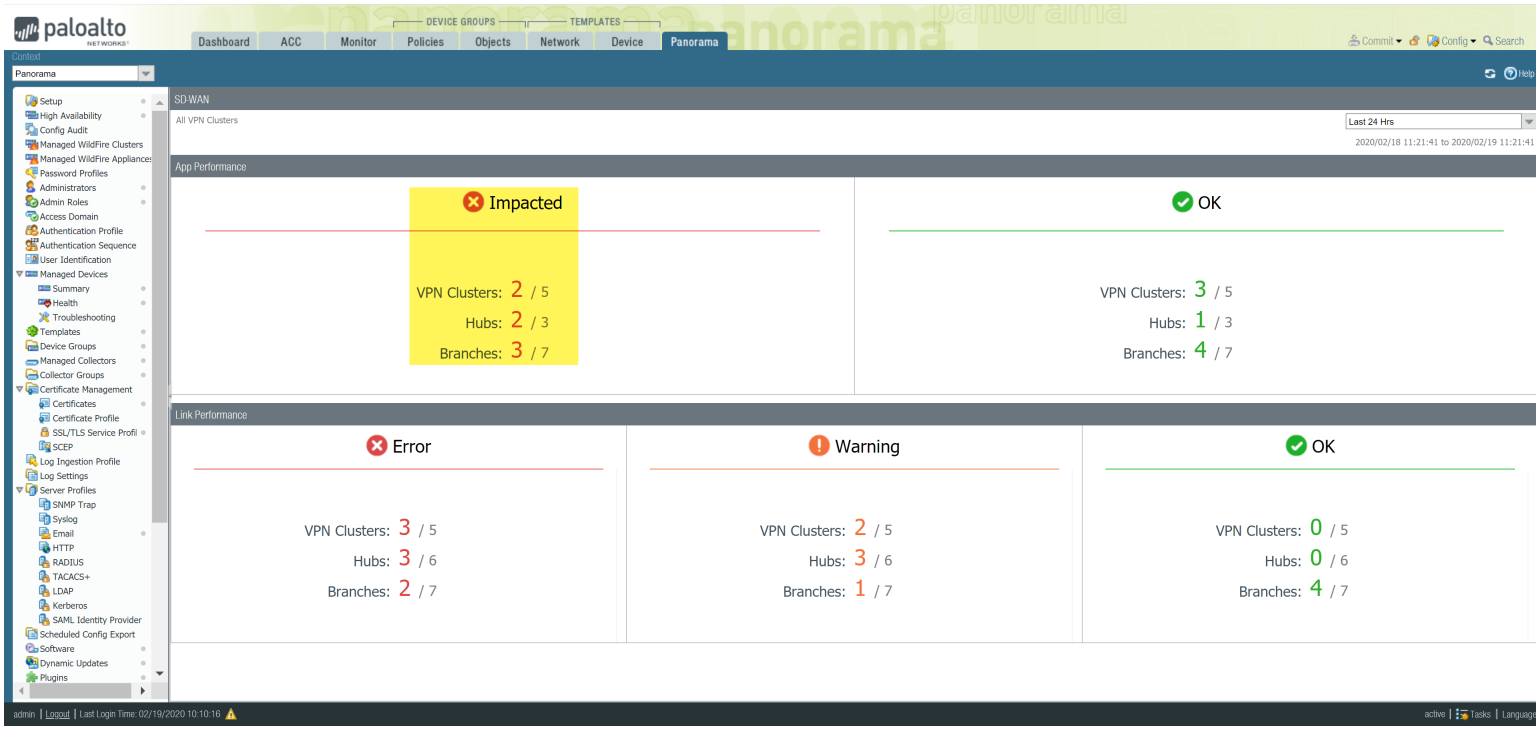
STEP 6 | Cliquez sur une application impactée pour afficher les informations au niveau des applications ou des liens.

Résoudre les problèmes de performance des applications

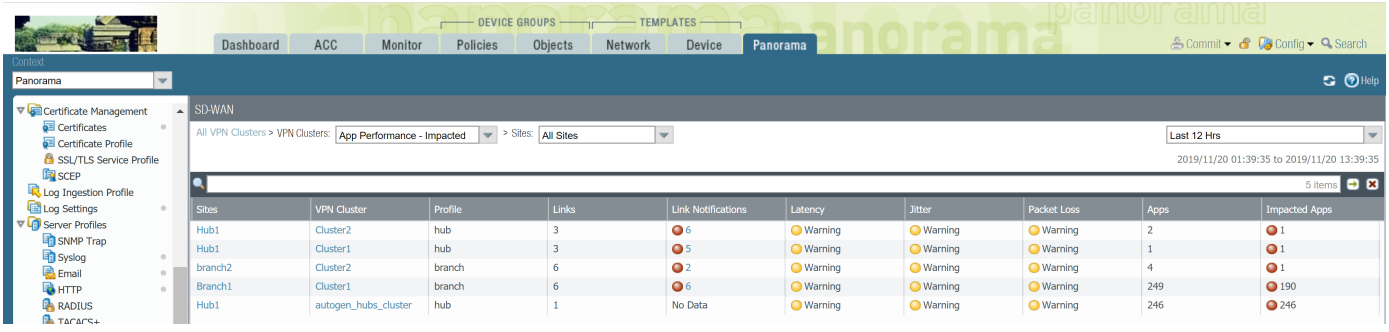
Comprendre ce qui provoque une dégradation de la performance de vos applications est crucial pour garantir que l'expérience de l'utilisateur ne soit pas impactée. Comprendre pourquoi vos clusters de VPN sont impactés et pourquoi le trafic de l'application a basculé vers différents liens aide à ajuster votre configuration SD-WAN.

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

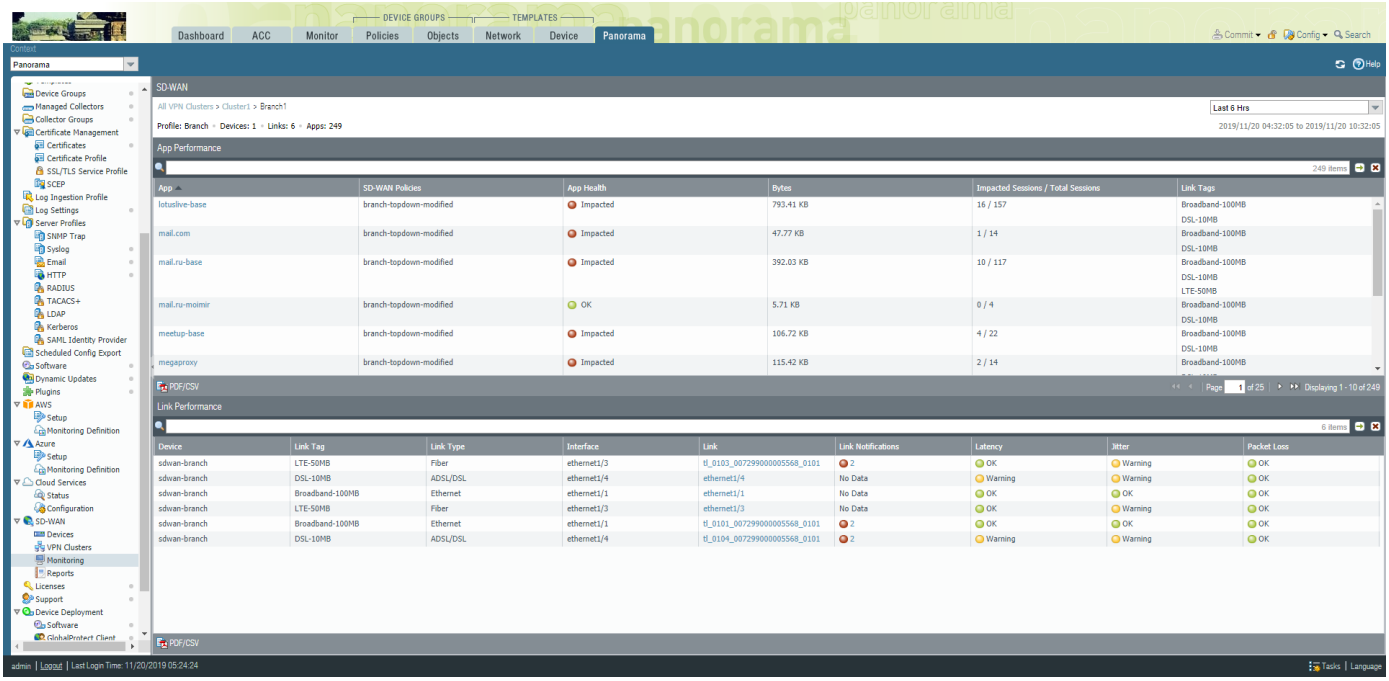
STEP 2 | Sélectionnez **Panorama** > **SD-WAN** > **Monitoring** (Surveillance SD-WAN Panorama) et affichez les clusters de VPN **Impacted** (impactés).



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 dernières 12 heures.

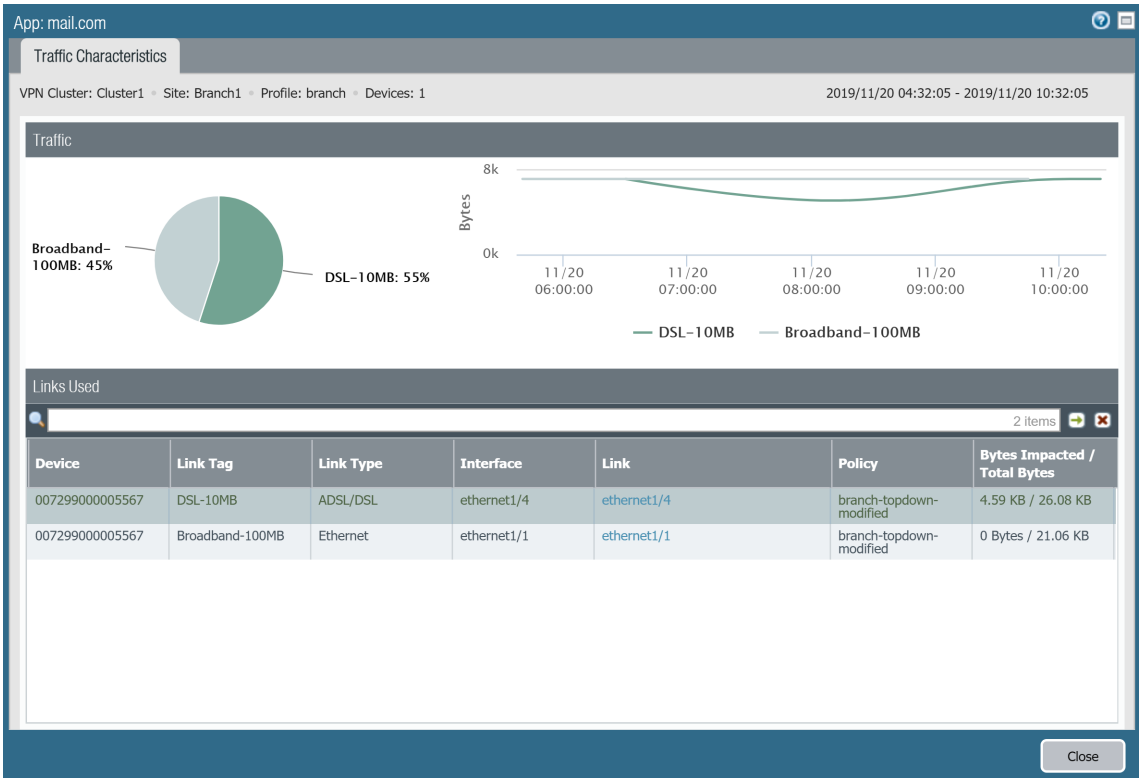


STEP 4 | Dans les colonnes des Sites, sélectionnez le pare-feu du hub ou de la branche impacté afin d'afficher les appli impactées et la performance du lien correspondant.



STEP 5 | Dans la partie App Performance (Performance des appli), cliquez sur une appli afin d'afficher les informations détaillées de Taffic Characteristic (caractéristiques du trafic) relatives au trafic de l'application comme le(s) service(s) internet et les liens utilisés :

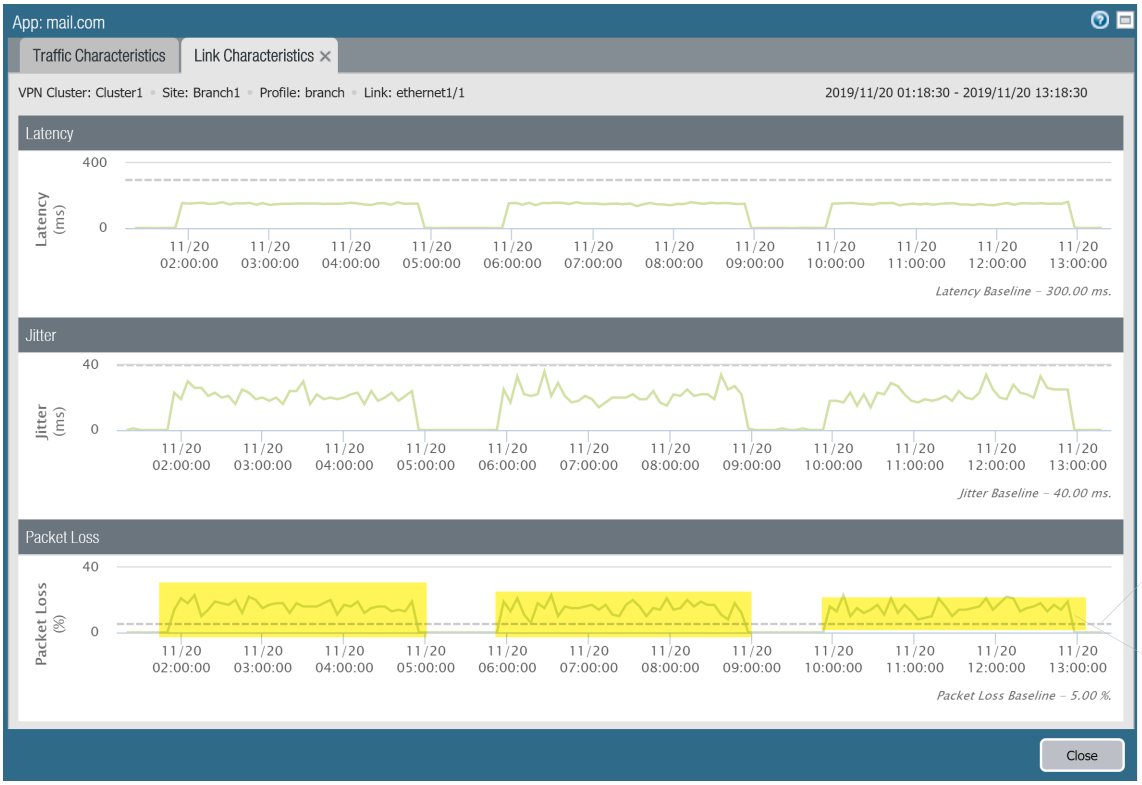
- Passez en revue le diagramme en camembert afin de comprendre le détail du trafic de l'application sur vos services internet.
- Passez en revue le graphique linéaire afin de comprendre combien de bytes (octets) de données ont été transférés sur chaque service internet dans le temps.
- Passez en revue 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.

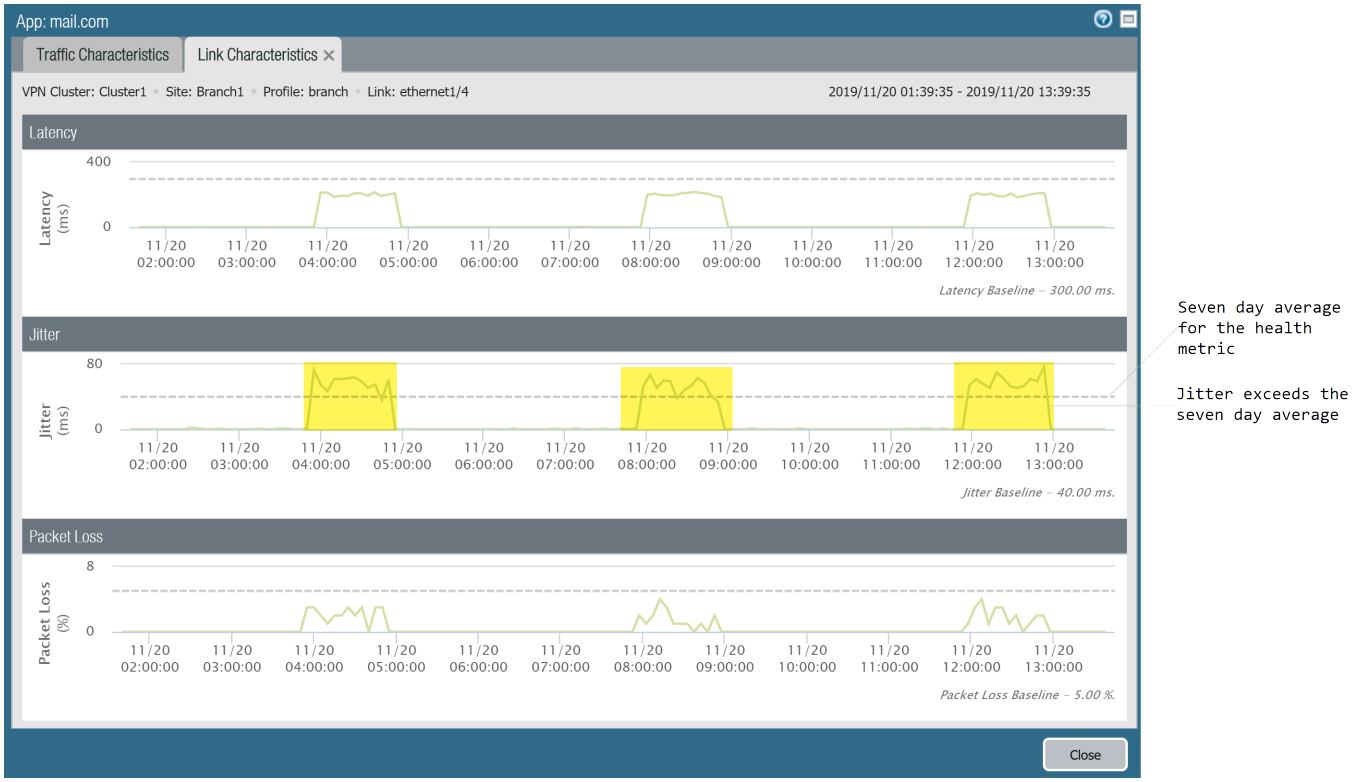
La ligne en pointillé indique la moyenne de sept jours de la mesure de l'état.

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. Dans cet exemple, nous affichons Ethernet 1/1 et nous pouvons voir que le pourcentage de paquets perdus a régulièrement dépassé le seuil de la moyenne de sept jours 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 instabilité du lien qui a dépassé le seuil de la moyenne des sept jours. 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 :

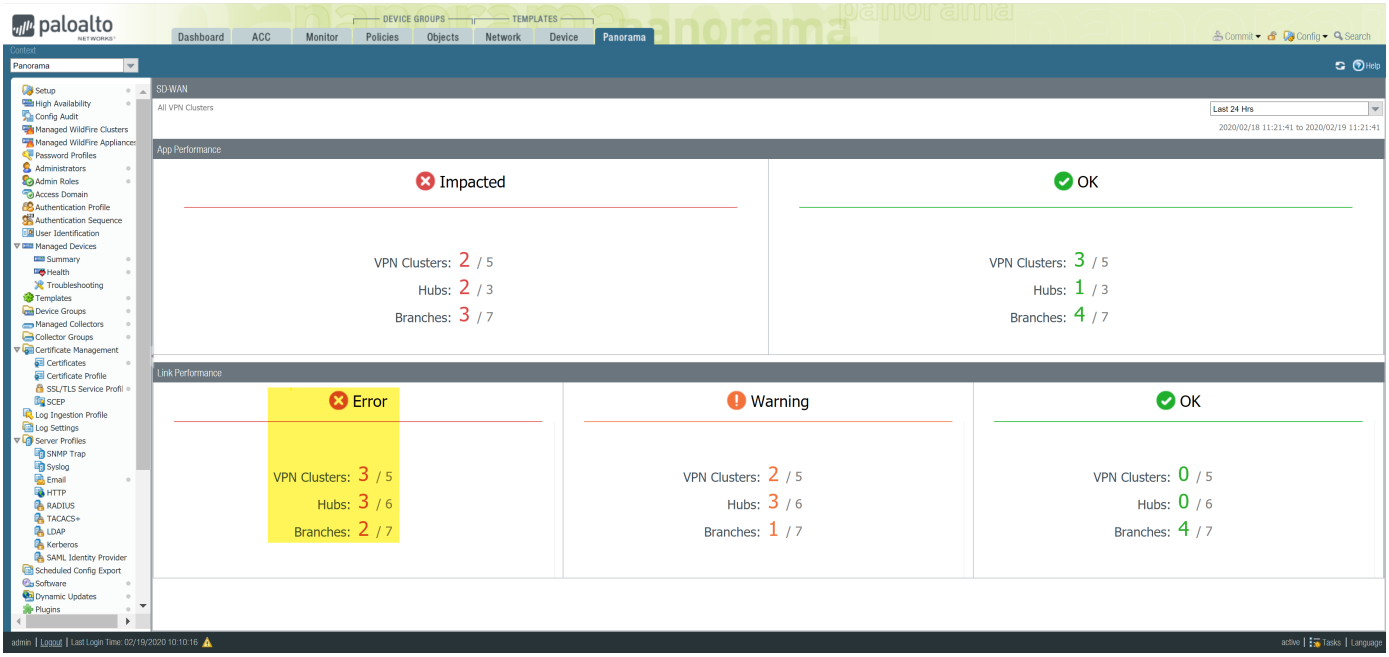
- Envisagez d'ajouter des liens supplémentaires au Traffic Distribution Profile (profil de distribution du trafic). En ajoutant des liens supplémentaires pour que le trafic de l'application bascule dessus, vous vous assurez que le trafic de l'application et l'expérience de l'utilisateur ne sont pas impactés 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 subit 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 ne 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.

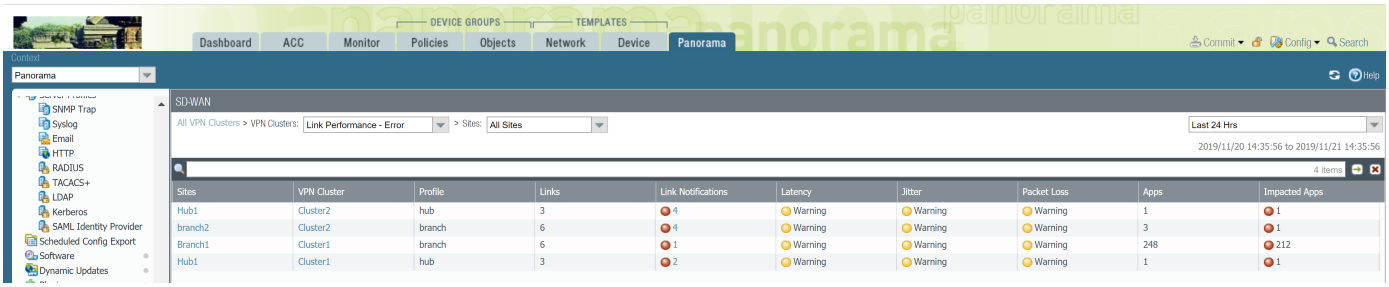
STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Sélectionnez **Panorama** > **SD-WAN** > **Monitoring** (Surveillance SD-WAN Panorama) et affichez les clusters de VPN **Impacted** (impactés).

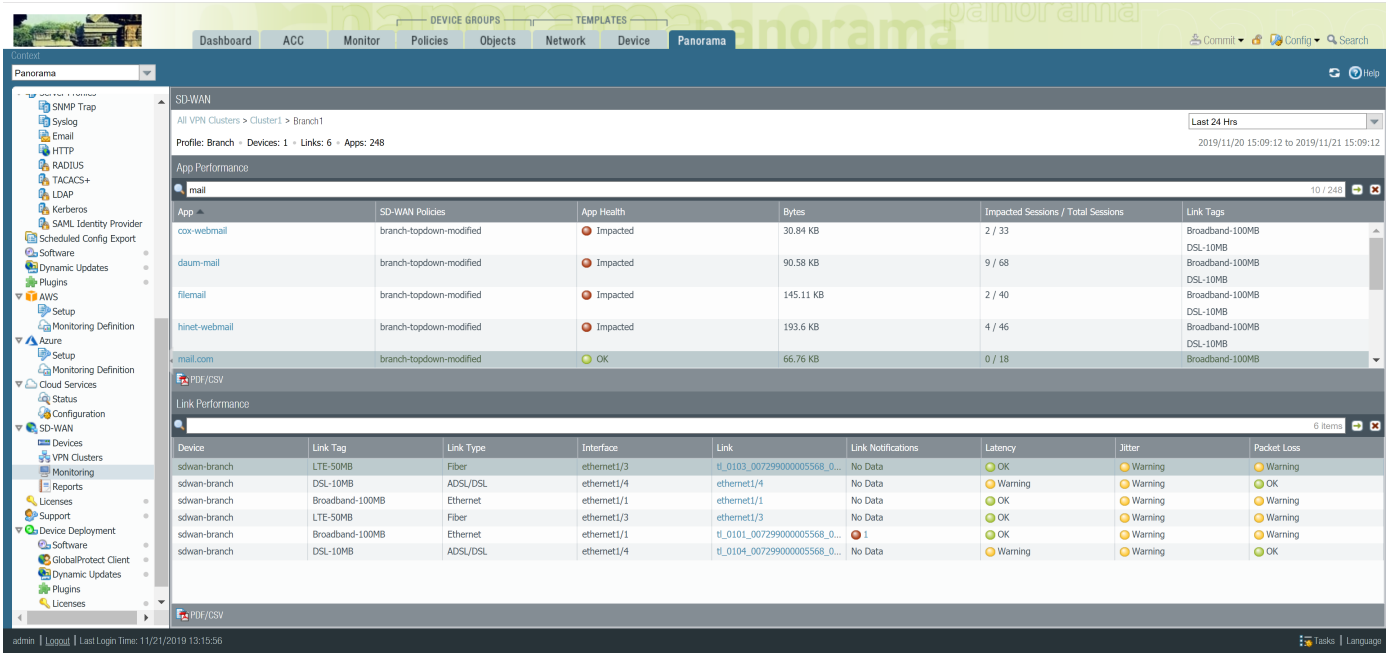


STEP 3 | Filtrez les clusters de VPN sur la base de votre mesure préférée dans la liste déroulante du **Site** et sélectionnez le délai. Dans les colonnes des Sites, sélectionnez le pare-feu du hub ou de la branche impacté afin d'afficher les appli impactées et la performance du lien correspondant.

Dans cet exemple, nous affichons **All Sites** (tous les sites) contenant des clusters de VPN impactés au cours des dernières 24 heures.

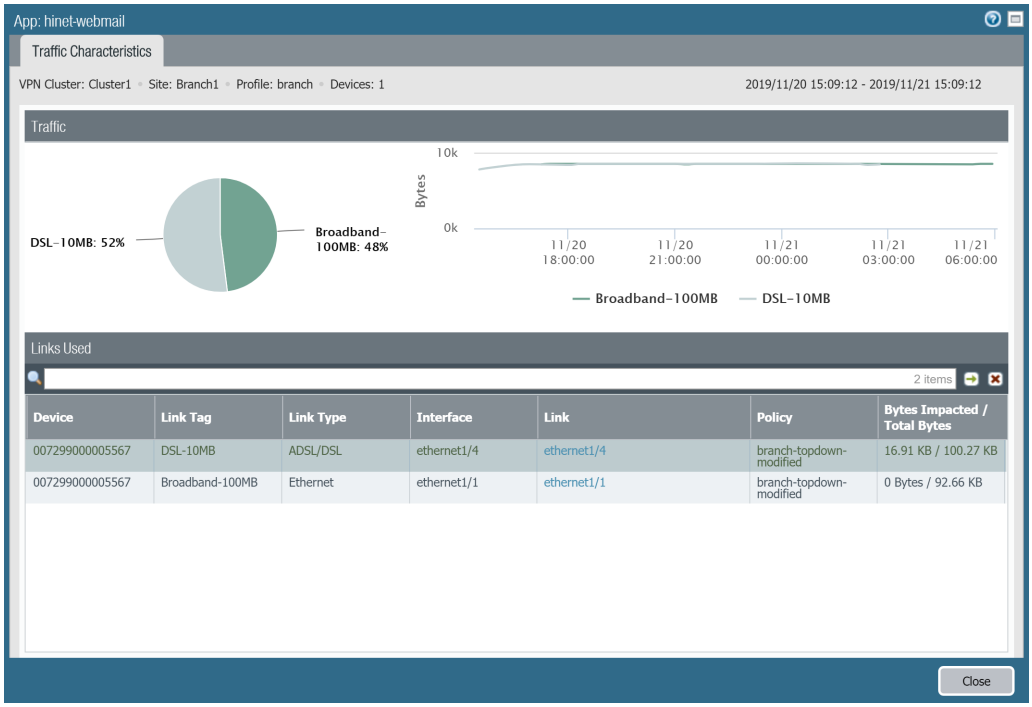


STEP 4 | Dans les colonnes des Sites, sélectionnez le pare-feu du hub ou de la branche impacté afin d'afficher les appli impactées et la performance du lien correspondant.



STEP 5 | Dans la partie App Performance (Performance des appli), cliquez sur une appli afin d'afficher les informations détaillées de Taffic Characteristic (caractéristiques du trafic) relatives au trafic de l'application comme le(s) service(s) internet et les liens utilisés :

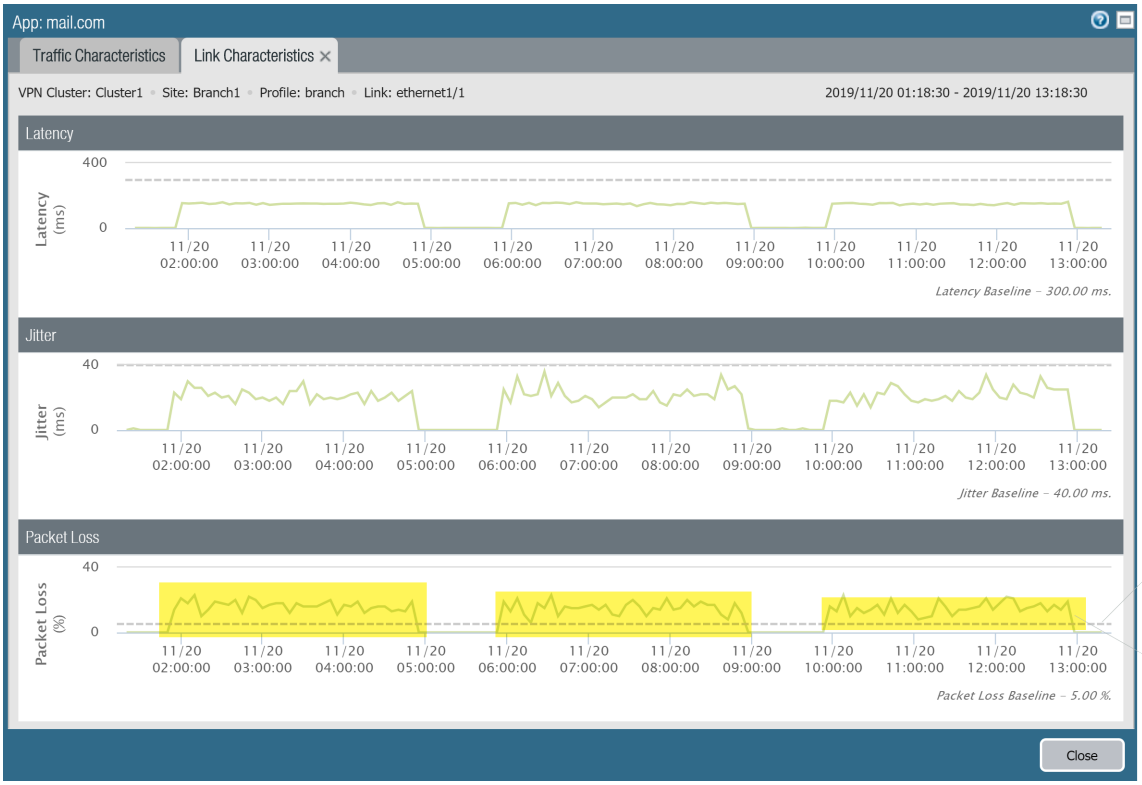
- Passez en revue le diagramme en camembert afin de comprendre le détail du trafic de l'application sur vos services internet.
- Passez en revue le graphique linéaire afin de comprendre combien de bytes (octets) de données ont été transférés sur chaque service internet dans le temps.
- Passez en revue 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.

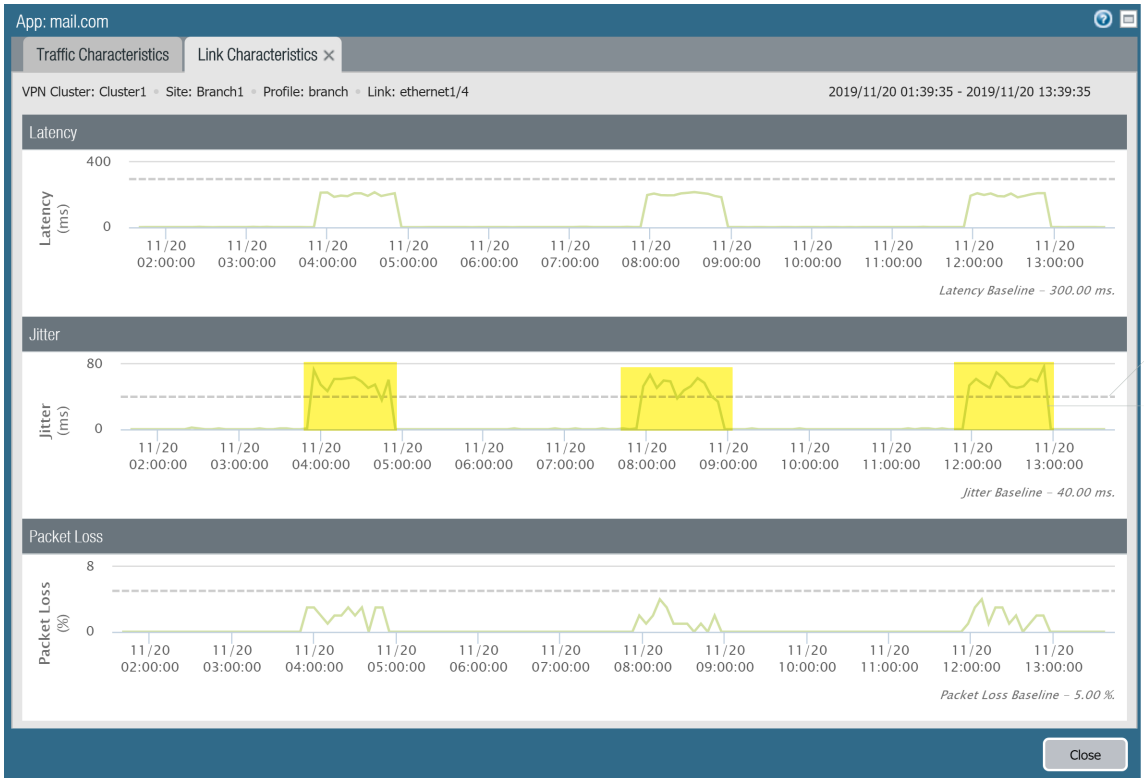
La ligne en pointillé indique le seuil que vous configurez lorsque Créer un Path Quality Profile (Profil de qualité du chemin d'accès).

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 subit 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 ne 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.

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.

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.

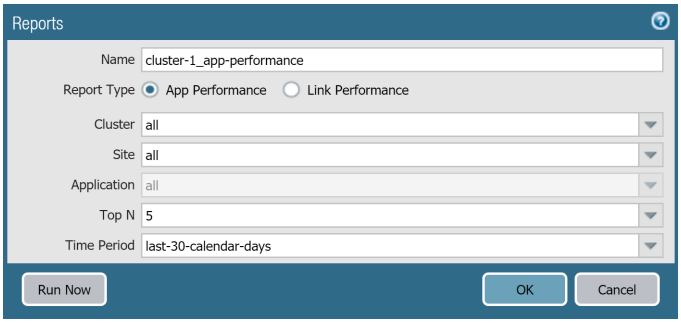
STEP 3 | Configurez les paramètres du rapport SD-WAN.

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.

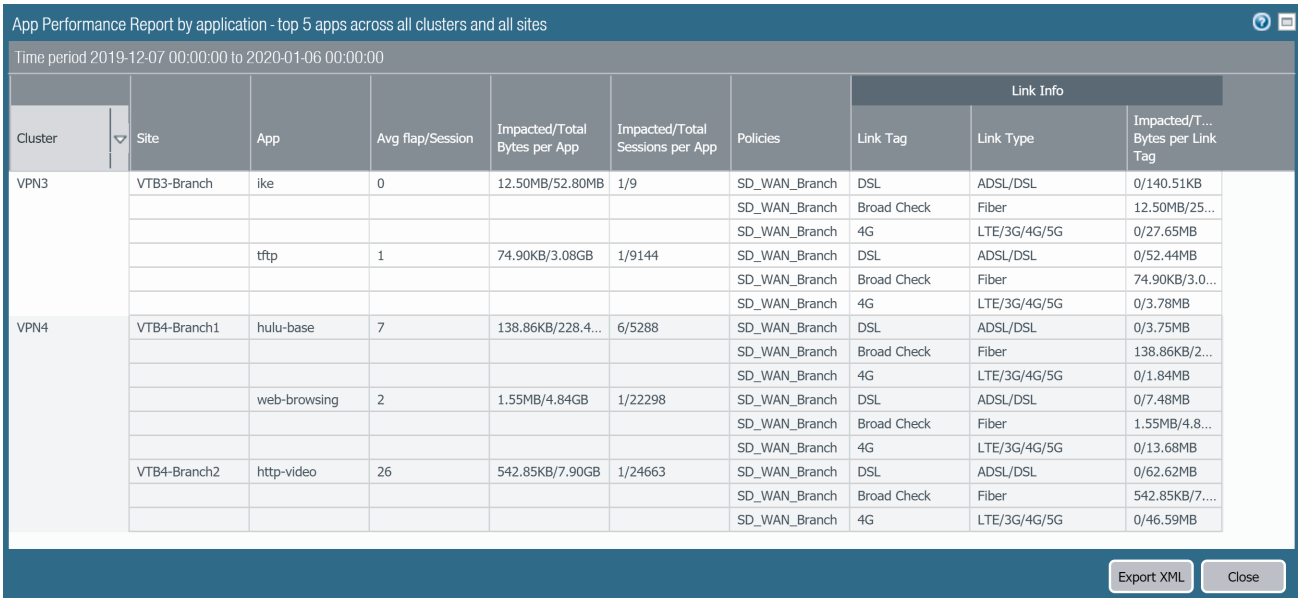
   Si vous avez sélectionné **all** (tous) les Clusters, alors ce champ est grisé et aucun Site ne peut être sélectionné.
5. (Performance des applications uniquement) Sélectionnez l'**Application** pour laquelle générer le rapport.

   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).



Cluster	Site	App	Avg flap/Session	Impacted/Total Bytes per App	Impacted/Total Sessions per App	Policies	Link Info		
							Link Tag	Link Type	Impacted/T... Bytes per Link Tag
VPN3	VTB3-Branch	ike	0	12.50MB/52.80MB	1/9	SD_WAN_Branch	DSL	ADSL/DSL	0/140.51KB
						SD_WAN_Branch	Broad Check	Fiber	12.50MB/25...
						SD_WAN_Branch	4G	LTE/3G/4G/5G	0/27.65MB
		tftp	1	74.90KB/3.08GB	1/9144	SD_WAN_Branch	DSL	ADSL/DSL	0/52.44MB
						SD_WAN_Branch	Broad Check	Fiber	74.90KB/3.0...
						SD_WAN_Branch	4G	LTE/3G/4G/5G	0/3.78MB
VPN4	VTB4-Branch1	hulu-base	7	138.86KB/228.4...	6/5288	SD_WAN_Branch	DSL	ADSL/DSL	0/3.75MB
						SD_WAN_Branch	Broad Check	Fiber	138.86KB/2...
						SD_WAN_Branch	4G	LTE/3G/4G/5G	0/1.84MB
		web-browsing	2	1.55MB/4.84GB	1/22298	SD_WAN_Branch	DSL	ADSL/DSL	0/7.48MB
						SD_WAN_Branch	Broad Check	Fiber	1.55MB/4.8...
						SD_WAN_Branch	4G	LTE/3G/4G/5G	0/13.68MB
	VTB4-Branch2	http-video	26	542.85KB/7.90GB	1/24663	SD_WAN_Branch	DSL	ADSL/DSL	0/62.62MB
						SD_WAN_Branch	Broad Check	Fiber	542.85KB/7....
						SD_WAN_Branch	4G	LTE/3G/4G/5G	0/46.59MB

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
> Désinstaller le plug-in SD-WAN

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.	`> show sdwan connection all | <sdwan-interface>`
• Afficher le nombre et le pourcentage de sessions distribuées vers chaque membre du tunnel d'une interface SD-WAN virtuelle.	`> show sdwan session distribution policy-name <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.	`> show sdwan rule 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.	`> show sdwan event`
• Effacer les événements SD-WAN.	`> clear sdwan event`
• 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	`> show sdwan path-monitor stats vif <sdwan.x>` `> show sdwan path-monitor stats vif <sdwan-interface-name>`

Si vous souhaitez...	Utilisez ...
valeur en temps réel a dépassé le seuil pour la dernière fois.	
• 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.	`> show sdwan session path-select session-id <session-id>`
• Afficher le mode de surveillance pour le lien SD-WAN virtuel (Agressif ou Souple) et les intervalles de mise à jour.	`> show sdwan path-monitor parameter path-name <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.	`> show sdwan path-monitor parameter vif <sdwan.x>`
Afficher les Compteurs généraux afin de diagnostiquer les problèmes SD-WAN	

• 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.
	`> show counter global filter delta yes`
	`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.
	`> show counter global filter delta yes`
	`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.	`> show vpn flow`
• Afficher les détails des tunnels individuels identifiés par leur nom.	`> show vpn flow name <name>`

Si vous souhaitez...	Utilisez ...
• Afficher les détails des tunnels individuels identifiés par leur ID.	`> show vpn flow tunnel-id <tunnel-id>`
• Afficher les détails de Internet Key Exchange (échange de clés Internet - IKE) Phase 1 et Phase 2 pour tous les tunnels.	`> show vpn ike-sa`
• Afficher Security Association (association de sécurité - SA) IKEv2 et les SA child IPSec IKEv2 d'une passerelle spécifique.	`> show vpn ike-sa gateway <gateway>`
• Afficher les détails du tunnel.	`> show vpn tunnel`
Afficher les informations BGP	
• Afficher le résumé BGP pour Virtual Router (routeur virtuel - VR).	`> show routing protocol bgp summary virtual-router <virtual-router>`
• Afficher le résumé des pairs BGP.	`> show routing protocol bgp peer peer-name <peer-name> virtual-router <virtual-router>`
• Afficher le résumé de Routing Information Base (base d'informations de routage - RIB)	`> show routing protocol bgp loc-rib`
Afficher les informations de l'interface SD-WAN parmi RIB et FIB	
• Afficher la nouvelle interface de sortie SD-WAN.	`> show routing route`
• Afficher les interfaces SD-WAN dans Forwarding Information Base (base d'informations de transfert - FIB).	`> show routing fib`

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 | (Pour le plug-in SD-WAN 1.0.2 et les versions ultérieures uniquement) 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.