Paramètres VPN généraux

La mise en œuvre des réseaux privés virtuels par l'ASA comprend des fonctionnalités utiles qui ne s'inscrivent pas clairement dans des catégories précises. Ce chapitre décrit certaines de ces fonctionnalités.

Lignes directrices et limites relatives à la licence

Cette section comprend les lignes directrices et les limites de cette fonctionnalité.

Directives relatives au mode contextuel

Pris en charge en mode contexte unique et multiple. Dans la version appropriée du Guide de configuration de l'interface de ligne de commande pour les opérations générales d'ASA, consultez les sections *Lignes directrices pour le mode contexte multiple* pour obtenir la liste de ce qui n'est pas pris en charge en mode contexte multiple et *Nouvelles fonctionnalités* qui présente le détail des éléments ajoutés au fil des versions.

Directives sur le mode pare-feu

Pris en charge uniquement en mode pare-feu routé. Le mode transparent n'est pas pris en charge.

Traduction d'adresses réseau (NAT)

Pour obtenir des lignes directrices et des renseignements sur la configuration de NAT, consultez la section *NAT pour VPN* du *Guide de configuration de l'interface de ligne de commande de Cisco Secure Firewall ASA*.

Configurer IPsec pour contourner les ACL

Pour autoriser tous les paquets provenant d'un tunnel IPsec sans vérifier les ACL des interfaces source et destination, saisissez la commande **sysopt connection permit-vpn** en mode de configuration globale.

Vous pouvez contourner les ACL d'interface pour le trafic IPsec si vous utilisez un concentrateur VPN distinct derrière l'ASA et que vous souhaitez maximiser les performances de l'ASA. En règle générale, vous créez une ACL qui autorise les paquets IPsec à l'aide de la commande **access-list** et l'appliquez à l'interface source. L'utilisation d'une liste de contrôle d'accès (ACL) vous permet de spécifier le trafic exact que vous souhaitez autoriser sur l'ASA.

L'exemple suivant autorise le trafic IPsec à travers l'ASA sans vérifier les ACL :

```
hostname(config)# sysopt connection permit-vpn
```

Remarque Le trafic déchiffré de transit est autorisé depuis le client malgré la présence d'un groupe d'accès sur l'interface externe, qui appelle une ACL **deny ip any any**, alors que **no sysopt connection permit-vpn** est configuré.

La tentative de contrôler l'accès au réseau protégé au moyen d'un VPN de site à site ou d'accès à distance à l'aide de la commande **no sysopt permit-vpn** conjuguée à une ACL sur l'interface externe ne réussit pas.

sysopt connection permit-vpn contourne les ACL de l'interface, tant entrantes que sortantes, où la carte de chiffrement pour ce trafic intéressant est activée, ainsi que les ACL de sortie de toutes les autres interfaces, mais non les ACL d'entrée.

Dans cette situation, lorsque l'accès de gestion interne est activé, l'ACL n'est pas appliquée et les utilisateurs peuvent toujours se connecter à l'ASA à l'aide de SSH. Le trafic vers les hôtes sur le réseau interne est bloqué correctement par la liste de contrôle d'accès, mais le trafic traversant déchiffré vers l'interface interne n'est pas bloqué.

Les commandes **ssh** et **http** ont une priorité supérieure à celle des ACL. Pour refuser le trafic SSH, Telnet ou ICMP vers le boîtier depuis la session VPN, utilisez les commandes **ssh**, **telnet** et **icmp**.

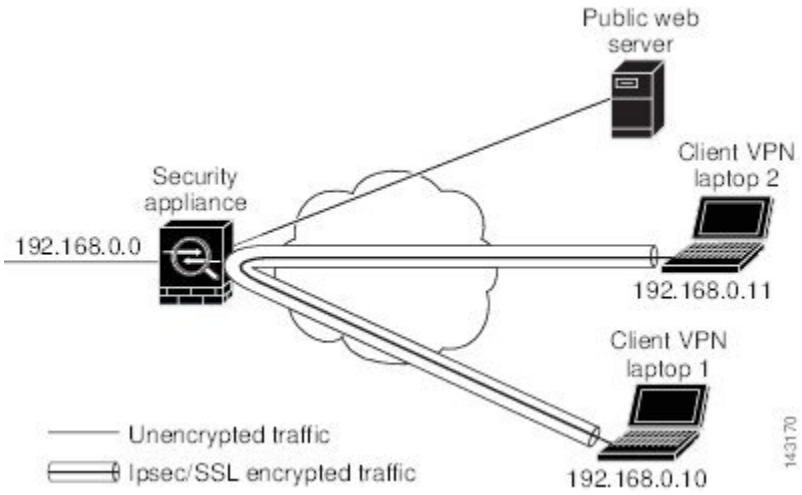
Permettre le trafic intra-interface (hairpinning)

L'ASA comprend une fonctionnalité qui permet à un client VPN d'envoyer un trafic protégé par IPsec à un autre utilisateur VPN en autorisant ce trafic à entrer et à sortir de la même interface. C'est ce qu'on appelle également le « hairpinning », qu'on peut considérer comme des sites distants VPN (clients) se connectant par l'intermédiaire d'un concentrateur VPN (l'ASA).

Le hairpinning peut également rediriger le trafic VPN entrant vers l'extérieur par la même interface que le trafic non chiffré. Cela peut être utile, par exemple, pour un client VPN qui n'a pas de tunnellisation fractionnée, mais qui doit à la fois accéder à un VPN et naviguer sur le Web.

La figure ci-dessous montre le client VPN 1 qui envoie un trafic IPsec sécurisé au client VPN 2 tout en envoyant un trafic non chiffré à un serveur Web public.

Illustration 1 : Client VPN utilisant la fonctionnalité intra-interface pour le hairpinning



Pour configurer cette fonctionnalité, utilisez la commande **same-security-traffic** en mode de configuration globale avec son argument intra-interface.

La syntaxe de la commande est same-security-traffic permit {*inter-interface* | *intra-interface*}.

L'exemple suivant montre comment activer le trafic intra-interface :

```
hostname(config)# same-security-traffic permit intra-interface
hostname(config)#
```

Remarque Utilisez la commande **same-security-traffic** avec l'argument **inter-interface** pour autoriser la communication entre les interfaces ayant le même niveau de sécurité. Cette fonctionnalité n'est pas propre aux connexions IPsec. Pour en savoir plus, consultez le chapitre « Configuration des paramètres d'interface » de ce guide.

Pour utiliser le hairpinning, vous devez appliquer les règles NAT appropriées à l'interface ASA, comme décrit dans les considérations NAT pour le trafic intra-interface.

Considérations sur la NAT pour le trafic intra-interface

Pour que l'ASA renvoie le trafic non chiffré par l'interface, vous devez activer la NAT pour l'interface afin que les adresses routables publiquement remplacent vos adresses IP privées (sauf si vous utilisez déjà des adresses IP publiques dans votre ensemble d'adresses IP locales). L'exemple suivant applique une règle PAT d'interface au trafic provenant de l'ensemble d'adresses IP du client :

```
hostname(config)# ip local pool clientpool 192.168.0.10-192.168.0.100
hostname(config)# object network vpn_nat
```

```
hostname(config-network-object)# subnet 192.168.0.0 255.255.255.0
hostname(config-network-object)# nat (outside,outside) interface
```

Lorsque l'ASA renvoie le trafic VPN chiffré à partir de cette même interface, la NAT est facultative. L'épinglage de VPN à VPN fonctionne avec ou sans NAT. Pour appliquer la NAT à tout le trafic sortant, mettez en œuvre uniquement les commandes ci-dessus. Pour exempter le trafic de VPN à VPN de la NAT, ajoutez des commandes (à l'exemple ci-dessus) qui mettent en œuvre l'exemption de NAT pour le trafic de VPN à VPN, comme par exemple :

```
hostname(config)# nat (outside,outside) source static vpn_nat vpn_nat destination static
vpn_nat vpn_nat
```

Pour en savoir plus sur les règles de NAT, consultez le chapitre « Application de la NAT » de ce guide.

Définition du nombre maximal de sessions VPN IPsec ou SSL actives

Pour limiter les sessions VPN à une valeur inférieure à celle autorisée par l'ASA, saisissez la commande **vpn-sessiondb** en mode de configuration globale :

vpn-sessiondbmax-anyconnect-premium-or-essentials-limit <number> | **max-other-vpn-limit** <number>

Le mot-clé **max-AnyConnect-premium-or-essentials-limit** spécifie le nombre maximal de Secure Client (services client sécurisés) sessions, de 1 au nombre maximal de sessions autorisées par la licence.

Remarque La licence, la durée, le niveau et le nombre d'utilisateurs appropriés ne sont plus déterminés avec ces commandes. Consultez le Secure Client (services client sécurisés) guide de commande : http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf

Le mot-clé **max-other-vpn-limit** spécifie le nombre maximal de sessions VPN autres que les sessions Secure Client (services client sécurisés), de 1 au nombre maximal de sessions autorisées par la licence. Cela inclut le client VPN Cisco (IPsec IKEv1) et les sessions VPN LAN à LAN (IPsec).

Cette limite affecte le pourcentage de charge calculé pour l'équilibrage de charge VPN.

L'exemple suivant montre comment définir une limite maximale de session VPN AnyConnect de 450 :

```
hostname(config)# vpn-sessiondb max-anyconnect-premium-or-essentials-limit 450
hostname(config)#
```

Utiliser la mise à jour du client pour assurer des niveaux de révision acceptables du client IPsec

Remarque Les renseignements de cette section s'appliquent uniquement aux connexions IPsec.

La fonctionnalité de mise à jour du client permet aux administrateurs d'un emplacement central d'aviser automatiquement les utilisateurs du client VPN qu'il est temps de mettre à jour le logiciel client VPN.

Les utilisateurs distants peuvent utiliser des versions logicielles ou matérielles obsolètes du client VPN. Vous pouvez utiliser la commande **client-update** à tout moment pour activer la mise à jour des révisions client, préciser les types et les numéros de révision des clients auxquels la mise à jour s'applique, fournir une URL ou une adresse IP à partir de laquelle obtenir la mise à jour et, dans le cas des clients Windows, aviser éventuellement les utilisateurs qu'ils doivent mettre à jour la version de leur client VPN. Pour les clients Windows, vous pouvez fournir un mécanisme permettant aux utilisateurs d'effectuer cette mise à jour. Cette commande s'applique uniquement au type de groupe de tunnels d'accès à distance IPsec.

Pour effectuer une mise à jour de client, saisissez la commande **client-update** en mode de configuration générale ou en mode de configuration tunnel-group ipsec-attributes. Si le client exécute déjà une version de logiciel dans la liste des numéros de révision, il n'a pas besoin de mettre à jour son logiciel. Si le client n'exécute pas de version logicielle dans la liste, il doit être mis à jour. La procédure suivante explique comment effectuer une mise à jour du client :

Procédure

Étape 1 En mode de configuration globale, activez la mise à jour du client en saisissant cette commande :

```
hostname(config)# client-update enable
hostname(config)#
```

Étape 2 En mode de configuration globale, précisez les paramètres de mise à jour client que vous souhaitez appliquer à tous les clients d'un type particulier. C'est-à-dire préciser le type de client, l'URL ou l'adresse IP à partir desquels obtenir l'image mise à jour, ainsi que le ou les numéros de révision acceptables pour ce client. Vous pouvez spécifier jusqu'à quatre numéros de révision, séparés par des virgules.

Si le numéro de révision du client correspond à l'un des numéros de révision spécifiés, il n'est pas nécessaire de mettre à jour le client. Cette commande spécifie les valeurs de mise à jour de clients pour tous les clients du type spécifié dans l'ensemble de l'ASA.

Utilisez cette syntaxe :

```
hostname(config)# client-update type type url url-string rev-nums rev-numbers
hostname(config)#
```

Les types de clients disponibles sont **win9X** (comprend les plateformes Windows 95, Windows 98 et Windows ME), **winnt** (comprend les plateformes Windows NT 4.0, Windows 2000 et Windows XP), **windows** (comprend toutes les plateformes basées sur Windows).

Si le client exécute déjà une version de logiciel dans la liste des numéros de révision, il n'a pas besoin de mettre à jour son logiciel. Si le client n'exécute pas de version logicielle dans la liste, il doit être mis à jour. Vous pouvez spécifier jusqu'à trois de ces entrées de mise à jour client. Le mot-clé **windows** couvre toutes les plateformes Windows autorisées. Si vous spécifiez **windows**, ne spécifiez pas les types de clients Windows individuels.

Remarque
Pour tous les clients Windows, vous devez utiliser le protocole http:// ou https:// comme préfixe de l'URL.

L'exemple suivant configure les paramètres de mise à jour de client pour le groupe de tunnels d'accès à distance. Il désigne le numéro de révision 4.6.1 et l'URL permettant de récupérer la mise à jour, soit https://support/updates.

```
hostname(config)# client-update type windows url https://support/updates/ rev-nums 4.6.1
hostname(config)#
```

Vous pouvez également configurer la mise à jour client uniquement pour des groupes de tunnels individuels, plutôt que pour tous les clients d'un type particulier. (Consultez l'étape 3.)

Remarque
Vous pouvez faire en sorte que le navigateur lance automatiquement une application en ajoutant le nom de l'application à la fin de l'URL ; par exemple : **https://support/updates/vpnclient.exe.**

Étape 3 Définissez un ensemble de paramètres de mise à jour client pour un groupe de tunnels ipsec-ra particulier.

En mode tunnel-group ipsec-attributes, précisez le nom et le type du groupe de tunnels, l'URL ou l'adresse IP à partir desquels obtenir l'image mise à jour, ainsi qu'un numéro de révision. Si le numéro de révision du client de l'utilisateur correspond à l'un des numéros de révision précisés, il n'est pas nécessaire de mettre à jour le client ; par exemple, pour un client Windows, saisissez cette commande :

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-tunnel-ipsec)# client-update type windows url https://support/updates/
rev-nums 4.6.1
hostname(config-tunnel-ipsec)#
```

Étape 4 (Facultatif) Envoyez un avis aux utilisateurs actifs dont les clients Windows sont obsolètes pour les informer que leur client doit être mis à jour. Pour ces utilisateurs, une fenêtre contextuelle s'affiche et leur offre la possibilité de lancer un navigateur et de télécharger le logiciel mis à jour à partir du site précisé dans l'URL. La seule partie de ce message que vous pouvez configurer est l'URL. (Consultez l'étape 2 ou 3.) Les utilisateurs qui ne sont pas actifs reçoivent un message de notification lors de leur prochaine connexion. Vous pouvez envoyer cet avis à tous les clients actifs de tous les groupes de tunnels, ou aux clients d'un groupe de tunnels particulier. Par exemple, pour aviser tous les clients actifs de tous les groupes de tunnels, saisissez la commande suivante en mode EXEC privilégié :

```
hostname# client-update all
hostname#
```

Si le numéro de révision du client de l'utilisateur correspond à l'un des numéros de révision spécifiés, il n'est pas nécessaire de mettre à jour le client, et aucun message de notification n'est envoyé à l'utilisateur.

Prochaine étape

Remarque Si vous spécifiez le type de mise à jour client comme **windows** (spécifiant toutes les plateformes basées sur Windows) et que vous souhaitez ultérieurement saisir un type de mise à jour client **win9x** ou **winnt** pour la même entité, vous devez d'abord supprimer le type de client Windows avec le **no** de la commande, puis utilisez les nouvelles commandes client-update pour préciser les nouveaux types de clients.

Mettre en œuvre une connexion entre une adresse IP attribuée par NAT et une adresse IP publique

Dans de rares cas, vous pouvez vouloir utiliser l'adresse IP réelle d'un homologue VPN sur le réseau interne au lieu d'une adresse IP locale attribuée. Normalement, avec le VPN, l'homologue reçoit une adresse IP locale attribuée pour accéder au réseau interne. Cependant, vous pouvez vouloir retraduire l'adresse IP locale en adresse IP publique réelle de l'homologue si, par exemple, vos serveurs internes et la sécurité du réseau reposent sur l'adresse IP réelle de l'homologue.

L'ASA a introduit un moyen de traduire l'adresse IP attribuée au client VPN sur le réseau interne/protégé en son adresse IP publique (source). Cette fonctionnalité prend en charge le scénario dans lequel les serveurs et services cibles sur le réseau interne ainsi que la politique de sécurité réseau exigent une communication avec l'adresse IP publique/source du client VPN plutôt qu'avec l'adresse IP attribuée sur le réseau interne de l'entreprise.

Vous pouvez activer cette fonctionnalité sur une interface par groupe de tunnels. Les règles de NAT d'objet sont ajoutées et supprimées dynamiquement lorsque la session VPN est établie ou lorsqu'elle est déconnectée.

En raison de problèmes de routage, nous ne recommandons pas d'utiliser cette fonctionnalité, sauf si vous savez que vous en avez besoin.

- Prend uniquement en charge l'ancien protocole (IKEv1) et Secure Client (services client sécurisés).
- Le trafic de retour vers les adresses IP publiques doit être réacheminé vers l'ASA afin que la politique NAT et la politique VPN puissent être appliquées.
- Prend uniquement en charge les adresses IPv4 attribuées et publiques.
- Plusieurs homologues derrière un périphérique NAT/PAT ne sont pas pris en charge.
- Ne prend pas en charge l'équilibrage de charge (en raison d'un problème de routage).
- Ne prend pas en charge l'itinérance.

Procédure

Étape 1 En mode de configuration globale, saisissez **tunnel general (tunnel général)**.

Étape 2 Utilisez cette syntaxe pour activer la traduction d'adresse :

```
hostname(config-tunnel-general)# nat-assigned-to-public-ip interface
```

Cette commande installe dynamiquement des politiques NAT pour traduire l'adresse IP attribuée en adresse IP publique de la source. L'*interface* détermine où appliquer la NAT.

Étape 3 Utilisez cette syntaxe pour désactiver la traduction d'adresse :

```
hostname(config-tunnel-general)# no nat-assigned-to-public-ip
```

Affichage des politiques de NAT du VPN

La traduction d'adresses utilise les mécanismes NAT de l'objet sous-jacent ; par conséquent, la politique de NAT VPN s'affiche tout comme les politiques de NAT d'objets configurées manuellement. Cet exemple utilise 95.1.226.4 comme adresse IP attribuée et 75.1.224.21 comme adresse IP publique de l'homologue :

```
hostname# show nat
Auto NAT Policies (Section 2)
1 (outside) to (inside) source static _vpn_nat_95.1.226.4 75.1.224.21
    translate_hits = 315, untranslate_hits = 315

prompt# show nat detail

Auto NAT Policies (Section 2)
1 (outside) to (inside) source static _vpn_nat_95.1.226.4 75.1.224.21
    translate_hits = 315, untranslate_hits = 315
    Source - Origin: 95.1.226.4/32, Translated: 75.1.224.21/32
```

Outside est l'interface à laquelle le Secure Client (services client sécurisés) se connecte et *inside* est l'interface spécifique au nouveau groupe de tunnels.

Remarque Comme les politiques de NAT VPN sont dynamiques et non ajoutées à la configuration, les commandes show run object et show run nat sont masquées dans l'objet d'exécution d'affichage et les rapports d'exécution de NAT.

Configurer les limites de session VPN

Vous pouvez exécuter autant de sessions IPsec et SSL que votre plateforme et votre licence ASA en prennent en charge. Pour afficher les renseignements sur la licence, y compris le nombre maximal de sessions pour votre ASA, saisissez la commande **show version** en mode de configuration globale et recherchez la section des licences. L'exemple suivant montre la commande et les renseignements de licence tirés de sa sortie ; le reste de la sortie est expurgé pour plus de clarté.

```
hostname(config)# show version
...
Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 500            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
Encryption-DES                    : Enabled        perpetual
```

```
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 100            perpetual
Carrier                           : Enabled        perpetual
AnyConnect Premium Peers          : 5000           perpetual
AnyConnect Essentials             : 5000           perpetual
Other VPN Peers                   : 5000           perpetual
Total VPN Peers                   : 5000           perpetual
AnyConnect for Mobile             : Enabled        perpetual
AnyConnect for Cisco VPN Phone    : Enabled        perpetual
Advanced Endpoint Assessment      : Enabled        perpetual
Shared License                    : Disabled       perpetual
Total TLS Proxy Sessions          : 3000           perpetual
Botnet Traffic Filter             : Disabled       perpetual
IPS Module                        : Disabled       perpetual
Cluster                           : Enabled        perpetual
Cluster Members                   : 2              perpetual

This platform has an ASA5555 VPN Premium license.
```

Afficher l'allocation des ressources de licence

Utilisez la commande suivante pour afficher l'allocation des ressources :

```
asa2(config)# sh resource allocation
Resource       Total    % of Avail
Conns[rate]    100(U)      0.00%
Inspects[rate] unlimited
Syslogs[rate]  unlimited
Conns          unlimited
Hosts          unlimited
IPsec          unlimited
Mac-addresses  unlimited
ASDM           10          5.00%
SSH            10          10.00%
Telnet         10          10.0%
Xlates         unlimited
AnyConnect     1000        10%
AnyConnectBurst 200        2%
OtherVPN       2000        20%
OtherVPNBurst  1000        10%
```

Afficher l'utilisation des ressources de licence

Utilisez la commande suivante pour afficher l'utilisation des ressources :

Remarque Vous pouvez également utiliser la commande **sh resource usage system controller all 0** pour afficher l'utilisation au niveau du système avec la limite comme limite de la plateforme.

```
ASA(config-ca-trustpoint)# sh resource usage
Resource        Current  Peak  Limit  Denied  Context
Conns           1        16    280000 0       System
Hosts           2        10    N/A    0       System
AnyConnect      2        25    1000   0       cust1
AnyConnectBurst 0        0     200    0       cust1
OtherVPN        1        1     2000   0       cust2
OtherVPNBurst   0        0     1000   0       cust2
```

Limiter les sessions VPN

Pour limiter les sessions VPN AnyConnect (IPsec/IKEv2 ou SSL) à une valeur inférieure à celle autorisée par l'ASA, utilisez la commande **vpn-sessiondb** max-AnyConnect-premium-or-essentials-limit en mode de configuration globale. Pour supprimer la limite de session, utilisez la version **no** de cette commande.

Si la licence ASA autorise 500 sessions VPN SSL et que vous souhaitez limiter le nombre de sessions VPN AnyConnect à 250, saisissez la commande suivante :

```
hostname(config)# vpn-sessiondb max-anyconnect-premium-or-essentials-limit 250
hostname(config)#
```

Pour supprimer la limite de session, utilisez la version **no** de cette commande :

```
hostname(config)# no vpn-sessiondb max-anyconnect-premium-or-essentials-limit 250
hostname(config)#
```

Utilisation d'un certificat d'identité lors de la négociation

L'ASA doit utiliser un certificat d'identité lors de la négociation du tunnel IKEv2 avec Secure Client (services client sécurisés). Pour la configuration du point de confiance d'accès à distance IKEv2, utilisez les commandes suivantes

```
crypto ikev2 remote-access trustpoint <name> [line<number>]
```

L'utilisation de cette commande permet à Secure Client (services client sécurisés) de prendre en charge la sélection de groupe pour l'utilisateur final. Vous pouvez configurer deux points de confiance en même temps : deux RSA, deux ECDSA ou un de chaque. L'ASA analyse la liste des points de confiance configurés et choisit le premier pris en charge par le client. Si ECDSA est préféré, vous devez configurer ce point de confiance avant le point de confiance RSA.

L'option de numéro de ligne spécifie l'endroit dans la ligne où vous souhaitez insérer le point de confiance. En règle générale, cette option est utilisée pour insérer un point de confiance en haut sans supprimer et rajouter l'autre ligne. Si une ligne n'est pas spécifiée, l'ASA ajoute le point de confiance à la fin de la liste.

Si vous essayez d'ajouter un point de confiance qui existe déjà, vous recevez une erreur. Si vous utilisez la commande *no crypto ikev2 remote-access trustpoint* sans préciser le nom de point de confiance à supprimer, toute la configuration de point de confiance est supprimée.

Configurer le pool de cœurs de chiffrement

Vous pouvez modifier l'allocation des cœurs de chiffrement sur les plateformes de traitement multiprocesseur symétrique (SMP) afin d'augmenter le débit du trafic TLS/DTLS de Secure Client (services client sécurisés). Ces modifications peuvent accélérer le chemin de données du VPN SSL et offrir des gains de performance visibles par la clientèle dans Secure Client (services client sécurisés), les tunnels intelligents et le transfert de ports. Ces étapes décrivent la configuration de l'ensemble de cœurs de chiffrement en mode contexte unique ou multiple.

Procédure

Spécifiez comment allouer les processeurs accélérateurs de chiffrement :

crypto engine accelerator-bias

- **équilibré** : distribue également les ressources matérielles de chiffrement (cœurs Admin/SSL et IPsec).
- **ipsec** : alloue les ressources matérielles de chiffrement en vue d'IPsec (y compris le trafic vocal chiffré SRTP).
- **ssl** : alloue les ressources matérielles de chiffrement en faveur d'Admin/SSL. Utilisez ce biais lorsque vous prenez en charge les sessions VPN d'accès à distance Secure Client (services client sécurisés) basées sur SSL.

Exemple :

```
hostname(config)# crypto engine accelerator-bias ssl
```

Configurer la tunnellisation fractionnée dynamique

Avec la tunnellisation fractionnée dynamique, vous pouvez provisionner dynamiquement des exclusions de tunnellisation fractionnée après l'établissement du tunnel, en fonction du nom de domaine DNS de l'hôte. La tunnellisation dynamique fractionnée est configurée en créant un attribut personnalisé et en l'ajoutant à une politique de groupe.

Avant de commencer

Pour utiliser cette fonctionnalité, vous devez avoir AnyConnect version 4.5 (ou ultérieure). Consultez À propos de la tunnellisation fractionnée dynamique pour obtenir plus d'explications.

Procédure

Étape 1 Définissez le type d'attribut personnalisé dans le contexte WebVPN à l'aide de la commande suivante : `anyconnect-custom-attr dynamic-split-exclude-domains description dynamic split exclude domains`

Étape 2 Définissez les noms d'attribut personnalisés pour chaque service en nuage ou Web qui doit être accessible par le client en dehors du tunnel VPN. Par exemple, ajoutez Google_domains pour représenter une liste de noms de domaine DNS relatifs aux services Web de Google. La valeur de l'attribut contient la liste des noms de domaine à exclure du tunnel VPN et doit être au format CSV (valeurs séparées par des virgules), comme suit : `anyconnect-custom-data dynamic-split-exclude-domains webex.com, webexconnect.com, tags.tiqcdn.com`

Étape 3 Associez l'attribut personnalisé défini précédemment à une stratégie de groupe à l'aide de la commande suivante, exécutée dans le contexte des attributs de stratégie de groupe : `anyconnect-custom dynamic-split-exclude-domains value webex_service_domains`

Prochaine étape

Si la tunnellisation d'inclusion fractionnée est configurée, une exclusion de fractionnement dynamique est appliquée uniquement si au moins une des adresses IP de réponse DNS fait partie du réseau d'inclusion fractionnée. S'il n'y a aucun chevauchement entre les adresses IP des réponses DNS et les réseaux de la liste d'inclusion fractionnée, il n'est pas nécessaire d'appliquer l'exclusion dynamique, car le trafic correspondant à toutes les adresses IP renvoyées par DNS est déjà exclu de la tunnellisation.

Configuration du tunnel VPN de gestion

Un tunnel VPN de gestion assure la connectivité au réseau d'entreprise chaque fois que le système client est sous tension, pas seulement lorsqu'une connexion VPN est établie par l'utilisateur final. Vous pouvez effectuer la gestion des correctifs sur les terminaux hors du bureau, notamment les périphériques rarement connectés par l'utilisateur, via VPN, au réseau d'entreprise. Les scripts de connexion du système d'exploitation des terminaux qui nécessitent une connectivité au réseau d'entreprise en bénéficieront également.

Le tunnel VPN de gestion est censé être transparent pour l'utilisateur final ; par conséquent, le trafic réseau initié par les applications des utilisateurs n'est pas touché par défaut, mais est plutôt acheminé à l'extérieur du tunnel VPN de gestion.

Si un utilisateur se plaint de connexions lentes, cela peut indiquer que le tunnel de gestion n'a pas été configuré correctement. Consultez le Guide d'administration de Cisco Secure Client pour connaître les exigences supplémentaires, les incompatibilités, les limites et le dépannage du tunnel VPN de gestion.

Avant de commencer

Nécessite AnyConnect version 4.7 (ou ultérieure)

Procédure

Étape 1 Ajoutez le profil téléchargé (profileMgmt) à la stratégie de groupe (MgmtTunGrpPolicy) mappée au groupe de tunnels utilisé par la connexion du tunnel de gestion :

Pour indiquer que le profil est le profil VPN de gestion AnyConnect, incluez **type vpn-mgmt** dans la commande **anyconnect profiles**. Un profil VPN AnyConnect normal est de type utilisateur.

```
group-policy MgmtTunGrpPolicy attributes
  webvpn
     anyconnect profiles value profileMgmt type vpn-mgmt
```

Étape 2 Pour déployer le profil VPN de gestion par le biais de la connexion du tunnel de l'utilisateur, ajoutez le profil chargé *(profileMgmt)* à la stratégie de groupe *(DfltGrpPolicy)* mappée au groupe de tunnels utilisé par la connexion du tunnel de l'utilisateur :

```
group-policy DfltGrpPolicy attributes
```

```
webvpn
   anyconnect profiles value profileMgmt type vpn-mgmt
```

Affichage des sessions VPN actives

Les rubriques suivantes expliquent comment afficher les informations de session VPN.

Affichage des sessions actives Secure Client (services client sécurisés) par type d'adresse IP

Pour afficher les sessions Secure Client (services client sécurisés) actives à l'aide de l'interface de ligne de commande, saisissez la commande **show vpn-sessiondb anyconnect filter p-ipversion** ou **show vpn-sessiondb anyconnect filter a-ipversion** en mode d'exécution privilégié.

- Affichez les sessions actives Secure Client (services client sécurisés) qui sont filtrées en fonction de l'adresse publique IPv4 ou IPv6 du terminal. L'adresse publique est l'adresse attribuée au terminal par l'entreprise.

  show vpn-sessiondb anyconnect filter p-ipversion {v4 | v6}

- Affichez les sessions actives Secure Client (services client sécurisés) qui sont filtrées en fonction de l'adresse IPv4 ou IPv6 attribuée au terminal. L'adresse attribuée est l'adresse attribuée au Secure Client (services client sécurisés) par l'ASA.

  show vpn-sessiondb anyconnect filter a-ipversion {v4 | v6}

Exemple de sortie de la commande show vpn-sessiondb anyconnect filter p-ipversion [v4 | v6]

```
hostname(config)# show vpn-sessiondb anyconnect filter p-ipversion v4

Session Type: AnyConnect

Username     : user1                  Index        : 40
Assigned IP  : 192.168.17.10          Public IP    : 198.51.100.1
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1
Bytes Tx     : 10570                  Bytes Rx     : 8085
Group Policy : GroupPolicy_SSLACCLIENT
Tunnel Group : SSLACCLIENT
Login Time   : 15:17:12 UTC Mon Oct 22 2012
Duration     : 0h:00m:09s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

Sortie de la commande show vpn-sessiondb anyconnect filter a-ipversion [v4 | v6]

```
hostname(config)# show vpn-sessiondb anyconnect filter a-ipversion v6

Session Type: AnyConnect

Username     : user1                  Index        : 45
Assigned IP  : 192.168.17.10
Public IP    : 2001:DB8:8:1:90eb:3fe5:9eea:fb29
Assigned IPv6: 2001:DB8:9:1::24
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1
Bytes Tx     : 10662                  Bytes Rx     : 17248
Group Policy : GroupPolicy_SSL_IPv6   Tunnel Group : SSL_IPv6
Login Time   : 17:42:42 UTC Mon Oct 22 2012
Duration     : 0h:00m:33s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

Affichage des sessions VPN de site à site actives par type d'adresse IP

Pour afficher les sessions VPN de site à site actives à l'aide de l'interface de ligne de commande, saisissez la commande **show vpn-sessiondb l2l filter ipversion** en mode d'exécution privilégié.

Cette commande affiche les sessions VPN de site à site actives filtrées en fonction de l'adresse publique IPv4 ou IPv6 de la connexion.

L'adresse publique est l'adresse attribuée au terminal par l'entreprise.

```
show vpn-sessiondb l2l filter ipversion {v4 | v6}
```

À propos de l'application des politiques ISE :

Cisco Identity Services Engine (ISE) est une plateforme de gestion et de contrôle des politiques de sécurité. Il automatise et simplifie le contrôle d'accès et la conformité de sécurité pour la connectivité filaire, sans fil et VPN. Cisco ISE est principalement utilisé pour fournir un accès sécurisé et l'accès des invités, prendre en charge les projets BYOD (Bring Your Own Device) et appliquer les politiques d'utilisation en collaboration avec Cisco TrustSec.

La fonctionnalité Change of Authorization (CoA) d'ISE fournit un mécanisme permettant de modifier les attributs d'une session d'authentification, d'autorisation et de comptabilité (AAA) après son établissement. Lorsqu'une politique est modifiée pour un utilisateur ou un groupe d'utilisateurs dans AAA, des paquets CoA peuvent être envoyés directement à l'ASA depuis l'ISE pour réinitialiser l'authentification et appliquer la nouvelle politique. Un point d'application de posture en ligne (IPEP) n'est pas nécessaire pour appliquer les listes de contrôle d'accès (ACL) à chaque session VPN établie avec l'ASA.

L'application des politiques ISE est prise en charge sur les clients VPN suivants :

- IPSec
- Secure Client (services client sécurisés)
- L2TP/IPSec

Remarque Certains éléments de politique tels que l'ACL dynamique (dACL) et la balise de groupe de sécurité (SGT) sont pris en charge, alors que les éléments de politique tels que l'affectation de VLAN et l'affectation d'adresses IP ne sont pas pris en charge.

Le flux du système est le suivant :

1. Un utilisateur final demande une connexion VPN.
2. L'ASA authentifie l'utilisateur auprès de l'ISE et reçoit une liste de contrôle d'accès d'utilisateur qui fournit un accès limité au réseau.
3. Un message de début de comptabilité est envoyé à l'ISE pour enregistrer la session.
4. L'évaluation de la posture se produit directement entre l'agent NAC et l'ISE. Ce processus est transparent pour l'ASA.
5. L'ISE envoie une mise à jour de politique à l'ASA au moyen d'un « policy push » CoA. Cela identifie une nouvelle ACL utilisateur qui fournit des privilèges d'accès réseau accrus.

Remarque Des évaluations de politiques supplémentaires peuvent se produire pendant la durée de vie de la connexion, de manière transparente pour l'ASA, par le biais des mises à jour ultérieures de CoA.

Ce modèle de flux diffère de la plupart des scénarios qui utilisent RADIUS CoA. Pour les authentifications 802.1x filaires ou sans fil, RADIUS CoA n'inclut aucun attribut. Il déclenche uniquement la deuxième authentification dans laquelle tous les attributs, tels que DACL, sont associés. Pour la posture VPN ASA, il n'y a pas de deuxième authentification. Tous les attributs sont retournés dans le RADIUS CoA. La session VPN est active et il est impossible de modifier la plupart des paramètres utilisateur VPN. Les seuls paramètres qui peuvent être modifiés par une activation CoA sont RedirectURL, RedirectACL et la balise de groupe de sécurité (SGT).

Configurer les groupes de serveurs RADIUS pour l'application des politiques ISE

Pour permettre l'évaluation et l'application des politiques ISE, configurez un groupe de serveurs RADIUS AAA pour les serveurs ISE et ajoutez les serveurs au groupe. Lorsque vous configurez le groupe de tunnels pour le VPN, vous spécifiez ce groupe de serveurs pour les services AAA dans le groupe.

Procédure

Étape 1 Créez le groupe de serveurs AAA RADIUS.

aaa-server *group_name* **protocol radius**

```
hostname(config)# aaa-server servergroup1 protocol radius
hostname(config-aaa-server-group)#
```

Étape 2 Activez les services d'autorisation dynamique RADIUS (CoA) pour le groupe de serveurs AAA.

dynamic-authorization [**port** *number*]

La définition d'un port est facultative. La valeur par défaut est 1700, la plage est comprise entre 1024 et 65535.

Lorsque vous utilisez le groupe de serveurs dans un tunnel VPN, le groupe de serveurs RADIUS sera enregistré pour la notification CoA et l'ASA écoutera le port pour détecter les mises à jour de politique CoA d'ISE.

```
hostname(config-aaa-server-group)# dynamic-authorization
```

Étape 3 Si vous ne souhaitez pas utiliser ISE pour l'authentification, activez le mode d'autorisation seulement pour le groupe de serveurs RADIUS.

authorize-only

Cela indique que lorsque ce groupe de serveurs est utilisé pour l'autorisation, le message de demande d'accès RADIUS sera généré en tant que demande « Autorize Only » (Autorisation uniquement), par opposition aux méthodes de mot de passe configurées pour le serveur AAA. Si vous configurez un mot de passe commun à l'aide de la commande **radius-common-pw** pour le serveur RADIUS, il sera ignoré.

Par exemple, vous utiliserez le mode d'autorisation seulement si vous souhaitez utiliser des certificats pour l'authentification plutôt que ce groupe de serveurs. Vous utiliserez toujours ce groupe de serveurs pour l'autorisation et la gestion de comptes dans le tunnel VPN.

```
hostname(config-aaa-server-group)# authorize-only
```

Étape 4 Activez la génération périodique de messages RADIUS interim-accounting-update.

interim-accounting-update [**periodic** [*hours*]]

ISE gère un répertoire des sessions actives en fonction des enregistrements de traçabilité qu'il reçoit des périphériques NAS comme l'ASA. Cependant, si ISE ne reçoit aucune indication que la session est toujours active (message de traçabilité ou transactions de posture) pendant une période de 5 jours, il supprimera l'enregistrement de session de sa base de données. Pour vous assurer que les connexions VPN de longue durée ne sont pas supprimées, configurez le groupe pour envoyer des messages interim-accounting-update périodiques à ISE pour toutes les sessions actives.

- **periodic** [*hours*] permet la génération et la transmission périodiques des enregistrements de comptabilité pour chaque session VPN configurée pour envoyer des enregistrements de comptabilité au groupe de serveurs en question. Vous pouvez éventuellement inclure l'intervalle, en heures, pour l'envoi de ces mises à jour. La valeur par défaut est de 24 heures, la plage est comprise entre 1 et 120.
- (Aucun paramètre.) Si vous utilisez cette commande sans le mot clé **periodic**, l'ASA envoie des messages interim-accounting-update uniquement lorsqu'une connexion de tunnel VPN est ajoutée à une session VPN sans client. Lorsque cela se produit, la mise à jour de comptabilité est générée afin d'informer le serveur RADIUS de la nouvelle adresse IP attribuée.

```
hostname(config-aaa-server-group)# interim-accounting-update periodic 12
```

Étape 5 (Facultatif) Fusionnez une ACL téléchargeable avec l'ACL reçue dans la paire AV de Cisco à partir d'un paquet RADIUS.

merge-dacl {**before-avpair** | **after-avpair**}

Cette option s'applique uniquement aux connexions VPN. Pour les utilisateurs de VPN, les ACL peuvent prendre la forme d'ACL de paire attribut/valeur de Cisco, d'ACL téléchargeables et d'une ACL configurée sur l'ASA. Cette option détermine si l'ACL téléchargeable et l'ACL de la paire attribut/valeur sont fusionnées, et ne s'applique à aucune ACL configurée sur l'ASA.

Le paramètre par défaut est **no merge dacl**, ce qui indique que les ACL téléchargeables ne seront pas fusionnées avec les ACL de paire attribut/valeur de Cisco. Si une paire AV et une ACL téléchargeable sont reçues, la paire AV a la priorité et est utilisée.

L'option **before-avpair** signifie que les entrées d'ACL téléchargeables doivent être placées avant les entrées de la paire d'AV de Cisco.

L'option **after-avpair** signifie que les entrées d'ACL téléchargeables doivent être placées après les entrées de la paire d'AV de Cisco.

```
hostname(config)# aaa-server servergroup1 protocol radius
hostname(config-aaa-server-group)# merge-dacl before-avpair
```

Étape 6 (Facultatif) Précisez le nombre maximum de demandes envoyées à un serveur RADIUS du groupe avant d'essayer le serveur suivant.

max-failed-attempts *nombre*

La plage se situe entre 1 et 5. La valeur par défaut est de 3.

Si vous avez configuré une méthode de secours à l'aide de la base de données locale (pour l'accès de gestion uniquement), et que tous les serveurs du groupe ne répondent pas, le groupe est considéré comme ne répondant pas et la méthode de secours est essayée. Le groupe de serveurs reste marqué comme ne répondant pas pendant une période de 10 minutes (par défaut), de sorte que les demandes AAA supplémentaires effectuées dans cette période ne résultent pas en une tentative d'entrer en contact avec le groupe de serveurs et que la méthode de secours est utilisée immédiatement. Pour modifier la période de non-réponse par défaut, consultez la commande **reactivation-mode** à l'étape suivante.

Si vous n'avez pas de méthode de secours, l'ASA continue de réessayer les serveurs du groupe.

```
hostname(config-aaa-server-group)# max-failed-attempts 2
```

Étape 7 (Facultatif) Précisez la méthode (politique de réactivation) par laquelle les serveurs défaillants d'un groupe sont réactivés.

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

Lieu :

- **depletion** [**deadtime** *minutes*] réactive les serveurs défaillants seulement après que tous les serveurs du groupe sont inactifs. Il s'agit du mode de réactivation par défaut. Vous pouvez préciser la durée, entre 0 et 1 440 minutes, qui s'écoule entre la désactivation du dernier serveur du groupe et la réactivation ultérieure de tous les serveurs. La valeur par défaut est 10 minutes.
- **timed** réactive les serveurs défaillants après 30 secondes de temps d'arrêt.

```
hostname(config-aaa-server-group)# reactivation-mode deadtime 20
```

Étape 8 (Facultatif) Envoyez des messages de traçabilité à tous les serveurs du groupe.

accounting-mode simultaneous

Pour rétablir la valeur par défaut d'envoi de messages uniquement au serveur actif, saisissez la commande **accounting-mode single**.

```
hostname(config-aaa-server-group)# accounting-mode simultaneous
```

Étape 9 Ajoutez les serveurs ISE RADIUS au groupe.

aaa-server *group_name* [(*interface_name*)] **host** {*server_ip* | *name*} [*key*]

Lieu :

- *group_name* est le nom du groupe de serveurs RADIUS.
- (*interface_name*) est le nom de l'interface par laquelle le serveur est accessible. La valeur par défaut est (inside). Les parenthèses sont obligatoires.
- **host** {*server_ip* | *name*} est l'adresse IP ou le nom d'hôte du serveur ISE RADIUS.
- *key* est la clé facultative pour chiffrer la connexion. Vous pouvez plus facilement saisir cette clé dans la commande **key** après être passé en mode aaa-server-host. Si vous ne configurez pas de clé, la connexion n'est pas chiffrée (texte en clair). La clé est une chaîne alphanumérique sensible à la casse pouvant comporter jusqu'à 127 caractères, ce qui correspond à la même valeur que la clé sur le serveur RADIUS.

Vous pouvez ajouter plusieurs serveurs au groupe.

```
hostname(config)# aaa-server servergroup1 (inside) host 10.1.1.3
hostname(config-aaa-server-host)# key sharedsecret
hostname(config-aaa-server-host)# exit
```

Exemples de configuration pour l'application de la politique ISE

Configurer le tunnel VPN pour l'authentification dynamique ISE avec des mots de passe

L'exemple suivant montre comment configurer un groupe de serveurs ISE pour les mises à jour d'autorisation dynamique (CoA) et la comptabilité périodique horaire. La configuration du groupe de tunnels qui configure l'authentification par mot de passe avec ISE est incluse.

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

Configurer le tunnel VPN pour l'autorisation ISE uniquement

L'exemple suivant montre comment configurer un groupe de tunnels pour la validation et l'autorisation des certificats locaux avec ISE. Incluez la commande authorize-only dans la configuration du groupe de serveurs, car le groupe de serveurs ne sera pas utilisé pour l'authentification.

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

Dépannage de l'application des politiques

Les commandes suivantes peuvent être utilisées pour le débogage.

Pour suivre l'activité CoA :

```
debug radius dynamic-authorization
```

Pour suivre la fonctionnalité d'URL de redirection :

```
debug aaa url-redirect
```

Pour afficher les règles de classification NP correspondant à la fonctionnalité de redirection d'URL :

```
show asp table classify domain url-redirect
```

Configurer les paramètres avancés SSL

L'ASA utilise le protocole SSL (Secure Sockets Layer) et le protocole TLS (Transport Layer Security) pour prendre en charge la transmission sécurisée des messages pour ASDM, Clientless SSL VPN, VPN et les sessions basées sur le navigateur. L'ASA prend en charge les protocoles SSLv3, TLSv1, TLv1.1, TLSv1.2, et TLSv1.3 pour les connexions VPN et de gestion basées sur SSL. En outre, DTLS est utilisé pour les connexions du client VPN AnyConnect

Les suites de chiffrement suivantes sont prises en charge, comme indiqué :

Chiffre	TLSv1.1 / DTLS V1	TLSv1.2 / DTLSV 1.2	TLSv1.3
TLS_AES_128_GCM_SHA256	Non	Non	Oui
TLS_CHACHA20_POLY1305_SHA256	Non	Non	Oui

Chiffre	TLSv1.1 / DTLS V1	TLSv1.2 / DTLSV 1.2	TLSv1.3
TLS_AES_256_GCM_SHA384	Non	Non	Oui
AES128-GCM-SHA256	Non	Oui	Non
AES128-SHA	Oui	oui	Non
AES128-SHA256	Non	Oui	Non
AES256-GCM-SHA384	Non	Oui	Non
AES256-SHA	Oui	oui	Non
AES256-SHA256	Non	Oui	Non
DERS-CBC-SHA	Non	Non	Non
DES-CBC-SHA	Oui	oui	Non
DHE-RSA-AES128-GCM-SHA256	Non	Oui	Non
DHE-RSA-AES128-SHA	Oui	oui	Non
DHE-RSA-AES128-SHA256	Non	Oui	Non
DHE-RSA-AES256-GCM-SHA384	Non	l	Non
DHE-RSA-AES256-SHA	Oui	oui	Non
ECDHE-ECDSA-AES128-GCM-SHA256	Non	Oui	Non
ECDHE-ECDSA-AES128-SHA256	Non	Oui	Non
ECDHE-ECDSA-AES256-GCM-SHA384	Non	Oui	Non
ECDHE-ECDSA-AES256-SHA384	Non	Oui	Non
ECDHE-RSA-AES128-GCM-SHA256	Oui	oui	Non
ECDHE-RSA-AES128-SHA256	Non	Oui	Non
ECDHE-RSA-AES256-GCM-SHA384	Non	Oui	Non
ECDHE-RSA-AES256-SHA384	Non	Oui	Non
NULL-SHA	Non	Non	Non
RC4-MD5	Non	Non	Non
RC4-SHA	Non	Non	Non

Remarque Pour la version 9.4(1), tous les mots-clés SSLv3 ont été supprimés de la configuration ASA et la prise en charge SSLv3 a été supprimée de l'ASA. Si SSLv3 est activé, une erreur de démarrage s'affichera à partir de la commande avec l'option SSLv3. L'ASA reviendra ensuite à l'utilisation par défaut de TLSv1.

Le récepteur mobile Citrix peut ne pas prendre en charge les protocoles TLS 1.1/1.2 ; consultez https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-receiver-feature-matrix.pdf pour la compatibilité

Pour spécifier la version minimale du protocole pour laquelle l'ASA négociera les connexions SSL/TLS et DTLS, procédez comme suit :

Procédure

Étape 1 Définissez la version de protocole minimale pour laquelle l'ASA négociera une connexion.

ssl server-version [**tlsv1** | **tlsv1.1** | **tlsv1.2** | **tlsv1.3**] [**dtlsv1** | **dtlsv1.2**]

Lieu :

- **tlsv1** : saisissez ce mot-clé pour accepter les ClientHellos SSLv2 et négocier TLSv1 (ou supérieur)
- **tlsv1.1** : saisissez ce mot-clé pour accepter les ClientHellos SSLv2 et négocier TLSv1.1 (ou supérieur)
- **tlsv1.2** : saisissez ce mot-clé pour accepter les ClientHellos SSLv2 et négocier TLSv1.2 (ou supérieur)
- **tlsv1.3** : saisissez ce mot-clé pour accepter les ClientHellos SSLv2 et négocier TLSv1.3 (ou supérieur)
- **dtlsv1** : saisissez ce mot-clé pour accepter les ClientHellos DTLSv1 et négocier DTLSv1 (ou supérieur)
- **dtlsv1.2** : saisissez ce mot-clé pour accepter les messages client hello DTLSv1.2 et négocier DTLSv1.2 (ou version supérieure)

Remarque
La configuration et l'utilisation de DTLS s'appliquent uniquement aux connexions d'accès à distance Secure Client (services client sécurisés).

Assurez-vous que la session TLS est aussi sécurisée ou plus sécurisée que la session DTLS en utilisant une version de TLS égale ou supérieure à DTLS. Compte tenu de cela, tlsv1.2 est la seule version TLS acceptable lors du choix de dtls1.2 ; et toute version TLS peut être utilisée avec dtls1, car elles sont toutes égales ou supérieures à DTLS 1.0.

Exemple :

Exemples :

```
hostname(config)# ssl server-version tlsv1.1

hostname(config)# ssl server-version tlsv1.2 dtlsv1.2
```

Étape 2 Spécifiez la version maximale du protocole SSL/TLS que l'ASA utilise lorsqu'il agit comme serveur.

ssl server-max-version [**tlsv1** | **tlsv1.1** | **tlsv1.2** | **tlsv1.3**]

Si server-max-version est configuré à TLSV1.2, vous ne pourrez pas configurer TLSV1.3 comme server-version.

Étape 3 Spécifiez la version du protocole SSL/TLS que l'ASA utilise lorsqu'il agit comme client.

ssl client-version [**tlsv1** | **tlsv1.1** | **tlsv1.2** | **tlsv1.3**]

Lieu :

- **tlsv1** : saisissez ce mot-clé pour spécifier que l'ASA transmet les messages client hello TLSv1 et négocie TLSv1 (ou version supérieure).
- **tlsv1.1** : saisissez ce mot-clé pour spécifier que l'ASA transmet les messages client hello TLSv1.1 et négocie TLSv1.1 (ou version supérieure).
- **tlsv1.2** : saisissez ce mot-clé pour spécifier que l'ASA transmet les messages client hello TLSv1.2 et négocie TLSv1.2 (ou version supérieure).
- **tlsv1.3** : saisissez ce mot-clé pour spécifier que l'ASA transmet les messages client hello TLSv1.3 et négocie TLSv1.3 (ou version supérieure).

DTLS n'est pas disponible pour le rôle de client SSL.

Exemple :

Exemples :

```
hostname(config)# ssl client-version tlsv1
```

Étape 4 Spécifiez la version maximale du protocole SSL/TLS que l'ASA utilise lorsqu'il agit comme client.

ssl client-max-version [**tlsv1** | **tlsv1.1** | **tlsv1.2** | **tlsv1.3**]

Si client-max-version est configuré à TLSV1.2, vous ne pourrez pas configurer TLSV1.3 comme client-version.

Étape 5 Précisez les algorithmes des suites de chiffrement pour les protocoles SSL, DTLS et TLS.

ssl cipher *version* [*level* | **custom** *string*]

Lieu :

- L'argument *version* spécifie la version du protocole SSL, DTLS ou TLS. Versions prises en charge :
  - default : ensemble des suites de chiffrement pour les connexions sortantes.
  - dtlsv1 : suites de chiffrement pour les connexions entrantes DTLSv1.
  - dtlsv1.2 : suites de chiffrement pour les connexions entrantes DTLSv1.2.
  - tlsv1 : suites de chiffrement pour les connexions entrantes TLSv1.
  - tlsv1.1 : suites de chiffrement pour les connexions entrantes TLSv1.1.
  - tlsv1.2 : suites de chiffrement pour les connexions entrantes TLSv1.2.
  - tlsv1.3 : suites de chiffrement pour les connexions entrantes TLSv1.3.
- L'argument *level* précise la robustesse des suites de chiffrement et indique le niveau minimal configuré. Les valeurs valides, par ordre croissant de robustesse, sont les suivantes :
  - all : comprend toutes les suites de chiffrement.

- low : comprend toutes les suites de chiffrement, sauf NULL-SHA.
- medium (il s'agit du paramètre par défaut pour toutes les versions de protocole) : comprend toutes les suites de chiffrement (sauf NULL-SHA, DES-CBC-SHA, RC4-MD5, RC4-SHA, et DES-CBC3-SHA).
- fips : comprend toutes les suites de chiffrement conformes à FIPS (sauf NULL-SHA, DES-CBC-SHA, RC4-MD5, RC4-SHA, et DES-CBC3-SHA).
- high(s'applique uniquement à TLSv1.2 et TLSv1.3) : comprend uniquement AES-256 avec chiffrements SHA-2 pour TLSv1.2. La robustesse de toutes les suites de chiffrement TLSv1.3 est élevée.

- Le fait de spécifier l'option **custom***string* vous permet d'exercer un contrôle total sur la suite de chiffrement à l'aide des chaînes de définition de chiffrement OpenSSL. Pour en savoir plus, consultez https://www.openssl.org/docs/apps/ciphers.html.

Le paramètre recommandé est **medium**. L'utilisation de **high** peut limiter la connectivité. L'utilisation de custom peut limiter les fonctionnalités si seulement quelques suites de chiffrement sont configurées. Le fait de restreindre la valeur custom par défaut limite la connectivité sortante, y compris la mise en grappe.

L'ASA spécifie l'ordre de priorité des chiffrements pris en charge. Consultez la référence de commande pour en savoir plus.

Cette commande remplace la commande ssl encryption, qui est déconseillée depuis la version 9.3(2).

Étape 6 Autorisez plusieurs points de confiance sur une seule interface.

ssl trust-point *name* [[**interface** *vpnlb-ip*] | [**domain** *domain-name*]

```
hostname(config)# ssl trust-point www-cert domain www.example.com
```

L'argument **name** spécifie le nom du point de confiance. L'argument **interface** spécifie le nom de l'interface sur laquelle un point de confiance est configuré. Le mot-clé vpnlb-ip s'applique uniquement aux interfaces et associe ce point de confiance à l'adresse IP du cluster d'équilibrage de charge VPN sur cette interface. La paire mot-clé-argument **domain***domain-name* spécifie un point de confiance associé à un nom de domaine particulier utilisé pour accéder à l'interface.

Vous pouvez configurer jusqu'à 16 points de confiance par interface.

Si vous ne précisez ni interface ni domaine, cette commande crée le point de confiance de secours pour toutes les interfaces qui n'ont pas de point de confiance configuré.

Si vous saisissez la commande **ssl trustpoint ?**, les points de confiance configurés disponibles s'affichent. Si vous saisissez la commande **ssl trust-point** *name* **?** (par exemple, **ssl trust-point mysslcert ?**), les interfaces configurées disponibles pour l'association entre le point de confiance et le certificat SSL s'affichent.

Suivez ces consignes lorsque vous utilisez cette commande :

- La valeur du point de confiance doit être le nom du point de confiance de l'autorité de certification tel qu'il est configuré dans la commande **crypto ca trustpoint name**.
- La valeur de interface doit être le nom nameif d'une interface préalablement configurée.
- La suppression d'un point de confiance supprime également toutes les entrées **ssl trust-point** qui font référence à ce point de confiance.

- Vous pouvez avoir une entrée ssl trust-point pour chaque interface et une entrée qui ne spécifie aucune interface.
- Vous pouvez réutiliser le même point de confiance pour plusieurs entrées.
- Un point de confiance configuré avec le mot-clé domain peut s'appliquer à plusieurs interfaces (selon la façon dont vous vous connectez).
- Vous ne pouvez avoir qu'un seul **ssl trust-point** par valeur *domain-name*.
- Si l'erreur suivante s'affiche après avoir saisi cette commande :

```
error:0B080074:x509 certificate routines:X509_check_private_key:key values
mismatch@x509_cmp.c:339
```

  Cela signifie qu'un utilisateur a configuré un nouveau certificat pour remplacer un certificat précédemment configuré. Vous n'avez rien à faire.
- Les certificats sont choisis dans l'ordre suivant :
  - Si une connexion correspond à la valeur du mot-clé **domain**, ce certificat est choisi en premier. (commande **ssl trust-point***name***domain***domain-name*)
  - Si une connexion est établie à l'adresse d'équilibrage de charge, le certificat vpnlb-ip est choisi. (**ssl trust-point** *name* **interface** *vpnlb-ip* command)
  - Le certificat configuré pour l'interface. (**ssl trust-point** *name* interface command)
  - Le certificat par défaut n'est pas associé à une interface. **ssl trust-point** *name*
  - Le certificat autosigné et autogénéré de l'ASA.

Étape 7 Précisez le groupe DH à utiliser avec les suites de chiffrement DHE-RSA utilisées par TLS.

```
ssl dh-group [group14 | group15]

hostname(config)# ssl dh-group group14
```

Le mot-clé group14 et group15configure le groupe DH 14 (module de 2 048 bits, sous-groupe d'ordre premier de 224 bits).

Le groupe 14 n'est pas compatible avec Java 7. Tous les groupes sont compatibles avec Java 8. Le groupe 14 est conforme à la norme FIPS. La valeur par défaut est ssl dh-group group14.

Étape 8 Précisez le groupe à utiliser avec les suites de chiffrement ECDHE-ECDSA utilisées par TLS.

```
ssl ecdh-group [group19 | group20 | group21]

hostname(config)# ssl ecdh-group group20
```

Le mot-clé group19 configure le groupe 19 (EC 256 bits). Le mot-clé group20 configure le groupe 20 (EC de 384 bits). Le mot-clé group21 configure le groupe 21 (EC 521 bits).

La valeur par défaut est ssl ecdh-group group19.

Remarque

Les chiffrements ECDSA et DHE ont la priorité la plus élevée.

Prochaine étape

Vous pouvez utiliser les commandes suivantes pour afficher la configuration TLS/DTLS :

- **show run ssl** s'il ne s'agit pas de la version TLS/DTLS par défaut.
- **show run ssl all** s'il s'agit de la version TLS/DTLS par défaut.

Flux persistants tunnelisés IPsec

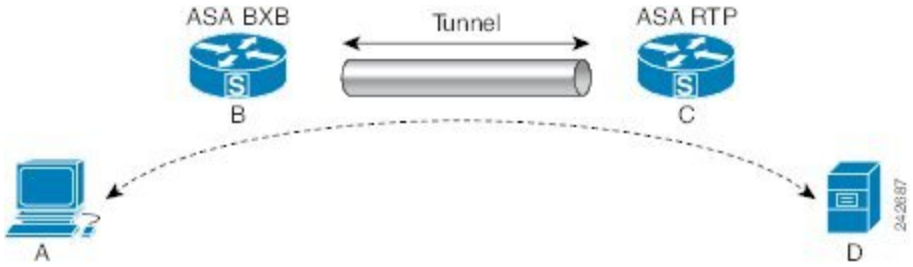
Dans les réseaux exécutant une version du logiciel ASA antérieure à la version 8.0.4, les flux de trafic IPsec LAN à LAN ou TCP d'accès à distance traversant un tunnel IPsec sont abandonnés lorsque le tunnel tombe. Les flux sont recréés au besoin lorsque et si le tunnel est de nouveau disponible. Cette politique fonctionne bien du point de vue de la gestion des ressources et de la sécurité. Cependant, dans certains cas, ce comportement peut poser problème pour les utilisateurs, en particulier pour ceux qui migrent d'environnements PIX vers des environnements ASA uniquement et pour les applications TCP héritées qui ne redémarrent pas facilement, ou dans les réseaux comprenant des passerelles qui ont tendance à interrompre fréquemment les tunnels. (Consultez CSCsj40681 et CSCsi47630 pour en savoir plus.)

La fonctionnalité de flux de tunnel IPsec persistant résout ce problème. Avec cette fonctionnalité activée, l'ASA conserve et reprend les flux tunnelisés avec état (TCP). Tous les autres flux sont abandonnés lorsque le tunnel tombe et doivent se rétablir lorsqu'un nouveau tunnel apparaît.

Remarque Cette fonctionnalité prend en charge les tunnels IPsec LAN à LAN et les tunnels d'accès à distance IPsec fonctionnant en mode Network-Extension. Il ne prend pas en charge les tunnels d'accès à distance IPsec ou AnyConnect/SSL.

L'exemple suivant montre le fonctionnement de la fonctionnalité de flux persistants de tunnellisation IPsec.

Illustration 2 : Scénario de réseau



Dans cet exemple, les réseaux BXB et RTP sont connectés via un tunnel sécurisé LAN à LAN par une paire d'équipements de sécurité. Un ordinateur dans le réseau BXB exécute un transfert FTP à partir d'un serveur dans le réseau RTP par l'intermédiaire du tunnel sécurisé. Dans ce scénario, supposons que, pour une raison quelconque, le tunnel soit abandonné après que le PC se soit connecté au serveur et ait lancé le transfert. Bien que le tunnel soit rétabli puisque les données tentent toujours de circuler, le transfert FTP ne se termine pas. L'utilisateur doit mettre fin au transfert et recommencer en se connectant au serveur. Toutefois, si la

fonctionnalité de flux de tunnel IPsec persistants est activée, tant que le tunnel est recréé dans l'intervalle de temporisation, les données continuent de circuler correctement dans le nouveau tunnel, car les équipements de sécurité conservent l'état de ce flux.

Scénario

Les sections suivantes décrivent les situations de flux de données pour un tunnel abandonné et récupéré, d'abord avec la fonctionnalité des flux persistants de tunnellisation IPsec désactivée, puis avec la fonctionnalité activée. Dans les deux cas, reportez-vous à la figure précédente pour une illustration du réseau. Dans cette illustration :

- Le flux B-C définit le tunnel et transporte les données ESP chiffrées.
- Le flux A-D est la connexion TCP du transfert FTP et traverse le tunnel défini par le flux B-C. Ce flux contient également des informations d'état utilisées par le pare-feu pour inspecter ce flux TCP/FTP. Les informations sur l'état sont essentielles et sont constamment mises à jour par le pare-feu à mesure que le transfert progresse.

Remarque Les flux inverses dans chaque direction sont omis pour des raisons de simplicité.

Flux persistants de tunnellisation IPsec désactivés

Lorsque le tunnel LAN à LAN tombe, le flux A-D et le flux B-C et toutes les informations d'état leur appartenant sont supprimées. Par la suite, le tunnel est rétabli et le flux B-C est recréé et peut reprendre le transport des données tunnelisées. Mais le flux TCP/FTP A-D rencontre des problèmes. Comme les informations d'état décrivant le flux jusqu'à ce stade du transfert FTP ont été supprimées, le pare-feu avec état bloque les données FTP en transit et rejette la création du flux A-D. Ayant perdu l'historique de l'existence même de ce flux, le pare-feu traite le transfert FTP comme des paquets TCP parasites et les abandonne. Il s'agit du comportement par défaut.

Flux de tunnel IPsec persistants activés

Avec la fonctionnalité de flux persistants de tunnellisation IPsec activée, tant que le tunnel est recréé dans la fenêtre de délai d'expiration, les données continuent de circuler correctement, car l'ASA a toujours accès aux informations d'état du flux A-D.

Avec cette fonctionnalité activée, l'ASA traite les flux de manière indépendante. Cela signifie que le flux A-D n'est pas supprimé lorsque le tunnel défini par le flux B-C est abandonné. L'ASA conserve et reprend les flux tunnelisés avec état (TCP). Tous les autres flux sont abandonnés et doivent être rétablis sur le nouveau tunnel. Cela n'affecte pas la politique de sécurité pour les flux tunnelisés, car l'ASA abandonne tous les paquets entrants sur le flux A-D lorsque le tunnel est en panne.

Les flux TCP tunnelisés ne sont pas abandonnés, ils reposent donc sur le délai d'expiration TCP pour le nettoyage. Toutefois, si le délai d'expiration est désactivé pour un flux tunnelisé particulier, ce flux reste dans le système jusqu'à ce qu'il soit effacé manuellement ou par d'autres moyens (par exemple, par un TCP RST de l'homologue).

Configurer les flux de tunnel IPsec persistants à l'aide de l'interface de ligne de commande

Exemple de configuration

Dépannage des flux persistants tunnelisés IPsec

Les commandes **show asp table** et **show conn** peuvent être utiles pour résoudre les problèmes liés aux flux IPsec tunnelisés persistants.

La fonctionnalité des flux de tunnel IPsec persistants est-elle activée ?

Pour voir si cette fonctionnalité est activée dans un tunnel particulier, consultez le contexte VPN associé au tunnel à l'aide de la commande **show asp table**. La commande show asp table vpn-context affiche un indicateur « +PRESERVE » pour chaque contexte qui maintient les flux avec état après l'interruption du tunnel, comme illustré dans l'exemple suivant (gras ajoutés pour la lisibilité) :

```
hostname(config)# show asp table vpn-context
VPN CTX=0x0005FF54, Ptr=0x6DE62DA0, DECR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
VPN CTX=0x0005B234, Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0

------------------------------------------------------------------------------

hostname(config)# show asp table vpn-context detail

VPN CTX  = 0x0005FF54

Peer IP  = ASA_Private
Pointer  = 0x6DE62DA0
State    = UP
Flags    = DECR+ESP+PRESERVE
SA       = 0x001659BF
SPI      = 0xB326496C
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0

VPN CTX  = 0x0005B234

Peer IP  = ASA_Private
Pointer  = 0x6DE635E0
State    = UP
Flags    = ENCR+ESP+PRESERVE
SA       = 0x0017988D
SPI      = 0x9AA50F43
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
```

```
Rekey Pkt  = 0
Rekey Call = 0
hostname(config)#
Configuration and Restrictions
This configuration option is subject to the same CLI configuration restrictions as other
sysopt VPN CLI.
```

Localisation des flux orphelins

Si un tunnel LAN à LAN / Network-Extension Mode tombe et ne se rétablit pas avant l'expiration du délai, il peut subsister un certain nombre de flux de tunnel orphelins. Ces flux ne sont pas interrompus en raison de la panne du tunnel, mais toutes les données qui tentent de les traverser sont abandonnées. Pour voir ces flux, utilisez la commande **show conn**, comme dans les exemples suivants (le gras est ajouté pour mettre en évidence les entrées utilisateur) :

```
asa2(config)# show conn detail
9 in use, 14 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, C - CTIQBE media, D - DNS, d - dump,
       E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media, n - GUP
       O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       X - inspected by service module
```

L'exemple suivant montre un exemple de sortie de la commande **show conn** lorsqu'un flux orphelin existe, comme indiqué par l'indicateur **V** :

```
hostname# show conn
16 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:21 idle 0:00:00 bytes 1048 flags UOVB
TCP out 192.168.110.251:21137 in 192.168.150.252:21 idle bytes 1048 flags UIOB
```

Pour limiter le rapport aux connexions comportant des flux orphelins, ajoutez l'option **vpn_orphan** à la commande **show conn state**, comme dans l'exemple suivant :

```
hostname# show conn state vpn_orphan
14 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:5013 idle 0:00:00 bytes 2841019 flags UOVB
```

Effacer les configurations WebVPN de l'ASA

Lorsque vous utilisez les commandes **no webvpn** et **clear configure webvpn**, les configurations WebVPN par défaut ne sont pas supprimées. Les compteurs **http_in** et **http_out** sont conservés pour recueillir des statistiques de compression.

Pour effacer les configurations WebVPN de l'ASA, effectuez l'une des opérations suivantes :

- Désactivez les statistiques de compression après un démarrage à l'aide de la commande **no compression all**.
- Effacez les compteurs de statistiques de compression à l'aide de la commande **clear compression all**.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.