paloalto TECHDOCS

Administration VPN IPSec

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Last Revised

June 9, 2023

Table of Contents

Principes de base du VPN IPSec

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Prisma Access • PAN-OS	Aucune licence requise

Les Virtual Private Networks (réseaux privés virtuels - VPN) créent des tunnels qui permettent aux utilisateurs/systèmes de se connecter en toute sécurité à un réseau public comme s’ils se connectaient sur un réseau local (LAN). Pour configurer un tunnel VPN, vous avez besoin d'une paire de périphériques qui peuvent s'authentifier mutuellement et crypter le flux d'informations entre eux. Ces périphériques peuvent être une paire de pare-feu Palo Alto Networks, ou un pare-feu Palo Alto Networks et un périphérique VPN d'un autre fournisseur.

En savoir plus sur les concepts de base du VPN :

- VPN IPSec
- Informations sur le tunnel IPSec
- Types de VPN IPSec
- Tunnels VPN IPSec
- Déploiements de VPN
- Internet Key Exchange (échange de clés Internet ; IKE) pour VPN

VPN IPSec

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Prisma Access • PAN-OS	Aucune licence requise

Le VPN IPSec fournit une communication IP privée et sécurisée sur une infrastructure réseau publique (par exemple, Internet). Grâce à cette technologie, différents sites ou utilisateurs dans différentes zones géographiques peuvent communiquer sur un réseau et ainsi utiliser leurs ressources en toute sécurité. IPSec assure la confidentialité et l’intégrité des données, y compris l’authentification, le contrôle d’intégrité et le chiffrement.

Le VPN IPSec est l’un des deux protocoles VPN courants, ou ensembles de normes utilisées pour établir une connexion VPN. Au niveau de la couche IP, IPSec fournit un accès distant sécurisé à l’ensemble du réseau (plutôt qu’à un seul périphérique).

Les VPN IPSec sont de deux types :

- Mode tunnel
- Mode de transport

Différences entre IPSec et VPN

SÉCURITÉ IP (IPSec)	VPN
Fournit aux hôtes IP des méthodes de chiffrement et d’authentification des données envoyées sur le réseau IP.	Utilise le chiffrement pour masquer toutes les données envoyées entre le client VPN et le serveur.
En utilisant IPSec, les entités qui ont des adresses IP peuvent créer un tunnel sécurisé.	De nombreux types de protocoles VPN offrent différents niveaux de sécurité et d’autres fonctionnalités. Les protocoles de tunnellisation les plus couramment utilisés dans l’industrie VPN sont le protocole PPTP (Point-to-Point Tunnel Protocol), le protocole L2TP (Layer Two Tunneling Protocol) ou IPSec, le protocole SSTP (Secure Socket Tunneling Protocol) et OpenVPN.

Informations sur le tunnel IPSec

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Le mode de transport tunnel IPSec n'est pas encore pris en charge pour Prisma Access) • PAN-OS	Aucune licence requise

Les normes IPSec définissent deux modes distincts d'exploitation IPSec : les modes tunnel et transport. La principale différence entre le mode transport et le mode tunnel réside dans l'application de la règle de politique. Alors qu'en mode tunnel, le paquet d'origine est encapsulé dans un autre en-tête IP, les paquets peuvent être protégés par l'en-tête d'authentification (AH), l'encapsulation de la charge utile de sécurité (ESP) ou les deux dans l'un ou l'autre mode.

- *AH ne fonctionne pas avec NAT, car l'intégrité est calculée à l'aide de certains champs de l'en-tête IP. La raison en est que AH inclut l'en-tête IP externe dans le calcul du code d'authentification de message basé sur le hachage (HMAC) qui provoque la rupture de NAT.*
- *Le mode de transport IPSec est utilisé pour les communications de bout en bout, par exemple entre un client et un serveur, ou entre un poste de travail et une passerelle si la passerelle est traitée comme un hôte. Un bon exemple serait une session Telnet ou Bureau à distance chiffrée d'un poste de travail vers un serveur.*
- *Alors que PAN-OS® prend en charge le mode tunnel par défaut, la prise en charge du mode transport est la nouvelle option introduite à partir de la version 11.0 de PAN-OS.*

Types de VPN IPSec

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Prisma Access • PAN-OS	Aucune licence requise

Le VPN site à site (ou passerelle à passerelle) et le VPN d’accès à distance (client à site) sont deux types distincts de VPN. Là où le VPN client à site représente une connexion utilisateur unique, les VPN site à site gèrent les connexions à distance entre des réseaux entiers.

Dans un VPN site à site, la méthode de sécurité IPSec est utilisée pour créer un tunnel crypté entre un réseau client et un site distant du client. Les tunnels VPN de Palo Alto Networks peuvent également être utilisés entre partenaires.

Les VPN de site à site n’autorisent pas plusieurs terminaux.

Dans le VPN d’accès à distance, les terminaux individuels sont connectés à un réseau privé pour accéder à distance aux services et aux ressources de ce réseau privé. Le VPN d’accès à distance est le plus approprié pour les utilisateurs professionnels et domestiques, car il permet plusieurs terminaux.

Tunnels VPN IPSec

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access • PAN-OS	Aucune licence requise

Le processus de création d'un tunnel IPSec commence par établir un tunnel préparatoire chiffré et sécurisé, puis, à partir de ce tunnel sécurisé, négocie les clés de chiffrement et les paramètres du tunnel IPSec.

Les négociations VPN se déroulent en deux phases définies : la première phase et la deuxième phase. L'objectif principal de la première phase est de configurer un canal crypté sécurisé à travers lequel les deux homologues peuvent négocier. Lorsque la première phase se termine avec succès, les homologues passent rapidement à la deuxième phase de négociations.

Si l'interface du tunnel se trouve dans une zone différente de la zone de départ du trafic, définissez une règle de politique pour permettre au trafic de circuler de la zone source vers la zone contenant l'interface du tunnel. La configuration de l'adresse IP sur l'interface du tunnel est facultative. Vous aurez besoin de cette adresse IP si vous avez l'intention d'exécuter des protocoles de routage dynamique sur l'interface du tunnel.

Bien qu'IPSec intègre de nombreuses technologies de composants et offre plusieurs options de chiffrement, le fonctionnement de base comprend les cinq procédures principales suivantes :

- **Trafic intéressant ou à la demande** : la règle de politique de tunnel IPSec et la table de routage déterminent quel type de trafic est considéré comme « intéressant » ou est capturé « à la demande » et, par conséquent, protégé. La manière dont la politique de sécurité VPN PAN-OS est mise en œuvre dépend de la plateforme de l'appareil. Les listes d'accès interprètent la règle de politique IPSec pour déterminer quel trafic sera protégé par IPSec.

  Le tunnel IPSec n'apparaît que lorsqu'il y a un trafic intéressant destiné au tunnel. Pour lancer manuellement le tunnel, vérifiez l'état du tunnel et effacez les tunnels en vous référant au dépannage des problèmes VPN de site à site à l'aide de l'interface CLI.
- **Phase 1 du protocole IKE** : IKE est une norme de protocole de gestion de clés utilisée avec IPSec. IKE authentifie chaque homologue dans une session IPSec, négocie automatiquement deux niveaux de SA et gère l'échange de clés de session réalisé en deux phases : phase 1 et phase 2.

  L'objectif principal de la phase 1 du protocole IKE est d'authentifier les homologues IPSec et de configurer un canal sécurisé entre les pairs.
- **Phase 2 du protocole IKE** : IKE négocie les paramètres d'association de sécurité (SA) IPSec les plus stricts entre les homologues.
- **Transfert de données IPSec** : les données éligibles sont transférées entre homologues IPSec. Les informations sont échangées via des sessions IPSec basées sur la méthode de définition du trafic intéressant. Les paquets sont cryptés et décryptés au niveau des homologues IPSec à l'aide de tout chiffrement spécifié dans la SA IPSec.
- **Terminaison de session de tunnel IPSec** : la session IPSec peut être arrêtée parce que le trafic s'est terminé et que la SA IPSec a été supprimée ou que la SA peut atteindre son délai d'expiration en fonction de l'un ou l'autre des paramètres de durée de vie de la SA. Le délai d'expiration de SA

peut survenir après un nombre spécifié de secondes ou un nombre spécifié d'octets transmis via la connexion.

Les clés sont supprimées lorsque les SA se terminent, ce qui oblige IKE à effectuer une nouvelle phase deux et, éventuellement, une nouvelle négociation de phase une. De nouvelles SA peuvent être établies avant l'expiration des actuelles, maintenant ainsi des flux de données ininterrompus.

La session IPSec se termine par suppression ou par expiration du délai.

Implémentation des règles de politique de tunnel IPSec sur les pare-feux nouvelle génération Palo Alto Networks

L'encapsulation d'un paquet pour un transport sécurisé sur le réseau se fait au moyen du protocole IPsec. Par exemple, dans le cas d'un VPN site à site, un hôte source d'un réseau transmet un paquet IP. Lorsque ce paquet atteint la périphérie du réseau, il entre en contact avec une passerelle VPN. La passerelle VPN qui correspond à ce réseau crypte le paquet IP privé et le relaie via un tunnel ESP vers une passerelle VPN homologue à la périphérie du réseau suivant, dont la passerelle décrypte le paquet et le fournit à l'hôte de destination.

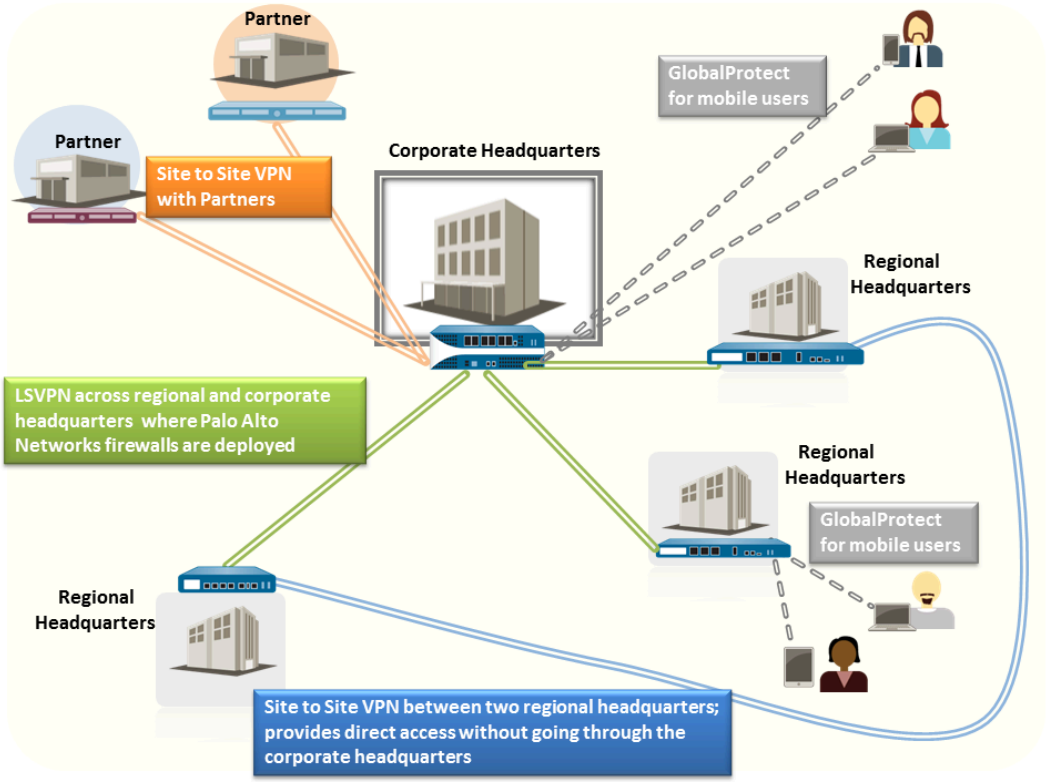
Les VPN basés sur des politiques ont des règles de sécurité, des règles de politique ou des listes d'accès spécifiques (telles que des adresses source, des adresses de destination et des ports) configurées pour autoriser le trafic intéressant via les tunnels IPSec. Ces règles sont référencées lors du mode rapide (ou phase IPSec 2) et sont échangées dans le premier ou le deuxième message en tant qu'ID de proxy. Si le pare-feu de Palo Alto Networks n'est pas configuré avec les paramètres d'ID de proxy, le pare-feu définit l'ID de proxy avec les valeurs par défaut (IP source = 0.0.0.0/0, IP de destination = 0.0.0.0/0, application : any) et l'échange avec l'homologue lors du premier ou du deuxième message du mode rapide.

Déploiements de VPN

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Prisma Access • PAN-OS	Aucune licence requise

Le pare-feu Palo Alto Networks prend en charge les déploiements de VPN suivants :

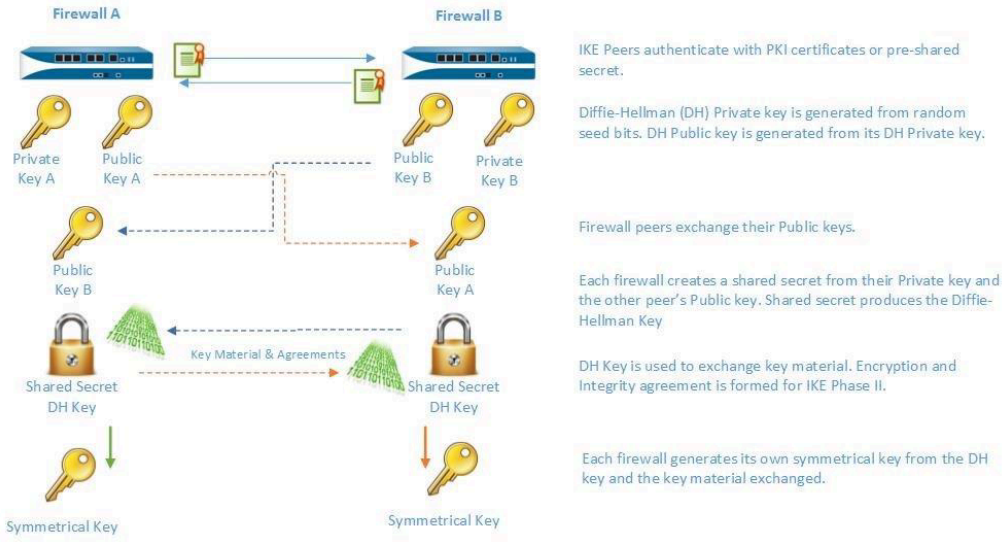
- **VPN de site à site** : un VPN simple qui connecte un site central et un site distant, ou un VPN Hub and Spoke qui connecte un site central à plusieurs sites distants. Le pare-feu utilise l’ensemble de protocoles IPSec (Internet Protocol Security) pour configurer un tunnel sécurisé pour le trafic entre les deux sites. Consultez Présentation du VPN de site à site.
- **VPN d'utilisateur distant à site** : une solution qui utilise l'agent GlobalProtect pour permettre à un utilisateur distant d'établir une connexion sécurisée via le pare-feu. Cette solution utilise SSL et IPSec pour établir une connexion sécurisée entre l'utilisateur et le site. Reportez-vous au Guide de l'administrateur GlobalProtect.
- **VPN à grande échelle** : le VPN à grande échelle GlobalProtect de Palo Alto Networks (LSVPN) fournit une méthode simplifiée pour déployer un VPN Hub and Spoke évolutif comportant jusqu'à 1 024 bureaux satellites. Cette solution nécessite le déploiement de pare-feu Palo Alto Networks sur le concentrateur et sur chaque terminaison. Elle utilise des certificats pour l'authentification des périphériques, SSL pour sécuriser la communication entre tous les composants et IPSec pour sécuriser les données. Reportez-vous à la section VPN à grande échelle (LSVPN).
- **VPN de site distant** : les sites distants utilisent des tunnels IPSec pour sécuriser les utilisateurs et les périphériques situés dans des emplacements réseau distants. En outre, les utilisateurs mobiles sécurisés avec GlobalProtect et les utilisateurs sur les sites distants accèdent aux applications privées à l’aide de tunnels IPSec (pour les connexions de service ou les connecteurs ZTNA) ou de tunnels GRE (pour les connexions Colo-Connect).



Internet Key Exchange (échange de clés Internet ; IKE) pour VPN

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Le processus IKE permet aux homologues VPN à chaque extrémité du tunnel de crypter et de décrypter à l'aide de clés mutuellement convenues ou d'un certificat et d'une méthode de cryptage. Ce processus se déroule en deux phases : IKE de phase 1 et IKE de phase 2. Chacune de ces phases utilise des clés et des algorithmes de chiffrement qui sont définis à l’aide de profils cryptographiques (profil crypto IKE et profil crypto IPSec) ; le résultat de la négociation IKE est une Security Association (association de sécurité - SA). Une SA est un ensemble d'algorithmes et de clés mutuellement convenues qui sont utilisés par les deux homologues VPN pour autoriser la circulation des données via le tunnel VPN. L'illustration suivante décrit le processus d'échange de clés pour la configuration du tunnel VPN :



Passerelle IKE

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Des pare-feu Palo Alto Networks ou un pare-feu et un autre périphérique de sécurité qui établissent et mettent fin à des connexions VPN entre deux réseaux sont appelés des passerelles IKE. Pour configurer le tunnel VPN et envoyer le trafic entre les passerelles IKE, chaque homologue doit disposer d'une adresse IP (statique ou dynamique) ou d'un FQDN. Les homologues VPN utilisent des clés pré-partagées ou des certificats pour s’authentifier mutuellement.

Les homologues doivent également négocier le mode (Principal ou Agressif) de configuration du tunnel VPN et de la durée de vie de la SA dans la phase 1 du protocole IKE. Le mode Principal protège l'identité des homologues et est davantage sécurisé, car plus de paquets sont échangés lors de la configuration du tunnel. Le mode Principal est recommandé pour la négociation IKE si les deux homologues la prennent en charge. Le mode Agressif utilise moins de paquets pour configurer le tunnel VPN et est donc plus rapide mais moins sécurisé.

Pour plus d'informations sur la configuration, reportez-vous à la section Configuration d'une passerelle IKE.

Phase 1 du protocole IKE

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Dans cette phase, les pare-feu utilisent les paramètres définis dans la configuration de passerelle IKE et le profil crypto IKE pour s'authentifier mutuellement et configurer un canal de contrôle sécurisé. Cette phase du protocole IKE prend en charge l’utilisation de clés pré-partagées ou de certificats numériques (qui utilisent l’infrastructure à clé publique [PKI]) pour l’authentification mutuelle des homologues VPN. Les clés pré-partagées sont une solution simple pour sécuriser des réseaux plus petits, car elles ne nécessitent pas la prise en charge d’une infrastructure PKI. Les certificats numériques peuvent être plus pratiques pour les réseaux plus grands ou les implémentations qui nécessitent une sécurité d'authentification renforcée.

Lors de l'utilisation de certificats, assurez-vous que l'autorité de certification qui émet le certificat est approuvée par les deux homologues de passerelle et que le nombre maximum de certificats dans la chaîne de certificats est de 5. Lorsque la fragmentation IKE est activée, le pare-feu peut réassembler les messages IKE avec un nombre maximum de 5 certificats dans la chaîne de certificats et établir un tunnel VPN.

Le profil crypto IKE définit les options suivantes qui sont utilisées dans la négociation de SA IKE :

- Le groupe Diffie-Hellman (DH) pour la génération de clés symétriques pour IKE.

  L'algorithme Diffie-Hellman utilise la clé privée d'une partie et la clé publique de l'autre pour créer un secret partagé, qui est une clé cryptée partagée par les deux homologues du tunnel PN. Les groupes DH pris en charge sur le pare-feu sont les suivants :

Numéro de groupe	Nombre de bits
Groupe 1	768 bits
Groupe 2	1 024 bits (par défaut)
Groupe 5	1 536 bits
Groupe 14	2 048 bits
Groupe 15	(PAN-OS 10.2.0 et versions ultérieures) Groupe exponentiel modulaire 3072 bits

Numéro de groupe	Nombre de bits
Groupe 16	(PAN-OS 10.2.0 et versions ultérieures) Groupe exponentiel modulaire 4096 bits
Groupe 19	Groupe de courbes elliptiques 256 bits
Groupe 20	Groupe de courbes elliptiques 384 bits
Groupe 21	(PAN-OS 10.2.0 et versions ultérieures) Groupe de courbes elliptiques aléatoires 512 bits

- Algorithmes d'authentification : sha1, sha 256, sha 384, sha 512 ou md5.
- Algorithmes de chiffrement : aes-256-gcm, aes-128-gcm, 3des, aes-128-cbc, aes-192-cbc, aes-256-cbc ou des.

- *PAN-OS 10.0.3 et les versions ultérieures prennent en charge les algorithmes aes-256-gcm et aes-128-gcm.*
- *PAN-OS 10.1.0 et les versions antérieures prennent en charge l'algorithme de chiffrement des.*

Phase 2 du protocole IKE

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Une fois le tunnel sécurisé et authentifié, dans la phase 2, le canal est davantage sécurisé pour le transfert de données entre les réseaux. La phase 2 utilise les clés qui ont été établies à la phase 1 du processus et le profil crypto IPSec, qui définit les clés et les protocoles IPSec utilisés pour la SA IKE de phase 2.

IPSec utilise les protocoles suivants pour permettre la communication sécurisée :

- Encapsulating Security Payload (encapsulation de la charge utile de sécurité - ESP) : vous permet de crypter l'ensemble du paquet IP, d'authentifier la source et de vérifier l'intégrité des données. Bien qu'ESP nécessite le cryptage et l'authentification du paquet, vous pouvez choisir le cryptage seul (ou l'authentification seule) en sélectionnant Nul en regard de l'option de cryptage (ou d'authentification) ; l'utilisation du cryptage sans l'authentification n'est pas recommandée.
- Authentication Header (en-tête d'authentification - AH) : vous permet d'authentifier la source du paquet et de vérifier l'intégrité des données. AH ne crypte pas la charge utile de données et n'est pas adapté aux déploiements où la confidentialité des données est importante. AH est communément utilisé lorsque l'objectif principal est la vérification de la légitimité de l'homologue et lorsque la confidentialité des données n'est pas requise.

Table 1: Algorithmes pris en charge pour le chiffrement et l'authentification IPSec

ESP	AH
Options d'échange Diffie-Hellman (DH) prises en charge	
• Groupe 1 : 768 bits • Groupe 2 : 1024 bits (par défaut) • Groupe 5 : 1536 bits • Groupe 14 : 2048 bits • (PAN-OS 10.2.0 et versions ultérieures) Groupe 15 : groupe exponentiel modulaire de 3 072 bits • (PAN-OS 10.2.0 et versions ultérieures) Groupe 16 : groupe exponentiel modulaire de 4 096 bits • Groupe 19 : groupe de courbe elliptique 256 bits • Groupe 20 : groupe de courbe elliptique 384 bits • (PAN-OS 10.2.0 et versions ultérieures) Groupe 21 : groupe de courbes elliptiques aléatoires de 512 bits • PFS désactivé : par défaut, le secret de transfert idéal est activé, ce qui signifie qu'une nouvelle clé DH est générée dans la phase 2 du protocole IKE à l'aide de l'un des groupes indiqués ci-dessus. Cette clé est indépendante des clés échangées dans la phase 1 du protocole IKE et offre une meilleure sécurité du transfert de données. Si vous sélectionnez PFS désactivé, la clé DH créée à la phase 1 n'est pas renouvelée et une seule clé est utilisée pour les négociations SA IPSec. Les deux homologues VPN doivent être activés ou désactivés pour l'option PFS.	
Algorithmes de chiffrement pris en charge	
• des	(PAN-OS 10.1.0 et versions antérieures) Data Encryption Standard (DES) avec un niveau de sécurité de 56 bits.
• 3des	Triple Data Encryption Standard (norme de chiffrement de données triple, 3DES) avec une puissance de sécurité de 112 bits.
• aes-128-cbc	Advanced Encryption Standard (norme de chiffrement avancée - AES) utilisant le chaînage de bloc de chiffrement (CBC) avec une puissance de sécurité de 128 bits.
• aes-192-cbc	AES utilisant CBC avec une puissance de sécurité de 192 bits.
• aes-256-cbc	AES utilisant CBC avec une puissance de sécurité de 256 bits.
• aes-128-ccm	AES utilisant Counter with CBC-MAC (compteur avec CBC-MAC - CCM) avec une puissance de sécurité de 128 bits.
• aes-128-gcm	AES utilisant Galois/Counter Mode (mode Galois/Compteur - GCM) avec une puissance de sécurité de 128 bits.

ESP	AH
• aes-256-gcm	AES utilisant GCM avec une puissance de sécurité de 256 bits.
Algorithmes d’authentification pris en charge	
• md5	• md5
• sha 1	• sha 1
• sha 256	• sha 256
• sha 384	• sha 384
• SHA512	• sha512

Méthodes de sécurisation des tunnels VPN IPSec (phase 2 du protocole IKE)

Les tunnels VPN IPSec peuvent être sécurisés à l'aide de clés manuelles ou automatiques. De plus, les options de configuration IKE incluent un groupe Diffie-Hellman pour l’accord de clés, un algorithme de chiffrement et un hachage pour l’authentification des messages.

- **Clé manuelle** : une clé manuelle est généralement utilisée si le pare-feu Palo Alto Networks établit un tunnel VPN avec un périphérique d'ancienne génération, ou si vous souhaitez réduire les frais de génération de clés de session. Lors de l'utilisation de clés manuelles, la même clé doit être configurée sur les deux homologues.

  Les clés manuelles ne sont pas recommandées pour l’établissement d’un tunnel VPN, car les clés de session peuvent être compromises lors de la transmission des informations de clé entre les homologues ; si les clés sont compromises, le transfert de données n’est plus sécurisé.
- **Clé automatique** : une clé automatique vous permet de générer automatiquement des clés pour la configuration et le maintien du tunnel IPSec en fonction des algorithmes définis dans le profil crypto IPSec.

IKEv2

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Une passerelle VPN IPSec utilise IKEv1 ou IKEv2 pour négocier l'association de sécurité (SA) IKE et le tunnel IPSec. IKEv2 est défini dans RFC 5996.

Contrairement à IKEv1, qui utilise une SA de phase 1 et une SA de phase 2, IKEv2 utilise une SA enfant pour l'encapsulation de la charge utile de sécurité (ESP) ou l'en-tête d'authentification (AH), qui est configuré avec une SA IKE.

NAT traversal (NAT-T) doit être activé sur les deux passerelles si NAT se produit sur un périphérique situé entre les deux passerelles. Une passerelle peut uniquement voir l'adresse IP publique (globalement routable) du périphérique NAT.

IKEv2 offre les avantages suivants par rapport à IKEv1 :

- Les terminaux du tunnel échangent moins de messages pour établir un tunnel. IKEv2 utilise quatre messages; IKEv1 en utilise neuf messages (en mode Principal) ou six (en mode Agressif).
- La fonctionnalité NAT-T intégrée améliore la compatibilité entre les fournisseurs.
- La vérification de l’état intégrée rétablit automatiquement un tunnel s’il est arrêté. La vérification de l'activité remplace la détection des homologues inactifs utilisée dans IKEv1.
- Prend en charge des sélecteurs de trafic (un par échange). Les sélecteurs de trafic sont utilisés dans les négociations IKE pour contrôler le trafic pouvant accéder au tunnel.
- Prend en charge l'échange de certificat Hachage et URL pour réduire la fragmentation.
- Protection contre les attaques DoS avec une meilleure validation de l'homologue. Un nombre excessif de SA demi-ouvertes peut déclencher une validation du cookie.

Avant de configurer IKEv2, vous devez connaître les concepts suivants :

- Vérification de l'activité
- Seuil d'activation du cookie et validation du cookie stricte
- Sélecteurs de trafic
- Échange de certificat Hachage et URL
- Durée de vie de la clé et intervalle de réauthentification SA

Après la Configuration d'une passerelle IKE, si vous avez choisi IKEv2, effectuez les tâches facultatives suivantes liées à IKEv2 si nécessaire dans votre environnement :

- Exportation d'un certificat pour l'accès d'un homologue à l'aide de Hachage et URL
- Importation d'un certificat pour l'authentification de passerelle IKEv2
- Modification de la durée de vie de la clé ou de l'intervalle d'authentification pour IKEv2
- Modification du seuil d'activation du cookie pour IKEv2
- Configuration des sélecteurs de trafic IKEv2

Vérification de l'activité

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

La vérification de l'activité pour IKEv2 est identique à la Dead Peer Detection (détection des homologues inactifs ; DPD), qui est utilisée dans IKEv1 pour déterminée si un homologue est toujours disponible.

Dans IKEv2, la vérification de l’activité est possible via la transmission de tout paquet IKEv2 ou un message informatif vide envoyé par la passerelle à l’homologue à un intervalle configurable (5 secondes par défaut). Si nécessaire, l’expéditeur tente de le retransmettre jusqu’à 10 fois. S'il ne reçoit pas de réponse, l'expéditeur ferme et supprime les IKE_SA et CHILD_SA correspondants. L'expéditeur commence à envoyer un autre message IKE_SA_INIT.

Seuil d'activation du cookie et validation du cookie stricte

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

La validation du cookie est toujours activée pour IKEv2 ; elle vous protège contre les attaques DoS SA demi-ouvertes. Vous pouvez configurer le nombre limite global de SA demi-ouvertes qui déclenchera une validation du cookie. Vous pouvez également configurer des passerelles IKE pour appliquer la validation du cookie pour chaque nouvelle SA IKEv2.

- Le **Cookie Activation Threshold (Seuil d'activation du cookie)** est un paramètre de session VPN global qui limite le nombre de SA demi-ouvertes simultanées (par défaut, 500). Lorsque le nombre de SA IKE demi-ouvertes est supérieur au **Cookie Activation Threshold (Seuil d'activation du cookie)**, le répondeur demande un cookie, et l'initiateur doit répondre par un IKE_SA_INIT contenant un cookie pour valider la connexion. Si la validation du cookie réussit, une autre SA peut être ouverte. Une valeur de 0 signifie que la validation du cookie est toujours activée.

  Le répondeur ne garde pas l'état d'initiateur, et ne procède pas à un échange de clé Diffie-Hellman, tant que l'initiateur n'a pas renvoyé le cookie. La validation du cookie IKEv2 atténue une attaque DoS qui tenterait de maintenir plusieurs connexions demi-ouvertes.

  Le **Cookie Activation Threshold (Seuil d'activation du cookie)** doit être inférieur au paramètre **Maximum Half Opened SA (Nombre max de SA demi-ouvertes)**. Si vous Modification du seuil d'activation du cookie pour IKEv2 sur un nombre plus élevé (65534 par exemple) et que le paramètre **Maximum Half Opened SA (Nombre maximum de SA demi-ouvertes)** est toujours défini sur la valeur par défaut de 65535, la validation du cookie est désactivée.
- Vous pouvez activer l'option **Strict Cookie Validation (Validation du cookie stricte)** si vous souhaitez qu'une validation du cookie soit effectuée pour chaque nouvelle SA IKEv2 reçue par une passerelle, quel que soit le seuil global. La **Strict Cookie Validation (Validation du cookie stricte)** n'affecte que la passerelle IKE configurée et est désactivée par défaut. Lorsque la **Strict Cookie Validation (Validation du cookie stricte)** est désactivée, le système utilise le **Cookie Activation Threshold (Seuil d'activation du cookie)** pour déterminer si un cookie est nécessaire ou non.

Sélecteurs de trafic

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Dans IKEv1, un pare-feu comprenant un VPN basé sur un itinéraire doit utiliser un ID de proxy local et distant pour configurer un tunnel IPSec. Chaque homologue compare ses ID de proxy avec ceux qu'il a reçu dans le paquet afin de négocier avec succès la phase 2 du protocole IKE. IKE phase 2 concerne la négociation des SA pour configurer un tunnel IPSec. (Pour plus d'informations sur les ID de proxy, reportez-vous à la section en texte clair.)

Dans IKEv2, une Configuration des sélecteurs de trafic IKEv2 est possible, qui sont des composants de trafic réseau utilisés pendant une négociation IKE. Les sélecteurs de trafic sont utilisés pendant CHILD_SA (création de tunnel) phase 2 pour configurer le tunnel et déterminer le trafic autorisé dans le tunnel. Les deux homologues de passerelle IKE doivent négocier et s'accorder sur leurs sélecteurs

de trafic ; sinon, un côté réduit sa plage d'adresses pour parvenir à un accord. Une connexion IKE peut comporter plusieurs tunnels ; par exemple, vous pouvez affecter différents tunnels à chaque service pour isoler son trafic. La séparation du trafic permet également de mettre en œuvre des fonctionnalités telles que QoS.

Les sélecteurs de trafic IPv4 et IPv6 sont les suivants :

- **Adresse IP source** : préfixe réseau, plage d'adresses, hôte spécifique ou caractère générique.
- **Adresse IP de destination** : préfixe réseau, plage d'adresses, hôte spécifique ou caractère générique.
- **Protocole** : protocole de transport, TCP ou UDP par exemple.
- **Port source** : port d'origine du paquet.
- **Port de destination** : port auquel le paquet est destiné.

Pendant une négociation IKE, plusieurs sélecteurs de trafic sont possibles pour différents réseaux et protocoles. Par exemple, l'initiateur peut indiquer qu'il souhaite envoyer des paquets TCP de l'adresse 172.168.0.0/16, via le tunnel, à son homologue de destination 198.5.0.0/16. Il souhaite également envoyer des paquets UDP de l'adresse 172.17.0.0/16, via le même tunnel, à la même passerelle de destination 0.0.0.0 (n'importe quel réseau). La passerelle homologue doit accepter ces sélecteurs de trafic pour pouvoir déterminer à quoi s'attendre.

Il est possible qu’une passerelle commence une négociation à l’aide d’un sélecteur de trafic avec une adresse IP plus spécifique que l’adresse IP de l’autre passerelle.

- Par exemple, la passerelle A propose une adresse IP source 172.16.0.0/16 et une adresse IP de destination 192.16.0.0/16. Cependant, la passerelle B est configurée avec l'adresse IP source 0.0.0.0 (n'importe quelle source) et l'adresse IP de destination 0.0.0.0 (n'importe quelle destination). La passerelle B réduit donc son adresse IP source à 192.16.0.0/16 et son adresse IP de destination à 172.16.0.0/16. Ainsi, la réduction permet d'inclure les adresses de la passerelle A et les sélecteurs de trafic des deux passerelles correspondent.
- Si la passerelle B (configurée avec l'adresse IP source 0.0.0.0) est l'initiateur et non le répondeur, la passerelle A répondra avec son adresse IP plus spécifique, et la passerelle B réduira ses adresses pour parvenir à un accord.

Échange de certificat Hachage et URL

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

IKEv2 prend en charge l’échange de certificats Hachage et URL, qui est utilisé pendant une négociation IKEv2 d’une SA. Vous stockez le certificat sur un serveur HTTP, qui est spécifié par une URL. L'homologue extrait le certificat du serveur à la réception de l'URL vers le serveur. Le hachage permet de vérifier si le contenu du certificat est valide ou non. Les deux homologues échangent ainsi des certificats avec la CA HTTP plutôt qu'entre eux.

La partie hachage de Hachage et URL réduit la taille du message et l'échange de certificat Hachage et URL permet donc de réduire le risque de fragmentation des paquets pendant une négociation IKE. L'homologue reçoit le certificat et le hachage attendu, ce qui signifie que la phase 1 du protocole IKE a validé l'homologue. La réduction de la fragmentation permet de vous protéger contre les attaques DoS.

Vous pouvez activer l'échange de certificat Hachage et URL pendant la configuration d'une passerelle IKE en sélectionnant **HTTP Certificate Exchange (Échange de certificat HTTP)** et en saisissant la **Certificate URL (URL du certificat)**. L'homologue doit également utiliser l'échange de certificats Hachage et URL pour que l'échange réussisse. Si l'homologue ne peut pas utiliser la méthode Hachage et URL, les certificats X.509 sont échangés comme dans IKEv1.

Si vous activez l'échange de certificat Hachage et URL, vous devez exporter votre certificat vers le serveur de certificats (s'il ne s'y trouve pas déjà). Lorsque vous exportez le certificat, le format du fichier doit être **Binary Encoded Certificate (DER) (Certificat codé en binaire (DER))**. Reportez-vous à la section Exportation d'un certificat pour l'accès d'un homologue à l'aide de Hachage et URL.

Durée de vie de la clé et intervalle de réauthentification SA

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Dans IKEv2, deux valeurs de profil crypto IKE, **Key Lifetime (Durée de vie de la clé)** et **IKEv2 Authentication Multiple (Multiple d'authentification IKEv2)**, contrôlent l'établissement de SA IKEv2. La durée de vie de la clé correspond à la durée de validité d'une clé SA IKE négociée. Avant que la durée de vie de la clé expire, la clé de la SA doit être changée sinon, lors de l'expiration, la SA doit démarrer un nouveau changement de clé de SA IKEv2. La valeur par défaut est 8 heures.

L'intervalle de réauthentification est obtenu en multipliant la valeur **Key Lifetime (Durée de vie de la clé)** par la valeur **IKEv2 Authentication Multiple (Multiple d'authentification IKEv2)**. Le multiple d'authentification par défaut est 0, ce qui désactive la fonction de réauthentification.

La plage des multiples d'authentification est comprise entre 0 et 50. Par exemple, si vous envisagiez de configurer un multiple d'authentification de 20, le système effectuerait une réauthentification tous les 20 changements de clef, à savoir toutes les 160 heures. Cela signifie que la passerelle pourrait créer une SA enfant de 160 heures avant de devoir se réauthentifier auprès d'IKE pour recréer entièrement la toute nouvelle SA IKE.

Dans IKEv2, les passerelles initiateur et répondeur disposent de valeurs de durée de vie de la clé propres, et la passerelle présentant la durée de vie de la clé la plus courte est celle qui demandera la nouvelle SA.

Prise en main du VPN IPSec (site à site)

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access • PAN-OS	Aucune licence requise

Une connexion VPN fournit un accès sécurisé aux informations entre deux sites ou plus. Afin de fournir un accès sécurisé aux ressources et une connexion fiable, une connexion VPN nécessite les composants suivants : Passerelle IKE, interface de tunnel, surveillance de tunnel, Internet Key Exchange (échange de clés Internet - IKE) pour VPN et IKEv2.

Avant de planifier la configuration de votre tunnel VPN IPSec, il est important de vous informiez sur ce qui suit :

- en texte clair
- Surveillance du tunnel
- ID proxy pour VPN IPSec

Présentation du VPN de site à site

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Prisma Access • PAN-OS	Aucune licence requise

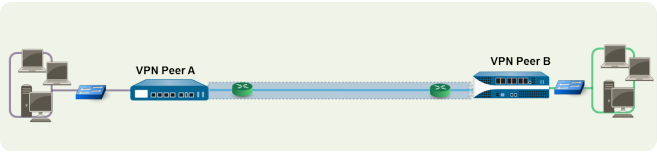
Une connexion VPN qui vous permet de connecter deux réseaux locaux (LAN) est appelée VPN site à site. Vous pouvez configurer des réseaux privés virtuels de routage pour connecter des pare-feu Palo Alto Networks à deux sites ou un pare-feu Palo Alto Networks à un périphérique de sécurité tiers à un autre emplacement. Le pare-feu peut également interagir avec des périphériques VPN tiers basés sur une politique ; le pare-feu Palo Alto Networks prend en charge les VPN de routage.

Le pare-feu Palo Alto Networks configure un VPN de routage, où il prend une décision de routage en fonction de l'adresse IP de destination. Si le trafic est acheminé vers une destination spécifique via un tunnel VPN, il est alors traité en tant que trafic VPN.

L’ensemble de protocoles IPSec (Internet Protocol Security) permet de configurer un tunnel sécurisé pour le trafic VPN et les informations contenues dans le paquet TCP/IP sont sécurisées (et cryptées si le type de tunnel est ESP). Le paquet IP (en-tête et charge utile) est incorporé dans une autre charge utile IP, et un nouvel en-tête est appliqué puis envoyé via le tunnel IPSec. L'adresse IP source contenue dans le nouvel en-tête est celle de l'homologue VPN local et l'adresse IP de destination est celle de l'homologue VPN à l'autre extrémité du tunnel. Lorsque le paquet atteint l'homologue VPN distant (le pare-feu à l'autre extrémité du tunnel), l'en-tête externe est supprimé et le paquet d'origine est envoyé à sa destination.

Les homologues doivent d'abord être authentifiés afin de pouvoir configurer le tunnel VPN. Une fois authentifiés, les homologues négocient la méthode de cryptage et les algorithmes pour sécuriser la communication. Le processus Internet Key Exchange (échange de clés Internet - IKE) permet d’authentifier les homologues VPN, et les Security Associations (associations de sécurité - SA) IPSec sont définies à chaque extrémité du tunnel pour sécuriser la communication VPN. IKE utilise des certificats numériques ou des clefs pré-partagées, et des clefs Diffie Hellman pour configurer les associations de sécurité pour le tunnel IPSec. Les associations de sécurité spécifient tous les paramètres requis pour la transmission sécurisée [notamment le Security Parameter Index (index de paramètre de sécurité ; SPI), le protocole de sécurité, les clés cryptographiques et l'adresse IP de destination], le cryptage, l'authentification des données, l'intégrité des données et l'authentification du point de terminaison.

La figure suivante illustre un tunnel VPN entre deux sites. Lorsqu'un client sécurisé par l'homologue VPN A nécessite le contenu d'un serveur se trouvant sur l'autre site, l'homologue VPN A initie une requête de connexion auprès de l'homologue VPN B. Si la politique de sécurité autorise la connexion, l'homologue VPN A utilise les paramètres du profil crypto IKE (IKE de phase 1) pour établir une connexion sécurisée et authentifier l'homologue VPN B. Ensuite, l'homologue VPN A établit le tunnel VPN à l'aide du profil crypto IPSec, qui définit les paramètres IKE de phase 2 pour permettre le transfert sécurisé des données entre les deux sites.



en texte clair

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Prisma Access • PAN-OS	Aucune licence requise

Afin de pouvoir configurer un tunnel VPN, l'interface de couche 3 à chaque extrémité doit disposer d'une interface de *tunnel* à laquelle le pare-feu doit se connecter pour établir un tunnel VPN. Une interface tunnel est une interface logique (virtuelle) utilisée pour acheminer le trafic entre les deux terminaux. Si vous configurez des ID de proxy, l'ID de proxy est compté pour la capacité de tunnel IPsec.

L’interface du tunnel doit appartenir à une zone de sécurité pour appliquer une règle de politique et elle doit être affectée à un routeur virtuel afin d’utiliser l’infrastructure de routage existante. Assurez-vous que l'interface de tunnel et l'interface physique sont affectées au même routeur virtuel pour que le pare-feu puisse effectuer une recherche d'itinéraire et déterminer le tunnel approprié à utiliser.

Généralement, l'interface de couche 3 à laquelle l'interface de tunnel est associée appartient à une zone externe, par exemple, la zone non approuvée. Bien que l'interface de tunnel puisse être dans la même zone de sécurité que l'interface physique, pour renforcer la sécurité et améliorer la visibilité, vous pouvez créer une zone distincte pour l'interface de tunnel. Si vous créez une zone distincte pour l’interface de tunnel, par exemple, une zone VPN, vous devrez créer des politiques de sécurité pour permettre au trafic de circuler entre la zone VPN et la zone approuvée.

Pour acheminer le trafic entre les sites, une interface de tunnel n’a pas besoin d’adresse IP. Une adresse IP est uniquement requise si vous souhaitez activer la surveillance des tunnels ou si vous utilisez un protocole de routage dynamique pour acheminer le trafic dans le tunnel. Lors du routage dynamique, l'adresse IP du tunnel sert d'adresse IP de saut suivant pour acheminer le trafic vers le tunnel VPN.

Si vous configurez le pare-feu Palo Alto Networks avec un homologue VPN qui exécute un VPN basé sur des stratégies, vous devez configurer un ID de proxy local et distant lors de la configuration du tunnel IPSec. Chaque homologue compare les ID de proxy configurés avec le contenu réel du paquet reçu afin de permettre la réussite d’une négociation de la phase 2 du protocole IKE. Si plusieurs tunnels sont requis, configurez des ID de proxy uniques pour chaque interface de tunnel ; une interface de tunnel peut disposer de 250 ID de proxy maximum. Chaque ID de proxy est pris en compte dans le calcul de la capacité du tunnel VPN IPSec du pare-feu, et la capacité du tunnel varie en fonction du modèle de pare-feu.

Pour plus d'informations sur la configuration, reportez-vous à la section Configuration d'un tunnel IPSec.

Surveillance du tunnel

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Pour un tunnel VPN, vous pouvez vérifier la connexion à une adresse IP de destination via le tunnel. Le profil de surveillance réseau sur le pare-feu vous permet de vérifier la connexion (à l'aide d'ICMP) à une adresse IP de destination ou un saut suivant à un intervalle d'interrogation donné, et de spécifier une action en cas d'échec de l'accès à l'adresse IP surveillée.

Si l’adresse IP de destination est inaccessible, configurez le pare-feu pour attendre la récupération du tunnel ou configurez le basculement automatique vers un autre tunnel. Dans tous les cas, le pare-feu génère un journal système qui vous alerte d'une défaillance du tunnel et renégocie les clés IPSec pour accélérer la récupération.

Pour plus d'informations sur la configuration, reportez-vous à la section Surveiller votre tunnel VPN IPSec.

ID proxy pour VPN IPSec

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

L’identité du proxy ou ID du proxy fait référence à un ensemble de trafic appartenant à un VPN IPSec qui est soumis à la négociation de la SA entre homologues (ou à la configuration une fois la négociation réussie).

Cela permet d’identifier puis d’orienter le trafic :

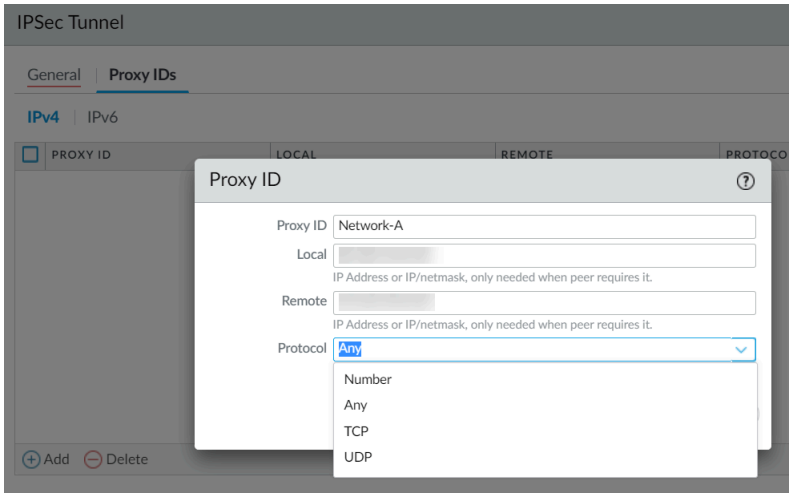
- au tunnel approprié où plusieurs tunnels coexistent entre les deux mêmes homologues partageant la même passerelle IKE.
- permet à des SA uniques et partagées avec différents paramètres de coexister.

Utilisez des ID de proxy dans les configurations où des tunnels VPN sont configurés entre les deux mêmes homologues.

Les ID proxy aident à identifier le trafic appartenant à un VPN IPSec particulier. Cela permet à un système d’exploitation d’installer les hooks appropriés pour diriger le trafic qui correspond à l’adresse source et à l’adresse de destination dans l’ID de proxy (ID client) et de le diriger vers la SA IPSec correspondante ou le VPN vers et depuis les SA IPSec correspondantes.

Configuration de l’ID de proxy

Palo Alto Networks fait partie des quelques autres fournisseurs qui utilisent des identifiants proxy. La figure suivante montre la fenêtre d’ID de proxy de Palo Alto Networks ainsi que ses options.



Sélectionnez **Network (Réseau)** > **IPSec Tunnel (Tunnel IPSec)** > **Proxy IDs (ID de proxy)**. Entrez le nom de l'ID du proxy, l'adresse IP locale, l'adresse IP distante si l'homologue l'exige, ainsi que le type de protocole ainsi que ses numéros de port local et distant.

Chaque ID de proxy est considéré comme un tunnel VPN et est donc pris en compte dans la capacité du tunnel VPN IPSec du pare-feu. Par exemple, la limite maximale pour un tunnel VPN IPSec de site à site est de 1 000 pour PA-3020, de 100 pour PA-2050 et de 25 pour PA-200.

Les ID proxy se comportent différemment avec les versions IKE :

- **IKEv1** : les périphériques Palo Alto Networks prennent en charge uniquement les correspondances exactes d'ID proxy. Si les ID proxy des homologues ne correspondent pas, le VPN ne fonctionne pas correctement.
- **IKEv2** : prend en charge le rétrécissement du sélecteur de trafic lorsque le paramètre d'ID de proxy est différent sur les deux passerelles VPN.

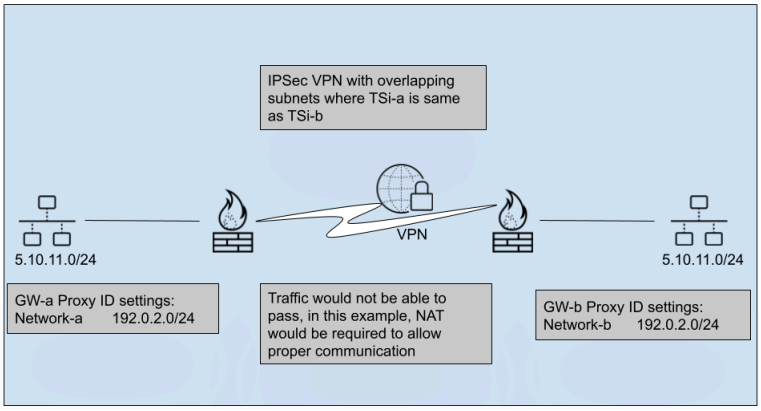
Utilisation des ID de proxy

L'exemple suivant montre deux passerelles VPN : A et B.

La négociation IKE est lancée par VPN GW-az, i=initiator, r=responder. VPN GW-a définit le sélecteur de trafic TSi-a/TSr-a et VPN GW-b spécifie le sélecteur de trafic TSi-b/TSr-b. Bien que TSr-a soit identique à TSr-b et puisse donc être ignoré, TSi-a peut être différent de TSi-b.

Dans ce cas, le trafic ne peut pas transiter par le tunnel VPN puisque le même réseau existe des deux côtés du tunnel.

Cependant, comme indiqué ci-dessous, la seule façon de résoudre ce problème est que les deux passerelles homologues créent des NAT pour traduire un nouveau sous-réseau réseau unique vers le réseau interne, sinon l'un des côtés doit modifier l'adresse IP du sous-réseau.



De cette façon, tout le trafic de chaque côté serait destiné à la nouvelle adresse NAT plutôt qu'à l'autre réseau similaire. Les deux passerelles doivent effectuer un NAT pour que cela fonctionne correctement afin d'éliminer toute confusion quant au réseau qui se trouve de quel côté.

Configuration d'un VPN IPSec pour un pare-feu Palo Alto Networks

Si l'autre côté du tunnel est un périphérique VPN tiers ou un pare-feu non PAN-OS, vous devez alors spécifier un ID de proxy local et un ID de proxy distant correspondants : généralement les sous-réseaux LAN local et distant.

Lors de la configuration d’un ID de proxy de tunnel IPSec pour identifier les réseaux IP locaux et distants pour le trafic NAT, la configuration de l’ID proxy pour le tunnel IPSec doit être configurée avec les informations du réseau IP post-NAT. La raison en est que les informations d’ID de proxy définissent les réseaux qui seront autorisés à traverser le tunnel des deux côtés pour la configuration IPSec.

Planifier la configuration de votre tunnel VPN IPSec

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access • PAN-OS	Aucune licence requise

Avant de configurer un tunnel IPSec, il est important de choisir les facteurs suivants et de planifier la configuration de votre tunnel IPSec avec succès.

STEP 1 | Décidez du type de VPN : Accès de site à site ou à distance

Le VPN site à site permet d'utiliser la méthode de sécurité IPSec pour créer un tunnel crypté entre un réseau client et un site distant du client. Cependant, le VPN d'accès à distance permet aux utilisateurs individuels de se connecter à un réseau privé pour accéder à ses services et ressources.

STEP 2 | Sélectionnez une méthode de sécurité pour votre VPN

Dans le VPN site à site, la méthode de sécurité IPSec est utilisée pour créer un tunnel crypté entre un réseau client et un site distant du client.

Dans le VPN d'accès à distance, les utilisateurs individuels sont connectés au réseau privé.

STEP 3 | Choisissez votre client VPN

Le VPN site à site n'a pas besoin d'être configuré sur chaque client. Le VPN d'accès à distance peut ou non nécessiter une configuration sur chaque client.

STEP 4 | Décidez de la configuration de votre tunnel VPN

Le VPN de site à site ne nécessite pas que chaque utilisateur lance la configuration du tunnel VPN. Le VPN d'accès à distance nécessite que chaque utilisateur d'accès distant lance la configuration du tunnel VPN.

STEP 5 | Choisissez votre technologie de sécurité

Alors que le VPN de site à site prend en charge la technologie IPSec, le VPN d'accès à distance prend en charge SSL ainsi que la technologie IPSec.

STEP 6 | Décidez si vous souhaitez un ou plusieurs utilisateurs sur votre VPN

Dans le VPN site à site, plusieurs utilisateurs ne sont pas autorisés ; Dans le VPN d'accès à distance, cependant, plusieurs utilisateurs sont autorisés.

Configurer les tunnels VPN IPSec (site à site)

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access • PAN-OS	Aucune licence requise

Pour configurer un VPN site à site :

- Vérifiez que vos interfaces Ethernet, vos routeurs virtuels et vos zones sont correctement configurés. Pour plus d'informations, consultez Configurer des interfaces et des zones.
- Créez vos interfaces de tunnel. Dans l'idéal, placez les interfaces de tunnel dans une zone distincte, afin que le trafic par tunnel puisse utiliser des règles de politique différentes.
- Configurez des itinéraires statiques ou affectez des protocoles de routage pour rediriger le trafic vers les tunnels VPN. Pour prendre en charge le routage dynamique (les protocoles OSPF, BGP et RIP sont pris en charge), vous devez affecter une adresse IP à l'interface de tunnel.
- Définissez des passerelles IKE pour établir la communication entre les homologues à chaque extrémité du tunnel VPN ; définissez également le profil cryptographique qui spécifie les protocoles et les algorithmes d'identification, d'authentification et de cryptage à utiliser pour la configuration de tunnels VPN dans la phase 1 du protocole IKEv1. Consultez les sections Configuration d'une passerelle IKE et Définition de profils crypto IKE.
- Configurez les paramètres requis pour établir la connexion IPSec pour le transfert de données via le tunnel VPN ; reportez-vous à la section Configuration d'un tunnel IPSec. Pour la phase 2 du protocole IKEv1, consultez la section Définition de profils crypto IPSec.
- (Facultatif) Indiquez la manière dont le pare-feu surveillera les tunnels IPSec. Voir Surveiller votre tunnel VPN IPSec.
- Définissez des politiques de sécurité pour filtrer et inspecter le trafic.

Si une règle de déni figure à la fin de la base de règles de sécurité, le trafic intra-zone est bloqué, sauf autorisation contraire. Les règles pour autoriser des applications IKE et IPSec doivent être explicitement incluses au-dessus de la règle de refus.

Si votre trafic VPN passe par (mais qu'il ne provient pas ni n'ayant comme destination) un pare-feu des séries PA-7000 ou PA-5200, configurez des règles de politique de sécurité bidirectionnelles pour autoriser le trafic ESP ou AH dans les deux directions.

Une fois ces tâches terminées, le tunnel est prêt à être utilisé. Le trafic destiné aux zones/adresses définies dans la règle de politique est automatiquement acheminé en fonction de l'itinéraire de destination de la table d'acheminement et traité en tant que trafic VPN. Pour obtenir quelques exemples de VPN site à site, reportez-vous à la section Exemples de configurations VPN de site à site.

Configuration d'une passerelle IKE

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Pour configurer un tunnel VPN, les passerelles ou les homologues VPN doivent s'authentifier mutuellement à l'aide de clés prépartagées ou de certificats numériques et établir un canal sécurisé dans lequel négocier l'association de sécurité SA IPSec qui sera utilisée pour sécuriser le trafic entre les homologues de chaque côté.

STEP 1 | Définissez la passerelle IKE.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Gateways (Passerelles IKE)**, **Add (Ajoutez)** une passerelle, puis saisissez le **Name (Nom)** de la passerelle (onglet **General (Général)**).
2. Définissez la **Version** sur **IKEv1 only mode (Mode IKEv1 uniquement)**, **IKEv2 only mode (Mode IKEv2 uniquement)** ou **IKEv2 preferred mode (Mode IKEv2 préféré)**. La passerelle IKE commence sa négociation avec son homologue dans le mode que vous spécifiez ici. Si vous sélectionnez **IKEv2 preferred mode (Mode IKEv2 préféré)**, les deux homologues utiliseront IKEv2 si l’homologue distant le prend en charge ; sinon, ils utiliseront IKEv1.

   La **Version** que vous sélectionnez détermine également les options que vous pouvez configurer dans l'onglet **Advanced Options (Options avancées)**.

STEP 2 | Établissez le terminal local du tunnel (passerelle).

1. Sélectionnez le **Address Type (Type d’adresse)** : **IPv4** ou **IPv6**.
2. Sélectionnez l'**Interface** sortante physique sur le pare-feu sur laquelle se trouve la passerelle locale.
3. Dans la liste **Local IP Address (Adresse IP locale)**, sélectionnez l'adresse IP qui sera utilisée comme terminal de la connexion VPN. Il s'agit de l'interface externe qui dispose d'une adresse IP pouvant être acheminée en public sur le pare-feu.

STEP 3 | Établissez l'homologue à l'autre extrémité du tunnel (passerelle).

Sous **Peer IP Address Type (Type d’adresse IP de l’homologue)**, sélectionnez l’un des paramètres suivants et saisissez les informations correspondantes de l’homologue :

- **IP** : saisissez une **Peer Address (Adresse de l'homologue)** qui est une adresse IPv4 ou IPv6 ou saisissez un objet d'adresse qui est une adresse IPv4 ou IPv6.
- **FQDN** : saisissez une **Peer Address (Adresse de l'homologue)** qui est une chaîne de FQDN ou un objet d'adresse utilisant une chaîne de FQDN. Si l’objet FQDN ou FQDN address se résout en plusieurs adresses IP, le pare-feu sélectionne l’adresse préférée dans l’ensemble d’adresses qui correspondent au type d’adresse (IPv4 ou IPv6) de la passerelle IKE comme suit :
  - Si aucune association de sécurité IKE (SA) n’est négociée, l’adresse préférée est l’adresse IP avec la plus petite valeur.

- Si la passerelle IKE utilise une adresse qui figure dans l'ensemble d'adresses renvoyées, le pare-feu sélectionne cette adresse (qu'il s'agisse de l'adresse qui possède la plus faible valeur de l'ensemble ou non).
- Si la passerelle IKE utilise une adresse qui ne figure pas dans l'ensemble d'adresses renvoyées, le pare-feu sélectionne une nouvelle adresse et il s'agit de l'adresse qui possède la plus faible valeur de l'ensemble.

- **Dynamique (Dynamic**) : sélectionnez **Dynamique** si l'adresse IP de l'homologue ou la valeur du nom de domaine complet est inconnue afin que l'homologue lance la négociation.

L'utilisation d'un objet d'adresse FQDN ou FQDN réduit les problèmes dans les environnements où l'homologue est soumis à des modifications d'adresse IP dynamiques (et vous obligerait autrement à reconfigurer cette adresse d'homologue de passerelle IKE).

STEP 4 | Indiquez comment authentifier l'homologue.

Sélectionnez la méthode d'**Authentication (Authentification)** : **Pre-Shared Key (Clé prépartagée)** ou **Certificate (Certificat)**. Si vous choisissez une clé prépartagée, passez à l'étape suivante. Si vous choisissez un certificat, passez à l'étape 6, Configurer l'authentification basée sur un certificat.

STEP 5 | Configurez une clé prépartagée.

1. Saisissez une **Pre-shared Key (Clé prépartagée)**, qui est la clé de sécurité à utiliser pour l'authentification dans le tunnel. Saisissez à nouveau la valeur pour **Confirm Pre-shared Key (Confirmer la clé pré-partagée)**. Utilisez un maximum de 255 caractères ASCII ou non ASCII.

   Générez une clé difficile à décoder par des attaques par dictionnaire ; utilisez un générateur de clés prépartagées, si nécessaire.
2. Sous **Local Identification (Identification locale)**, sélectionnez l'un des types suivants et saisissez une valeur que vous déterminez : **FQDN (hostname) (FQDN (nom d'hôte))**, **IP address (Adresse IP)**, **KEYID (binary format ID string in HEX) (KEYID (chaîne d'ID au format binaire hexadécimal))** et **User FQDN (email address) (FQDN de l'utilisateur (adresse e-mail))**. L'identification locale définit le format et l'identification de la passerelle locale. Si vous ne spécifiez pas de valeur, l'adresse IP locale est utilisée comme valeur d'identification locale.
3. Sous **Peer Identification (Identification de l'homologue)**, sélectionnez l'un des types suivants et saisissez une valeur que vous déterminez : **FQDN (hostname) (FQDN (nom d'hôte))**, **IP address (Adresse IP)**, **KEYID (binary format ID string in HEX) (KEYID (chaîne d'ID au format binaire hexadécimal))** et **User FQDN (email address) (FQDN de l'utilisateur (adresse e-mail))**. L'identification de l'homologue définit le format et l'identification de la passerelle homologue. Si vous ne spécifiez aucune valeur, l'adresse IP de l'homologue est utilisée comme valeur d'Identification de l'homologue.
4. Passez à l'étape 7 (Configurer des options avancées pour la passerelle).

STEP 6 | Configurez l'authentification basée sur les certificats.

Effectuez les étapes restantes de cette procédure si vous avez sélectionné **Certificate (Certificat)** comme méthode d'authentification de la passerelle homologue à l'extrémité opposée du tunnel.

1. Sélectionnez un **Local Certificate (Certificat local)** se trouvant déjà sur le pare-feu, **Import (Importez)** un certificat ou **Generate (Générez)** un nouveau certificat.
   - Pour **Import (Importer)** un nouveau certificat, procédez d'abord à l'Importation d'un certificat pour l'authentification de passerelle IKEv2. Revenez ensuite à cette tâche.
   - Pour **Generate (Générer)** un nouveau certificat, procédez d'abord à la Génération d'un certificat sur le pare-feu. Revenez ensuite à cette tâche.
2. (Facultatif) Activez (sélectionnez) le **HTTP Certificate Exchange (Échange des certificats HTTP)** pour configurer le hachage et l'URL (IKEv2 uniquement). Pour un échange de certificat HTTP, saisissez l'**Certificate URL (URL du certificat)**. Pour plus d'informations, reportez-vous à la section Échange de certificat Hachage et URL.
3. Sélectionnez le type de **Local Identification (Identification locale)** (**Distinguished Name (Subject), FQDN (hostname) (Nom unique (objet)), FQDN (nom d'hôte))**, **IP address (Adresse IP)** ou **User FQDN (email address) (FQDN de l'utilisateur (adresse e-mail))**), puis saisissez la valeur. L'identification locale définit le format et l'identification de la passerelle locale.
4. Sélectionnez le type de **Peer Identification (Identification de l'homologue)** (**Distinguished Name (Subject), FQDN (hostname) (Nom unique (objet)), FQDN (nom d'hôte))**, **IP address (Adresse IP)** ou **User FQDN (email address) (FQDN de l'utilisateur (adresse e-mail))**), puis saisissez la valeur. L'identification de l'homologue définit le format et l'identification de la passerelle homologue.
5. Précisez le type de **Peer ID Check (Vérification de l'ID d'homologue)** :
   - **Exact** : vous assure que le paramètre local et la charge utile ID IKE de l'homologue correspondent parfaitement.
   - **Wildcard (Caractère générique)** : permet à l'identification de l'homologue de correspondre tant que chaque caractère situé avant le caractère générique (*) correspond. Les caractères situés après le caractère générique ne doivent pas nécessairement correspondre.
6. (Facultatif) **Permit peer identification and certificate payload identification mismatch (Autoriser une non-correspondance de l'identification de l'homologue et de l'identification des données utiles du certificat)** pour autoriser une SA IKE réussie même si l'identification de l'homologue ne correspond pas à l'identification de l'homologue dans le certificat.
7. Choisissez un **Certificate Profile (Profil de certificat)**. Un profil de certificat contient des informations sur comment authentifier la passerelle homologue.
8. (Facultatif) **Enable strict validation of peer's extended key use (Activer la validation stricte de l'utilisation de la clé étendue de l'homologue)** pour contrôler strictement l'utilisation de la clé.

STEP 7 | Configurez des options avancées pour la passerelle.

1. (Facultatif) **Enable Passive Mode (Activez le mode passif)** dans les Options courantes (**Advanced Options (Options avancées)**) pour indiquer que le pare-feu ne fait que répondre aux requêtes de connexion IKE et qu'il ne les initie jamais.
2. Si vous disposez d'un périphérique qui exécute NAT entre les passerelles, **Enable NAT Traversal (Activez le parcours NAT)** pour utiliser l'encapsulation UDP sur les protocoles IKE et UDP, ce qui leur permet de passer par des périphériques NAT intermédiaires.
3. Si vous avez sélectionné **IKEv1 only mode (Mode IKEv1 uniquement)** à l'étape 1, alors, à l'onglet IKEv1 :
   - Sélectionnez le **Exchange Mode (Mode d'échange)** : **auto (automatique)**, **aggressive (agressif)** ou **main (principal)**. Lorsque vous configurez un pare-feu pour qu'il utilise le mode d'échange **auto (automatique)**, il peut accepter des demandes de négociation en mode **main (principal)** et **aggressive (agressif)**. Toutefois, chaque fois que cela est possible, il initiera des échanges en mode **main (principal)**.

     *Si vous ne définissez pas le mode d'échange sur **auto (automatique)**, vous devez alors configurer les deux homologues avec le même mode d'échange pour autoriser chaque homologue à accepter les requêtes de négociation.*
   - Sélectionnez un profil existant ou conservez le profil par défaut dans la liste **IKE Crypto Profile (Profil crypto IKE)**. Au besoin, vous pouvez procéder à la Définition des profils crypto IKE.
   - (Uniquement si vous utilisez l'authentification basée sur les certificats et que le mode d'échange n'est pas défini sur le mode agressif) Cliquez sur **Enable Fragmentation (Activer la fragmentation)** pour permettre au pare-feu de fonctionner avec la fragmentation IKE.
   - Cliquez sur **Dead Peer Detection (Détection des homologues inactifs)** et saisissez un **Interval (Intervalle)** (plage de 2 à 100 secondes). Pour **Retry (Réessayer)**, spécifiez le nombre d'essais (la plage est de 2 à 100) avant de vous déconnecter du pair IKE. L'option Détection des homologues inactifs identifie les homologues IKE inactifs ou indisponibles en envoyant une charge utile de notification IKE de phase 1 à l'homologue et en attendant un accusé de réception.
4. Si vous configurez le **mode IKEv2 uniquement** ou le **mode IKEv2 préféré** à l'étape 1, alors, à l'onglet IKEv2 :
   - Sélectionnez un **IKE Crypto Profile (Profil crypto IKE)**, qui configure les options IKE de phase 1 comme le groupe DH, l'algorithme de hachage et l'authentification ESP. Pour plus d'informations sur les profils crypto IKE, reportez-vous à la section Phase 1 du protocole IKE.
   - (Facultatif) Activez la **Strict Cookie Validation (validation du cookie stricte)** Seuil d'activation du cookie et validation du cookie stricte.
   - (Facultatif) **Enable Liveness Check (Activez la vérification de l'activité)** et saisissez un **Interval (sec) (Intervalle (sec)** (5 par défaut)si vous souhaitez que la passerelle envoie une requête de message à son homologue en lui demandant une réponse. Si nécessaire, l'initiateur tente la vérification de l'activité jusqu'à 10 fois. S'il ne reçoit pas de réponse, l'initiateur ferme et supprime les IKE_SA et CHILD_SA. L'initiateur commence à envoyer un autre message IKE_SA_INIT.

STEP 8 | Cliquez sur **OK (OK)** et sur **Commit (Valider)** pour enregistrer vos modifications.

Exportation d'un certificat pour l'accès d'un homologue à l'aide de Hachage et URL

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

IKEv2 prend en charge la méthode Échange de certificat Hachage et URL permettant à l’homologue situé à l’extrémité distante du tunnel d’extraire le certificat d’un serveur sur lequel vous avez exporté le certificat. Effectuez cette tâche pour exporter votre certificat sur ce serveur. Vous devez déjà avoir créé un certificat via Device **(Périphérique)** > **Certificate Management (Gestion des certificats)**.

STEP 1 | Sélectionnez **Device (Périphérique)** > **Certificates (Certificats)** et, si votre plate-forme prend en charge plusieurs systèmes virtuels, dans **Location (Emplacement)**, sélectionnez le système virtuel approprié.

STEP 2 | Dans l'onglet **Device Certificates (Certificats de périphérique)**, sélectionnez le certificat à **Export (Exporter)** vers le serveur.

L'état du certificat doit être valide, et non expiré. Le pare-feu ne vous empêche pas d’exporter un certificat non valide.

STEP 3 | Dans **File Format (Format de fichier)**, sélectionnez **Binary Encoded Certificate (DER) (Certificat codé en binaire (DER))**.

STEP 4 | Ne cochez pas la case **Export private key (Exporter la clé privée)**. L'exportation de la clé privée n'est pas nécessaire pour l'échange de certificat Hachage et URL.

STEP 5 | Cliquez sur **OK**.

Importation d'un certificat pour l'authentification de passerelle IKEv2

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Effectuez cette tâche si vous authentifiez un homologue pour une passerelle IKEv2 et que vous n’avez pas utilisé un certificat local existant sur le pare-feu. Vous souhaitez importer un certificat depuis n’importe quel emplacement.

Cette tâche implique que vous avez sélectionné **Network (Réseau)** > **IKE Gateways (Passerelles IKE)**, que vous avez ajouté une passerelle et que, dans **Local Certificate (Certificat local)**, vous avez cliqué sur **Import (Importer)**.

STEP 1 | Importez un certificat.

1. Sélectionnez **Network (Réseau)** > **IKE Gateways (Passerelles IKE)**, cliquez sur **Add (Ajouter)** pour ajouter une passerelle puis, dans l'onglet **General (Général)**, sous

Authentication (Authentification), sélectionnez **Certificate (Certificat)**. Sous **Local Certificate (Certificat local)**, cliquez sur **Import (Importer)**.

2. Dans la fenêtre d'importation du certificat, saisissez un **Certificate Name (Nom du certificat)** pour le certificat que vous importez.
3. Sélectionnez **Shared (Partagé)** si vous souhaitez que ce certificat soit partagé par plusieurs systèmes virtuels.
4. Dans **Certificate File (Fichier de certificat)**, cliquez sur **Browse (Parcourir)** pour chercher le fichier de certificat. Cliquez sur le nom du fichier et sur **Open (Ouvrir)** pour renseigner le champ **Certificate File (Fichier de certificat)**.
5. Sous **File Format (Format de fichier)**, sélectionnez l'une des options suivantes :
   - **Base64 Encoded Certificate (PEM) (Certificat codé en Base64 (PEM))** - Contient le certificat mais pas la clé. C'est du texte en clair.
   - **Encrypted Private Key and Certificate (PKCS12) (Clé privée et certificat cryptés (PKCS12))** - Contient le certificat et la clé.
6. Sélectionnez **Import private key (Importer la clé privée)** si la clé se trouve dans un autre fichier que le fichier de certificat. La clé est facultative, à l'exception suivante :
   - Importez une clé si vous avez défini **File Format (Format de fichier)** sur **PEM**. Saisissez un **Key file (Fichier de clé)** en cliquant sur **Browse (Parcourir)** et en accédant au fichier de clé à importer.
   - Saisissez une **Passphrase (Phrase secrète)** et **Confirm Passphrase (Confirmez la phrase secrète)**.
7. Cliquez sur **OK**.

STEP 2 | Passez à la tâche suivante.

Étape Configurez l'authentification basée sur les certificats.

Modification de la durée de vie de la clé ou de l'intervalle d'authentification pour IKEv2

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Cette tâche est facultative ; le paramètre par défaut de durée de vie de la clé SA IKEv2 est de 8 heures. Le paramètre par défaut du multiple d'authentification IKEv2 est 0, ce qui désactive la fonctionnalité de réauthentification. Pour obtenir de plus amples renseignements, reportez-vous à la section Durée de vie de la clé et intervalle de réauthentification SA.

Procédez comme suit pour modifier les valeurs par défaut : Un profil crypto IKE doit déjà exister (condition préalable).

STEP 1 | Modifiez la durée de vie de la clé ou de l'intervalle d'authentification SA pour un profil crypto IKE.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Crypto (Crypto IKE)** et sélectionnez le profil crypto IKE qui s'applique à la passerelle locale.
2. Sous **Key Lifetime (Durée de vie de la clé)**, sélectionnez une unité (**Seconds (Secondes)**, **Minutes (Minutes)**, **Hours (Heures)** ou **Days (Jours)** et saisissez une valeur. Le minimum est de 3 minutes.
3. Sous **IKE Authentication Multiple (Multiple d'authentification IKE)**, saisissez une valeur qui est multipliée par la durée de vie de la clé pour déterminer l'intervalle de réauthentification.

STEP 2 | Validez vos modifications.

Cliquez sur **OK**, puis sur **Commit (Valider)**.

Modification du seuil d'activation du cookie pour IKEv2

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Effectuez la tâche suivante si vous souhaitez qu'un pare-feu dispose d'un seuil différent du paramètre par défaut de 500 sessions SA demi-ouvertes avant qu'une validation du cookie ne soit nécessaire. Pour obtenir de plus amples renseignements sur l'activation du cookie, reportez-vous à la section Seuil d'activation du cookie et validation du cookie stricte.

STEP 1 | Modifiez le seuil d'activation du cookie.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Session (Session)** et modifiez les paramètres de session VPN. Sous **Cookie Activation Threshold (Seuil d'activation du cookie)**, saisissez le nombre maximum de SA demi-ouvertes avant que le répondeur ne demande un cookie à l'initiateur (plage de 0 à 65535 ; par défaut 500).
2. Cliquez sur **OK**.

STEP 2 | Validez vos modifications.

Cliquez sur **OK**, puis sur **Commit (Valider)**.

Configuration des sélecteurs de trafic IKEv2

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Dans IKEv2, vous pouvez configurer des Sélecteurs de trafic, qui sont des composants de trafic réseau utilisés pendant une négociation IKE. Les sélecteurs de trafic sont utilisés pendant CHILD_SA (création de tunnel) phase 2 pour configurer le tunnel et déterminer le trafic autorisé dans le tunnel. Les deux homologues de passerelle IKE doivent négocier et s'accorder sur leurs sélecteurs de trafic ; sinon, un côté réduit sa plage d'adresses pour parvenir à un accord. Une connexion IKE peut comporter plusieurs tunnels ; par exemple, vous pouvez affecter différents tunnels à chaque service pour isoler son trafic. La séparation

du trafic permet également de mettre en œuvre des fonctionnalités telles que QoS. Servez-vous des flux de travail suivants pour configurer les sélecteurs de trafic.

STEP 1 | Sélectionnez **Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)** > **Proxy IDs (ID de proxy)**.

STEP 2 | Sélectionnez l'onglet **IPv4 (IPv4)** ou **IPv6 (IPv6)**.

STEP 3 | Cliquez sur **Add (Ajouter)** et saisissez un **Name (Nom)** dans le champ **Proxy ID (ID de proxy)**.

STEP 4 | Dans le champ **Local (Local)**, saisissez la **Source IP Address (Adresse IP source)**.

STEP 5 | Dans le champ **Remote (Distant)**, saisissez la **Destination IP Address (Adresse IP de destination)**.

STEP 6 | Dans le champ **Protocol (Protocole)**, sélectionnez le protocole de transport (**TCP (TCP)** ou **UDP (UDP)**).

STEP 7 | Cliquez sur **OK**.

Définition de profils cryptographiques

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access • PAN-OS	Aucune licence requise

Un profil cryptographique spécifie les cryptages utilisés pour l'authentification et/ou le cryptage entre deux homologues IKE, ainsi que la durée de vie de la clé. La période entre chaque renégociation est appelée durée de vie ; lorsque le délai spécifié expire, le pare-feu renégocie un nouvel ensemble de clés.

Afin de sécuriser la communication via le tunnel VPN, le pare-feu nécessite des profils cryptographiques IKE et IPSec pour pouvoir effectuer respectivement les négociations IKE de phase 1 et de phase 2. Le pare-feu inclut un profil crypto IKE par défaut et un profil crypto IPSec par défaut prêts à l'emploi.

- Définition de profils crypto IKE
- Définition de profils crypto IPSec

Définition de profils crypto IKE

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access • PAN-OS	Aucune licence requise

Le profil crypto IKE permet de configurer les algorithmes de chiffrement et d'authentification utilisés pour le processus d'échange de clés à la phase 1 du protocole IKE, ainsi que la durée de vie des clés qui spécifie leur durée de validité. Pour appeler le profil, vous devez l'associer à la configuration de passerelle IKE.

*Toutes les passerelles IKE configurées sur la même interface ou adresse IP locale doivent utiliser le même profil cryptographique lorsque le **Peer IP Address Type (Type d'adresse IP homologue)** de la passerelle IKE est configuré comme **Dynamic (Dynamique)** et que le mode principal IKEv1 ou IKEv2 est appliqué. Si les profils de chiffrement sont les mêmes sur les passerelles, même si la connexion initiale peut démarrer sur une passerelle différente, la connexion sera transférée vers la passerelle appropriée lorsque des clés ou certificats pré-partagés et des identifiants de pairs seront échangés.*

Que votre homologue VPN provienne ou non du même fournisseur, les homologues VPN doivent avoir les mêmes paramètres IKE configurés afin de réussir une négociation IKE.

Les paramètres suivants doivent correspondre pour une négociation IKE réussie :

- Groupe DH pour l'échange de clés
- Algorithmes de chiffrement
- Algorithmes d'authentification

Par exemple, si vous avez configuré l'homologue VPN 1 avec **group20** pour le groupe DH, **sha384** pour l'authentification et **aes-256-gcm** pour le chiffrement. Ensuite, l'homologue VPN 2 avec lequel vous souhaitez établir le tunnel IPSec doit également avoir les mêmes valeurs configurées.

- PAN-OS 10.1 et versions ultérieures et Prisma Access (Panorama géré)
- #unique_39

Définition de profils crypto IPSec

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access • PAN-OS	Aucune licence requise

Le profil crypto IPSec est appelé à la phase 2 du protocole IKE. Il indique la manière dont les données sont sécurisées dans le tunnel lorsque l'échange de clés automatiques est utilisé pour générer automatiquement les clés pour les SA IKE.

Que votre homologue VPN provienne ou non du même fournisseur, les homologues VPN doivent avoir les mêmes paramètres IPSec configurés afin de réussir une négociation IPSec.

La négociation IPSec réussira lorsque les paramètres suivants correspondront entre les homologues VPN :

- Protocole IPSec (ESP ou AH)
- Groupe DH (ou PFS) pour l'échange de clés
- Algorithmes de chiffrement
- Algorithmes d'authentification

Par exemple, si vous avez configuré l'homologue VPN 1 avec **ESP** pour le protocole IPSec, **group20** pour le groupe DH, **sha384** pour l'authentification et **aes-256-gcm** pour le chiffrement. Ensuite, l'homologue VPN 2 avec lequel vous souhaitez établir le tunnel IPSec doit également être configuré exactement avec les mêmes valeurs.

Par défaut, la confidentialité de transfert parfait (PFS) est activée sur les tunnels IPSec pour générer une clé plus aléatoire. Pour ce faire, PFS effectue un échange de clé supplémentaire pendant la négociation SA IPSec, génère un nouveau secret partagé et le combine dans les nouvelles clés SA IPSec. Lors de la configuration de PFS, assurez-vous que les deux homologues VPN ont la même configuration PFS. Tout échec dans la négociation SA IPSec entraînera l'échec de l'établissement du tunnel IPSec.

- PAN-OS 10.1 et versions ultérieures et Prisma Access (Panorama géré)
- Prisma Access (gestion du cloud)

Configuration d'un tunnel IPSec

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Prisma Access (le mode de transport tunnel IPSec n’est pas encore pris en charge pour Prisma Access) • PAN-OS	Aucune licence requise

IPSec est une suite de protocoles utilisés pour sécuriser les communications entre pairs. Dans IPSec, vous pouvez configurer divers paramètres, tels que les algorithmes de chiffrement et d’authentification et les délais d’expiration des associations de sécurité. L’une de ces configurations est le mode IPSec : mode tunnel ou mode transport.

Lors de la configuration d’un tunnel IPSec, vous pouvez sélectionner le mode IPSec comme tunnel ou mode transport pour établir une connexion sécurisée. Autrement dit, vous pouvez choisir de crypter ou d’authentifier les paquets en mode tunnel ou en mode transport. PAN-OS® prend en charge le mode tunnel par défaut, authentifiant ou cryptant les données (paquet IP) lors de leur traversée du tunnel. À partir de PAN-OS 11.0.0, vous pouvez utiliser le mode transport.

Différences entre le tunnel et le mode de transport

Mode tunnel	Mode Transport
Chiffre l’intégralité du paquet, y compris l’en-tête IP. Un nouvel en-tête IP est ajouté au paquet après le chiffrement.	Chiffre uniquement la charge utile, tandis que l’en-tête IP d’origine est conservé.
La surveillance des tunnels utilise l’adresse IP de l’interface du tunnel.	La surveillance du tunnel utilise automatiquement l’adresse IP de l’interface physique (adresse IP de l’interface passerelle), et l’adresse IP de l’interface tunnel est ignorée.
Prend en charge la double encapsulation.	Pas de prise en charge de la double encapsulation.
Ce mode est couramment utilisé pour les communications de site à site.	Ce mode est couramment utilisé pour les communications d’hôte à hôte.

Configurer un tunnel IPSec (mode tunnel)

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Prisma Access • PAN-OS	Aucune licence requise

La configuration du tunnel IPSec vous permet de vous authentifier et/ou de crypter les données (paquet IP) dans le tunnel.

Si vous configurez le pare-feu pour qu'il fonctionne avec un homologue qui prend en charge un VPN basé sur une politique, vous devez définir des ID de proxy. Les périphériques qui prennent en charge un VPN basé sur une politique utilisent des règles/politiques de sécurité spécifiques ou des listes d'accès (adresses sources, adresses de destination et ports) pour autoriser le trafic intéressant via un tunnel IPSec. Ces règles sont référencées en mode rapide ou lors de la négociation de la phase 2 du protocole IKE et sont échangées sous forme d'ID de proxy dans le premier ou le second message du processus. Par conséquent, si vous configurez le pare-feu pour fonctionner avec un homologue VPN basé sur une politique, pour une négociation de phase 2 réussie, vous devez définir l'ID de proxy de manière à ce que la configuration des deux homologues soit identique. Si l'ID de proxy n'est pas configuré, comme le pare-feu prend en charge un VPN de routage, les valeurs par défaut utilisées comme ID de proxy sont adresse IP source : 0.0.0.0/0, adresse IP de destination : 0.0.0.0/0 et application : indifférente ; lorsque ces valeurs sont échangées avec l'homologue, il est impossible de configurer la connexion VPN.

Pour établir un tunnel IPSec avec succès, les négociations IKE et IPSec doivent aboutir :

- La négociation IKE ne réussira que lorsque les deux homologues VPN échangeront les mêmes paramètres IKE configurés.
- La négociation IPSec ne réussira que lorsque les deux homologues VPN échangeront les mêmes paramètres IPSec configurés.
- PAN-OS 10.1 et versions ultérieures
- #unique_43
- #unique_44

Configurer un tunnel IPSec (mode transport)

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Le mode Transport est nouveau à partir de la version 11.0.0 de PAN-OS et prend en charge ce qui suit :

- Adresse IPv4 uniquement.
- Encapsulation du protocole ESP (Security Payload) uniquement.
- IKEv2 uniquement.
- DH-groupe 20 pour le groupe Diffie-Hellman (DH) et PFS.
- Uniquement AES avec des clés 256 bits en mode GCM.

Vous pouvez choisir le mode IPSec en fonction de vos besoins réseau :

- Si vous souhaitez chiffrer les paquets BGP (du protocole du plan de gestion) échangés entre votre pare-feu nouvelle génération et le terminal du tunnel, vous devez configurer le mode de transport IPSec. Le mode Transport vous permet de chiffrer le trafic de contrôle (tel que le protocole de routage et les messages de signalisation) avec le protocole le plus robuste. Avec le mode transport, vous pouvez chiffrer le trafic point à point appartenant à l'adresse IP du pare-feu.

- Si vous souhaitez chiffrer le trafic du plan de données échangé entre votre pare-feu nouvelle génération et le terminal du tunnel, vous devez configurer le mode tunnel IPSec.

Points importants à retenir avant d'activer le mode de transport :

- Vous ne pouvez pas sélectionner le mode de transport lorsque NAT-T est activé.
- Vous ne pouvez pas configurer une passerelle IKE sur une interface en boucle vers un tunnel IPSec avec le mode de transport.
- Le mode de transport IPSec n'utilise pas les paramètres d'ID proxy pour la négociation. Par conséquent, vous ne pouvez pas configurer un ID proxy en mode transport. Si vous tentez de configurer l'ID proxy par une autre méthode, il sera automatiquement remplacé par 0.0.0.0/0.
- Vous ne pouvez utiliser le mode transport qu'avec un échange automatique **auto-key (clé automatique)** .
- Si vous configurez une passerelle IKE sans tunnel IPSec, IKE négocie par défaut une association de sécurité enfant (SA) en mode tunnel.
- En mode de transport IPSec sans encapsulation GRE, n'acheminez pas le trafic utilisateur via l'interface de tunnel associée. Configurez les protocoles de contrôle (comme les sessions d'appairage BGP) sur une interface physique (par exemple, ethernet1/1) au lieu d'une interface de tunnel. Alors que le mode tunnel IPSec pour les itinéraires BGP fonctionne avec l'interface tunnel, le mode de transport IPSec pour les itinéraires BGP fonctionne uniquement avec l'interface physique.
- Par défaut, le tunnel IPSec fonctionne en mode **Tunnel**.
- Vous devez activer **Add GRE Encapsulation (Ajouter une encapsulation GRE)** en mode **Transport** pour encapsuler les paquets de multidiffusion.

Étant donné que PAN-OS 10.2 et les versions antérieures ne prennent pas en charge le mode de transport, toute rétrogradation vers les versions précédentes entraînera des problèmes de compatibilité. Avant de passer à une version antérieure, vous devez supprimer manuellement tous les tunnels en mode transport ou passer en mode tunnel. Sinon, la rétrogradation entraînera un échec.

- PAN-OS 11.0 et versions ultérieures

Surveiller votre tunnel VPN IPSec

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Pour fournir un service VPN ininterrompu, vous pouvez utiliser la détection des homologues inactifs ainsi que la fonction de surveillance des tunnels sur le pare-feu. Vous pouvez également surveiller l'état du tunnel. Ces tâches de surveillance sont décrites dans les sections suivantes :

- Définition d'un profil de surveillance des tunnels
- #unique_47

À des fins de dépannage, une Activation/désactivation, actualisation ou redémarrage d’une passerelle IKE ou d’un tunnel IPSec est possible.

Définition d'un profil de surveillance des tunnels

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Un profil de surveillance des tunnels vous permet de vérifier la connexion entre les homologues VPN ; vous pouvez configurer l'interface de tunnel pour envoyer une requête ping à une adresse IP de destination à un intervalle donné et spécifier l'action si la communication via le tunnel est rompue.

STEP 1 | Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **Monitor (Surveillance)**. Un profil de surveillance des tunnels par défaut peut être utilisé.

STEP 2 | Cliquez sur **Add (Ajouter)**, puis donnez un **Name (Nom)** au profil.

STEP 3 | Sélectionnez l'**Action (Action)** à prendre si l'adresse IP de destination est inaccessible.

- **Wait Recover (Attente de la récupération)** : le pare-feu attend la récupération du tunnel. Il continue d'utiliser l'interface de tunnel dans les décisions de routage comme si le tunnel était encore actif.
- **Fail Over (Basculement)** : force le trafic vers un chemin d'accès des sauvegardes, le cas échéant. Le pare-feu désactive l'interface de tunnel, et par là même tous les itinéraires de la table de routage qui utilisent l'interface.

Dans tous les cas, le pare-feu tente d'accélérer la récupération en négociant de nouvelles clés IPSec.

STEP 4 | Spécifiez l'**Interval (sec) (Intervalle (sec.)** et le **Threshold (Seuil)** de déclenchement de l'action donnée.

- **Threshold (Seuil)** précise le nombre de pulsations pendant lesquelles il faut attendre avant d'appliquer l'action définie (intervalle compris entre 2 et 100 ; valeur par défaut : 5).
- **Interval (sec) (Intervalle (sec.))** précise le délai (en secondes) entre les pulsations (intervalle compris entre 2 et 10, valeur par défaut : 3).

STEP 5 | Associez le profil de surveillance à la configuration de tunnel IPSec. Reportez-vous à la section Activez la surveillance des tunnels.

Afficher l’état du tunnel

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• PAN-OS • Cloud Management	❑ Aucune licence requise ❑ AIOps pour licence NGFW Premium

L'état du tunnel vous informe si des SA IKE de phase 1 et de phase 2 valides ont été établies, et si l'interface de tunnel est active et disponible pour la transmission du trafic.

Comme l’interface de tunnel est une interface logique, elle ne peut pas indiquer l’état d’une liaison physique. Par conséquent, vous devez activer la surveillance des tunnels de manière à ce que l'interface de tunnel puisse vérifier la connexion à une adresse IP et déterminer si le chemin d'accès peut encore être utilisé. Si l'adresse IP est inaccessible, le pare-feu attend la récupération du tunnel ou le basculement vers un autre tunnel. Lorsqu’un basculement se produit, le tunnel existant est démoli et des modifications de routage sont déclenchées pour configurer un nouveau tunnel et rediriger le trafic.

- PAN-OS
- Gestion du cloud

Afficher l’état du tunnel VPN IPSec

STEP 1 | Sélectionnez **Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)**.

STEP 2 | Affichez l'**état du tunnel**.

- La couleur verte indique un tunnel de SA IPSec valide.
- Le rouge indique que la SA IPSec n’est pas disponible ou a expiré.

STEP 3 | Affichez l'**IKE Gateway Status (état de la passerelle IKE)**.

- La couleur verte indique une SA IKE de phase 1 valide.
- La couleur rouge indique qu’une SA IKE de phase 1 n’est pas disponible ou a expiré.

STEP 4 | Affichez **Tunnel Interface Status (l'état de l'interface de tunnel)**.

- La couleur verte indique que l'interface de tunnel est active.
- La couleur rouge indique que l'interface de tunnel est inactive, car la surveillance des tunnels est activée et l'état est inactif.

Pour rendre actif un tunnel VPN, reportez-vous à la section Interprétation des messages d'erreur VPN.

Afficher l’état du tunnel VPN IPSec

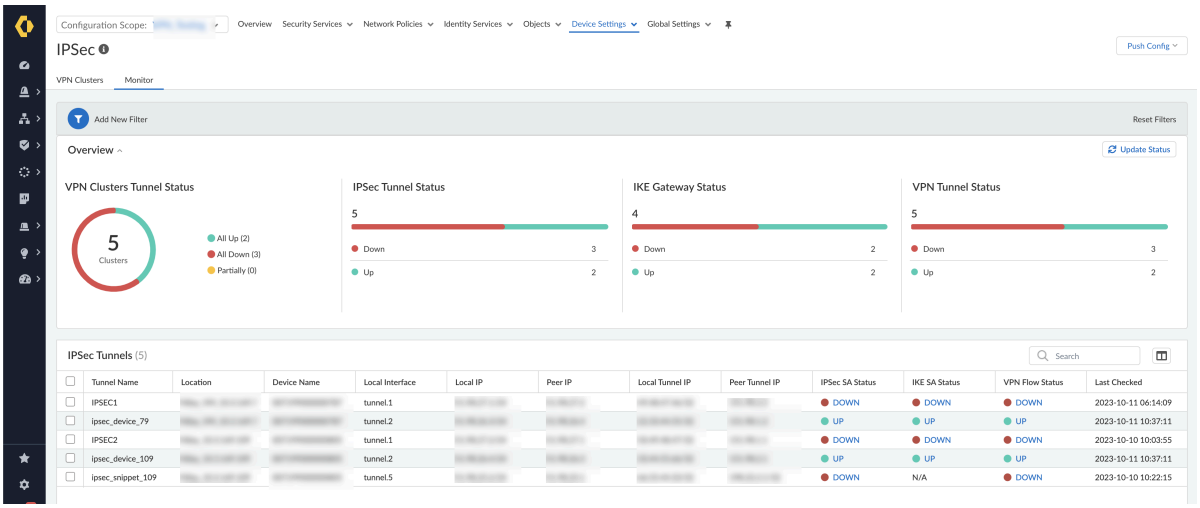
STEP 1 | Connectez-vous à Strata Cloud Manager.

STEP 2 | Sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device Settings (Paramètres des périphériques)** > **IPSec Tunnels (Tunnels IPSec)** et sélectionnez **Monitor (Surveiller)**.

STEP 3 | Sélectionnez l'**étendue de configuration** pour afficher l'état du tunnel VPN IPSec. Vous pouvez sélectionner un dossier ou un pare-feu dans vos **dossiers** pour surveiller le tunnel VPN IPSec que vous avez créé sur les pare-feux :

- Pour afficher l'état des tunnels IPSec sur tous les pare-feux, sélectionnez le dossier **Tous les pare-feux**.
- Pour afficher l'état des tunnels IPSec pour le groupe de pare-feux associé à un dossier, sélectionnez le dossier spécifique.
- Pour afficher l'état des tunnels IPSec sur un pare-feu spécifique, sélectionnez le pare-feu.

- *Si vous avez créé le cluster VPN à l'aide d'AutoVPN, vous ne pouvez pas surveiller l'état du tunnel IPSec de ces pare-feux.*
- *Vous pouvez surveiller uniquement les pare-feux sur site et non les composants gérés par Prisma Access.*
- *La surveillance est désactivée au niveau Global et au niveau des extraits. Par conséquent, vous pouvez créer un tunnel IPSec dans l'étendue de configuration globale ou d'extrait, mais vous pouvez surveiller le tunnel IPSec uniquement au niveau du dossier ou du pare-feu.*



STEP 4 | Affichez l'**état du tunnel de cluster VPN** qui fournit la représentation graphique du nombre de tunnels en hausse, du nombre de tunnels hors service et du nombre de tunnels partiellement en fonctionnement.

STEP 5 | Affichez l'**état IPSec SA** dans les **IPSec Tunnels (Tunnels IPSec)**.

- Le vert (**UP**) indique un tunnel IPSec SA valide. Sélectionnez **UP** pour afficher des informations détaillées sur le tunnel IPSec.
- Le rouge (**DOWN**) indique que la SA IPSec n'est pas disponible ou a expiré. Sélectionnez **DOWN** pour afficher les informations détaillées afin d'interpréter la raison de l'échec.

STEP 6 | Affichez l'**état de la SA IKE** dans **IPSec Tunnels (Tunnels IPSec)**.

- La couleur verte (**UP**) indique une SA IKE de phase 1 valide. Sélectionnez **UP** pour afficher des informations détaillées sur la passerelle IKE.
- La couleur rouge (**DOWN**) indique qu'une association de sécurité de SA IKE de phase 1 n'est pas disponible ou a expiré. Sélectionnez **DOWN** pour afficher les informations détaillées afin d'interpréter la raison de l'échec.

STEP 7 | Affichez l'**état du flux VPN** pour les informations de flux de trafic VPN dans **IPSec Tunnels (Tunnels IPSec)**.

- Le vert (**UP**) indique que le tunnel IPSec est en place. Sélectionnez **UP** pour afficher des informations détaillées sur le flux de trafic VPN.
- Le rouge (**DOWN**) indique que le tunnel IPSec est en panne. Sélectionnez **DOWN** pour afficher les informations détaillées afin d'interpréter la raison de l'échec.

STEP 8 | Sélectionnez **Ajouter un nouveau** de filtre et sélectionnez le champ pour afficher les résultats en fonction du champ sélectionné. Par exemple, **ajoutez un nouveau filtre** en sélectionnant le **nom de périphérique** dans la liste, pour afficher l'état du tunnel IPSec pour le périphérique sélectionné.

Sélectionnez **Reset Filters (Réinitialiser les filtres)** Reset Filters pour supprimer un ou plusieurs filtres.

STEP 9 | Sélectionnez **Update Status (Mettre à jour l'état)** pour mettre à jour toutes les données de surveillance du tunnel IPSec présentes à ce niveau (pare-feu, dossier ou tous les pare-feux).

Activer, désactiver, actualiser ou redémarrer une passerelle IKE ou un tunnel IPSec

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Vous pouvez activer, désactiver, actualiser ou redémarrer une passerelle IKE ou un tunnel IPSec pour simplifier le dépannage.

- Activation ou désactivation d'une passerelle IKE ou d'un tunnel IPSec
- Activation ou redémarrage d'une passerelle IKE ou d'un tunnel IPSec

Activation ou désactivation d'une passerelle IKE ou d'un tunnel IPSec

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Activez ou désactivez une passerelle IKE ou un tunnel IPSec pour faciliter le dépannage.

- Activez ou désactivez une passerelle IKE.
  1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Gateways (Passerelles IKE)** et sélectionnez la passerelle que vous souhaitez activer ou désactiver.
  2. Au bas de l'écran, cliquez sur **Enable (Activer)** ou **Disable (Désactiver)**.

- Activez ou désactivez un tunnel IPSec.
  1. Sélectionnez **Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)** et sélectionnez le tunnel que vous souhaitez activer ou désactiver.
  2. Au bas de l'écran, cliquez sur **Enable (Activer)** ou **Disable (Désactiver)**.

Activation ou redémarrage d'une passerelle IKE ou d'un tunnel IPSec

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Vous pouvez actualiser ou redémarrer une passerelle IKE ou un tunnel IPSec. Les comportements d'actualisation et de redémarrage sont différents pour une passerelle IKE et un tunnel IPSec, comme suit :

Phase	Actualiser	Redémarrer
Passerelle IKE (Phase 1 du protocole IKE)	Met à jour les statistiques à l'écran pour la passerelle IKE sélectionnée. Équivalent à l'exécution d'une seconde commande `show` dans la CLI (après une première `show`).	Redémarre la passerelle IKE sélectionnée. **IKEv2** : Redémarre également toute association de sécurité (SA) IPSec enfant associée. **IKEv1** : Ne redémarre pas les SA IPSec associées. Un redémarrage arrête toutes les sessions existantes. Équivalent à l'exécution d'une séquence de commande **`clear`**, **`test`**, **`show`** dans la CLI.
Tunnel IPSec (Phase 2 du protocole IKE)	Met à jour les statistiques à l'écran pour le tunnel IPSec sélectionné. Équivalent à l'exécution d'une seconde commande `show` dans la CLI (après une première `show`).	Redémarre le tunnel IPSec. Un redémarrage arrête toutes les sessions existantes. Équivalent à l'exécution d'une séquence de commande **`clear`**, **`test`**, **`show`** dans la CLI.

N’oubliez pas que le résultat du redémarrage d’une passerelle IKE est différent, selon qu’il s’agit du protocole IKEv1 ou IKEv2.

- Actualisez ou redémarrez une passerelle IKE.
  1. Sélectionnez **Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)** et sélectionnez le tunnel pour la passerelle que vous souhaitez actualiser ou redémarrer.
  2. Dans la ligne de ce tunnel, sous la colonne État, cliquez sur **IKE Info (Informations sur IKE)**.
  3. Au bas de l'écran d'informations sur IKE, cliquez sur l'action souhaitée :
     - **Refresh (Actualiser)** : met à jour les statistiques à l'écran.
     - **Restart (Redémarrer)** : efface les SA. Le trafic est donc interrompu jusqu'à ce que la négociation IKE recommence et que le tunnel soit recréé.

- Actualisez ou redémarrez un tunnel IPSec.

  Vous pouvez déterminer que le tunnel doit être actualisé ou redémarré car vous avez utilisé la surveillance des tunnels pour surveiller l'état des tunnels, ou que vous avez utilisé une surveillance réseau externe pour surveiller la connectivité réseau via le tunnel IPSec.

  1. Sélectionnez **Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)** et sélectionnez le tunnel que vous souhaitez actualiser ou redémarrer.
  2. Dans la ligne de ce tunnel, sous la colonne État, cliquez sur **Tunnel Info (Informations sur le tunnel)**.
  3. Au bas de l'écran d'informations sur le tunnel, cliquez sur l'action souhaitée :
     - **Refresh (Actualiser)** : met à jour les statistiques à l'écran.
     - **Restart (Redémarrer)** : efface les SA. Le trafic est donc interrompu jusqu'à ce que la négociation IKE recommence et que le tunnel soit recréé.

Exemples de configuration VPN site à site

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

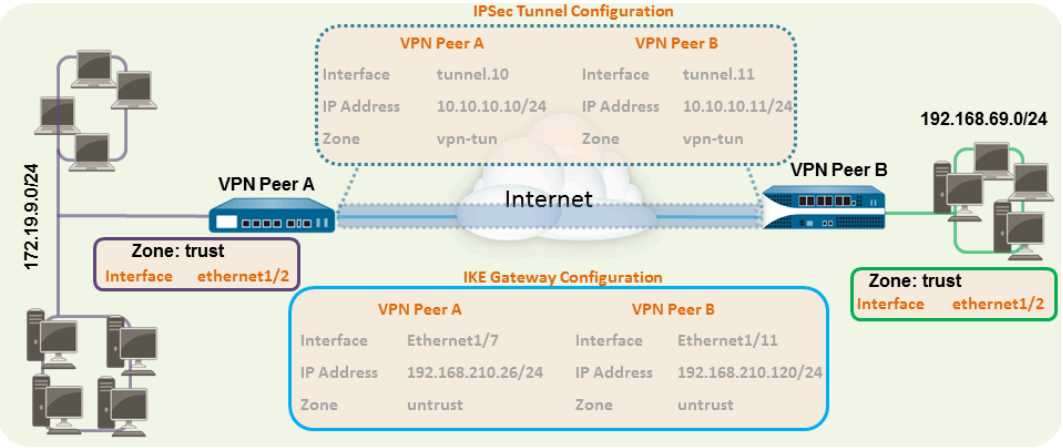
Les sections suivantes fournissent des instructions pour la configuration de certains déploiements VPN courants :

- VPN de site à site avec routage statique
- VPN de site à site avec OSPF
- VPN de site à site avec routage statique et dynamique

VPN de site à site avec routage statique

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

L'exemple suivant indique une connexion VPN entre deux sites qui utilisent des itinéraires statiques. Sans routage dynamique, les interfaces de tunnel sur les homologues VPN A et B ne nécessitent aucune adresse IP, car le pare-feu utilise automatiquement l’interface de tunnel comme saut suivant pour acheminer le trafic entre les sites. Toutefois, pour permettre la surveillance des tunnels, une adresse IP statique a été affectée à chaque interface de tunnel.



STEP 1 | Configurez une interface de couche 3.

Cette interface est utilisée pour le tunnel IKE de phase 1

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet** et choisissez l'interface que vous souhaitez configurer pour le réseau privé virtuel.
2. Sélectionnez **Layer3 (Couche 3)** comme **Interface Type (Type de liaison)**.
3. Dans l'onglet **Config (Configuration)**, sélectionnez la **Security Zone (Zone de sécurité)** à laquelle appartient l'interface :
   - L'interface doit être accessible depuis une zone en dehors de votre réseau approuvé. Envisagez de créer une zone VPN dédiée pour améliorer la visibilité et le contrôle de votre trafic VPN.
   - Si vous n’avez pas encore créé de zone, sélectionnez **New Zone (Nouvelle zone)** dans la **zone de sécurité**, définissez un **nom** pour la zone, puis cliquez sur **OK**.
4. Sélectionnez le **Virtual Router (Routeur virtuel)** à utiliser.
5. Pour assigner une adresse IP à l'interface, cliquez sur l'onglet **IPv4**, puis sur **Add (Ajouter)** dans la section IP et saisissez l'adresse IP, ainsi que le masque réseau à assigner à l'interface, par exemple : 192.168.210.26/24.
6. Pour enregistrer la configuration de l’interface, cliquez sur **OK**.

   Dans cet exemple, la configuration de l'homologue VPN A est la suivante :

   - **Interface** : ethernet1/7
   - **Security Zone (Zone de sécurité)** : non approuvée
   - **Virtual Router (Routeur virtuel)** : par défaut
   - **IPv4** (IPv4) : 192.168.210.26/24

   La configuration de l'homologue VPN B est la suivante :

   - **Interface** : ethernet1/11
   - **Security Zone (Zone de sécurité)** : non approuvée
   - **Virtual Router (Routeur virtuel)** : par défaut
   - **IPv4** : 192.168.210.120/24

STEP 2 | Créez une interface de tunnel et associez-la à un routeur virtuel et une zone de sécurité.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Tunnel** et cliquez sur **Add (Ajouter)**.
2. Dans le champ **Interface Name (Nom de l'interface)**, spécifiez un suffixe numérique, tel que **.1**.
3. Dans l'onglet **Config (Configuration)**, développez la liste **Security Zone (Zone de sécurité)** pour définir la zone de la manière suivante :
   - Pour utiliser votre zone approuvée comme point de terminaison du tunnel, sélectionnez la zone.
   - (Recommandé) Pour créer une zone séparée pour la terminaison du tunnel VPN, cliquez sur **New Zone (Nouvelle zone)**. Dans la boîte de dialogue Zone, définissez un **Nom** pour une nouvelle zone (par exemple *vpn-tun*), puis cliquez sur **OK.**
4. Sélectionnez le **Virtual Router (Routeur virtuel)**.
5. (Facultatif) Affectez une adresse IP à l'interface de tunnel, sélectionnez l'onglet **IPv4** ou **IPv6**, puis cliquez sur **Add (Ajouter)** dans la section IP et saisissez l'adresse IP, ainsi que le masque réseau à affecter à l'interface.

   Avec les routes statiques, l’interface du tunnel ne nécessite pas d’adresse IP. Pour le trafic destiné à une adresse IP/un sous-réseau donné(e), l'interface de tunnel deviendra automatiquement le saut suivant. Envisagez d'ajouter une adresse IP si vous souhaitez activer la surveillance des tunnels.
6. Pour enregistrer la configuration de l’interface, cliquez sur **OK**.

   Dans cet exemple, la configuration de l'homologue VPN A est la suivante :
   - **Interface** : tunnel.10
   - **Zone de sécurité** : vpn_tun
   - **Virtual Router (Routeur virtuel)** : par défaut
   - **IPv4** (IPv4) : 172.19.9.2/24

   La configuration de l'homologue VPN B est la suivante :
   - **Interface** : tunnel.11
   - **Zone de sécurité** : vpn_tun
   - **Virtual Router (Routeur virtuel)** : par défaut
   - **IPv4** (IPv4) : 192.168.69.2/24

STEP 3 | Configurez un itinéraire statique, sur le routeur virtuel, vers le sous-réseau de destination.

1. Sélectionnez **Network (Réseau)** > **Virtual Router (Routeur virtuel)**, puis cliquez sur le routeur que vous avez défini à l'étape précédente.
2. Sélectionnez **Static Route (Itinéraire statique)**, cliquez sur **Add (Ajouter)** et saisissez un nouvel itinéraire pour accéder au sous-réseau à l'autre extrémité du tunnel.

   Dans cet exemple, la configuration de l'homologue VPN A est la suivante :

   - **Destination** : 192.168.69.0/24
   - **Interface** : tunnel.10

   La configuration de l'homologue VPN B est la suivante :

   - **Destination** : 172.19.9.0/24
   - **Interface** : tunnel.11

STEP 4 | Configurez les profils crypto (profils crypto IKE pour la phase 1 et profil crypto IPSec pour la phase 2).

Effectuez cette tâche sur les deux homologues et assurez-vous de définir des valeurs identiques.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE crypto (Crypto IKE)**. Dans cet exemple, le profil par défaut est utilisé.
2. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IPSec crypto (Crypto IPSec)**. Dans cet exemple, le profil par défaut est utilisé.

STEP 5 | Configurez la passerelle IKE.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Gateway (Passerelle IKE)**.
2. Cliquez sur **Add (Ajouter)**, puis configurez les options dans l'onglet **General (Général)**.

   Dans cet exemple, la configuration de l'homologue VPN A est la suivante :

   - **Interface** : ethernet1/7
   - **Adresse IP locale** : 192.168.210.26/24
   - **Type d'adresse IP/Adresse IP de l'homologue** : statique/192.168.210.120
   - **Clés prépartagées** : saisissez une valeur
   - **Local identification (Identification locale)** : aucune ; l'adresse IP locale sera utilisée comme valeur d'identification locale.
   - La configuration de l'homologue VPN B est la suivante :
   - **Interface** : ethernet1/11
   - **Local IP Address (Adresse IP locale)** : 192.168.210.120/24
   - **Type d'adresse IP/Adresse IP de l'homologue** : statique/192.168.210.26
   - **Clés prépartagées** : saisissez la même valeur que sur l'homologue A
   - **Local identification (Identification locale)** : aucune
3. Sélectionnez **Options de phase 1 avancées**, puis le profil crypto IKE créé précédemment à utiliser pour la phase 1 du protocole IKE.

STEP 6 | Configurez le tunnel IPSec.

1. Sélectionnez **Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)**.
2. Cliquez sur **Add (Ajouter)**, puis configurez les options dans l'onglet **General (Général)**.

   Dans cet exemple, la configuration de l'homologue VPN A est la suivante :

   - **Tunnel Interface (Interface de tunnel)** : tunnel.10
   - **Type** : clé automatique
   - **IKE Gateway (Passerelle IKE)** : sélectionnez la passerelle IKE définie ci-dessus
   - **IPSec Crypto Profile (Profil crypto IPSec)** : sélectionnez le profil crypto IPSec défini à l'étape 4.

   La configuration de l'homologue VPN B est la suivante :

   - **Tunnel Interface (Interface de tunnel)** : tunnel.11
   - **Type** : clé automatique
   - **IKE Gateway (Passerelle IKE)** : sélectionnez la passerelle IKE définie ci-dessus
   - **IPSec Crypto Profile (Profil crypto IPSec)** : sélectionnez le profil crypto IPSec défini à l'étape 4.
3. (Facultatif) Sélectionnez **Show Advanced Options (Afficher les options avancées)**, puis **Tunnel Monitor (Surveillance des tunnels)** et spécifiez une adresse IP de destination à laquelle envoyer une requête ping pour vérifier la connexion. Généralement, l'adresse IP de l'interface de tunnel de l'homologue VPN est utilisée.
4. (Facultatif) Pour définir l'action en cas d'échec de la connexion, reportez-vous à la section Définition d'un profil de surveillance de tunnel.

STEP 7 | Créez des règles de politique pour autoriser le trafic entre les sites (sous-réseaux).

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**.
2. Créez des règles pour autoriser le trafic provenant d'adresses IP source et de destination spécifiées entre la zone non approuvée et la zone vpn-tun.

STEP 8 | Enregistrez toutes les modifications de configuration en attente.

Cliquez sur **Commit (Valider)**.

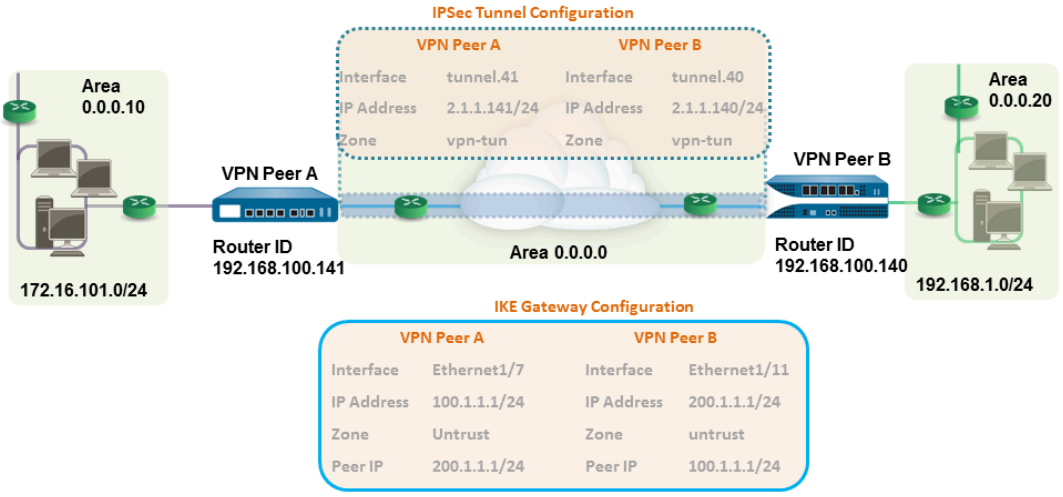
STEP 9 | Test de la connexion du VPN.

Reportez-vous également à la section Affichage de l'état des tunnels.

VPN de site à site avec OSPF

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Dans cet exemple, chaque site utilise OSPF pour le routage dynamique du trafic. L'adresse IP du tunnel sur chaque homologue VPN est affectée de manière statique et sert de saut suivant pour acheminer le trafic entre les deux sites.



STEP 1 | Configurez les interfaces de couche 3 sur chaque pare-feu.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet** et choisissez l'interface que vous souhaitez configurer pour le réseau privé virtuel.
2. Sélectionnez **Layer3 (Couche 3)** dans la liste **Interface Type (Type d'interface)**.
3. Dans l'onglet **Config (Configuration)**, sélectionnez la **Security Zone (Zone de sécurité)** à laquelle appartient l'interface :
   - L'interface doit être accessible depuis une zone en dehors de votre réseau approuvé. Envisagez de créer une zone VPN dédiée pour améliorer la visibilité et le contrôle de votre trafic VPN.
   - Si vous n’avez pas encore créé de zone, sélectionnez **New Zone (Nouvelle zone)** dans la liste **Security Zone (Zone de sécurité)**, définissez un **nom** pour la nouvelle zone et cliquez sur **OK**.
4. Sélectionnez le **Virtual Router (Routeur virtuel)** à utiliser.
5. Pour assigner une adresse IP à l'interface, cliquez sur l'onglet **IPv4**, puis sur **Add (Ajouter)** dans la section IP et saisissez l'adresse IP, ainsi que le masque réseau à assigner à l'interface, par exemple : 192.168.210.26/24.
6. Pour enregistrer la configuration de l’interface, cliquez sur **OK**.

   Dans cet exemple, la configuration de l'homologue VPN A est la suivante :

   - **Interface** : ethernet1/7
   - **Security Zone (Zone de sécurité)** : non approuvée
   - **Virtual Router (Routeur virtuel)** : par défaut
   - **IPv4** (IPv4) : 100.1.1.1/24

   La configuration de l'homologue VPN B est la suivante :

   - **Interface** : ethernet1/11
   - **Security Zone (Zone de sécurité)** : non approuvée
   - **Virtual Router (Routeur virtuel)** : par défaut
   - **IPv4** (IPv4) : 200.1.1.1/24

STEP 2 | Créez une interface de tunnel et associez-la à un routeur virtuel et une zone de sécurité.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Tunnel** et cliquez sur **Add (Ajouter)**.
2. Dans le champ **Interface Name (Nom de l'interface)**, spécifiez un suffixe numérique, tel que **.11**.
3. Dans l'onglet **Config (Configuration)**, développez la liste **Security Zone (Zone de sécurité)** pour définir la zone de la manière suivante :
   - Pour utiliser votre zone approuvée comme point de terminaison du tunnel, sélectionnez la zone.
   - (Recommandé) Pour créer une zone séparée pour la terminaison du tunnel VPN, cliquez sur **New Zone (Nouvelle zone)**. Dans la boîte de dialogue, définissez un **nom** pour la nouvelle zone (par exemple, vpn-tun), puis cliquez sur **OK**.
4. Sélectionnez le **Virtual Router (Routeur virtuel)**.
5. Affectez une adresse IP à l'interface de tunnel, sélectionnez l'onglet **IPv4** ou **IPv6** puis cliquez sur **Ajouter** dans la section IP et saisissez l'adresse IP, ainsi que le préfixe/masque réseau à affecter à l'interface, par exemple, 172.19.9.2/24.

   Cette adresse IP sera utilisée comme adresse IP de saut suivant pour acheminer le trafic vers le tunnel et peut également être utilisée pour surveiller l'état du tunnel.
6. Pour enregistrer la configuration de l'interface, cliquez sur **OK**.

   Dans cet exemple, la configuration de l'homologue VPN A est la suivante :
   - **Interface** : tunnel.41
   - **Zone de sécurité** : vpn_tun
   - **Virtual Router (Routeur virtuel)** : par défaut
   - **IPv4** (IPv4) : 2.1.1.141/24

   La configuration de l'homologue VPN B est la suivante :
   - **Interface** (Interface) : tunnel.40
   - **Zone de sécurité** : vpn_tun
   - **Virtual Router (Routeur virtuel)** : par défaut
   - **IPv4** (IPv4) : 2.1.1.140/24

STEP 3 | Configurez les profils crypto (profils crypto IKE pour la phase 1 et profil crypto IPSec pour la phase 2).

Effectuez cette tâche sur les deux homologues et assurez-vous de définir des valeurs identiques.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE crypto (Crypto IKE)**. Dans cet exemple, le profil par défaut est utilisé.
2. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IPSec crypto (Crypto IPSec)**. Dans cet exemple, le profil par défaut est utilisé.

STEP 4 | Définissez la configuration OSPF sur le routeur virtuel et associez les zones OSPF aux interfaces appropriées sur le pare-feu.

Pour plus d'informations sur les options OSPF disponibles sur le pare-feu, reportez-vous à la section Configuration d'OSPF.

Utilisez Diffusion comme type de liaison lorsque plus de deux routeurs OSPF ont besoin d'échanger des informations de routage.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**, puis choisissez le routeur par défaut ou ajoutez-en un nouveau.
2. Sélectionnez **OSPF** (pour IPv4) ou **OSPFv3** (pour IPv6), puis **Enable (Activer)**.
3. Dans cet exemple, la configuration OSPF de l'homologue VPN A est la suivante :
   - **ID de routeur** : 192.168.100.141
   - **ID de zone** : 0.0.0.0 qui est affecté à l'interface tunnel.1 avec le type de liaison p2p
   - **ID de zone** : 0.0.0.10 qui est affecté à l'interface Ethernet1/1 avec le type de liaison Diffusion

   La configuration OSPF de l'homologue VPN B est la suivante :
   - **ID de routeur** : 192.168.100.140
   - **ID de zone** : 0.0.0.0 qui est affecté à l'interface tunnel.1 avec le type de liaison p2p
   - **ID de zone** : 0.0.0.20 qui est affecté à l'interface Ethernet1/15 avec le type de liaison : Diffusion

STEP 5 | Configurez la passerelle IKE.

Cet exemple utilise des adresses IP statiques pour les deux homologues VPN. Généralement, le siège social utilise une adresse IP configurée de manière statique et la succursale peut disposer d'une adresse IP dynamique ; les adresses IP dynamiques ne sont pas les mieux adaptées à la configuration de services stables tels que les VPN.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Gateway (Passerelle IKE)**.
2. Cliquez sur **Add (Ajouter)**, puis configurez les options dans l'onglet **General (Général)**.

   Dans cet exemple, la configuration de l'homologue VPN A est la suivante :
   - **Interface** : ethernet1/7
   - **Local IP Address (Adresse IP locale)** : 100.1.1.1/24
   - **Peer IP address (Adresse IP de l'homologue)** : 200.1.1.1/24
   - **Clés prépartagées** : saisissez une valeur

   La configuration de l'homologue VPN B est la suivante :
   - **Interface** : ethernet1/11
   - **Local IP Address** (Adresse IP locale) : 200.1.1.1/24
   - **Peer IP address** (Adresse IP de l'homologue) : 100.1.1.1/24
   - **Clés prépartagées** : saisissez la même valeur que sur l'homologue A
3. Sélectionnez le profil crypto IKE créé précédemment à utiliser pour la phase 1 du protocole IKE.

STEP 6 | Configurez le tunnel IPSec.

1. Sélectionnez **Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)**.
2. Cliquez sur **Add (Ajouter)**, puis configurez les options dans l'onglet **General (Général)**.

   Dans cet exemple, la configuration de l'homologue VPN A est la suivante :

   - **Tunnel Interface (Interface de tunnel)** : tunnel.41
   - **Type** : clé automatique
   - **IKE Gateway (Passerelle IKE)** : sélectionnez la passerelle IKE définie ci-dessus
   - **Profil crypto IPSec** : sélectionnez la passerelle IKE définie ci-dessus

   La configuration de l'homologue VPN B est la suivante :

   - **Tunnel Interface (Interface de tunnel)** : tunnel.40
   - **Type** : clé automatique
   - **IKE Gateway (Passerelle IKE)** : sélectionnez la passerelle IKE définie ci-dessus
   - **Profil crypto IPSec** : sélectionnez la passerelle IKE définie ci-dessus
3. Sélectionnez **Afficher les options avancées**, puis **Surveillance des tunnels** et spécifiez une adresse IP de destination à laquelle envoyer une requête ping pour vérifier la connexion.
4. Pour définir l'action en cas d'échec de la connexion, reportez-vous à la section Définition d’un profil de surveillance de tunnel.

STEP 7 | Créez des règles de politique pour autoriser le trafic entre les sites (sous-réseaux).

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**.
2. Créez des règles pour autoriser le trafic provenant d'adresses IP source et de destination spécifiées entre la zone non approuvée et la zone vpn-tun.

STEP 8 | Vérifiez les itinéraires et les éléments adjacents OSPF à partir de la CLI.

Vérifiez que les deux pare-feu peuvent se voir comme voisins, ainsi que toutes les informations d'état. Vérifiez également l'adresse IP de l'interface de tunnel de l'homologue VPN et l'ID du routeur OSPF. Utilisez les commandes CLI suivantes sur chaque homologue VPN :

- **show routing protocol ospf neighbor**

```
admin@FW-A> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.140
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.140
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no

admin@FW-B> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.141
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.141
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no
```

- **show routing route type ospf**

```
admin@FW-A> show routing route type ospf

flags: A:active, ?:loose, C:connect, H:host, S:static, ~:internal, R:rip, O:ospf, B:bgp,
       Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2


VIRTUAL ROUTER: vr1 (id 1)
  ==========
destination             nexthop             metric flags      age   interface          next-AS
2.1.1.0/24              0.0.0.0                 10   Oi       6760  tunnel.41
172.16.101.0/24         0.0.0.0                 10   Oi       6854  ethernet1/1
192.168.1.0/24          2.1.1.140               20 A Oo       6754  tunnel.40
total routes shown: 3
```

```
admin@FW-B> show routing route type ospf

flags: A:active, C:connect, H:host, S:static, R:rip, O:ospf,
       Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2


VIRTUAL ROUTER: vr1 (id 1)
  ==========
destination             nexthop             metric flags      age   interface
2.1.1.0/24              0.0.0.0             10      Oi        20033 tunnel.40
172.16.101.0/24         2.1.1.141           20     AOo        6896  tunnel.40
192.168.1.0/24          0.0.0.0             10      Oi        8058  ethernet1/15
total routes shown: 3
```


STEP 9 | Test de la connexion du VPN.

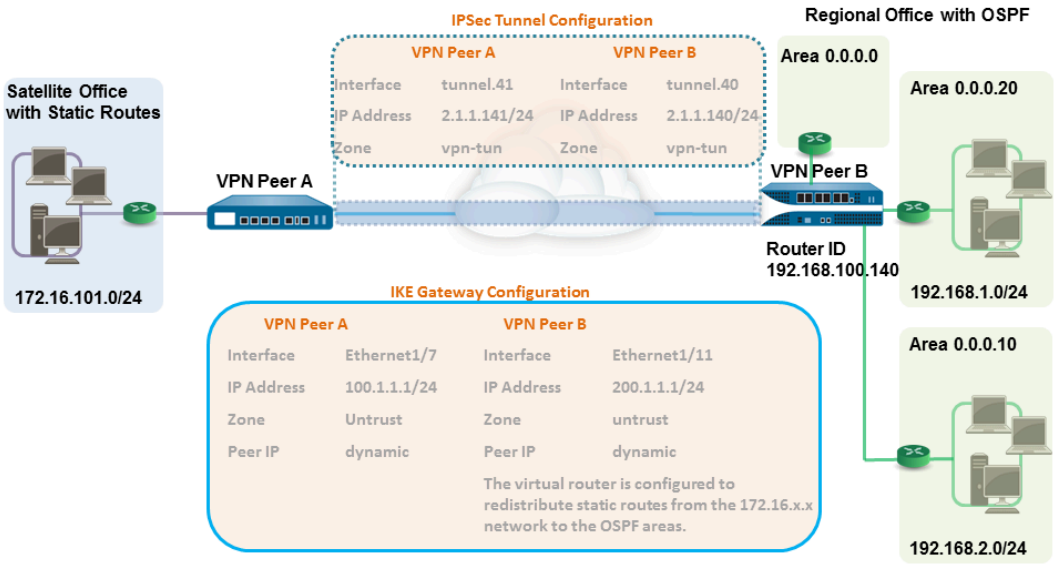
Reportez-vous aux sections Configuration de la surveillance des tunnels et Affichage de l’état des tunnels.

VPN de site à site avec routage statique et dynamique

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Dans cet exemple, un site utilise des itinéraires statiques et l'autre utilise OSPF. Lorsque le protocole de routage n'est pas identique sur les deux sites, l'interface de tunnel sur chaque pare-feu doit être configurée avec une adresse IP statique. Ensuite, pour permettre l'échange des informations de routage, le pare-feu qui participe au processus de routage statique et dynamique doit être configuré avec un profil de redistribution. La configuration du profil de redistribution permet au routeur virtuel de redistribuer et de filtrer les itinéraires entre les protocoles (itinéraires statiques, itinéraires connectés et hôtes) du système statique autonome au système OSPF autonome. Sans ce profil de redistribution, chaque protocole fonctionne de manière autonome et n'échange aucune information d'itinéraire avec les autres protocoles exécutés sur le même routeur virtuel.

Dans cet exemple, le bureau satellite dispose d'itinéraires statiques et tout le trafic destiné au réseau 192.168.x.x est acheminé vers l'interface tunnel.41. Le routeur virtuel sur l'homologue VPN B participe au processus de routage statique et dynamique ; il est configuré avec un profil de redistribution afin de propager (exporter) les itinéraires statiques sur le système OSPF autonome.



STEP 1 | Configurez les interfaces de couche 3 sur chaque pare-feu.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet** et choisissez l'interface que vous souhaitez configurer pour le réseau privé virtuel.
2. Sélectionnez **Layer3 (Couche 3)** comme **Interface Type (Type de liaison)**.
3. Dans l'onglet **Config (Configuration)**, sélectionnez la **Security Zone (Zone de sécurité)** à laquelle appartient l'interface :
   - L'interface doit être accessible depuis une zone en dehors de votre réseau approuvé. Envisagez de créer une zone VPN dédiée pour améliorer la visibilité et le contrôle de votre trafic VPN.
   - Si vous n’avez pas encore créé de zone, sélectionnez **New Zone (Nouvelle zone)** dans la **zone de sécurité**, définissez un **nom** pour la zone, puis cliquez sur **OK**.
4. Sélectionnez le **Virtual Router (Routeur virtuel)** à utiliser.
5. Pour assigner une adresse IP à l'interface, cliquez sur l'onglet **IPv4**, puis sur **Add (Ajouter)** dans la section IP et saisissez l'adresse IP, ainsi que le masque réseau à assigner à l'interface, par exemple : 192.168.210.26/24.
6. Pour enregistrer la configuration de l’interface, cliquez sur **OK**.

   Dans cet exemple, la configuration de l'homologue VPN A est la suivante :

   - **Interface** : ethernet1/7
   - **Security Zone (Zone de sécurité)** : non approuvée
   - **Virtual Router (Routeur virtuel)** : par défaut
   - **IPv4** (IPv4) : 100.1.1.1/24

   La configuration de l'homologue VPN B est la suivante :

   - **Interface** : ethernet1/11
   - **Security Zone (Zone de sécurité)** : non approuvée
   - **Virtual Router (Routeur virtuel)** : par défaut
   - **IPv4** (IPv4) : 200.1.1.1/24

STEP 2 | Configurez les profils crypto (profils crypto IKE pour la phase 1 et profil crypto IPSec pour la phase 2).

Effectuez cette tâche sur les deux homologues et assurez-vous de définir des valeurs identiques.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE crypto (Crypto IKE)**. Dans cet exemple, le profil par défaut est utilisé.
2. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IPSec crypto (Crypto IPSec)**. Dans cet exemple, le profil par défaut est utilisé.

STEP 3 | Configurez la passerelle IKE.

Grâce aux clés prépartagées, pour renforcer l'authentification lors de la configuration du tunnel IKE de phase 1, vous pouvez configurer les attributs d'identification locale et de l'homologue, ainsi qu'une valeur correspondante mise en correspondance dans le processus de négociation IKE.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Gateway (Passerelle IKE)**.
2. Cliquez sur **Add (Ajouter)**, puis configurez les options dans l'onglet **General (Général)**.

   Dans cet exemple, la configuration de l'homologue VPN A est la suivante :

   - **Interface** : ethernet1/7
   - **Local IP Address (Adresse IP locale)** : 100.1.1.1/24
   - **Type d'adresse IP de l'homologue** : dynamique
   - **Clés prépartagées** : saisissez une valeur
   - **Identification locale** : sélectionnez **Nom de domaine complet (nom d'hôte)** et saisissez la valeur pour l'homologue VPN A.
   - **Identification de l'homologue** : sélectionnez **Nom de domaine complet (nom d'hôte)** et saisissez la valeur pour l'homologue VPN B.

   La configuration de l'homologue VPN B est la suivante :

   - **Interface** : ethernet1/11
   - **Local IP Address** (Adresse IP locale) : 200.1.1.1/24
   - **Type d'adresse IP de l'homologue** : dynamique
   - **Clés prépartagées** : saisissez la même valeur que sur l'homologue A
   - **Identification locale** : sélectionnez **Nom de domaine complet (nom d'hôte)** et saisissez la valeur pour l'homologue VPN B.
   - **Identification de l'homologue** : sélectionnez **Nom de domaine complet (nom d'hôte)** et saisissez la valeur pour l'homologue VPN A.
3. Sélectionnez le profil crypto IKE créé précédemment à utiliser pour la phase 1 du protocole IKE.

STEP 4 | Créez une interface de tunnel et associez-la à un routeur virtuel et une zone de sécurité.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Tunnel** et cliquez sur **Add (Ajouter)**.
2. Dans le champ **Nom de l'interface**, spécifiez un suffixe numérique, tel que **.41**.
3. Dans l'onglet **Config (Configuration)**, développez la liste **Security Zone (Zone de sécurité)** pour définir la zone de la manière suivante :
   - Pour utiliser votre zone approuvée comme point de terminaison du tunnel, sélectionnez la zone.
   - (Recommandé) Pour créer une zone séparée pour la terminaison du tunnel VPN, cliquez sur **New Zone (Nouvelle zone)**. Dans la boîte de dialogue Zone, définissez un **Nom** pour la nouvelle zone (par exemple *vpn-tun*), puis cliquez sur **OK.**
4. Sélectionnez le **Virtual Router (Routeur virtuel)**.
5. Affectez une adresse IP à l'interface de tunnel, sélectionnez l'onglet **IPv4** ou **IPv6** puis cliquez sur **Ajouter** dans la section IP et saisissez l'adresse IP, ainsi que le préfixe/masque réseau à affecter à l'interface, par exemple, 172.19.9.2/24.

   Cette adresse IP sera utilisée pour acheminer le trafic vers le tunnel et Surveiller l'état du tunnel.
6. Pour enregistrer la configuration de l'interface, cliquez sur **OK**.

   Dans cet exemple, la configuration de l'homologue VPN A est la suivante :
   - **Interface** : tunnel.41
   - **Zone de sécurité** : vpn_tun
   - **Virtual Router (Routeur virtuel)** : par défaut
   - **IPv4** (IPv4) : 2.1.1.141/24

   La configuration de l'homologue VPN B est la suivante :
   - **Interface** : tunnel.42
   - **Zone de sécurité** : vpn_tun
   - **Virtual Router (Routeur virtuel)** : par défaut
   - **IPv4** (IPv4) : 2.1.1.140/24

STEP 5 | Spécifiez l'interface qui acheminera le trafic vers une destination sur le réseau 192.168.x.x.

1. Sélectionnez le routeur virtuel sur l'homologue VPN A.
2. Sélectionnez **Static Routes (Itinéraires statiques)**, puis cliquez sur **Add (Ajouter)** pour ajouter tunnel.41 comme **Interface** pour acheminer le trafic vers une **Destination** sur le réseau 192.168.x.x.

STEP 6 | Définissez l'itinéraire statique et la configuration OSPF sur le routeur virtuel, puis associez les zones OSPF aux interfaces appropriées sur le pare-feu.

1. Sur l'homologue VPN B, sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**, puis choisissez le routeur par défaut ou ajoutez-en un nouveau.
2. Sélectionnez **Static Routes (Itinéraires statiques)** et cliquez sur **Add (Ajouter)** pour ajouter l'adresse IP comme saut suivant du trafic sur le réseau 172.168.x.x.

   Affectez la mesure d'itinéraire souhaitée ; plus la valeur est faible, plus la priorité de sélection de l'itinéraire dans la table de transfert est élevée.
3. Sélectionnez **OSPF** (pour IPv4) ou **OSPFv3** (pour IPv6), puis **Enable (Activer)**.
4. Dans cet exemple, la configuration OSPF de l'homologue VPN B est la suivante :
   - Router ID (ID de routeur) : 192.168.100.140
   - Area ID (ID de zone) : 0.0.0.0 qui est affecté à l'interface Ethernet1/12 avec le type de liaison Diffusion
   - Area ID (ID de zone) : 0.0.0.10 qui est affecté à l'interface Ethernet1/1 avec le type de liaison Diffusion
   - Area ID (ID de zone) : 0.0.0.20 qui est affecté à l'interface Ethernet1/15 avec le type de liaison Diffusion

STEP 7 | Créez un profil de redistribution pour injecter les itinéraires statiques dans le système OSPF autonome.

1. Créez un profil de redistribution sur l'homologue VPN B.
   1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**, puis choisissez le routeur utilisé ci-dessus.
   2. Sélectionnez **Redistribution Profiles (Profils de redistribution)** et cliquez sur **Add (Ajouter)**.
   3. Donnez un nom au profil, puis sélectionnez **Redistribution** et affectez-lui une valeur de **priorité**. Si vous avez configuré plusieurs profils, le profil dont la valeur de priorité est la plus faible est d'abord mis en correspondance.
   4. Définissez le **Source Type (Type de source)** comme **static (statique)** et cliquez sur **OK**. L'itinéraire statique que vous avez défini à l'étape 6 sera utilisé pour la redistribution.
2. Injectez les itinéraires statiques dans le système OSPF.
   1. Sélectionnez **OSPF** > **Export Rules (Exporter les règles)** (pour IPv4) ou **OSPFv3** > **Export Rules (Exporter les règles)** (pour IPv6).
   2. Cliquez sur **Ajouter**, puis sélectionnez le profil de redistribution que vous avez créé.
   3. Déterminez la manière dont les itinéraires externes sont injectés dans le système OSPF. L'option par défaut, **Ext2**, calcule le coût total de l'itinéraire uniquement à l'aide des mesures externes. Pour utiliser des mesures OSPF internes et externes, sélectionnez **Ext1**.
   4. Affectez une **Metric (Mesure)** (valeur de coût) aux itinéraires injectés dans le système OSPF. Cette option vous permet de modifier la mesure de l'itinéraire lorsqu'il est injecté dans le système OSPF.
   5. Cliquez sur **OK**.

STEP 8 | Configurez le tunnel IPSec.

1. Sélectionnez **Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)**.
2. Cliquez sur **Add (Ajouter)**, puis configurez les options dans l'onglet **General (Général)**.

   Dans cet exemple, la configuration de l'homologue VPN A est la suivante :

   - **Tunnel Interface (Interface de tunnel)** : tunnel.41
   - **Type** : clé automatique
   - **IKE Gateway (Passerelle IKE)** : sélectionnez la passerelle IKE définie ci-dessus
   - **Profil crypto IPSec** : sélectionnez la passerelle IKE définie ci-dessus

   La configuration de l'homologue VPN B est la suivante :

   - **Tunnel Interface (Interface de tunnel)** : tunnel.40
   - **Type** : clé automatique
   - **IKE Gateway (Passerelle IKE)** : sélectionnez la passerelle IKE définie ci-dessus
   - **Profil crypto IPSec** : sélectionnez la passerelle IKE définie ci-dessus
3. Sélectionnez **Afficher les options avancées**, puis **Surveillance des tunnels** et spécifiez une adresse IP de destination à laquelle envoyer une requête ping pour vérifier la connexion.
4. Pour définir l'action en cas d'échec de la connexion, reportez-vous à la section Définition d’un profil de surveillance de tunnel.

STEP 9 | Créez des règles de politique pour autoriser le trafic entre les sites (sous-réseaux).

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**.
2. Créez des règles pour autoriser le trafic provenant d'adresses IP source et de destination spécifiées entre la zone non approuvée et la zone vpn-tun.

STEP 10 | Vérifiez les itinéraires et les éléments adjacents OSPF à partir de la CLI.

Vérifiez que les deux pare-feu peuvent se voir comme voisins, ainsi que toutes les informations d'état. Vérifiez également l'adresse IP de l'interface de tunnel de l'homologue VPN et l'ID du routeur OSPF. Utilisez les commandes CLI suivantes sur chaque homologue VPN :

- **`show routing protocol ospf neighbor`**

```
admin@FW-A> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.140
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.140
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no

admin@FW-B> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.141
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.141
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no
```

- **`show routing route`**

Voici un exemple de résultat sur chaque homologue VPN :

```
VPN PeerA

destination             next hop        metric  flags   age     interface       next-AS
192.168.1.0/24          2.1.1.141       20      A S             tunnel.41
192.168.2.0/24          2.1.1.141       20      A S             tunnel.41
172.16.101.0/24         0.0.0.0         1       A H             ethernet1/1
2.1.1.140/24            2.1.1.141       20      A S             tunnel.41

VPN PeerB

destination             next hop        metric  flags   age     interface       next-AS
192.168.1.0/24          0.0.0.0         10      A Oo            ethernet1/1
192.168.2.0/24          0.0.0.0         10      A Oo            ethernet1/15
172.16.101.0/24         2.1.1.140       20      A H             tunnel.40
2.1.1.141/24            2.1.1.140       10      A C             tunnel.40
```

STEP 11 | Test de la connexion du VPN.

Reportez-vous aux sections Configuration de la surveillance des tunnels et Affichage de l’état des tunnels.

Dépannage

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Ce chapitre partage les tâches de test de la connectivité VPN et d’interprétation des messages d’erreur VPN, le cas échéant. Utilisez les commandes CLI pour surveiller et dépanner les connexions VPN site à site.

- Dépanner votre connexion au tunnel VPN IPSec
- Résoudre les problèmes de tunnel VPN IPSec de site à site à l’aide de l’interface CLI

Dépanner votre connexion au tunnel VPN IPSec

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Testez et dépannez votre connexion VPN IPSec pour obtenir des performances maximales :

- Test de la connexion du VPN
- Interprétation des messages d'erreur VPN

Test de la connexion du VPN

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Effectuez cette tâche pour tester la connectivité VPN.

STEP 1 | Initiez la phase 1 du protocole IKE en envoyant une requête ping à un hôte via le tunnel, ou en utilisant la commande CLI suivante :

```
test vpn ike-sa gateway <gateway_name>
```

STEP 2 | Saisissez la commande suivante pour déterminer si la phase 1 du protocole IKE est configurée :

```
show vpn ike-sa gateway <gateway_name>
```

Dans la sortie, vérifiez si l'association de sécurité s'affiche. Si ce n'est pas le cas, consultez les messages du journal système pour interpréter la raison de l'échec.

STEP 3 | Initiez la phase 2 du protocole IKE en envoyant une requête ping à un hôte via le tunnel, ou en utilisant la commande CLI suivante :

```
test vpn ipsec-sa tunnel <tunnel_name>
```

STEP 4 | Saisissez la commande suivante pour déterminer si la phase 2 du protocole IKE est configurée :

```
show vpn ipsec-sa tunnel <tunnel_name>
```

Dans la sortie, vérifiez si l'association de sécurité s'affiche. Si ce n'est pas le cas, consultez les messages du journal système pour interpréter la raison de l'échec.

STEP 5 | Pour afficher le informations relatif au flux de trafic VPN, utilisez la commande suivante :

```
show vpn flow total tunnels configured:             1 filter - type
 IPSec, state any total IPSec tunnel configured:        1 total
 IPSec tunnel shown:                1 name                    id
      state      local-ip       peer-ip       tunnel-i/f
 ------------------------------------------------------------------------------
 vpn-to-siteB       5       active
    100.1.1.1     200.1.1.1     tunnel.41
```

Interprétation des messages d'erreur VPN

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Le tableau suivant répertorie certains des messages d'erreur VPN courants consignés dans le journal système.

Table 2: Messages d'erreur Syslog relatifs aux problèmes VPN

Si l’erreur est la suivante :	Essayez ce qui suit :

`Echec de la négociation IKE phase-1 en tant qu’initiateur, mode principal Failed SA: x.x.x.x[500]-y.y.y.y[500] cookie:84222f276c2fa2e9:0000000000000000 due to timeout.`
ou
`Echec de la négociation IKE phase 1 impossible de localiser la demande IKE phase-1 d’adresse IP x.x.x.x[1929] homologue`
	• Vérifiez que l'adresse IP publique de chaque homologue VPN est exacte dans la configuration de passerelle IKE.
	• Vérifiez que les adresses IP peuvent recevoir une requête ping et que des problèmes de routage ne causent pas l’échec de la connexion.

`Received unencrypted notify payload (no proposal chosen) from IP x.x.x.x[500] to y.y.y.y[500], ignored...`
ou
`Echec de la négociation IKE phase-1 Impossible de traitre le SA payload de l’homologue.`
	Dans la configuration du profil crypto IKE, vérifiez que les propositions de cryptage, d'authentification et de groupe DH sont identiques des deux côtés.

`pfs group mismatched:my: 2peer: 0` ou	Dans la configuration du profil crypto IPSec, vérifiez ce qui suit :

Si l’erreur est la suivante :	Essayez ce qui suit :
`Echec de la négociation IKE phase-2 lors du traitement de SA payload. Aucune proposition adaptée trouvée dans le SA payload de l’homologue.`	• PFS est activé ou désactivé sur les deux pairs VPN • au moins un des groupes DH proposés par chaque homologue est identique.
`Echec de la négociation IKE phase-2 lors du traitement de l’ID proxy. Received local id x.x.x.x/x type IPv4 address protocol 0 port 0, received remote id y.y.y.y/y type IPv4 address protocol 0 port 0.`	L’homologue VPN à une extrémité utilise un VPN basé sur une politique. Vous devez configurer un ID de proxy sur le pare-feu Palo Alto Networks. Reportez-vous à la section Création d’un ID de proxy pour identifier les homologues VPN.
`Erreur de validation : Limite de liaison Tunnel interface tunnel.x multiple (xx) atteinte.`	Vous devez avoir atteint le maximum d’identifiants proxy pris en charge sur votre pare-feu. Vérifiez le maximum d’identifiants proxy pris en charge sur votre pare-feu avant d’établir un tunnel IPSec. Nous vous recommandons de vérifier les ID de proxy maximum pris en charge sur votre pare-feu avant de configurer les ID de proxy pour les homologues VPN. Si vous avez un cas d’utilisation où vous souhaitez implémenter un tunnel VPN IPSec avec plus du maximum d’ID proxy pris en charge sur un pare-feu, procédez comme suit : • Configurez un autre tunnel avec la même configuration de phase 1 et phase 2. • Utilisez SuperNet dans l’adresse IP des ID proxy. Par exemple, au lieu d’utiliser 10.1.0.0/16, 10.2.0.0/16, utilisez SuperNet pour amener la plage à 10.0.0.0/8 pour éviter les entrées multiples.
`Inadéquation de l’identifiant proxy`	L’inadéquation de l’ID proxy entraînera l’échec de l’établissement du tunnel VPN IPSec site à site. Par conséquent, configurez des ID de proxy identiques sur les deux homologues VPN pour

Si l’erreur est la suivante :	Essayez ce qui suit :
	établir le tunnel VPN IPSec site à site avec succès. Par exemple : Dans une configuration de tunnel IPSec site à site, si un homologue VPN est configuré avec une adresse IP pour un masque réseau de /32 et l’homologue VPN distant est configuré avec la même adresse IP mais avec le masque de réseau différent de /16, cela entraînera un échec dans l’établissement du tunnel VPN. *Les ID de proxy des autres fournisseurs de pare-feu sont appelés liste d’accès ou liste de contrôle d’accès (ACL).* Les ID de proxy dans les homologues VPN doivent être des miroirs exacts les uns des autres (c’est-à-dire être opposés), mais ne pas correspondre. Exemple de configuration d’ID de proxy pour les pairs VPN pour établir un tunnel VPN IPSec: Si le pare-feu VPN 1 est configuré avec 192.0.2.0/24 comme ID local et 192.0.2.25/24 comme ID pair. Ensuite, le pare-feu VPN 2 doit être configuré avec 192.0.2.25/24 comme ID local et 192.0.2.0/24 comme ID pair.

Résoudre les problèmes de VPN site à site à l'aide de l'interface CLI

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Utilisez les commandes CLI suivantes pour résoudre les problèmes de VPN site à site de phase 1 et de phase 2 :

- Commandes d'affichage
- Commandes d'effacement
- Commandes de test
- Commandes de débogage

Commandes d'affichage

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Si vous souhaitez . . .	Utilisez . . .
• Afficher les statistiques de base de tous les tunnels VPN	`> show running tunnel flow info`
• Afficher l'IKE SA pour une passerelle donnée	`> show vpn ike-sa gateway <gateway> | match <x.x.x.x/Y>`
• Afficher l'IKE SA pour un tunnel donné	`> show vpn ike-sa tunnel <tunnel>`
• Afficher les compteurs IPSec	`> show vpn flow`
• Afficher la liste de toutes les passerelles IPSec et leurs configurations	`> show vpn gateway`

Si vous souhaitez . . .	Utilisez . . .
• Afficher les IKE SA de la phase 1	`> show vpn ike-sa`
• Afficher les IKE SA phase 2	`> show vpn ipsec-sa`
• Afficher la liste des configurations de tunnel IPSec à clé automatique	`> show vpn tunnel`

Commandes d’effacement

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Si vous souhaitez . . .	Utilisez . . .
• Supprimer l’IKEv1 IKE SA pour une passerelle donnée	`> clear vpn ike-sa gateway <gateway>`
• Supprimer l’IKEv1 IKE SA pour un tunnel donné	`> clear vpn ike-sa tunnel <tunnel>`
• Supprimer l’IKEv1 IPSec SA pour un tunnel donné	`> clear vpn ipsec-sa tunnel <tunnel>`

Commandes de test

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Si vous souhaitez . . .	Utilisez . . .
• Lancer une négociation IKE avec la passerelle désignée	`> test vpn ike-sa gateway <gateway>`

Si vous souhaitez . . .	Utilisez . . .
• Lancer une négociation IPSec pour le tunnel désigné	`> test vpn ipsec-sa tunnel <tunnel>`

Commandes de débogage

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• PAN-OS	Aucune licence requise

Si vous souhaitez . . .	Utilisez . . .
• Activer le débogage pour afficher la journalisation détaillée et l'état	`> debug ike global on debug less mp-log ikemgr.log debug ike stat`
• Capture de paquets pour afficher et capturer les négociations en mode principal, agressif et rapide.	`> debug ike pcap on view-pcap no-dns-lookup yes no-port-lookup yes debug-pcap ikemgr.pcap`
• Désactiver le débogage	`> debug ike pcap off`

