VPN d’accès à distance

Le réseau privé virtuel (VPN) d’accès à distance permet aux utilisateurs individuels de se connecter à votre réseau à partir d’un emplacement distant à l’aide d’un ordinateur ou d’autres périphériques pris en charge connectés à Internet. Cela permet aux collaborateurs mobiles de se connecter à partir de leur réseau domestique ou d’un réseau Wi-Fi public, par exemple.

Les rubriques suivantes expliquent comment configurer le VPN d’accès à distance pour votre réseau.

Aperçu du VPN d’accès à distance Cisco Secure Firewall Threat Defense

Cisco Secure Firewall Threat Defense fournit des fonctionnalités de passerelle sécurisée qui prennent en charge les VPN d’accès à distance SSL et IPsec-IKEv2. Le client du tunnel complet, Secure Client, fournit des connexions SSL et IPsec-IKEv2 sécurisées à la passerelle de sécurité pour les utilisateurs distants. Lorsque le client négocie une connexion SSL VPN avec le périphérique défense contre les menaces , il se connecte à l’aide de Transport Layer Security (TLS) ou de Datagram Transport Layer Security (DTLS).

Secure Client est le seul client pris en charge sur les périphériques de point terminal pour la connectivité VPN à distance vers les périphériques défense contre les menaces . Le client offre aux utilisateurs distants les avantages d’un client VPN SSL ou IPsec-IKEv2 sans que les administrateurs réseau n’aient à installer et à configurer les clients sur les ordinateurs distants. Secure Client pour Windows, Mac et Linux est déployé à partir de la passerelle sécurisée lors de la connectivité. Les applications Secure Client pour les périphériques Apple iOS et Android sont installées à partir de l’App Store de la plateforme.

Utilisez l'assistant de politique VPN d'accès à distance dans centre de gestion pour configurer rapidement et facilement les VPN d'accès à distance SSL et IPsec-IKEv2 avec des fonctionnalités de base. Ensuite, améliorez la configuration de politique comme vous le souhaitez et déployez-la sur vos périphériques Cisco Secure Firewall Threat Defense de passerelle sécurisés.

Fonctionnalités du VPN d'accès à distance

Le tableau suivant décrit les fonctionnalités du VPN d'accès à distance Cisco Secure Firewall Threat Defense :

Tableau 1 : Fonctionnalités du VPN d'accès à distance

	Description
fonctionnalités du VPN d'accès à distance Cisco Secure Firewall Threat Defense	• Accès à distance SSL et IPsec-IKEv2 à l'aide de Secure Client. • Cisco Secure Firewall Management Center prend en charge toutes les combinaisons, notamment IPv6 sur un tunnel IPv4. • Assistance à la configuration sur centre de gestion et gestionnaire d'appareil. Remplacements propres au périphérique. • Prise en charge des environnements Cisco Secure Firewall Management Center et défense contre les menaces à haute disponibilité. • Prise en charge de plusieurs interfaces et de plusieurs serveurs AAA. • Prise en charge du contrôle rapide des menaces à l'aide du CoA RADIUS ou de l'autorisation dynamique RADIUS. • Prise en charge du protocole DTLS v1.2 avec Cisco Secure Client version 4.7 ou ultérieure. • Les modules Secure Client (services client sécurisés) prennent en charge des services de sécurité supplémentaires pour les connexions VPN d'accès à distance. • Équilibrage de la charge VPN

	Description
Fonctionnalités AAA	• Authentification du serveur à l'aide de certificats d'identité autosignés ou signés par une autorité de certification. • Authentification à distance par nom d'utilisateur et mot de passe AAA à l'aide du serveur RADIUS, LDAP ou AD. • Attributs d'autorisation de groupe et d'utilisateur RADIUS, et la comptabilité RADIUS. • Prise en charge de la double authentification avec utilisation d'un serveur AAA supplémentaire pour l'authentification secondaire. • Intégration du contrôle d'accès NGFW à l'aide de l'identité VPN. • Attributs d'autorisation LDAP ou AD au moyen de l'interface Web Cisco Secure Firewall Management Center. • Prise charge de l'authentification unique à l'aide de SAML 2.0 • Prise en charge de plusieurs points de confiance de fournisseurs d'identité avec Microsoft Azure qui peuvent avoir plusieurs applications pour le même ID d'entité, mais un certificat d'identité unique.
Fonctionnalités de tunnellisation VPN	• Affectation d'adresses • Tunnellisation fractionnée • DNS fractionné • ACL de pare-feu client • Expiration de session pour la durée maximale de connexion et d'inactivité.

	Description
Fonctionnalités de surveillance de VPN d'accès à distance	• Nouveau gadget de tableau de bord VPN affichant les utilisateurs VPN en fonction de diverses caractéristiques telles que la durée et l'application client. • Accès à distance aux événements VPN, y compris les informations d'authentification telles que le nom d'utilisateur et la plateforme de système d'exploitation. • Statistiques de tunnellisation disponibles à l'aide de l'interface de ligne de commande unifiée défense contre les menaces .

Composants Secure Client

Déploiement Secure Client

Votre politique de VPN d'accès à distance peut inclure Secure Client Image et Secure Client Profile pour la distribution aux points terminaux qui se connectent. Le logiciel client peut également être distribué par d'autres méthodes. Consultez le chapitre *Déployer Cisco Secure Client* dans Guide de l'administrateur de Cisco Secure Client (y compris AnyConnect), version 5.

Sans client installé précédemment, les utilisateurs distants saisissent l'adresse IP dans leur navigateur d'une interface configurée pour accepter les connexions VPN SSL ou IPsec-IKEv2. À moins que le périphérique de sécurité ne soit configuré pour rediriger les requêtes http:// vers https://, les utilisateurs distants doivent saisir l'URL sous la forme https://*adresse*. Une fois que l'utilisateur a saisi l'URL, le navigateur se connecte à cette interface et affiche l'écran de connexion.

Après la connexion d'un utilisateur, si la passerelle sécurisée estime que l'utilisateur a besoin du client VPN, elle télécharge le client qui correspond au système d'exploitation de l'ordinateur distant. Après le téléchargement, le client s'installe et se configure, établit une connexion sécurisée et reste ou se désinstalle (selon la configuration du périphérique de sécurité) lorsque la connexion s'interrompt. Dans le cas d'un client déjà installé, après la connexion, la passerelle de sécurité défense contre les menaces examine la version du client et le met à niveau au besoin.

Opération Secure Client

Lorsque le client négocie une connexion avec le périphérique de sécurité, il se connecte à l'aide de Transport Layer Security (TLS) et éventuellement de Datagram Transport Layer Security (DTLS). L'utilisation de DTLS évite les problèmes de latence et de bande passante associés à certaines connexions SSL et améliore la performance des applications en temps réel sensibles aux retards de paquets.

Lorsqu'un client VPN IPsec-IKEv2 établit une connexion à la passerelle sécurisée, la négociation consiste à authentifier le périphérique par le biais d'Internet Key Exchange (IKE), suivi de l'authentification de l'utilisateur au moyen de l'authentification étendue IKE (Xauth). Le profil de groupe est transmis au client VPN et une association de sécurité IPsec est créée pour terminer le VPN.

Secure Client Profile et Éditeur

Le Secure Client Profile est un groupe de paramètres de configuration, stocké dans un fichier XML que le client VPN utilise pour configurer son fonctionnement et son apparence. Ces paramètres (balises XML) comprennent les noms et les adresses des ordinateurs hôtes et les paramètres permettant d'activer davantage de fonctionnalités client.

Vous pouvez configurer un profil à l'aide de Secure Client Profile Editor. Cet éditeur est un outil de configuration pratique basé sur une interface graphique utilisateur et disponible avec le progiciel Secure Client. Il s'agit d'un programme indépendant que vous exécutez en dehors de centre de gestion.

Authentification du VPN d'accès à distance

Authentification du serveur VPN d'accès à distance

Les passerelles sécurisées Cisco Secure Firewall Threat Defense utilisent toujours des certificats pour s'identifier et s'authentifier auprès du point terminal client VPN.

Pendant que vous utilisez l'assistant de politique VPN d'accès à distance, vous pouvez inscrire le certificat sélectionné sur le périphérique défense contre les menaces ciblé. Dans l'assistant, sous **Access and Certificate** (Accès et certificats), sélectionnez l'option « Inscrire l'objet de certificat sélectionné sur les périphériques cibles ». L'inscription du certificat est automatiquement lancée sur les périphériques précisés. Pendant que vous terminez la configuration de la politique VPN d'accès à distance, vous pouvez afficher l'état du certificat inscrit sur la page d'accueil du certificat du périphérique. L'état indique clairement si l'inscription au certificat a réussi ou non. La configuration de votre politique VPN d'accès à distance est maintenant entièrement terminée et prête à être déployée.

L'obtention d'un certificat pour la passerelle sécurisée, également connu sous le nom d'inscription PKI, est expliqué dans Certificats. Ce chapitre contient une description complète de la configuration, de l'inscription et de la maintenance des certificats de passerelle.

Client d'accès à distance pour le VPN AAA

Pour SSL et IPsec-IKEv2, l'authentification de l'utilisateur distant est effectuée à l'aide des noms d'utilisateur et des mots de passe uniquement, des certificats uniquement ou des deux.

Remarque Si vous utilisez des certificats clients dans votre déploiement, ils doivent être ajoutés à la plateforme de votre client indépendamment de Cisco Secure Firewall Threat Defense ou Cisco Secure Firewall Management Center. Des installations telles que SCEP ou CA Services ne sont pas fournies pour remplir vos clients avec des certificats.

Les serveurs AAA permettent aux périphériques gérés servant de passerelles sécurisées de déterminer qui est un utilisateur (authentification), ce que l'utilisateur est autorisé à faire (autorisation) et ce qu'il a fait (comptabilité). RADIUS, LDAP/AD, TACACS+ et Kerberos sont des exemples de serveurs AAA. Pour le VPN d'accès à distance sur les périphériques défense contre les menaces , les serveurs AD, LDAP et RADIUS AAA sont pris en charge pour l'authentification.

Reportez-vous à la section Comprendre l'application des politiques d'autorisations et d'attributs pour en savoir plus sur l'autorisation VPN d'accès à distance.

Avant d'ajouter ou de modifier la politique VPN d'accès à distance, vous devez configurer le domaine et les groupes de serveurs RADIUS que vous souhaitez spécifier. Pour plus de renseignements, consultez les sections

Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine et Ajouter un groupe de serveurs RADIUS.

Sans DNS configuré, le périphérique ne peut pas résoudre les noms de serveur AAA, les URL nommées et les serveurs CA avec FQDN ou noms d'hôte, il ne peut résoudre que les adresses IP.

Les informations de connexion fournies par un utilisateur distant sont validées par un domaine LDAP ou AD ou un groupe de serveurs RADIUS. Ces entités sont intégrées à la passerelle sécurisée Cisco Secure Firewall Threat Defense.

Remarque Si les utilisateurs s'authentifient auprès du VPN d'accès à distance en utilisant Active Directory comme source d'authentification, ils doivent se connecter avec leur nom d'utilisateur; le format `domaine\nom_utilisateur` ou `nom_utilisateur@domaine` échoue. (Active Directory fait référence à ce nom d'utilisateur sous le nom de *nom de connexion* ou parfois sous le nom de `sAMAccountName`.) Pour en savoir plus, consultez Attributs de dénomination des utilisateurs sur MSDN.

Si vous utilisez RADIUS pour l'authentification, les utilisateurs peuvent se connecter dans l'un des formats mentionnés ci-dessus.

Une fois authentifié au moyen d'une connexion VPN, l'utilisateur distant prend une *identité VPN*. Cette identité VPN est utilisée par *les politiques d'identité* sur la passerelle sécurisée Cisco Secure Firewall Threat Defense pour reconnaître et filtrer le trafic réseau appartenant à cet utilisateur distant.

Les politiques d'identité sont associées aux politiques de contrôle d'accès, qui déterminent qui a accès aux ressources réseau. C'est de cette façon que l'utilisateur distant a bloqué ou autorisé l'accès à vos ressources réseau.

Pour en savoir plus, consultez les sections À propos des politiques d'identité et Politiques de contrôle d'accès.

Sujets connexes

Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 26

Comprendre l'application des politiques d'autorisations et d'attributs

Le périphérique Cisco Secure Firewall Threat Defense prend en charge l'application d'attributs d'autorisation d'utilisateur (également appelés droits ou autorisations d'utilisateur) aux connexions VPN à partir d'un serveur d'authentification externe ou d'un serveur d'autorisation AAA (RADIUS) ou d'une politique de groupe sur le périphérique défense contre les menaces . Si le périphérique défense contre les menaces reçoit des attributs du serveur AAA externe qui sont en conflit avec ceux configurés dans la politique de groupe, les attributs du serveur AAA prévalent toujours.

Le périphérique défense contre les menaces applique les attributs dans l'ordre suivant :

1. **Attributs de l'utilisateur sur le serveur AAA externe** : le serveur renvoie ces attributs une fois l'authentification ou l'autorisation de l'utilisateur réussie.
2. **Politique de groupe configurée sur le périphérique Firepower Threat Defense** : Si un serveur RADIUS renvoie la valeur de l'attribut de classe RADIUS IETF-Class-25 (OU= group-policy) pour l'utilisateur, le périphérique défense contre les menaces place l'utilisateur dans la politique de groupe de du même nom et applique les attributs de la politique de groupe qui ne sont pas renvoyés par le serveur.
3. **Politiques de groupe affectées par le profil de connexion (également appelé groupes de tunnels)** : le profil de connexion contient les paramètres préliminaires pour la connexion et comprend une politique de groupe par défaut appliquée à l'utilisateur avant l'authentification.

Remarque Le périphérique défense contre les menaces ne prend pas en charge la transmission des attributs du système par défaut de la politique de groupe par défaut, *DfltGRPPlicy*. Les attributs de la politique de groupe affectés au profil de connexion sont utilisés pour la session utilisateur, s'ils ne sont pas remplacés par les attributs d'utilisateur ou la politique de groupe du serveur AAA, comme indiqué ci-dessus.

Sujets connexes

Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 26

Comprendre la connectivité des serveurs AAA

Les serveurs LDAP, AD et RADIUS AAA doivent être accessibles à partir du périphérique défense contre les menaces aux fins prévues : uniquement le traitement de l'identité de l'utilisateur, l'authentification VPN uniquement ou les deux activités. Les serveurs AAA sont utilisés dans le VPN d'accès à distance pour les activités suivantes :

- Gestion de l'**identité de l'utilisateur** : les serveurs doivent être accessibles par l'interface de gestion.

  Sur le défense contre les menaces , l'interface de gestion nécessite une configuration et un processus de routage distincts pour les interfaces de les interfaces normales utilisées par le VPN.

- **Authentification VPN** : les serveurs doivent être accessibles sur l'une des interfaces standard : l'interface de dépistage ou une interface de données.

  Pour les interfaces standard, deux tables de routage sont utilisées. Une table de routage de gestion uniquement pour l'interface de dépistage ainsi que toute autre interface configurée pour la gestion uniquement, et une table de routage des données utilisée pour les interfaces de données. Lorsqu'une recherche de routage est terminée, la table de routage de gestion uniquement est vérifiée en premier, puis la table de routage des données. La première correspondance est choisie pour atteindre le serveur AAA.

Remarque Si vous placez un serveur AAA sur une interface de données, assurez-vous que les politiques de routage de gestion uniquement ne correspondent pas au trafic destiné à une interface de données. Par exemple, si vous avez une voie de routage par défaut par l'interface de dépistage, le trafic ne reviendra jamais vers la table de routage des données. Utilisez les commandes **show route management-only** et **show route** pour vérifier la détermination du routage.

Pour les deux activités sur les mêmes serveurs AAA, en plus de rendre les serveurs accessibles par l'interface de gestion pour le traitement de l'identité de l'utilisateur, effectuez l'une des opérations suivantes pour fournir un accès d'authentification VPN aux mêmes serveurs AAA :

- Activez et configurez l'interface de dépistage avec une adresse IP sur le même sous-réseau que l'interface de gestion, puis configurez une voie de routage vers le serveur AAA par cette interface. L'accès de l'interface de dépistage sera utilisé pour l'activité VPN et l'accès de l'interface de gestion pour le traitement de l'identité.

Remarque Lorsqu'elle est configurée de cette façon, vous ne pouvez pas avoir une interface de données sur le même sous-réseau que les interfaces de dépistage et de gestion. Si vous souhaitez que l'interface de gestion et une interface de données se trouvent sur le même réseau, par exemple lorsque vous utilisez le périphérique lui-même comme passerelle, vous ne pourrez pas utiliser cette solution, car l'interface de dépistage doit rester désactivée.

- Configurer un routage par l'intermédiaire d'une interface de données vers le serveur AAA. L'accès à l'interface de données sera utilisé pour l'activité VPN et l'accès à l'interface de gestion pour le traitement de l'identité de l'utilisateur.

Pour plus d'informations sur les différentes interfaces, consultez Interfaces de pare-feu standard.

Après le déploiement, utilisez les commandes CLI suivantes pour surveiller et dépanner la connectivité du serveur AAA à partir du périphérique défense contre les menaces :

- **show aaa-server** pour afficher les statistiques du serveur AAA.
- **show route management-only** pour afficher les entrées de la table de routage destinées à la gestion uniquement.
- **show network** et **show network-static-routes** pour afficher la route par défaut de l'interface de gestion et les routes statiques.
- **show route** pour afficher les entrées de la table de routage du trafic de données.
- **ping system** et **traceroute system** pour vérifier le chemin d'accès au serveur AAA via l'interface de gestion.
- le**ping interface** *ifname* et **traceroute** *destination* pour vérifier le chemin d'accès au serveur AAA à l'aide des interfaces de dépistage et de données.
- **test aaa-server authentication** et **test aaa-server authorization** pour tester l'authentification et l'autorisation sur le serveur AAA.
- **clear aaa-server statistics** *groupname* ou **clear aaa-server statistics protocol** *protocol* pour effacer les statistiques d'un serveur AAA par groupe ou protocole.
- **aaa-server** *groupname* **active host** *hostname* pour activer un serveur AAA en panne ou **aaa-server** *groupname* **fail host** *hostname* pour activer un serveur AAA en panne.
- **debug ldap level**, **debug aaa authentication**, **debug aaa authorization** et **debug aaa accounting**.

Exigences de licence pour le VPN d'accès à distance

Licence de défense contre les menaces

Défense contre les menaces le VPN d'accès à distance nécessite Chiffrement renforcé et l'une des licences suivantes pour Secure Client :

- Secure Client Advantage

- Secure Client Premier
- VPN client sécurisé uniquement

Exigences et conditions préalables pour le VPN d'accès à distance

Prise en charge des modèles

Défense contre les menaces

Domaines pris en charge

N'importe quel

Rôles utilisateur

Admin

Lignes directrices et limites pour le VPN d'accès à distance

Configuration du protocole VPN d'accès à distance

- Vous ne pouvez ajouter une nouvelle politique VPN d'accès à distance qu'en utilisant l'assistant. Vous devez parcourir tout l'assistant pour créer une nouvelle politique; la politique ne sera pas enregistrée si vous annulez avant de terminer l'assistant.
- Deux utilisateurs ne doivent **pas** modifier une politique VPN d'accès à distance en même temps. cependant, l'interface Web n'interdit pas la modification simultanée. Si cela se produit, la dernière configuration enregistrée persiste.
- Le déplacement d'un périphérique Cisco Secure Firewall Threat Defense d'un domaine à un autre n'est pas possible si une politique VPN d'accès à distance est affectée à ce périphérique.
- Le VPN d'accès à distance ne prend pas en charge SSL lors de l'utilisation de logiciels-services ou d'ECMP. Nous vous recommandons d'utiliser IPsec-IKEv2.
- Les périphériques Firepower 9300 et 4100 en mode grappe ne prennent pas en charge la configuration VPN d'accès à distance.
- La connectivité VPN d'accès à distance peut échouer s'il y a une règle de NAT défense contre les menaces mal configurée.
- Si vous utilisez DHCP pour fournir des adresses IP au client et que le client ne peut pas obtenir d'adresse, vérifiez les règles NAT. Toute règle NAT qui s'applique au réseau VPN d'accès à distance doit inclure l'option de recherche de routage. La recherche de routage peut permettre de s'assurer que les requêtes DHCP sont envoyées au serveur DHCP par l'intermédiaire d'une interface appropriée.
- Chaque fois que les ports IKE 500/4500 ou le port SSL 443 sont utilisés ou que certaines traductions PAT sont actives, Secure Client IPSec-IKEv2 ou le VPN d'accès à distance SSL ne peut pas être configuré

sur le même port, car il ne démarre pas le service. ces ports. Ces ports ne doivent pas être utilisés sur le périphérique défense contre les menaces avant la configuration de la politique VPN d'accès à distance.

- Lors de la configuration des VPN d'accès à distance à l'aide de l'assistant, vous pouvez créer des objets d'inscription de certificat en ligne, mais vous ne pouvez pas les utiliser pour installer le certificat d'identité. Les objets d'inscription de certificat sont utilisés pour générer le certificat d'identité sur le périphérique défense contre les menaces en cours de configuration comme passerelle VPN d'accès à distance. Installez le certificat d'identité sur le périphérique avant de déployer la politique VPN d'accès à distance sur le périphérique.

  Pour plus d'informations sur l'installation du certificat d'identité en fonction de l'objet d'inscription de certificat, consultez Le gestionnaire d'objets.

- Les interfaces de zone ECMP peuvent être utilisées dans le VPN d'accès à distance avec IPsec activé.
- Les interfaces de zone ECMP ne peuvent pas être utilisées dans le VPN d'accès à distance lorsque SSL est activé. La configuration de déploiement de VPN d'accès à distance (SSL activé) échoue si toutes les interfaces de VPN d'accès à distance qui appartiennent à des zones de sécurité ou à des groupes d'interfaces appartiennent également à une ou plusieurs zones ECMP. Toutefois, si seulement certaines des interfaces VPN d'accès à distance appartenant aux zones de sécurité ou aux groupes d'interfaces appartiennent également à une ou plusieurs zones ECMP, le déploiement de la configuration VPN d'accès à distance réussit, excluant ces interfaces.
- Après avoir modifié les configurations des politiques de VPN d'accès à distance, redéployez les modifications sur les périphériques défense contre les menaces . Le temps nécessaire au déploiement des modifications de configuration dépend de plusieurs facteurs tels que la complexité des politiques et des règles, le type et le volume de configurations que vous envoyez au périphérique, ainsi que la mémoire et le modèle du périphérique. Avant de déployer des modifications de politique VPN d'accès à distance, consultez Bonnes pratiques pour le déploiement des modifications de configuration.
- L'émission de commandes telles que **curl** sur la tête de réseau du VPN d'accès à distance n'est pas directement prise en charge et pourrait ne pas donner les résultats souhaitables. Par exemple, la tête de réseau ne répond pas aux requêtes HTTP HEAD.

Planification de la capacité de sessions VPN simultanées (modèles défense contre les menaces virtuelles)

Le nombre maximal de sessions VPN simultanées est régi par les défense contre les menaces virtuelles niveaux de droits installés sous licence Smart et appliqués par l'intermédiaire d'un limiteur de débit. Il y a une limite maximale au nombre de sessions VPN d'accès à distance simultanées autorisées sur un périphérique en fonction du modèle de périphérique sous licence. Cette limite est conçue pour que les performances du système ne se dégradent pas à des niveaux inacceptables. Utilisez ces limites pour la planification de la capacité.

Modèle du périphérique	Maximum de sessions VPN d'accès à distance simultanées
Défense contre les menaces virtuelles5	50
Défense contre les menaces virtuelles10	250
Défense contre les menaces virtuelles20	250
Défense contre les menaces virtuelles30	250
Défense contre les menaces virtuelles50	750

Modèle du périphérique	Maximum de sessions VPN d'accès à distance simultanées
Défense contre les menaces virtuelles100	10 000

Planification de la capacité de sessions VPN simultanées (modèles matériels)

Le nombre maximal de sessions VPN simultanées est régi par des limites spécifiques à la plateforme et ne dépendent pas de la licence. Il y a une limite maximale au nombre de sessions VPN d'accès à distance simultanées autorisées sur un périphérique en fonction du modèle de périphérique. Cette limite est conçue pour que les performances du système ne se dégradent pas à des niveaux inacceptables. Utilisez ces limites pour la planification de la capacité.

Modèle du périphérique	Maximum de sessions VPN d'accès à distance simultanées
Firepower 1010	75
Firepower 1120	150
Firepower 1140	400
Firepower de la série 2110	1 500
Firepower 2120	3500
Firepower 2130	7500
Firepower 2140	10 000
Secure Firewall 3110	3 000
Secure Firewall 3120	6000
Secure Firewall 3130	15 000
Secure Firewall 3140	20 000
Firepower 4100, tous les modèles	10 000
appareil Firepower 9300, tous les modèles	20 000
ISA 3000	25

Pour connaître la capacité des autres modèles de matériel, communiquez avec votre représentant commercial.

Remarque Le périphérique défense contre les menaces refuse les connexions VPN une fois que la limite maximale de session par plateforme est atteinte. La connexion est refusée avec un message syslog. Consultez les messages syslog %ASA-4-113029 et %ASA-4-113038 dans le guide des messages syslog. Pour en savoir plus, consultez la section Messages du journal système de Cisco Secure Firewall ASA.

Contrôle de l'utilisation du chiffrement pour le VPN

Pour empêcher l'utilisation de chiffrements supérieurs à DES, des vérifications de prédéploiement sont disponibles aux emplacements suivants dans le centre de gestion :

Devices (périphériques) > **Platform Settings (paramètres de la plateforme)** > **Edit (Modifier)** > **SSL**

Périphériques > **VPN** > **Accès à distanceModifier Avancé IPsec**.

Pour en savoir plus sur les paramètres SSL et IPsec, consultez SSL et Configurer les paramètres du VPN d'accès à distance IPsec/IKEv2, à la page 60.

Authentication, Authorization, and Accounting

Configurez le DNS sur chaque périphérique de la topologie en pour utiliser le VPN d'accès à distance. Sans DNS, le périphérique ne peut pas résoudre les noms de serveur AAA, les URL nommées et les serveurs CA avec nom de domaine complet ou noms d'hôte; il ne peut que résoudre les adresses IP.

Vous pouvez configurer le DNS à l'aide des **paramètres de la plateforme**. Pour plus de renseignements, consultez les sections DNS et Groupe de serveurs DNS.

Certificats client

Si vous utilisez des certificats clients dans votre déploiement, ils doivent être ajoutés à la plateforme de votre client indépendamment de Cisco Secure Firewall Threat Defense ou Cisco Secure Firewall Management Center. Des installations telles que SCEP ou CA Services ne sont pas fournies pour remplir vos clients avec des certificats.

fonctionnalités non prises en charge de Secure Client

Le seul client VPN pris en charge est Cisco Secure Client. Aucun autre client ni VPN natif n'est pris en charge. Le VPN sans client n'est pas pris en charge pour la connectivité VPN; il est uniquement utilisé pour déployer Secure Client (services client sécurisés) à l'aide d'un navigateur Web.

Les fonctionnalités suivantes Secure Client ne sont pas prises en charge lors de la connexion à une passerelle sécurisée défense contre les menaces :

- Prise en charge de la personnalisation et de la localisation Secure Client. Le périphérique défense contre les menaces ne configure pas et ne déploie pas les fichiers nécessaires à la configuration de Secure Client pour ces fonctionnalités.
- TACACS, Kerberos (authentification KCD et RSA SDI).
- Serveur mandataire du navigateur

Configuration d'une nouvelle connexion de VPN d'accès à distance

Cette section fournit des instructions pour configurer une nouvelle politique VPN d'accès à distance avec des périphériques Cisco Secure Firewall Threat Defense comme passerelles VPN et Cisco Secure Client comme client VPN.

Étape	Faire ceci	Plus d'informations
1	Passez en revue les directives et les conditions préalables.	Lignes directrices et limites pour le VPN d'accès à distance, à la page 9 Conditions préalables à la configuration du VPN d'accès à distance, à la page 13
2	Créez une nouvelle politique VPN d'accès à distance à l'aide de l'assistant.	Créer une nouvelle politique VPN d'accès à distance, à la page 14
3	Mettez à jour la politique de contrôle d'accès déployée sur le périphérique.	Mettre à jour la politique de contrôle d'accès sur le périphérique Cisco Secure Firewall Threat Defense, à la page 16
4	(Facultatif) Configurez une règle d'exemption de NAT si la NAT est configurée sur le périphérique.	(Facultatif) Configurer l'exemption de NAT, à la page 17
5	Configurez le DNS.	Configurer le DNS, à la page 18
6	Ajoutez un profil Secure Client (services client sécurisés).	Ajouter un fichier XML Secure Client Profile , à la page 18
7	Déployez la politique VPN d'accès à distance.	Déployer les modifications de configuration
8	(Facultatif) Vérifiez la configuration de la politique d'accès à distance au VPN.	Vérifier la configuration, à la page 22

Conditions préalables à la configuration du VPN d'accès à distance

- Déployez les périphériques Cisco Secure Firewall Threat Defense et configurez Cisco Secure Firewall Management Center pour gérer le périphérique avec les licences requises et les fonctionnalités d'exportation contrôlées activées. Pour en savoir plus, consultez Licences VPN.
- Configurez l'objet d'inscription de certificat utilisé pour obtenir le certificat d'identité pour chaque périphérique défense contre les menaces qui sert de passerelle VPN d'accès à distance.
- Configurez l'objet de groupe de serveurs RADIUS et tous les domaines AD ou LDAP utilisés par les politiques VPN d'accès à distance.
- Assurez-vous que le serveur AAA est accessible à partir du périphérique défense contre les menaces pour que la configuration du VPN d'accès à distance fonctionne. Configurez le routage (sous **Devices > Device Management > Edit Device > Routing**) (Périphériques > Gestion des périphériques > Modifier un périphérique > Routage) pour assurer la connectivité avec les serveurs AAA.

  Pour la double authentification du VPN d'accès à distance, assurez-vous que les serveurs d'authentification principal et secondaire sont accessibles à partir du périphérique défense contre les menaces pour que la configuration de double authentification fonctionne.
- Achetez et activez l'une des licences Cisco Secure Client (services client sécurisés) suivantes : Secure Client Advantage , Secure Client Premier ou VPN client sécurisé uniquement pour activer le VPN d'accès à distance défense contre les menaces .

- Téléchargez les derniers fichiers image Secure Client (services client sécurisés) depuis le centre de téléchargement de logiciels Cisco.

  Dans votre interface Web Cisco Secure Firewall Management Center, accédez à **Objets** > **Gestion des objets** > **VPN** > **Fichier Secure Client** et ajoutez les nouveaux fichiers images Secure Client (services client sécurisés).

- Créez une zone de sécurité ou un groupe d'interfaces contenant les interfaces réseau auxquelles les utilisateurs auront accès pour les connexions VPN. Consultez Interface.

- Téléchargez le Secure Client Profile Editor à partir du centre de téléchargement de logiciels Cisco pour créer le profilSecure Client du client. Vous pouvez utiliser l'éditeur de profil autonome pour créer un nouveau profil Secure Client ou modifier un profil existant.

Créer une nouvelle politique VPN d'accès à distance

L'assistant de politique VPN d'accès à distance vous guide pour configurer rapidement et facilement des VPN d'accès à distance avec des fonctionnalités de base. Vous pouvez améliorer encore la configuration de la politique en spécifiant des attributs supplémentaires comme vous le souhaitez et la déployer sur vos Cisco Secure Firewall Threat Defense périphériques de passerelle sécurisés.

Avant de commencer

- Assurez-vous de remplir tous les préalables énumérés dans Conditions préalables à la configuration du VPN d'accès à distance, à la page 13.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Cliquez sur **Add** (ajouter) pour créer une nouvelle politique de VPN d'accès à distance avec une configuration de politique de base, à l'aide de l'assistant de politique de VPN d'accès à distance.

Vous devez parcourir tout l'assistant pour créer une nouvelle politique; la politique n'est pas enregistrée si vous annulez avant d'avoir terminé la fermeture de l'assistant.

Étape 3 Sélectionnez les périphériques cibles et les protocoles.

Les périphériques défense contre les menaces que vous sélectionnez ici fonctionnent comme vos passerelles VPN d'accès à distance pour les utilisateurs du client VPN.

Vous pouvez sélectionner des périphériques défense contre les menaces lorsque vous créez une politique de VPN d'accès à distance ou les modifier ultérieurement. Consultez Définir les périphériques cibles pour une politique VPN d'accès à distance, à la page 23.

Vous pouvez sélectionner les protocoles VPN **SSL** ou **IPSec-IKEv2**, ou les deux. Défense contre les menaces prend en charge les deux protocoles permettant d'établir des connexions sécurisées sur un réseau public par l'intermédiaire de tunnels VPN.

Remarque Défense contre les menaces ne prend pas en charge les tunnels IPSec avec chiffrement NULL. Si vous avez sélectionné IPSec-IKEv2, assurez-vous de ne pas choisir le chiffrement NULL pour la proposition IPSec IKEv2. Consultez Configurer des objets de proposition IKEv2 IPsec.

Pour les paramètres SSL, consultez SSL.

Étape 4 Configurez les paramètres de **profil de connexion** et **de politique de groupe**.

Un profil de connexion spécifie un ensemble de paramètres qui définissent la façon dont les utilisateurs distants se connectent au périphérique VPN. Les paramètres comprennent les paramètres et les attributs pour l'authentification, les affectations d'adresses aux clients VPN et les politiques de groupe. Le périphérique Défense contre les menaces fournit un profil de connexion par défaut nommé *DefaultWEBVPNGroup* lorsque vous configurez une politique VPN d'accès à distance.

Pour en savoir plus, consultez Configurer les paramètres du profil de connexion, à la page 24.

Pour en savoir plus sur la configuration,

- paramètres AAA, consultez Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 26
- cartes d'attribut LDAP, consultez Configuration du mappage des attributs LDAP, à la page 51
- authentification de la connexion unique SAML 2.0, consultez Configuration de l'authentification de la connexion unique SAML, à la page 87

Une politique de groupe est un ensemble de paires d'attributs et de valeurs, stockées dans un objet de politique de groupe, qui définissent l'expérience de VPN d'accès à distance pour les utilisateurs de VPN. Vous configurez des attributs tels que le profil d'autorisation de l'utilisateur, les adresses IP, les paramètres Secure Client, le mappage VLAN et les paramètres de session utilisateur, etc. en utilisant la politique de groupe. Le serveur d'autorisation RADIUS attribue la politique de groupe, ou elle est obtenue à partir du profil de connexion actuel.

Pour en savoir plus, consultez Configuration des politiques de groupe, à la page 50.

Étape 5 Sélectionnez l' **l'image Secure Client** que les utilisateurs du VPN utiliseront pour se connecter au VPN d'accès à distance.

Secure Client fournit des connexions SSL ou IPSec sécurisées (IKEv2) vers le périphérique Cisco Secure Firewall Threat Defense pour les utilisateurs distants avec un profilage VPN complet pour les ressources de l'entreprise. Une fois la politique d'accès VPN à distance déployée sur le périphérique défense contre les menaces , les utilisateurs de VPN peuvent saisir l'adresse IP de l'interface du périphérique configurée dans leur navigateur pour télécharger et installer Secure Client (services client sécurisés).

Pour en savoir plus sur la configuration du profil client et des modules client, consultez Options de politique de groupe Secure Client (services client sécurisés).

Étape 6 Sélectionnez l'**interface réseau et le certificat d'identité**.

Les objets d'interface segmentent votre réseau pour vous aider à gérer et à classer le flux de trafic. Un objet zone de sécurité regroupe simplement des interfaces. Ces groupes peuvent couvrir plusieurs périphériques. Vous pouvez également configurer plusieurs objets d'interface de zone sur un seul périphérique. Il existe deux types d'objets d'interface :

- Zones de sécurité - Une interface ne peut appartenir qu'à une seule zone de sécurité.
- Groupes d'interfaces : une interface peut appartenir à plusieurs groupes d'interfaces.

Étape 7 Passez en revue le **résumé** de la configuration de la politique de VPN d'accès à distance.

La page Summary (Résumé) affiche tous les paramètres VPN d'accès à distance que vous avez configurés jusqu'à présent et fournit des liens vers les configurations supplémentaires qui doivent être effectuées avant de déployer la politique VPN d'accès à distance sur les périphériques sélectionnés.

Cliquez sur **Back** (retour) pour modifier la configuration, le cas échéant.

Étape 8 Cliquez sur **Finish** (terminer) pour terminer la configuration de base de la politique VPN d'accès à distance.

Lorsque vous avez terminé l'assistant de politique VPN d'accès à distance, la page de liste des politiques s'affiche. Plus tard, effectuez la configuration DNS, configurez le contrôle d'accès pour les utilisateurs VPN et activez l'exemption NAT (si nécessaire) pour terminer une configuration de base d'une politique VPN d'accès à distance.

Mettre à jour la politique de contrôle d'accès sur le périphérique Cisco Secure Firewall Threat Defense

Avant de déployer la politique VPN d'accès à distance, vous devez mettre à jour la politique de contrôle d'accès sur le périphérique Cisco Secure Firewall Threat Defense ciblé avec une règle autorisant le trafic VPN. La règle doit autoriser tout le trafic provenant de l'interface externe, avec la source comme réseaux d'ensembles VPN définis et la destination comme réseau d'entreprise.

Remarque Si vous avez sélectionné l'option **Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)** (Contourner la politique de contrôle d'accès pour le trafic déchiffré (sysopt permit-vpn)) dans l'onglet Interface d'accès, vous n'avez pas besoin de mettre à jour la politique de contrôle d'accès pour le VPN d'accès à distance.

Activez ou désactivez l'option pour toutes vos connexions VPN. Si vous désactivez cette option, assurez-vous que le trafic est autorisé par la politique de contrôle d'accès ou la politique de préfiltre.

Pour en savoir plus, consultez Configurer les interfaces d'accès pour le VPN d'accès à distance, à la page 44.

Avant de commencer

Terminez la configuration de la politique de VPN d'accès à distance à l'aide de l'assistant de politique de VPN d'accès à distance.

Procédure

Étape 1 Dans l'interface Web Cisco Secure Firewall Management Center, choisissez **Policies** > **Access Control** (Politiques > Contrôle d'accès).

Étape 2 Cliquez sur **Edit** (Modifier) dans la politique de contrôle d'accès que vous souhaitez mettre à jour.

Étape 3 Cliquez sur **Add Rule** (Ajouter une règle) pour ajouter une nouvelle règle.

Étape 4 Précisez le **nom** de la règle et sélectionnez **Enabled** (Activée).

Étape 5 Sélectionnez l'**Action**, **Allow** (Autoriser) ou **Trust** (Confiance).

Étape 6 Sélectionner les options suivantes sous l'onglet **Zones** (zones) :

a) Sélectionnez la zone extérieure dans Zones disponibles et cliquez sur **Ajouter à la source**.

b) Sélectionnez la zone intérieure dans Zones disponibles et cliquez sur **Ajouter à la destination**.

Étape 7 Sélectionner les options suivantes sous l'onglet **Networks** (réseaux) :

a) Sélectionnez le réseau interne (interface interne et/ou réseau d'entreprise) dans la liste des réseaux disponibles et cliquez sur **Add to Destination** (Ajouter à la destination).
b) Sélectionnez le réseau de l'ensemble d'adresses VPN dans la liste des réseaux **disponibles** et cliquez sur **Add to Source Networks** (ajouter aux réseaux source).

Étape 8 Configurez les autres paramètres de règle de contrôle d'accès requis et cliquez sur **Add** (ajouter).

Étape 9 Enregistrez la règle et la politique de contrôle d'accès.

(Facultatif) Configurer l'exemption de NAT

L'exemption de NAT exempte les adresses de la traduction et permet aux hôtes traduits et distants d'établir des connexions avec vos hôtes protégés. Tout comme la NAT d'identité, vous ne limitez pas la traduction pour un hôte sur des interfaces spécifiques; vous devez utiliser l'exemption NAT pour les connexions via toutes les interfaces. Cependant, l'exemption NAT vous permet de spécifier les adresses réelles et de destination lors de la détermination des adresses réelles à traduire (semblable à la politique NAT). Utilisez la NAT d'identité statique pour prendre en compte les ports dans la liste d'accès.

Lorsque vous configurez la NAT d'identité statique pour l'accès à distance ou le VPN de site à site, vous devez configurer la NAT avec l'option de recherche route. Sans recherche de routage, le défense contre les menaces envoie le trafic hors de l'interface spécifiée dans la commande NAT, indépendamment de ce que dit la table de routage. Par exemple, vous ne voulez pas que défense contre les menaces envoie le trafic de portée DHCP par une interface incorrecte; il ne reviendra jamais à l'adresse IP de l'interface. L'option recherche de routage permet à défense contre les menaces d'envoyer ou d'intercepter le trafic directement sur l'adresse IP de l'interface plutôt que de passer par l'interface. Pour le trafic du client VPN vers un hôte du réseau interne, l'option de recherche de routage aboutira toujours à l'interface de sortie correcte (interne), de sorte que le flux de trafic normal n'est pas affecté.

Avant de commencer

Vérifiez si la NAT est configurée sur les périphériques ciblés sur lesquels la politique VPN d'accès à distance est déployée. Si la NAT est activée sur les appareils ciblés, vous devez définir une politique de NAT pour exempter le trafic VPN.

Procédure

Étape 1 Sur votre interface Web Cisco Secure Firewall Management Center, cliquez sur **Devices** (périphériques) > **NAT**) .

Étape 2 Sélectionnez une politique NAT à mettre à jour ou cliquez sur **Nouvelle politique** > **NAT de défense contre les menaces** pour créer une politique NAT avec une règle NAT pour autoriser les connexions à travers toutes les interfaces.

Étape 3 Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle règle.

Étape 4 Dans la fenêtre Add NAT Rule (ajouter une règle NAT), sélectionnez les options suivantes :

a) Sélectionnez la règle NAT comme **Règle NAT manuelle**.
b) Sélectionnez le type comme **statique**.
c) Cliquez sur **Interface Objects** (Objets d'interface) et sélectionnez les objets d'interface source et destination.

Remarque Cet objet d'interface doit être identique à l'interface sélectionnée dans la politique VPN d'accès à distance.

Pour en savoir plus, consultez Configurer les interfaces d'accès pour le VPN d'accès à distance, à la page 44.

a) Cliquez sur **Translation** (traduction) et sélectionnez les réseaux source et de destination :

- **Source originale** et **source traduite**
- **Destination d'origine** et **destination traduite**

Étape 5 Dans l'onglet Avancé, sélectionnez **Do not proxy ARP on Destination Interface** (Désactiver le mandataire ARP sur l'interface de destination).

Do not proxy ARP on Destination Interface(désactiver le mandataire ARP sur l'interface de destination) : permet de désactiver le proxy (serveur mandataire) ARP pour les paquets entrants vers les adresses IP mappées. Si vous utilisez des adresses sur le même réseau que l'interface mappée, le système utilise un proxy ARP pour répondre à toute demande ARP pour les adresses mappées, interceptant ainsi le trafic destiné à une adresse mappée. Cette solution simplifie le routage, car l'appareil n'a pas à constituer la passerelle pour d'autres réseaux. Vous pouvez désactiver le proxy ARP si vous le souhaitez. Si vous le faites, vous devez vous assurer d'établir les voies de routage appropriées sur le routeur en amont.

Étape 6 Cliquez sur **OK**.

Configurer le DNS

Configurez le DNS sur chaque périphérique défense contre les menaces afin d'utiliser le VPN d'accès à distance. Sans DNS, les périphériques ne peuvent pas résoudre les noms de serveur AAA, les URL nommées et les serveurs CA avec nom de domaine complet ou noms d'hôte. Résoudre les adresses IP

Procédure

Étape 1 Configurer les détails du serveur DNS et les interfaces de recherche de domaine en utilisant les paramètres de la plateforme. Pour plus de renseignements, consultez DNS et Groupe de serveurs DNS.

Étape 2 Configurez le tunnel fractionné dans la politique de groupe pour autoriser le trafic DNS à travers le tunnel VPN d'accès à distance si le serveur DNS est accessible par le réseau VNP. Pour en savoir plus, consultez Configurer les objets de politique de groupe.

Ajouter un fichier XML Secure Client Profile

Le Secure Client Profile est un groupe de paramètres de configuration stockés dans un fichier XML que le client utilise pour configurer son fonctionnement et son apparence. Ces paramètres (balises XML) comprennent les noms et les adresses des ordinateurs hôtes et les paramètres permettant d'activer davantage de fonctionnalités client.

Vous pouvez créer le Secure Client Profile à l'aide de l'éditeur Secure Client Profile, un outil de configuration basé sur l'interface graphique utilisateur qui est disponible dans le cadre du progiciel Secure Client. Il s'agit

d'un programme indépendant que vous exécutez en dehors de centre de gestion. Pour en savoir plus sur l'éditeur Secure Client Profile, consultez Guide de l'administrateur de Cisco Secure Client (incluant AnyConnect).

Avant de commencer

Une politique VPN d'accès à distance Cisco Secure Firewall Threat Defense nécessite l'affectation de Secure Client Profile aux clients VPN. Vous pouvez associer le profil client à une politique de groupe.

Téléchargez l'éditeur Secure Client Profile depuis le centre de téléchargement de logiciels Cisco.

Procédure

Étape 1 Choisissez **Devices** > **Remote Access** (Périphériques > Accès à distance).

Étape 2 Cliquez sur **Edit** (Modifier) dans la politique VPN d'accès à distance que vous souhaitez mettre à jour.

Étape 3 Cliquez sur **Edit** (Modifier) sur le profil de connexion auquel vous souhaitez ajouter le profil Secure Client (services client sécurisés).

Étape 4 Cliquez sur **Edit Group POlicy** (Modifier la politique de groupe). Si vous choisissez d'ajouter une nouvelle politique de groupe, cliquez sur **Add** (Ajouter).

Étape 5 Choisissez **Secure Client** > **Profil**.

Étape 6 Choisissez un profil dans la liste déroulante **Client Profile** (Profil client). Si vous choisissez d'ajouter un nouveau profil client, cliquez sur **Add** (ajouter) et procédez comme suit :

a) Entrez le **nom** du profil.

b) Cliquez sur **Browse** (Parcourir) et sélectionnez le fichier XML Secure Client Profile.

Remarque Pour l'authentification à deux facteurs, assurez-vous que le délai d'expiration est défini à 60 secondes ou plus dans le profil Secure Client (services client sécurisés).

c) Cliquez sur **Save** (enregistrer).

Étape 7 Enregistrez vos modifications.

(Facultatif) Configurer le tunnellisation fractionnée

Le tunnel fractionné permet la connectivité VPN à un réseau distant par l'intermédiaire d'un tunnel sécurisé, ainsi qu'à un réseau en dehors du tunnel VPN. Configurez la tunnellisation fractionnée si vous souhaitez permettre à vos utilisateurs VPN d'accéder à un réseau externe pendant qu'ils restent connectés au VPN d'accès à distance. Pour configurer une liste de tunnels séparés, vous devez créer une liste d'accès standard ou une liste d'accès étendue.

Pour en savoir plus, consultez Configuration des politiques de groupe, à la page 50.

Procédure

Étape 1 Choisissez **Devices** > **Remote Access** (Périphériques > Accès à distance).

Étape 2 Cliquez sur **Edit** (Modifier) dans la politique VPN d'accès à distance pour laquelle vous souhaitez configurer la tunnellisation fractionnée.

Étape 3 Cliquez sur **Edit** (Modifier) dans le profil de connexion requis.

Étape 4 Cliquez sur **Add** (Ajouter) pour ajouter une politique de groupe ou cliquez sur **Edit Group Policy** (Modifier la politique de groupe).

Étape 5 Choisissez **General** > **Split Tunneling** (Général > Tunnelisation fractionnée).

Étape 6 Dans la liste **IPv4 Slip Tunneling** ou **IPv6 Split Tunneling** (Tunnelisation fractionnée IPv4 ou IPv6), sélectionnez **Exclure les réseaux spécifiés ci-dessous**, puis sélectionnez les réseaux que vous souhaitez exclure du trafic VPN.

Le paramètre par défaut autorise tout le trafic sur le tunnel VPN.

Étape 7 Cliquez sur **Standard Access List** ou **Extended Access List**, puis sélectionnez une liste d'accès (standard ou étendue) dans la liste déroulante ou ajoutez-en une nouvelle.

Étape 8 Si vous choisissez d'ajouter une nouvelle liste d'accès standard ou étendue, procédez comme suit :

a) Précisez le **Nom** de la nouvelle liste d'accès et cliquez sur **Add** (Ajouter).
b) Choisissez **Allow** (autoriser) dans la liste déroulante **Action**.
c) Sélectionnez le trafic réseau que vous souhaitez autoriser sur le tunnel VPN et cliquez sur **Add** (Ajouter).

Étape 9 Enregistrez vos modifications.

Sujets connexes

Liste d'accès

(Facultatif) Configurer le tunnelisation dynamique fractionnée

La tunnellisation fractionnée dynamique vous permet d'affiner le tunnellisation fractionnée en fonction des noms de domaine DNS. Vous pouvez configurer des domaines qui doivent être inclus ou exclus du tunnel VPN d'accès à distance. Les domaines exclus ne sont pas bloqués. Au lieu de cela, le trafic vers ces domaines est conservé en dehors du tunnel VPN. Par exemple, vous pourriez envoyer du trafic à Cisco Webex sur l'Internet public, libérant ainsi de la bande passante de votre tunnel VPN pour le trafic ciblant les serveurs de votre réseau protégé. Pour plus d'informations sur la configuration de cette fonctionnalité, consultez Configurer le tunnel dynamique AnyConnect sur le FTD géré par FMC.

Avant de commencer

Vous pouvez configurer cette fonctionnalité en utilisant les centre de gestion boutons et défense contre les menaces à partir des versions 7.0 ou ultérieures. Si vous avez une version antérieure de centre de gestion, vous pouvez la configurer à l'aide de FlexConfig en suivant les instructions de la section sur les déploiements avancés d'AnyConnect VPN pour Firepower Threat Defense avec FMC.

Procédure

Étape 1 Configurez la politique de groupe pour utiliser le tunnel de séparation dynamique.

a) Choisissez **Devices > Remote Access** (Périphériques > Accès à distance).
b) Cliquez sur **Edit** (Modifier) dans la politique VPN d'accès à distance pour laquelle vous souhaitez configurer la tunnellisation dynamique fractionnée.
c) Cliquez sur **Edit** (Modifier) dans le profil de connexion requis.
d) Cliquez sur **Edit Group POlicy** (Modifier la politique de groupe).

Étape 2 Configurez l'attribut personnalisé Secure Client (Services client sécurisé) dans la boîte de dialogue **Add/Edit Group Policy**(ajouter/modifier une politique de groupe).

a) Cliquez sur l'onglet Secure Client (Services client sécurisé).
b) Cliquez sur **Attributs personnalisés**, puis sur **+**.
c) Choisissez **Tunnelisation dynamique fractionnée** dans la liste déroulante **Secure Client (Services client sécurisé) Attribut**.
d) Cliquez sur le signe plus **(+)** pour créer un nouvel objet d'attribut personnalisé.
e) Saisissez le nom de l'objet d'attribut personnalisé.
f) **Include domains** (Inclure les domaines) : spécifiez les noms de domaine qui seront inclus dans le tunnel VPN d'accès à distance.

   Vous pouvez inclure des domaines dans le tunnel qui seront exclus en fonction des adresses IP.

g) **Exclure les domaines** : précisez les noms de domaines qui seront exclus du VPN d'accès à distance.

   Les domaines exclus ne sont pas bloqués, le trafic vers ces domaines est conservé en dehors du tunnel VPN.

h) Cliquez sur **Save** (enregistrer).
i) Cliquez sur **Add** (ajouter).

Étape 3 Vérifiez l'attribut personnalisé configuré et cliquez sur **Save** pour enregistrer la politique de groupe.

Étape 4 Cliquez sur **Save** pour enregistrer le profil de connexion.

Étape 5 Cliquez sur **Save** pour enregistrer la politique VPN d'accès à distance.

Prochaine étape

1. Déployer la configuration vers défense contre les menaces
2. Vérifiez la configuration du tunnel fractionné dynamique sur les défense contre les menaces et les Secure Client (services client sécurisés). Pour en savoir plus, consultez Vérifier la configuration de la tunnelisation dynamique fractionnée, à la page 21.

Vérifier la configuration de la tunnelisation dynamique fractionnée

Sur Défense contre les menaces

Utilisez les commandes suivantes pour vérifier la configuration de la tunnellisation dynamique fractionnée :

- **show running-config webvpn**
- **show running-config anyconnect-custom-data**
- **show running-config group-policy** *<group-policy-name>*

Sur Secure Client (services client sécurisés)

Cliquez sur l'icône Statistiques () et choisissez **VPN > Statistiques**. Vous pouvez confirmer les domaines dans la catégorie d'exclusion/inclusion dynamique de fractionnement.

Vérifier la configuration

Procédure

Étape 1 Ouvrez un navigateur Web sur un appareil du réseau externe.

Étape 2 Saisissez l'URL de défense contre les menaces .

Étape 3 Saisissez le nom d'utilisateur et le mot de passe lorsque vous y êtes invité, puis cliquez sur **Connexion**.

Remarque La connexion au VPN s'établit automatiquement si vous installez Secure Client sur le système.

Le VPN vous invite à télécharger Secure Client si Secure Client n'est pas installé.

Étape 4 Téléchargez Secure Client s'il n'est pas installé et connectez-vous au VPN.
Le Secure Client s'installe. Une fois l'authentification réussie, vous établissez la connexion à la passerelle VPN d'accès à distance Cisco Secure Firewall Threat Defense. Le VPN d'accès à distance applique la politique d'identité ou de QoS applicable en fonction de la configuration de votre politique VPN.

Créer une copie d'une politique VPN d'accès à distance existante

Vous pouvez copier une politique VPN d'accès à distance existante pour en créer une nouvelle avec tous les paramètres, y compris les profils de connexion et les interfaces d'accès. Vous pouvez ensuite affecter des périphériques à la nouvelle politique et déployer le VPN sur les périphériques concernés au besoin.

Remarque Les utilisateurs disposant d'une autorisation en lecture seule pour le VPN d'accès à distance ne peuvent pas créer de copie du VPN. Les utilisateurs disposant de privilèges en lecture seule dans le domaine peuvent copier les VPN d'accès à distance.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Cliquez sur **Copy** (copier) dans la politique que vous souhaitez copier.

Étape 3 Spécifiez un **Nom** pour le nouveau VPN d'accès à distance.

Étape 4 Cliquez sur **OK**.

Prochaine étape

Pour affecter des périphériques à la nouvelle politique, consultez Définir les périphériques cibles pour une politique VPN d'accès à distance, à la page 23.

Définir les périphériques cibles pour une politique VPN d'accès à distance

Après avoir créé la politique VPN d'accès à distance, vous pouvez l'affecter aux périphériques de défense contre les menaces.

Procédure

Étape 1 Choisissez **Devices** > **VPN** > **Remote Access** (Périphériques > VPN > Accès à distance).

Étape 2 Cliquez sur **Edit** ( ) à côté de la politique VPN d'accès à distance que vous souhaitez modifier.

Étape 3 Cliquez sur **Policy Assignments** (Attributions de politiques)

Étape 4 Effectuez l'une des actions suivantes :

- Pour affecter un périphérique, une une paire à haute disponibilité ou un groupe de périphériques à la politique, sélectionnez-le dans la liste des **périphériques disponibles** et cliquez sur **Add** (Ajouter). Vous pouvez également faire glisser et déposer les périphériques disponibles pour les sélectionner.
- Pour supprimer une affectation de périphérique, cliquez sur **Supprimer** ( ) à côté d'un périphérique, d'une d'une paire à haute disponibilité ou d'un groupe de périphériques dans la liste des **périphériques sélectionnés**.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les modifications de configuration.

Associer le domaine local à la politique VPN d'accès à distance

Vous pouvez associer un domaine local à une politique VPN d'accès à distance pour activer l'authentification de l'utilisateur local.

Pour en savoir plus sur la création et la gestion des domaines, consultez Gérer un domaine.

Pour en savoir plus sur la configuration de l'authentification externe pour le VPN d'accès à distance, consultez Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 26.

Procédure

Étape 1 Choisissez **Devices** > **VPN** > **Remote Access** (Périphériques > VPN > Accès à distance).

Étape 2 Cliquez sur **Edit** ( ) à côté de la politique VPN d'accès à distance que vous souhaitez modifier.

Étape 3 Cliquez sur le lien à côté de **Local Realm** (domaine local).

Étape 4 Sélectionnez le **serveur de domaine local** dans la liste ou cliquez sur **Add** (ajouter) pour ajouter un nouveau domaine local.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les modifications de configuration.

Configurations supplémentaires de VPN d'accès à distance

Configurer les paramètres du profil de connexion

La politique VPN d'accès à distance contient les profils de connexion ciblés pour des périphériques spécifiques. Ces politiques concernent la création du tunnel lui-même, par exemple la façon dont AAA est effectuée et la façon dont les adresses sont attribuées (DHCP ou ensemble d'adresses) aux clients VPN. Ils comprennent également les attributs utilisateur, qui sont identifiés dans les politiques de groupe configurées sur le périphérique défense contre les menaces ou obtenues à partir d'un serveur AAA. Un périphérique fournit également un profil de connexion par défaut nommé *DefaultWEBVPNGroup*. Le profil de connexion configuré à l'aide de l'assistant apparaît dans la liste.

Si vous décidez d'accorder des droits différents à différents groupes d'utilisateurs VPN, vous pouvez ajouter des profils de connexion spécifiques pour chacun des groupes d'utilisateurs et gérer plusieurs profils de connexion dans votre politique VPN d'accès à distance.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Sélectionnez une politique VPN d'accès à distance existante dans la liste et cliquez sur l'icône **Modifier** correspondante.

Étape 3 Sélectionnez un **profil de connexion** et cliquez sur **Edit** (Modifier).

Étape 4 (Facultatif) Si vous choisissez d'ajouter un nouveau profil de connexion, cliquez sur **Add** (Ajouter).

Étape 5 Configurez les adresses IP pour les clients VPN.
Configurer les adresses IP pour les clients VPN, à la page 25

Étape 6 (Facultatif) Mettez à jour les paramètres AAA pour les VPN d'accès à distance.
Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 26

Étape 7 (Facultatif) Créez ou mettez à jour des alias.
Créer ou mettre à jour des alias pour un profil de connexion, à la page 43

Étape 8 Enregistrez vos modifications.

Configurer les adresses IP pour les clients VPN

L'attribution d'adresses aux clients vous permet d'attribuer des adresses IP aux utilisateurs du VPN d'accès à distance.

Vous pouvez attribuer des adresses IP aux clients VPN distants à partir des ensembles d'adresses IP locaux, des serveurs DHCP et des serveurs AAA. Les serveurs AAA sont affectés en premier, suivi des autres. Configurez la **politique d'attribution d'adresses de clients** dans l'onglet **Avancé** pour définir les critères d'attribution. Les groupes d'adresses IP définis dans ce profil de connexion ne seront utilisés que si aucun groupe d'adresses IP n'est défini dans la politique de groupe associée au profil de connexion ou dans la politique de groupe par défaut du système **DfltGRPPlicy**.

Pools d'adresses IPv4 : les clients VPN SSL reçoivent de nouvelles adresses IP lorsqu'ils se connectent au périphérique Défense contre les menaces. Les ensembles d'adresses définissent une plage d'adresses que les clients distants peuvent recevoir. Vous pouvez ajouter un maximum de six ensembles d'adresses IPv4 et IPv6 chacun.

Remarque Vous pouvez utiliser l'adresse IP des ensembles d'adresses IP existants dans le Centre de gestion ou créer un nouveau regroupement à l'aide de l'option **Ajouter**. En outre, vous pouvez créer un ensemble d'adresses IP dans Centre de gestion à l'aide du chemin **Objects > Object Management > Address Pools** (Objets > Gestion des objets > Bassins d'adresses). Pour en savoir plus, consultez Réserves d'adresses.

Procédure

Étape 1 Choisissez **Devices** (Périphériques) > **VPN** > **Remote Access** (Accès à distance).
Les politiques d'accès à distance existantes sont répertoriées.

Étape 2 Sélectionnez une politique VPN d'accès à distance et cliquez sur l'icône de modification.

Étape 3 Sélectionnez le profil de connexion que vous souhaitez mettre à jour et cliquez sur l'icône de modification.

Étape 4 Sous l'onglet **Client Address Assignment** (affectation d'adresses de clients), procédez comme suit :

Étape 5 Cliquez sur le signe plus (+) à côté du **Bassin d'adresses** :

a) Cliquez sur le signe plus (+) à côté de **Bassins d'adresses** pour ajouter des adresses IP, puis sélectionnez **IPv4** ou **IPv6** pour ajouter l'ensemble d'adresses correspondant. Sélectionnez l'ensemble d'adresses IP dans **Available Pools** (Bassins disponibles) et cliquez sur **Add** (Ajouter).

Remarque Si vous partagez votre politique VPN d'accès à distance entre plusieurs périphériques Cisco Secure Firewall Threat Defense, gardez à l'esprit que tous les périphériques partagent le même ensemble d'adresses, sauf si vous utilisez les remplacements d'objet au niveau du périphérique pour remplacer la définition globale par un ensemble d'adresses unique pour chaque périphérique. Des ensembles d'adresses uniques sont nécessaires pour éviter le chevauchement d'adresses dans les cas où les périphériques n'utilisent pas la NAT.

b) Cliquez sur le signe plus (+) à côté de **Disponibles** dans la fenêtre **Address Pools** (Bassins d'adresses) pour ajouter un nouvel ensemble d'adresses IPv4 ou IPv6. Lorsque vous choisissez l'ensemble IPv4, fournissez une adresse IP de début et de fin. Lorsque vous choisissez d'inclure un nouveau ensemble d'adresses IPv6, saisissez le **`nombre d'adresses`** dans la plage 1 à 16 384. Sélectionnez l'option **Allow Overrides** (autoriser les remplacements) pour éviter les conflits d'adresses IP lorsque les objets sont partagés sur de nombreux périphériques. Pour en savoir plus, consultez Réserves d'adresses.

c) Cliquez sur **OK**.

Si vous prévoyez de modifier les ensembles d'adresses IP, nous vous recommandons d'effectuer les étapes suivantes au cours d'une fenêtre de maintenance :

1. Annulez l'attribution du périphérique au VPN d'accès à distance.
2. Sélectionnez le périphérique et cliquez sur **Deploy**(déployer).

   Ce déploiement supprime toutes les configurations VPN d'accès à distance du périphérique et met fin aux sessions VPN d'accès à distance, mais les sessions ne sont pas rétablies.
3. Cliquez sur l'icône de modification à côté de l'ensemble d'adresses IP pour le modifier, et modifiez toute autre configuration VPN d'accès à distance, le cas échéant, dans Centre de gestion.
4. Attribuez le périphérique à la politique VPN d'accès à distance mise à jour.
5. Déployez la configuration sur le périphérique.

   Les clients VPN d'accès à distance peuvent se connecter au périphérique après la fenêtre de maintenance.

Étape 6 Cliquez sur le signe plus (+) à côté de **DHCP Servers** pour ajouter des serveurs DHCP :

Remarque L'adresse du serveur DHCP ne peut être configurée qu'avec une adresse IPv4.

a) Précisez le nom et l'adresse du serveur DHCP (Dynamic Host Configuration Protocol) en tant qu'objets réseau. Cliquez sur **Add** (Ajouter) pour choisir le serveur dans la liste d'objets. Cliquez sur **Delete** pour supprimer un serveur DHCP.
b) Cliquez sur **Add** dans la page **New Objects** pour ajouter un nouvel objet réseau. Saisissez le nom, la description et le réseau du nouvel objet, puis sélectionnez l'option **Allow Overrides** (autoriser les remplacements), le cas échéant. Pour plus de renseignements, consultez les sections Création d'objets réseau et Autoriser les mises en priorité d'objets.
c) Cliquez sur **OK**.

Étape 7 Cliquez sur **Save** (enregistrer).

Sujets connexes

Configurer les paramètres du profil de connexion, à la page 24

Configurer les paramètres AAA pour le VPN d'accès à distance

Avant de commencer

- Assurez-vous que les certificats d'ordinateur et d'utilisateur requis sont déployés sur les points terminaux. Pour en savoir plus sur les certificats Cisco Secure Firewall Threat Defense, consultez Gestion des certificats Défense contre les menacesGestion du certificat VPN.
- Configurer les profils Secure Client avec les certificats requis. Pour plus d'informations, consultez *Guide de l'administrateur de Cisco Secure Client (y compris AnyConnect)*.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Sélectionnez une politique VPN d'accès à distance existante dans la liste et cliquez sur l'icône **Modifier** correspondante.

Étape 3 Sélectionnez un profil de connexion pour mettre à jour les paramètres AAA, cliquez sur **Edit (Modifier)** > **AAA**.

Étape 4 Sélectionnez les éléments suivants pour l'**Authentication** (authentification) :

- **Méthode d'authentification** : détermine la façon dont un utilisateur est identifié avant d'être autorisé à accéder au réseau et aux services réseau. Elle contrôle l'accès en exigeant des informations d'authentification valides, qui sont généralement un nom d'utilisateur et un mot de passe. Elle peut également inclure le certificat du client. Les méthodes d'authentification prises en charge sont les suivantes **AAA uniquement**, **Certificat client uniquement**, et **AAA + Certificat client**.

  Lorsque vous sélectionnez la **méthode d'authentification** :

  - **AAA uniquement** : Si vous sélectionnez le **serveur d'authentification** comme **RADIUS**, par défaut, le serveur d'autorisation a la même valeur. Sélectionnez le **Accounting Server** (Serveur de comptabilité) dans la liste déroulante. Chaque fois que vous sélectionnez **AD** et **LDAP** dans la liste déroulante Authentication Server, vous devez sélectionner le **serveur d'autorisation et le serveur** de **comptabilité** manuellement.

  - **SAML** : chaque utilisateur est authentifié à l'aide du serveur de connexion unique SAML. Pour en savoir plus, consultez Authentification de connexion unique Single Sign-On avec SAML 2.0, à la page 85.

    Remplacer le certificat du fournisseur d'identité : Sélectionnez cette option pour remplacer le certificat du fournisseur d'identité principal du fournisseur SAML par un certificat du fournisseur d'identité propre à un profil de connexion ou à une application SAML. Sélectionnez le certificat du fournisseur d'identité dans la liste déroulante.

    Microsoft Azure peut prendre en charge plusieurs applications pour le même ID d'entité. Chaque application (mappée à un profil de connexion différent) nécessite un certificat unique. Si vous souhaitez conserver un ID d'entité existant pour l'objet de connexion unique dans le profil de connexion actuel et utiliser un certificat du fournisseur d'identité différent, vous pouvez sélectionner cette option.

    Cela permet la prise en charge de plusieurs applications SAML par le fournisseur d'identité SAML Azure de Microsoft.

    Le certificat d'identité principal est configuré dans l'objet serveur d'authentification unique.

    Pour en savoir plus sur la configuration d'un objet serveur d'authentification unique, consultez Ajouter un serveur de connexion unique (SSO).

    Choisissez votre **expérience de connexion SAML** pour configurer un navigateur en vue de l'authentification Web SAML :

    - **Navigateur intégré du client VPN** : sélectionnez cette option pour utiliser le navigateur intégré au client VPN pour l'authentification Web. L'authentification s'applique uniquement à la connexion VPN.

    - **Navigateur du système d'exploitation par défaut** : choisissez cette option pour configurer le navigateur par défaut ou natif du système d'exploitation qui prend en charge WebAuthN (norme FIDO2 pour l'authentification Web). Cette option active l'authentification unique (SSO) et prend en charge les méthodes d'authentification Web, telles que l'authentification biométrique.

Le navigateur par défaut nécessite un ensemble de navigateur externe pour l'authentification Web. Le paquet Default-External-Browser-Package est configuré par défaut. Vous pouvez modifier le progiciel du navigateur externe par défaut en modifiant une politique VPN d'accès à distance et en sélectionnant le fichier sous **Advanced** > **Secure Client Images** > **Package File** (Avancé Progiciel).

Vous pouvez également ajouter un nouveau fichier progiciel en sélectionnant. **Objects** > **Object Management** > **VPN** > **Secure Client File** > **Add Secure Client File** (Objets > Gestion des objets > VPN > Fichier AnyConnect > Ajouter un fichier AnyConnect > Objets > Gestion des objets > VPN > Fichier Secure Client > Ajouter un fichier Secure Connect).

- **Certificat client uniquement** : chaque utilisateur est authentifié avec un certificat client. Le certificat client doit être configuré sur les points terminaux clients VPN. Par défaut, le nom d'utilisateur est dérivé des champs de certificat client CN et OU. Si le nom d'utilisateur est spécifié dans d'autres champs du certificat client, utilisez les champs « Principal » et « Secondaire » pour mapper les champs appropriés.

  Sélectionnez **Enable multiple certificate authentication** (activer l'authentification de certificats multiples) pour authentifier le client VPN à l'aide des certificats du périphérique et de l'utilisateur.

  Si vous avez activé l'authentification par certificat multiple, vous pouvez sélectionner l'un des certificats suivants pour mapper le nom d'utilisateur et authentifier l'utilisateur VPN :

  - **First Certificate** (premier certificat) : sélectionnez cette option pour mapper le nom d'utilisateur du certificat de la machine envoyé par le client VPN.
  - **Second Certificate** (second certificat) : sélectionnez cette option pour mapper le nom d'utilisateur du certificat utilisateur envoyé par le client.

  Remarque Si vous n'activez pas l'authentification par certificats multiples, le certificat utilisateur (deuxième certificat) est utilisé pour l'authentification par défaut.

  Si vous sélectionnez l'option **Mapper un champ spécifique**, qui comprend le nom d'utilisateur du certificat client, les champs **principal** et **secondaire** affichent les valeurs par défaut : **CN (nom commun)** et **OU (unité organisationnelle)**, respectivement. Si vous sélectionnez l'option **Use entire DN as username** (Utiliser le DN entier comme nom d'utilisateur), le système récupère automatiquement l'identité de l'utilisateur. Un nom distinctif (DN) est une identification unique, composée de champs individuels utilisés comme identifiant lors de la correspondance des utilisateurs avec un profil de connexion. Les règles de nom distinctif sont utilisées pour l'authentification améliorée des certificats.

  Les champs principal et secondaire appartenant à l'option de **champ spécifique à la carte** contiennent les valeurs communes suivantes :

  - C (Pays)
  - CN (Nom courant)
  - DNQ (Qualificatif du DN)
  - EA (Adresse courriel)
  - GENQ (Qualificatif générationnel)
  - GN (Prénom)
  - I (Initial)

- L (Localité)
- N (Nom)
- O (Organisation)
- OU (Unité organisationnelle)
- SER (Numéro de série)
- SN (Nom de famille)
- SP (État ou province)
- T (Titre)
- UID (Identifiant de l'utilisateur)
- UPN (Nom principal de l'utilisateur)

- **Certificat client et AAA** : chaque utilisateur est authentifié à l'aide d'un certificat client et d'un serveur AAA. Sélectionner le certificat et les configurations AAA requis pour l'authentification.

  Quelle que soit la méthode d'authentification que vous choisissez, cochez ou décochez la case **Allow connection only if user Existing in authentication database** (Autoriser la connexion uniquement si l'utilisateur existe dans la base de données d'authentification).

- **Certificat client et SAML** : chaque utilisateur est authentifié à l'aide d'un certificat client et d'un serveur SAML. Sélectionner le certificat et les configurations SAML requis pour l'authentification.
  - **Autoriser la connexion uniquement si le nom d'utilisateur du certificat et de SAML sont identiques** : sélectionnez cette option pour autoriser la connexion VPN uniquement si le nom d'utilisateur du certificat correspond au nom d'utilisateur de connexion unique SAML.
  - **Utilisez le nom d'utilisateur du certificat client pour l'autorisation** : lorsque vous choisissez l'option permettant de choisir le nom d'utilisateur sur le certificat client pour l'autorisation, vous devez configurer les champs pour choisir dans le certificat client.

    Vous pouvez choisir de mapper un champ spécifique comme nom d'utilisateur ou d'utiliser le nom distinctif (DN) complet pour l'autorisation :
    - **Mapper le champ spécifique** : sélectionnez cette option pour inclure le nom d'utilisateur du certificat client. les champs **principal** et **secondaire** affichent les valeurs par défaut : **NC (nom commun)** et **OU (unité organisationnelle)**, respectivement.
    - **Utiliser tout le DN comme nom d'utilisateur** : le système récupère automatiquement l'identité de l'utilisateur pour autorisation.

  Vous pouvez également créer une politique d'accès dynamique (DAP) pour faire correspondre les attributs d'assertion SAML ou le nom d'utilisateur aux attributs du certificat DAP. Consultez Configurer les paramètres des critères AAA pour une DAP.

- **Serveur d'authentification** : l'authentification est la façon dont un utilisateur est identifié avant d'être autorisé à accéder au réseau et aux services réseau. L'authentification nécessite des identifiants d'utilisateur valides, un certificat ou les deux. Vous pouvez utiliser l'authentification seule ou avec l'autorisation et la comptabilité.

Sélectionnez un serveur d'authentification dans la liste si vous avez déjà ajouté un serveur, ou créez-en un :

- **LOCAL** : utilisez une base de données locale de défense contre les menaces pour l'authentification de l'utilisateur.
  - **Local Realm**(domaine local) : sélectionnez un domaine local ou cliquez sur **Add** (Ajouter) pour configurer un domaine. Consultez Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine.
- **Realm** (Domaine) : configurez un domaine LDAP ou AD. Consultez Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine.
- **RADIUS Server Group**(groupe de serveurs RADIUS) : ajoutez un objet de groupe de serveurs RADIUS avec les serveurs RADIUS. Consultez Ajouter un groupe de serveurs RADIUS.
- **Serveur de connexion unique** : crée un objet de serveur de connexion unique pour l'authentification SAML. Consultez Ajouter un serveur de connexion unique (SSO).

Recours à l'authentification locale : l'utilisateur est authentifié à l'aide de la base de données locale et le tunnel VPN peut être établi même si le groupe de serveurs AAA n'est pas disponible, à condition que la base de données locale soit configurée.

- **Utilisez l'authentification secondaire** : l'authentification secondaire est configurée en complément de l'authentification principale pour fournir une sécurité supplémentaire pour les sessions VPN. L'authentification secondaire s'applique uniquement aux méthodes d'authentification **AAA uniquement** et par **certificat client et AAA**.

  L'authentification secondaire est une fonctionnalité facultative qui oblige un utilisateur VPN à saisir deux ensembles de nom d'utilisateur et de mot de passe sur l'écran de connexion Secure Client. Vous pouvez également configurer le système pour préremplir le nom d'utilisateur secondaire à partir du serveur d'authentification ou du certificat client. L'authentification VPN de l'accès à distance est accordée uniquement si les authentifications principale et secondaire réussissent. L'authentification VPN est refusée si l'un des serveurs d'authentification n'est pas accessible ou si une authentification échoue.

  Vous devez configurer un groupe de serveurs d'authentification secondaire (serveur AAA) pour le deuxième nom d'utilisateur et mot de passe avant de configurer l'authentification secondaire. Par exemple, vous pouvez définir le serveur d'authentification principal sur un domaine LDAP ou Active Directory et l'authentification secondaire sur un serveur RADIUS.

  Remarque Par défaut, l'authentification secondaire n'est pas requise.

  Authentication Server(serveur d'authentification) : le serveur d'authentification secondaire fournit un nom d'utilisateur et un mot de passe secondaires aux utilisateurs de VPN.

  - **Recours à l'authentification LOCALE** : cet utilisateur est authentifié à l'aide de la base de données locale et le tunnel VPN peut être établi même si le groupe de serveurs AAA n'est pas disponible, à condition que la base de données locale soit configurée.

  Sélectionnez les éléments suivants sous **Username for secondary authentication** (Nom d'utilisateur pour l'authentification secondaire) :

  - **Invite** : Invite les utilisateurs à saisir le nom d'utilisateur et le mot de passe lors de la connexion à la passerelle VPN.

- **Utiliser le nom d'utilisateur de l'authentification principale** : le nom d'utilisateur provient du serveur d'authentification principal pour l'authentification principale et secondaire. vous devez saisir deux mots de passe.
- **Mapper le nom d'utilisateur du certificat client** : préremplit le nom d'utilisateur secondaire du certificat client.

  Si vous avez activé l'authentification par certificat multiple, vous pouvez sélectionner l'un des certificats suivants :

  - **First Certificate (premier certificat)** : sélectionnez cette option pour mapper le nom d'utilisateur du certificat de la machine envoyé par le client VPN.
  - **Second Certificate (second certificat)** : sélectionnez cette option pour mapper le nom d'utilisateur du certificat utilisateur envoyé par le client.
  - Si vous sélectionnez l'option **Map specific field** (Mapper un champ spécifique), qui comprend le nom d'utilisateur du certificat client. Les champs **principal** et **secondaire** affichent les valeurs par défaut : **NC (nom commun)** et **OU (unité organisationnelle)**, respectivement. Si vous sélectionnez l'option **Use entire DN (Distinguished Name) (Utiliser le Nom distinctif complet DN) comme nom d'utilisateur**, le système récupère automatiquement l'identité de l'utilisateur.

    Consultez la section Descriptions des **méthodes d'authentification** pour de plus amples renseignements sur le mappage des champs principal et secondaire.
  - **Préremplir le nom d'utilisateur à partir du certificat sur la fenêtre de connexion** : préremplit le nom d'utilisateur secondaire à partir du certificat client lorsque l'utilisateur se connecte avec Secure Client.
    - **Masquer le nom d'utilisateur dans la fenêtre de connexion** : le nom d'utilisateur secondaire est prérempli à partir du certificat client, mais masqué pour l'utilisateur afin que ce dernier ne modifie pas le nom d'utilisateur prérempli.
- **Utilisez le nom d'utilisateur secondaire pour la session VPN** : le nom d'utilisateur secondaire est utilisé pour signaler l'activité de l'utilisateur au cours d'une session VPN.

Étape 5 Sélectionnez les options suivantes pour l'**autorisation** :

- **Authorization Server** (Serveur d'autorisation) : une fois l'authentification terminée, l'autorisation contrôle les services et les commandes disponibles pour chaque utilisateur authentifié. L'autorisation consiste à rassembler un ensemble d'attributs qui décrivent ce que l'utilisateur est autorisé à faire, ses capacités réelles et ses restrictions. Lorsque vous n'utilisez pas l'autorisation, l'authentification à elle seule fournit le même accès à tous les utilisateurs authentifiés. L'autorisation requiert une authentification.

  Pour en savoir plus sur le fonctionnement de l'autorisation du VPN d'accès à distance, consultez Comprendre l'application des politiques d'autorisations et d'attributs, à la page 6.

  Lorsqu'un serveur RADIUS est configuré pour l'autorisation utilisateur dans le profil de connexion, l'administrateur du système VPN d'accès à distance peut configurer plusieurs attributs d'autorisation pour les utilisateurs ou groupes d'utilisateurs. Les attributs d'autorisation configurés sur le serveur RADIUS peuvent être propres à un utilisateur ou à un groupe d'utilisateurs. Une fois les utilisateurs authentifiés, ces attributs d'autorisation spécifiques sont transmis au périphérique défense contre les menaces .

Remarque Les attributs du serveur AAA obtenus à partir du serveur d'autorisation remplacent les valeurs d'attributs qui ont pu être configurées précédemment dans la politique de groupe ou le profil de connexion.

- Si vous le souhaitez, cochez la case **Autoriser la connexion uniquement si l'utilisateur existe dans la base de données d'autorisation**.

  Lorsque cette option est activée, le système vérifie que le nom d'utilisateur du client doit exister dans la base de données des autorisations pour permettre une connexion réussie. Si le nom d'utilisateur n'existe pas dans la base de données des autorisations, la connexion est refusée.

- Lorsque vous sélectionnez un domaine comme serveur d'autorisation, vous devez configurer une mise en correspondance des attributs LDAP. Vous pouvez choisir un serveur unique pour l'authentification et l'autorisation, ou plusieurs serveurs. Cliquer sur **Configure LDAP Attribute Map** (configuration de la mise en correspondance des attributs LDAP) pour ajouter des mappages d'attributs LDAP pour l'autorisation.

  Remarque Défense contre les menaces ne prend pas en charge le fournisseur d'identité SAML comme serveur d'autorisation. Si Active Directory derrière le fournisseur d'identité SAML est accessible au moyen de centre de gestion et défense contre les menaces , vous pouvez configurer l'autorisation en procédant comme suit :

  - Ajoutez un domaine pour le serveur AD. Consultez Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine.
  - Sélectionnez l'objet de domaine comme serveur d'autorisation dans le profil de connexion VPN d'accès à distance.
  - Configurez la mise en correspondance des attributs LDAP pour le domaine sélectionné.

  Pour en savoir plus sur la configuration des mappages d'attributs LDAP, consultez Configuration du mappage des attributs LDAP, à la page 51.

Étape 6 Sélectionnez les options suivantes pour la **comptabilité** :

- **Serveur de comptabilité** : la fonction de traçabilité est utilisée pour suivre les services auxquels les utilisateurs accèdent et la quantité de ressources réseau qu'ils consomment. Lorsque la comptabilité AAA est activée, le serveur d'accès au réseau signale l'activité de l'utilisateur au serveur RADIUS. Les renseignements de comptabilité comprennent les heures de début et de fin des sessions, les noms d'utilisateurs, le nombre d'octets qui passent par le périphérique pour chaque session, les services utilisés et la durée de chaque session. Ces données peuvent ensuite être analysées pour la gestion du réseau, la facturation au client ou l'audit. Vous pouvez utiliser la comptabilité seule ou conjointement avec l'authentification et l'autorisation.

  Précisez l'objet de groupe de serveurs RADIUS qui sera utilisé pour prendre en compte la session VPN d'accès à distance.

Étape 7 Sélectionnez les **paramètres avancés** suivants :

- **Supprimer le domaine du nom d'utilisateur** : sélectionnez cette option pour supprimer le domaine du nom d'utilisateur avant de transmettre le nom d'utilisateur au serveur AAA. Par exemple, si vous sélectionnez cette option et fournissez *domaine\nom d'utilisateur*, le domaine est supprimé du nom d'utilisateur et envoyé au serveur AAA pour authentification. Par défaut, cette fonction est désactivée.

- **Supprimer le groupe du nom d'utilisateur** : sélectionnez cette option pour supprimer le nom du groupe du nom d'utilisateur avant de transmettre ce nom au serveur AAA. Par défaut, cette fonction est désactivée.

  Remarque Un domaine est un domaine administratif. L'activation de ces options permet à l'authentification d'être basée sur le nom d'utilisateur uniquement. Vous pouvez activer n'importe quelle combinaison de ces options. Cependant, vous devez cocher les deux cases si votre serveur ne peut pas analyser les délimiteurs.

- **Password Management** (gestion des mots de passe) : activez la gestion du mot de passe pour les utilisateurs du VPN d'accès à distance. Sélectionnez cette option pour recevoir une notification avant l'expiration du mot de passe ou le jour où le mot de passe expire.

Étape 8 Cliquez sur **Save** (enregistrer).

Sujets connexes

Comprendre l'application des politiques d'autorisations et d'attributs, à la page 6
Gérer un domaine

Attributs du serveur RADIUS pour Cisco Secure Firewall Threat Defense

Le périphérique défense contre les menaces prend en charge l'application d'attributs d'autorisation d'utilisateur (également appelés droits ou autorisations d'utilisateur) aux connexions VPN à partir du serveur RADIUS externe qui sont configurées pour l'authentification ou l'autorisation dans la politique VPN d'accès à distance.

Remarque Les périphériques Cisco Secure Firewall Threat Defense prennent en charge les attributs avec l'ID de fournisseur 3076.

Les attributs d'autorisation utilisateur suivants sont envoyés au périphérique défense contre les menaces par le serveur RADIUS.

- Les attributs RADIUS 146 et 150 sont envoyés des périphériques défense contre les menaces au serveur RADIUS pour les demandes d'authentification et d'autorisation.
- Les trois attributs (146, 150 et 151) sont envoyés des périphériques défense contre les menaces au serveur RADIUS pour les demandes de démarrage, de mise à jour provisoire et d'arrêt de gestion.

Tableau 2 : Attributs RADIUS envoyés de Cisco Secure Firewall Threat Defense au serveur RADIUS

Attribut	Numéro de l'attribut	Syntaxe, type	Valeur unique ou valeurs multiples	Description ou valeur
Nom du profil de connexion ou nom du groupe de tunnels	146	Chaîne	Unique	1 à 253 caractères
Type de client	150	nombre entier	Unique	2 = Secure Client (services client sécurisés) SSL VPN, 6 = Secure Client (services client sécurisés) IPsec VPN (IKEv2)

Attribut	Numéro de l'attribut	Syntaxe, type	Valeur unique ou valeurs multiples	Description ou valeur
Type de séance	151	nombre entier	Unique	1 = Secure Client (services client sécurisés) SSL VPN, 2 = Secure Client (services client sécurisés) IPsec VPN (IKEv2)

Tableau 3 : Attributs d'autorisation RADIUS pris en charge

Nom de l'attribut	Défense contre les menaces	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
Heures d'accès	O	1	Chaîne	Unique	Nom de la plage temporelle, par exemple, Heure ouvrables
Liste d'accès entrant	O	86	Chaîne	Unique	Les deux attributs Access-List prennent le nom ACL configurée sur le périphérique défense con menaces . Créez ces listes de contrôle d'accès en le type d'objet Smart CLI Extended Access List d'accès étendue Smart CLI). (Sélectionnez **Devi** (Périphérique) > **Advanced Configuration** (Configuration avancée)> **Smart CLI** > **Object** (Objets)). Ces listes de contrôle d'accès contrôlent le flux dans le sens entrant (trafic entrant sur le périphé défense contre les menaces) ou sortant (trafic so périphérique défense contre les menaces .
Liste d'accès sortante	O	87	Chaîne	Unique	
Ensembles des adresses	O	217	Chaîne	Unique	Le nom d'un objet réseau défini sur le périphéri défense contre les menaces qui identifie un sous qui sera utilisé comme groupement d'adresses p clients se connectant au VPN d'accès à distance Définissez l'objet réseau dans la page **Objects** (puis associez l'objet réseau à une politique de gr à un profil de connexion.
Allow-Network-Extension-Mode	O	64	Booléen	Unique	0 = Désactivé 1 = Activé
Authenticated-User-Idle-Timeout	O	50	nombre entier	Unique	1 à 35791394 minutes
Authorization-DN-Field	O	67	Chaîne	Unique	Valeurs possibles : UID, OU, O, CN, L, SP, C, E N, GN, SN, I, GENQ, DNQ, SER, use-entire-na
Authorization-Required		66	nombre entier	Unique	0 = non 1 = oui
Authorization-Type	O	65	nombre entier	Unique	0 = Aucun 1 = RADIUS 2 = LDAP
Banner1	O	15	Chaîne	Unique	Chaîne de caractères de bannière à afficher pour sessions d'accès à distance VPN Cisco : IPsec IK Secure Client SSL-TLS/DTLS/IKEv2 et Clientl

Nom de l'attribut	Défense contre les menaces	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
Banner2	O	36	Chaîne	Unique	Chaîne de caractères de bannière à afficher p sessions d'accès à distance VPN Cisco : IPse Secure Client SSL-TLS/DTLS/IKEv2 et Cli La chaîne Bannière2 est concaténée à la chaîne si elle est configurée.
Cisco-IP-Phone-Bypass	O	51	nombre entier	Unique	0 = Désactivé 1 = Activé
Cisco-LEAP-Bypass	O	75	nombre entier	Unique	0 = Désactivé 1 = Activé
Type de client	O	150	nombre entier	Unique	1 = Cisco VPN Client (IKEv1) 2 = Secure Cli client sécurisés) SSL VPN 3 = Clientless SS Cut-Through-Proxy 5 = L2TP/IPsec SSL VPN Client (services client sécurisés) IPsec VPN
Client-Type-Version-Limiting	O	77	Chaîne	Unique	Chaîne du numéro de version de VPN IPSec
DHCP-Network-Scope	O	61	Chaîne	Unique	Adresse IP
Extended-Authentication-On-Rekey	O	122	nombre entier	Unique	0 = Désactivé 1 = Activé
Framed-Interface-Id	O	96	Chaîne	Unique	ID de l'interface IPv6 affectée. Se combine a Framed-IPv6-Prefix pour créer une adresse IPv Par exemple : Framed-Interface-ID=1:1:1:1 co Framed-IPv6-Prefix= 2001:0db8::/64 donne attribuée 2001:0db8::1:1:1:1.
Framed-IPv6-Prefix	O	97	Chaîne	Unique	Préfixe et longueur IPv6 affectées. À combi Framed-Interface-Id pour créer une adresse I complète. Par exemple : prefix 2001:0db8::/ avec Framed-Interface-Id=1:1:1:1:1 donne l' 2001:0db8::1:1:1:1. Vous pouvez utiliser cet a attribuer une adresse IP sans utiliser Framed-I en attribuant l'adresse IPv6 complète avec la de préfixe /128, par exemple, Framed-IPv6-Prefix=2001:0db8::1/128.
Politique de groupe	O	25	Chaîne	Unique	Définit la politique de groupe pour la session V à distance. Vous pouvez utiliser l'un des forma • *nom de la politique de groupe* • OU=*nom de la politique de groupe* • OU=*nom de la politique de groupe*;
IE-Proxy-Bypass-Local		83	nombre entier	Unique	0 = aucun 1 = local

Nom de l'attribut	Défense contre les menaces	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
IE-Proxy-Exception-List		82	Chaîne	Unique	Nouvelle liste de domaines DNS séparés par des (\n)
URL-PAC-IE-Proxy	O	133	Chaîne	Unique	Chaîne d'adresse PAC
IE-Proxy-Server		80	Chaîne	Unique	Adresse IP
IE-Proxy-Server-Policy		81	nombre entier	Unique	1 = Aucune modification 2 = Aucun mandataire Détection automatique 4 = Utiliser le paramètre concentrateur
IKE-KeepAlive-Confidence-Interval	O	68	nombre entier	Unique	10 à 300 secondes
IKE-Keepalive-Retry-Interval	O	84	nombre entier	Unique	2 à 10 secondes
IKE-Keep-Alives	O	41	Booléen	Unique	0 = Désactivé 1 = Activé
Intercept-DHCP-Configure-Msg	O	62	Booléen	Unique	0 = Désactivé 1 = Activé
IPsec-Allow-Passwd-Store	O	16	Booléen	Unique	0 = Désactivé 1 = Activé
IPsec-Authentication		13	nombre entier	Unique	0 = Aucun 1 = RADIUS 2 = LDAP (autorisation seulement) 3 = Domaine NT 4 = SDI 5 = Interne RADIUS avec expiration 7 = Kerberos/Active D
IPsec-Auth-On-Rekey	O	42	Booléen	Unique	0 = Désactivé 1 = Activé
IPsec-Backup-Server-List	O	60	Chaîne	Unique	Adresses du serveur (délimitées par un espace)
IPsec-Backup-Servers	O	59	Chaîne	Unique	1 = Utiliser la liste configurée par le client 2 = Dé et effacer la liste du client 3 = Utiliser la liste du de sauvegarde
IPsec-Client-Firewall-Filter-Name		57	Chaîne	Unique	Spécifie le nom du filtre à envoyer au client en t politique de pare-feu
IPsec-Client-Firewall-Filter-Optional	O	58	nombre entier	Unique	0 = obligatoire 1 = facultatif
IPsec-Default-Domain	O	28	Chaîne	Unique	Spécifie le nom de domaine par défaut à envoyer (1 à 255 caractères).
IPsec-IKE-Peer-ID-Check	O	40	nombre entier	Unique	1 = Obligatoire 2 = Si pris en charge par le certi homologue 3 = Ne pas vérifier
IPsec-IP-Compression	O	39	nombre entier	Unique	0 = Désactivé 1 = Activé
IPsec-Mode-Config	O	31	Booléen	Unique	0 = Désactivé 1 = Activé
IPsec-Over-UDP	O	34	Booléen	Unique	0 = Désactivé 1 = Activé

Nom de l'attribut	Défense contre les menaces	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
IPsec-Over-UDP-Port	O	35	nombre entier	Unique	4001à 49151. La valeur par défaut est 10 00
IPsec-Required-Client-Firewall-Capability	O	56	nombre entier	Unique	0 = Aucune 1 = Politique définie par le micr Are You There (Ayt) distant 2 = Politique tra CPP 4 = Politique du serveur
IPsec-Sec-association		12	Chaîne	Unique	Nom de l'association de sécurité
IPsec-Split-DNS-Names	O	29	Chaîne	Unique	Spécifie la liste des noms de domaines secon envoyer au client (1 à 255 caractères).
IPsec-Split-Tunneling-Policy	O	55	nombre entier	Unique	0 = Aucun tunnellisation fractionnée 1 = Tu fractionnée 2 = LAN local autorisé
IPsec-Split-Tunnel-List	O	27	Chaîne	Unique	Spécifie le nom du réseau ou de la liste de c d'accès qui décrit la liste d'inclusion du tunne
IPsec-Tunnel-Type	O	30	nombre entier	Unique	1 = LAN à LAN 2 = Accès à distance
IPsec-User-Group-Lock		33	Booléen	Unique	0 = Désactivé 1 = Activé
IPv6-Address-Pools	O	218	Chaîne	Unique	Name of IP local pool-IPv6
IPv6-VPN-Filter	O	219	Chaîne	Unique	Valeur ACL
L2TP-Encryption		21	nombre entier	Unique	Bitmap : 1 = Chiffrement requis 2 = 40 bits 8 = Stateless-Req 15 = 40/128-Encr/Stateles
L2TP-MPPC-Compression		38	nombre entier	Unique	0 = Désactivé 1 = Activé
Member-Of	O	145	Chaîne	Unique	Chaîne délimitée par des virgules, par exemp `Engineering, Sales` Attribut administratif qui peut être utilisé da politiques d'accès dynamique. Elle ne défini politique de groupe.
MS-Client-Subnet-Mask	O	63	Booléen	Unique	Une adresse IP
NAC-Default-ACL		92	Chaîne		ACL
NAC-Enable		89	nombre entier	Unique	0 = non 1 = oui
NAC-Revalidation-Timer		91	nombre entier	Unique	300 à 86 400 secondes
NAC-Settings	O	141	Chaîne	Unique	Nom de la politique NAC
NAC-Status-Query-Timer		90	nombre entier	Unique	30 à 1800 secondes
Perfect-Forward-Secrecy-Enable	O	88	Booléen	Unique	0 = non 1 = oui

Nom de l'attribut	Défense contre les menaces	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
PPTP-Encryption		20	nombre entier	Unique	Bitmap : 1 = Chiffrement requis 2 = 40 bits 4 = 8 = Stateless-Requis 15= 40/128-Encr/Stateless-
PPTP-MPPC-Compression		37	nombre entier	Unique	0 = Désactivé 1 = Activé
Primary-DNS	O	5	Chaîne	Unique	Une adresse IP
Primary-WINS	O	7	Chaîne	Unique	Une adresse IP
Privilege-Level	O	220	nombre entier	Unique	Un nombre entier entre 0 et 15.
Required-Client- Firewall-Vendor-Code	O	45	nombre entier	Unique	1 = Cisco Systems (avec Cisco Integrated Client Zone Labs 3 = NetworkICE 4 = Sygate 5 = Cisco (avecCisco Intrusion Prevention Security Agent
Required-Client-Firewall-Description	O	47	Chaîne	Unique	Chaîne
Required-Client-Firewall-Product Code	O	46	nombre entier	Unique	Produits Cisco Systems : 1 = Cisco Intrusion Prevention Security Agent o Integrated Client (CIC) Produits Zone Labs : 1 = Alarme de zone 2 = Al zone Pro 3 = Zone Labs Integrity Produit NetworkICE : 1 = NoirIce Defender/Ag Produits Sygate : 1 = Personal Firewall 2 = Pers Firewall Pro 3 = security Agent
Required-Individual-User-Auth	O	49	nombre entier	Unique	0 = Désactivé 1 = Activé
Require-HW-Client-Auth	O	48	Booléen	Unique	0 = Désactivé 1 = Activé
Secondary-DNS	O	6	Chaîne	Unique	Une adresse IP
Secondary-WINS	O	8	Chaîne	Unique	Une adresse IP
SEP-Card-Attribution		9	nombre entier	Unique	Non utilisé
Sous-type de session	O	152	nombre entier	Unique	0 = Aucun 1 = Sans client 2 = Client 3 = Client se Le sous-type de session s'applique uniquement l l'attribut de type de session (151) a les valeurs su 1, 2, 3 et 4.
Type de séance	O	151	nombre entier	Unique	0 = Aucun 1 = Secure Client (services client séc VPN SSL 2 = Secure Client (services client sécu VPN IPSec (IKEv2) 3 = VPN SSL sans client 4 = mandataire de messagerie sans client 5 = Client VPN (IKEv1) 6 = IKEv1 LAN-LAN 7 = IKEv2 LAN-LAN 8 = Équilibrage de charge VPN

Nom de l'attribut	Défense contre les menaces	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
Connexions simultanées	O	2	nombre entier	Unique	0 à 2147483647
Smart-Tunnel	O	136	Chaîne	Unique	Nom d'un tunnel intelligent
Smart-Tunnel-Auto	O	138	nombre entier	Unique	0 = Désactivé 1 = Activé 2 = Démarrage aut
Smart-Tunnel-Auto-Signon-Enable	O	139	Chaîne	Unique	Nom d'une liste de connexion automatique c Smart à côté du nom de domaine
Strip-Realm	O	135	Booléen	Unique	0 = Désactivé 1 = Activé
SVC-Ask	O	131	Chaîne	Unique	0 = Désactivé 1 = Activé 3 = Active le servic 5 = Active l'absence de client par défaut (2 e utilisés)
SVC-Ask-Timeout	O	132	nombre entier	Unique	5 à 120 secondes
Client-SVC-DPD-Interval	O	108	nombre entier	Unique	0 = Désactivé, 5 à 3 600 secondes
Passerelle-SVC-DPD-Interval	O	109	nombre entier	Unique	0 = Désactivé) 5 à 3 600 secondes
SVC-DTLS	O	123	nombre entier	Unique	0 = faux 1 = vrai
SVC-Keepalive	O	107	nombre entier	Unique	0 = Désactivé, 15 à 600 secondes
SVC-Modules	O	127	Chaîne	Unique	Chaîne de caractères (nom d'un module)
SVC-MTU	O	125	nombre entier	Unique	Valeur MTU 256 à 1406 en octets
SVC-Profiles	O	128	Chaîne	Unique	Chaîne de caractères (nom d'un profil)
SVC-Rekey-Time	O	110	nombre entier	Unique	0 = Désactivé 1 à 10 080 minutes
Tunnel Group Name	O	146	Chaîne	Unique	1 à 253 caractères
Tunnel-Group-Lock	O	85	Chaîne	Unique	Nom du groupe de tunnels ou « none » (aucu
Tunneling-Protocoles	O	11	nombre entier	Unique	1 = PPTP 2 = L2TP 4 = IPSec (IKEv1) 8 = I 16 = WebVPN 32 = SVC 64 = IPsec (IKEv2 s'excluent mutuellement. 0 à 11, 16 à 27, 32 59 sont des valeurs autorisées.
Use-Client-Address		17	Booléen	Unique	0 = Désactivé 1 = Activé
VLAN	O	140	nombre entier	Unique	0 à 4094
WebVPN-Access-List	O	73	Chaîne	Unique	Nom de la liste d'accès
WebVPN ACL	O	73	Chaîne	Unique	Nom d'une ACL WebVPN sur le périphériqu
WebVPN-ActiveX-Relay	O	137	nombre entier	Unique	0 = Désactivé Sinon = Activé

Nom de l'attribut	Défense contre les menaces	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
WebVPN-Apply-ACL	O	102	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-Auto-HTTP-Signon	O	124	Chaîne	Unique	Réservé
WebVPN-Citrix-Metaframe-Enable	O	101	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-Content-Filter-Parameters	O	69	nombre entier	Unique	1 = Java ActiveX 2 = Java Script 4 = Image 8 = T dans les images
WebVPN-Customization	O	113	Chaîne	Unique	Nom de la personnalisation
WebVPN-Default-Homepage	O	76	Chaîne	Unique	Une URL telle que http://exemple-exemple.com
WebVPN-Deny-Message	O	116	Chaîne	Unique	Chaîne de caractères valide (jusqu'à 500 caractè
WebVPN-Download_Max-Size	O	157	nombre entier	Unique	0x7fffffff
WebVPN-File-Access-Enable	O	94	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-File-Server-Browsing-Enable	O	96	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-File-Server-Entry-Enable	O	95	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-Group-based-HTTP/HTTPS-Proxy-Exception-List	O	78	Chaîne	Unique	DNS/IP séparés par des virgules avec un caractè générique facultatif (*) (par exemple *.cisco.cor 192.168.1.*, wwwin.cisco.com)
WebVPN-Hidden-Shares	O	126	nombre entier	Unique	0 = aucun 1 = visible
WebVPN-Home-Page-Use-Smart-Tunnel	O	228	Booléen	Unique	Activé si la page d'accueil sans client doit être a par l'intermédiaire de Smart Tunnel.
WebVPN-HTML-Filter	O	69	Bitmap	Unique	1 = ActiveX Java 2 = Scripts 4 = Image 8 = Tén
WebVPN-HTTP-Compression	O	120	nombre entier	Unique	0 = Désactivé 1 = Décompression
WebVPN-HTTP-Proxy-IP-Address	O	74	Chaîne	Unique	DNS/IP séparé par des virgules:port, avec le préfi ou https= (par exemple http=10.10.10:80, https=11.11.11.11:443)
WebVPN-Idle-Timeout-Alert-Interval	O	148	nombre entier	Unique	0 à 30. 0 = Désactivé.
WebVPN-Keepalive-Ignore	O	121	nombre entier	Unique	0 à 900
WebVPN-Macro-Substitution	O	223	Chaîne	Unique	Illimité.
WebVPN-Macro-Substitution	O	224	Chaîne	Unique	Illimité.
WebVPN-Port-Forwarding-Enable	O	97	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	O	98	nombre entier	Unique	0 = Désactivé 1 = Activé

Nom de l'attribut	Défense contre les menaces	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
WebVPN-Port-Forwarding-HTTP-Proxy	O	99	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-Port-Forwarding-List	O	72	Chaîne	Unique	Nom de la liste de transferts de port
WebVPN-Port-Forwarding-Name	O	79	Chaîne	Unique	Nom de chaîne de caractères (par exemple, « Corporate-Apps »). Ce texte remplace la chaîne par défaut « App Access » dans la page d'accueil du portail sa
WebVPN-post-maximum-taille	O	159	nombre entier	Unique	0x7fffffff
WebVPN-Session-Timeout-Alert-Interval	O	149	nombre entier	Unique	0 à 30. 0 = Désactivé.
WebVPN Smart-Card-Removal-Disconnect	O	225	Booléen	Unique	0 = Désactivé 1 = Activé
WebVPN-Smart-Tunnel	O	136	Chaîne	Unique	Nom d'un tunnel intelligent
WebVPN-Smart-Tunnel-Auto-Sign-On	O	139	Chaîne	Unique	Nom d'une liste de connexion automatique d Tunnel ajouté par le nom de domaine
WebVPN-Smart-Tunnel-Auto-Start	O	138	nombre entier	Unique	0 = Désactivé 1 = Activé 2 = Démarrage aut
WebVPN-Smart-Tunnel-Tunnel-Policy	O	227	Chaîne	Unique	Un des choix « e networkname », « i networ « a », où networkname est le nom d'une liste Smart Tunnels, e indiquant le tunnel exclu, i spécifié et a indique tous les tunnels.
WebVPN-SSL-VPN-Client-Enable	O	103	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-SSL-VPN-Client-Keep- Installation	O	105	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-SSL-VPN-Client-Required	O	104	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-SSO-Server-Name	O	114	Chaîne	Unique	Chaîne de caractères valide
WebVPN-Storage-Key	O	162	Chaîne	Unique	
WebVPN-Storage-Objects	O	161	Chaîne	Unique	
WebVPN-SVC-Keepalive-Frequency	O	107	nombre entier	Unique	15 à 600 secondes, 0 = désactivé
WebVPN-SVC-Client-DPD-Frequency	O	108	nombre entier	Unique	5 à 3 600 secondes, 0 = désactivé
WebVPN-SVC-DTLS-Enable	O	123	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-SVC-DTLS-MTU	O	125	nombre entier	Unique	La valeur MTU est comprise entre 256 et 14
WebVPN-SVC-Gateway-DPD-Frequency	O	109	nombre entier	Unique	5 à 3 600 secondes, 0 = désactivé
WebVPN-SVC-Rekey-Time	O	110	nombre entier	Unique	4 à 10 080 minutes, 0 = Désactivé

Nom de l'attribut	Défense contre les menaces	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
WebVPN-SVC-Rekey-Method	O	111	nombre entier	Unique	0 (désactivé), 1 (SSL), 2 (nouveau tunnel)
WebVPN-SVC-Compression	O	112	nombre entier	Unique	0 (Désactivé), 1 (Décompression)
WebVPN-UNIX-Group-ID (GID)	O	222	nombre entier	Unique	ID de groupe UNIX valides
WebVPN-UNIX-User-ID (UIDs)	O	221	nombre entier	Unique	ID d'utilisateur UNIX valides
WebVPN-Upload-Max-Size	O	158	nombre entier	Unique	0x7fffffff
WebVPN-URL-Entry-Enable	O	93	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-URL-List	O	71	Chaîne	Unique	Nom de la liste d'URL
WebVPN-User-Storage	O	160	Chaîne	Unique	
WebVPN-VDI	O	163	Chaîne	Unique	Liste des paramètres

Tableau 4 : Attributs RADIUS envoyés à Cisco Secure Firewall Threat Defense

Attribut	Numéro de l'attribut	Syntaxe, type	Valeur unique ou valeurs multiples	Description ou valeur
Ensembles des adresses	217	Chaîne	Unique	Le nom d'un objet réseau défini sur le périphérique défense contre les menaces qui identifie un sous-réseau, qui sera utilisé comme groupement d'adresses pour les clients se connectant au VPN d'accès à distance. Définissez l'objet réseau dans la page **Objects** (objets).
Banner1	15	Chaîne	Unique	Bannière à afficher lorsque l'utilisateur se connecte.
Banner2	36	Chaîne	Unique	La deuxième partie de la bannière à afficher lorsque l'utilisateur se connecte. Bannière2 est ajouté à Bannière1.
Listes de contrôle d'accès téléchargeables	Cisco-AV-Pair	merge-dacl {before-avpair | after-avpair}		Pris en charge par la configuration Cisco-AV-Pair.
Filtrer les ACL	86, 87	Chaîne	Unique	Les ACL de filtres sont désignées par le nom d'ACL dans le serveur RADIUS. Cela nécessite que la configuration d'ACL soit déjà présente sur le périphérique défense contre les menaces , afin qu'elle puisse être utilisée lors de l'autorisation RADIUS. 86=Access-List-Inbound 87=Access-List-Outbound

Attribut	Numéro de l'attribut	Syntaxe, type	Valeur unique ou valeurs multiples	Description ou valeur
Politique de groupe	25	Chaîne	Unique	La politique de groupe à utiliser dans la connexion. Vous devez créer la politique de groupe sur la page des **politiques de groupe** VPN d'accès à distance. Vous pouvez utiliser l'un des formats suivants : • *nom de la politique de groupe* • OU=*nom de la politique de groupe* • OU=*nom de la politique de groupe*;
Connexions simultanées	2	nombre entier	Unique	Nombre de connexions simultanées distinctes que l'utilisateur est autorisé à établir, 0 à 2147483647.
VLAN	140	nombre entier	Unique	Le VLAN dans lequel limiter la connexion de l'utilisateur, 0 à 4094. Vous devez également configurer ce VLAN sur une sous-interface du périphérique défense contre les menaces .

Vous devez définir les valeurs de l'attribut IE-Proxy-Server-Method renvoyé par ISE à l'une des valeurs suivantes :

- IE_PROXY_METHOD_PACFILE: 8
- IE_PROXY_METHOD_PACFILE_AND_AUTODETECT: 11
- IE_PROXY_METHOD_PACFILE_AND_USE_SERVER: 12
- IE_PROXY_METHOD_PACFILE_AND_AUTODETECT_AND_USE_SERVER: 15

Défense contre les menaces ne fournit un paramètre de proxy que si l'une des valeurs ci-dessus est utilisée pour l'attribut IE-Proxy-Server-Method.

Créer ou mettre à jour des alias pour un profil de connexion

Les alias contiennent d'autres noms ou URL pour un profil de connexion spécifique. Les administrateurs VPN d'accès à distance peuvent activer ou désactiver les noms d'alias et les URL d'alias. Les utilisateurs de VPN peuvent choisir un nom d'alias lorsqu'ils se connectent au périphérique Cisco Secure Firewall Threat Defense. Les alias de toutes les connexions configurées sur ce périphérique peuvent être activés ou désactivés pour l'affichage. Vous pouvez également configurer la liste des URL d'alias, que vos points terminaux peuvent sélectionner lors du lancement de la connexion VPN d'accès à distance. Si les utilisateurs se connectent à l'aide de l'URL d'alias, le système les connecte automatiquement en utilisant le profil de connexion qui correspond à cette dernière.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Cliquez sur **Edit** dans la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (modifier) dans le profil de connexion pour lequel vous souhaitez créer ou mettre à jour des alias.

Étape 4 Cliquez sur **Alias**.

Étape 5 Pour ajouter un nom d'alias, procédez comme suit :

a) Cliquez sur **Add** (Ajouter) sous **Alias Names** (Noms d'alias).
b) Spécifiez le **nom de l'alias**.
c) Cochez la case **Enabled** (activer) dans chaque fenêtre pour activer les alias.
d) Cliquez sur **OK**.

Étape 6 Pour ajouter une URL d'alias, procédez comme suit :

a) Cliquez sur **Add** (Ajouter) sous **URL Alias** (alias d'URL).
b) Sélectionnez l' **URL d'alias** dans la liste ou créez un nouvel objet URL. Pour obtenir plus de renseignements, consultez Création d'objets URL.
c) Cochez la case **Enabled** (activer) dans chaque fenêtre pour activer les alias.
d) Cliquez sur **OK**.

Étape 7 Enregistrez vos modifications.

Sujets connexes

Configurer les paramètres du profil de connexion, à la page 24

Configurer les interfaces d'accès pour le VPN d'accès à distance

Le tableau **Interface d'accès** répertorie les groupes d'interfaces et les zones de sécurité qui contiennent les interfaces de périphérique. Ceux-ci sont configurés pour les connexions VPN SSL ou IPsec IKEv2 d'accès à distance. Le tableau affiche le nom de chaque groupe d'interfaces ou zone de sécurité, les points de confiance d'interface utilisés par l'interface et si DTLS (Datagram Transport Layer Security) est activé.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Sélectionnez une politique VPN d'accès à distance existante dans la liste et cliquez sur l'icône **Modifier** correspondante.

Étape 3 Cliquez sur **Access Interface** (interface d'accès).

Étape 4 Pour ajouter une interface d'accès, sélectionnez **Add** (ajouter) et définissez les valeurs des éléments suivants dans la fenêtre **Add Access Interface** (ajouter une interface d'accès) :

a) **Access Interface** (interface d'accès) : sélectionnez le groupe d'interfaces ou la zone de sécurité auquel l'interface appartient.

Le groupe d'interfaces ou la zone de sécurité devraient être de type routé. Les autres types d'interface ne sont pas pris en charge pour la connectivité VPN d'accès à distance.

b) Associez l'objet **Protocol** (protocole) à l'interface d'accès en sélectionnant les options suivantes :

- **Enable IPSet-IKEv2** (activer IPSet IKEv2) : sélectionnez cette option pour activer les paramètres **IKEv2**.
- **Enable SSL**(activer SSL) : sélectionnez cette option pour activer les paramètres **SSL**.

- Sélectionnez **Enable Datagram Transport Layer Security** (Activer la sécurité de la couche transport en datagramme).

  Lorsque cette option est sélectionnée, elle active Datagram Transport Layer Security (DTLS) sur l'interface et permet au Module AnyConnect VPN de Cisco Secure Client d'établir une connexion SSL VPN en utilisant deux tunnels simultanés, un tunnel SSL et un tunnel DTLS.

  L'activation de DTLS évite les problèmes de latence et de bande passante associés à certaines connexions SSL et améliore la performance des applications en temps réel sensibles aux retards de paquets.

  Pour configurer les paramètres SSL et les versions TLS et DTLS, consultez À propos des paramètres SSL.

  Pour configurer les paramètres SSL pour le module de Cisco Secure Client, consultez Options de politique de groupe Secure Client (services client sécurisés).

- Cochez la case **Configure InterfaceSpecific Identity Certificate** (configuration du certificat d'identité spécifique à l'interface), puis sélectionnez **Interface Identity Certificate** (Certificat d'identité d'interface) dans la liste déroulante.

  Si vous ne sélectionnez pas le certificat d'identité d'interface, le point de confiance **Trustpoint** sera utilisé par défaut.

  Si vous ne sélectionnez pas le certificat d'identité d'interface ou le point de confiance, le **certificat d'identité global SSL** sera utilisé par défaut.

c) Cliquez sur **OK** pour enregistrer les modifications.

Étape 5 Sélectionnez les éléments suivants sous **Paramètres d'accès** :

- **Autoriser les utilisateurs à sélectionner le profil de connexion lors de la connexion** : si vous avez plusieurs profils de connexion, la sélection de cette option permet à l'utilisateur de sélectionner le bon profil de connexion lors de la connexion. Vous devez sélectionner cette option pour les VPN **IPsec-IKEv2**.

Étape 6 Utilisez les options suivantes pour configurer **les paramètres SSL** :

- **Web Access Port Number** (numéro de port d'accès Web) : port à utiliser pour les sessions VPN. La valeur du port par défaut est 443.
- **DTLS Port Number** (Numéro de port DTLS) : le port UDP à utiliser pour les connexions DTLS. La valeur du port par défaut est 443.
- **Certificat d'identité global SSL** : le **certificat d'identité global SSL** sélectionné sera utilisé pour toutes les interfaces associées si le **certificat d'identité spécifique** à l'interface n'est pas fourni.

Étape 7 Pour les **Paramètres IPsec-IKEv2**, sélectionnez le **certificat d'identité IKEv2** dans la liste ou ajoutez un certificat d'identité.

Étape 8 Dans la section **Access Control for VPN Traffic** (contrôle d'accès pour le trafic VPN, sélectionnez l'option suivante si vous souhaitez contourner la politique de contrôle d'accès :

- **Contourner la politique de contrôle d'accès pour le trafic déchiffré (sysopt permit-vpn)** : le trafic déchiffré est soumis à une inspection de la politique de contrôle d'accès par défaut. Cette option contourne l'inspection de la politique de contrôle d'accès, mais le filtre VPN et l'autorisation de l'ACL téléchargés du serveur AAA sont toujours appliqués au trafic VPN.

Remarque Si vous sélectionnez cette option, vous n'avez pas besoin de mettre à jour la politique de contrôle d'accès pour le VPN d'accès à distance comme spécifié dans Mettre à jour la politique de contrôle d'accès sur le périphérique Cisco Secure Firewall Threat Defense, à la page 16.

Étape 9 Cliquez sur **Save** (Enregistrer) pour enregistrer les modifications apportées à l'interface d'accès.

Sujets connexes

Interface

Configurer les options avancées pour le VPN d'accès à distance

Image Cisco Secure Client

image Secure Client

Le Secure Client fournit des connexions SSL ou IPsec sécurisées (IKEv2) vers le périphérique défense contre les menaces pour les utilisateurs distants avec un profilage VPN complet pour les ressources de l'entreprise. Sans client préalablement installé, les utilisateurs distants peuvent saisir l'adresse IP d'une interface configurée pour accepter les connexions VPN sans client dans leur navigateur pour télécharger et installer Secure Client (services client sécurisés). Le périphérique défense contre les menaces télécharge le client correspondant au système d'exploitation de l'ordinateur distant. Après le téléchargement, le client installe et établit une connexion sécurisée. Dans le cas d'un client déjà installé, lorsque l'utilisateur s'authentifie, le périphérique défense contre les menaces examine la version du client et met ce dernier à niveau au besoin.

L'administrateur VPN d'accès à distance associe toutes les images Secure Client (services client sécurisés) nouvelles ou supplémentaires à la politique VPN. L'administrateur peut dissocier les ensembles clients non pris en charge ou en fin de vie qui ne sont plus nécessaires.

Le Cisco Secure Firewall Management Center détermine le type de système d'exploitation en utilisant le nom de l'ensemble de fichiers. Si l'utilisateur a renommé le fichier sans indiquer les informations sur le système d'exploitation, le type de système d'exploitation valide doit être sélectionné dans la zone de liste.

Téléchargez le fichier image Secure Client (services client sécurisés) en consultant le centre de téléchargement de logiciels Cisco.

Sujets connexes

Ajout d'une image Secure Client à Cisco Secure Firewall Management Center, à la page 46

Ajout d'une image Secure Client à Cisco Secure Firewall Management Center

Vous pouvez téléverser l'image Secure Client sur Cisco Secure Firewall Management Center en utilisant l'objet **Secure Client**. Pour en savoir plus, consultez Objets de fichier. Pour plus d'informations sur l'image client, consultez Image Cisco Secure Client, à la page 46.

Procédure

Étape 1 Sélectionner **Périphériques** > **Accès à distance**, choisissez et modifiez une politique d'accès à distance répertoriée, puis choisissez l'onglet **Avancé**.

Étape 2 Cliquez sur **Add** pour ajouter une image Secure Client.

Étape 3 Cliquez sur **Add** de la partie **Available Secure Client Images** de la boîte de dialogue **des images Secure Client**.

Étape 4 Saisissez le **nom** et la **description** (facultative) de l'image Secure Client disponible.

Étape 5 Cliquez sur **Browse** (Parcourir), localisez et sélectionnez l'image client que vous souhaitez téléverser.

Étape 6 Cliquez sur **Save** (Enregistrer) pour téléverser l'image vers centre de gestion.

Lorsque vous téléversez l'image client vers Cisco Secure Firewall Management Center, les informations sur le système d'exploitation de l'image s'affichent automatiquement.

Étape 7 Pour modifier l'ordre des images client, cliquez sur **Show Re-order buttons** (Afficher les boutons de réorganisation) et déplacez l'image client vers le haut ou le bas.

Sujets connexes

Image Cisco Secure Client, à la page 46

Mettre à jour Secure Client Image pour les clients VPN d'accès à distance

Lorsque de nouvelles mises à jour Secure Client sont disponibles dans le Centre de téléchargement de logiciels Cisco, vous pouvez télécharger les paquets manuellement et les ajouter à la politique VPN d'accès à distance afin que les nouveaux paquets clients soient mis à niveau sur les systèmes clients VPN en fonction de leurs systèmes d'exploitation.

Avant de commencer

Les instructions de cette section vous aident à mettre à jour les nouvelles images Secure Client des clients VPN d'accès à distance qui se connectent à la passerelle VPN Cisco Secure Firewall Threat Defense. Assurez-vous que les configurations suivantes sont terminées avant de mettre à jour vos images Secure Client :

- Téléchargez les derniers fichiers image Secure Client depuis le centre de téléchargement de logiciels Cisco.
- Sur votre interface Web Cisco Secure Firewall Management Center, accédez à **Objets** > **Gestion des objets** > **VPN** > **Fichier Secure Client** et ajoutez les nouveaux fichiers image Secure Client.

Procédure

Étape 1 Sur l'interface Web Cisco Secure Firewall Management Center, choisissez **Devices** (périphériques) > **VPN** > **Remote Access** (accès à distance).

Étape 2 Cliquez sur **Edit** (Modifier) dans la politique VPN d'accès à distance que vous souhaitez mettre à jour.

Étape 3 Cliquez sur **Advanced** > **Secure Client Image** > **Add**.

Étape 4 Sélectionnez un fichier image client dans **Images Secure Client disponibles** et cliquez sur **Add** (ajouter).

Si l'image client requise n'est pas répertoriée, cliquez sur **Add** (ajouter) pour rechercher et téléverser une image.

Étape 5 Cliquez sur **OK**.

Étape 6 Enregistrez la politique VPN d'accès à distance.
Une fois les modifications de la politique d'accès VPN à distance déployées, les nouvelles images Secure Client sont mises à jour sur le périphérique Cisco Secure Firewall Threat Defense configuré comme passerelle d'accès VPN à distance. Lorsqu'un nouvel utilisateur VPN se connecte à la passerelle VPN, l'utilisateur reçoit la nouvelle image Secure Client (services client sécurisés) à télécharger en fonction du système d'exploitation

du système client. Pour les utilisateurs VPN existants, l'image Secure Client (services client sécurisés) est mise à jour lors de leur prochaine session VPN.

Ajouter un progiciel de navigateur externe Cisco Secure Client au Cisco Secure Firewall Management Center

Si vous avez l'image du logiciel de navigateur externe Secure Client sur votre disque local, utilisez cette procédure pour la téléverser sur Cisco Secure Firewall Management Center. Après avoir téléchargé le progiciel de navigateur externe, vous pouvez le mettre à jour pour vos connexions VPN d'accès à distance.

Vous pouvez téléverser le fichier du progiciel de navigateur externe vers Cisco Secure Firewall Management Center en utilisant l'objet Fichier **Secure Client**. Pour en savoir plus, consultez Objets de fichier.

Points à retenir

- Un seul progiciel de navigateur externe peut être ajouté au périphérique défense contre les menaces .
- Une fois le progiciel de navigateur externe ajouté à centre de gestion, le navigateur est envoyé vers défense contre les menaces uniquement lorsque le navigateur externe est activé dans la configuration VPN d'accès à distance.

Procédure

Étape 1 Sur l'interface Web Cisco Secure Firewall Management Center, choisissez **Périphériques > Accès à distance**, choisissez et modifiez une politique d'accès à distance répertoriée, puis choisissez l'onglet **Avancé**.

Étape 2 Cliquez sur **Add** (Ajouter) dans la partie **Progiciel de navigateur externe Secure Client** de la page **Images Secure Client**.

Étape 3 Saisissez le **Nom** et la **Description** du progiciel Secure Client.

Étape 4 Cliquez sur **Parcourir** et localisez le fichier du progiciel du navigateur externe à téléverser.

Étape 5 Cliquez sur **Save** (Enregistrer) pour téléverser l'image vers Cisco Secure Firewall Management Center.

Remarque Si vous souhaitez mettre à jour la connexion VPN d'accès à distance avec un progiciel de navigateur externe existant, sélectionnez le fichier dans la liste déroulante **Progiciels**.

Étape 6 Enregistrez la politique VPN d'accès à distance.

Sujets connexes

Image Cisco Secure Client, à la page 46

Politique d'attribution d'adresse pour le VPN d'accès à distance

Le périphérique défense contre les menaces peut utiliser une politique IPv4 ou IPv6 pour attribuer des adresses IP aux clients VPN d'accès à distance. Si vous configurez plusieurs méthodes d'attribution d'adresse, le périphérique défense contre les menaces essaie chacune des options jusqu'à ce qu'il trouve une adresse IP.

Politique IPv4 ou IPv6

Vous pouvez utiliser la politique IPv4 ou IPv6 pour adresser une adresse IP aux clients VPN d'accès à distance. Vous devez essayer avec la politique IPv4 pour commencer, suivie de la politique IPv6.

- **Use Authorization Server**(utiliser le serveur d'autorisation) : récupère l'adresse d'un serveur d'autorisation externe pour chaque utilisateur. Si vous utilisez un serveur d'autorisation sur lequel une

adresse IP est configurée, nous vous recommandons d'utiliser cette méthode. L'attribution d'adresses est uniquement prise en charge par le serveur d'autorisation RADIUS. Elle n'est pas prise en charge pour les AD/LDAP. Cette méthode est disponible pour les politiques d'attribution IPv4 et IPv6.

- **Utiliser DHCP** : obtient les adresses IP d'un serveur DHCP configuré dans un profil de connexion. Vous pouvez également définir la plage d'adresses IP que le serveur DHCP peut utiliser en configurant la portée du réseau DHCP dans la politique de groupe. Si vous utilisez DHCP, configurez le serveur dans le volet **Objects > Object Management** (Objets > Gestion des objets). Cette méthode est disponible pour les politiques d'attribution IPv4.

  Pour plus d'informations sur la configuration de la portée du réseau DHCP, consultez Options générales de politique de groupe.

- **Utilisez un ensemble d'adresses interne** : les regroupements d'adresses configurées en interne constituent la méthode la plus facile d'attribution d'un ensemble d'adresses à configurer. Si vous utilisez cette méthode, créez les regroupements d'adresses IP dans le volet **Objects > Object Management > Address Pools** (Objets > Gestion des objets > Regroupements d'adresses) et sélectionnez-les dans le profil de connexion. Cette méthode est disponible pour les politiques d'attribution IPv4 et IPv6.

- **Allow reuse an IP address so many minutes après sa libération** : Retarde la réutilisation d'une adresse IP après son retour dans l'ensemble d'adresses. L'ajout d'un délai permet d'éviter les problèmes que les pare-feu peuvent rencontrer lorsqu'une adresse IP est réaffectée rapidement. Par défaut, le délai est mis à zéro. Si vous souhaitez prolonger le délai, saisissez un nombre de minutes compris entre 0 et 480 pour retarder la réattribution de l'adresse IP. Cet élément configurable est disponible pour les politiques d'attribution IPv4.

Sujets connexes

Configurer les paramètres du profil de connexion, à la page 24
Authentification du VPN d'accès à distance, à la page 5

Configurer les cartes de certificat

Les mappages de certificats vous permettent de définir des règles faisant correspondre un certificat utilisateur à un profil de connexion en fonction du contenu des champs de certificat. Les mappages de certificats fournissent l'authentification de certificat sur les passerelles sécurisées.

Les règles ou les mappages de certificats sont définis dans Objets carte de certificat.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Sélectionnez une politique VPN d'accès à distance existante dans la liste et cliquez sur l'icône **Modifier** correspondante.

Étape 3 Choisissez **Advanced** > **Certificate Maps** (Avancé > cartes de certificats).

Étape 4 Sélectionner les options suivantes dans le volet **General Settings for Connection Profile Mapping** (Paramètres généraux pour le mappage des profils de connexion) :

Les sélections sont basées sur la priorité, la correspondance se poursuit en bas de la liste d'options lorsque la première sélection ne correspond pas. La mise en correspondance est terminée lorsque les règles sont satisfaites. Si les règles ne sont pas respectées, le profil de connexion par défaut indiqué au bas de cette page est utilisé

pour la connexion. Sélectionnez une ou toutes les options suivantes pour établir l'authentification et déterminer quel profil de connexion (groupe de tunnels) doit être mappé au client.

- **Utilisez l'URL de groupe si l'URL de groupe et la carte de certificat correspondent à différents profils de connexion**
- **Use the configure Rules to match a certificate to a connection Profile**(utiliser les règles configurées pour faire correspondre un certificat à un profil de connexion) : activez cette option pour utiliser les règles définies dans les mappages de profils de connexion.

Remarque La configuration d'un mappage de certificat implique une authentification par certificat. L'utilisateur distant sera invité à saisir un certificat client, quelle que soit la méthode d'authentification configurée.

Étape 5 Dans la section **Mappage** du certificat au profil de connexion, cliquez sur **Add Mapping** (ajouter un mappage) pour créer un mappage du certificat au profil de connexion pour cette politique.

a) Sélectionnez ou créez un objet **de nom de carte e certificat**.
b) Sélectionnez le **profil de connexion** que vous souhaitez utiliser si les règles de l'objet de carte de certificat sont respectées.
c) Cliquez sur **OK** pour créer le mappage.

Étape 6 Cliquez sur **Save** (enregistrer).

Configuration des politiques de groupe

Une politique de groupe est un ensemble de paires d'attributs et de valeurs, stockées dans un objet de politique de groupe, qui définissent l'expérience du VPN d'accès à distance. Par exemple, dans l'objet de politiques de groupe, vous configurez les attributs généraux tels que les adresses, les protocoles et les paramètres de connexion.

La politique de groupe appliquée à un utilisateur est déterminée lors de l'établissement du tunnel VPN. Le serveur d'autorisation RADIUS attribue la politique de groupe, ou elle est obtenue à partir du profil de connexion actuel.

Remarque Il n'y a pas d'hérédité d'attributs de politiques de groupe sur défense contre les menaces . Un objet de politiques de groupe est utilisé entièrement pour un utilisateur. L'objet de politique de groupe identifié par le serveur AAA lors de la connexion est utilisé ou, s'il n'est pas spécifié, la politique de groupe par défaut configurée pour la connexion VPN est utilisée. La politique de groupe par défaut peut être définie selon vos valeurs par défaut, mais ne sera utilisée que si elle est affectée à un profil de connexion et qu'aucune autre politique de groupe n'a été définie pour l'utilisateur.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Sélectionnez une politique VPN d'accès à distance existante dans la liste et cliquez sur l'icône **Modifier** correspondante.

Étape 3 Choisissez **Avancé** > **Politiques de groupe** > **Ajouter**.

Étape 4 Sélectionnez les politiques de groupe dans la liste des **politiques de groupe disponibles** et cliquez sur **Add** (ajouter). Vous pouvez sélectionner une ou plusieurs politiques de groupe à associer à cette politique VPN d'accès à distance.

Étape 5 Cliquez sur **OK** pour terminer la sélection de la politique de groupe.

Étape 6 Enregistrez vos modifications.

Sujets connexes

Configurer les objets de politique de groupe

Configuration du mappage des attributs LDAP

Un nom d'attribut LDAP mappe le nom d'attribut d'utilisateur ou de groupe LDAP à un nom lisible par Cisco. La carte des attributs assimile les attributs qui existent dans Active Directory (AD) ou le serveur LDAP avec des noms d'attribut Cisco. Vous pouvez mapper n'importe quel attribut LDAP standard à un attribut spécifique au fournisseur (VSA) bien connu. Vous pouvez mapper un ou plusieurs attributs LDAP à un ou plusieurs attributs LDAP de Cisco. Lorsque le serveur AD ou LDAP renvoie l'authentification au périphérique défense contre les menaces lors de l'établissement de la connexion VPN d'accès à distance, le périphérique défense contre les menaces peut utiliser les informations pour régler la façon dont Secure Client (services client sécurisés) effectue la connexion.

Lorsque vous souhaitez fournir aux utilisateurs VPN différentes autorisations d'accès ou contenu VPN, vous pouvez configurer différentes politiques VPN sur le serveur VPN et affecter ces ensembles de politiques à chaque utilisateur en fonction de ses informations d'identification. Vous pouvez y parvenir dans défense contre les menaces en configurant l'autorisation LDAP avec des mappages d'attributs LDAP. Afin d'utiliser LDAP pour affecter une politique de groupe à un utilisateur, vous devez configurer une carte qui mappe un attribut LDAP.

Une mise en correspondance des attributs LDAP comprend trois composants :

- **Domaine** : spécifie le nom de la mise en correspondance des attributs LDAP. le nom est généré en fonction du domaine sélectionné.
- **Mappage de noms d'attributs** : mappe le nom de l'attribut d'utilisateur ou de groupe LDAP avec un nom lisible par Cisco.
- **Mappage des valeurs d'attribut** : met en correspondance la valeur de l'attribut d'utilisateur ou de groupe LDAP avec la valeur d'un attribut Cisco pour le mappage de nom sélectionné.

Les politiques de groupe utilisées dans une mise en correspondance d'attributs LDAP sont ajoutées à la liste des politiques de groupe dans la configuration VPN d'accès à distance. La suppression d'une politique de groupe de la configuration VPN d'accès à distance supprime également le mappage de l'attribut LDAP associé.

Dans les versions 6.4 à 6.6, vous pouvez configurer les mappages d'attributs LDAP uniquement à l'aide de FlexConfig. Pour en savoir plus, consultez Configurer les modules et profils AnyConnect à l'aide de FlexConfig.

Dans les versions 7.0 et ultérieures, vous pouvez utiliser la procédure suivante :

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Sélectionnez une politique VPN d'accès à distance existante dans la liste et cliquez sur l'icône **Modifier** correspondante.

Étape 3 Cliquez sur **Advanced (Avancé)** > **LDAP Attribute Mapping (Mappage d'attributs LDAP)**.

Étape 4 Cliquez sur **Add** (ajouter).

Étape 5 Dans la page Configure LDAP Attribute Map (configuration de la mise en correspondance des attributs LDAP), sélectionnez un **domaine** pour configurer la mise en correspondance des attributs.

Étape 6 Cliquez sur **Add** (ajouter).

Vous pouvez configurer plusieurs mappages d'attributs. Chaque mappage d'attribut nécessite la configuration d'une mappe de nom et de mappes de valeurs.

Remarque Assurez-vous de suivre ces instructions lors de la création d'une mise en correspondance des attributs LDAP :

- configurer au moins un mappage pour un attribut LDAP; plusieurs mappages avec le même nom d'attribut LDAP ne sont pas autorisés.
- Configurez au moins un mappage de noms pour créer une mise en correspondance d'attributs LDAP.
- Vous pouvez supprimer n'importe quel mappage d'attributs LDAP s'il n'est associée à aucun profil de connexion dans la configuration du VPN d'accès à distance.
- Utilisez l'orthographe et les majuscules correctes dans le mappage des attributs LDAP pour ***à la fois*** les noms et les valeurs des attributs Cisco et LDAP.

a) Précisez le **nom de l'attribut LDAP**, puis sélectionnez le **nom de l'attribut Cisco** requis dans la liste.
b) Cliquez sur **Add Value Map** (ajouter un mappage de valeurs) et spécifiez la valeur de l'**attribut LDAP** et la valeur de l'**attribut Cisco**.

Répétez cette étape pour ajouter d'autres mappages de valeurs.

Étape 7 Cliquez sur **OK** pour terminer la configuration de la mise en correspondance des attributs LDAP.

Étape 8 Cliquez sur **Save** (Enregistrer) pour enregistrer les modifications apportées au mappage de l'attribut LDAP.

Exemple

Pour un exemple détaillé, consultez Configurer le VPN d'accès à distance avec l'authentification et l'autorisation LDAP pour FTD.

Sujets connexes

Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 26
Comprendre l'application des politiques d'autorisations et d'attributs, à la page 6

Configuration de l'équilibrage de charge du VPN

À propos de l'équilibrage de charge VPN

L'équilibrage de charge VPN dans défense contre les menaces vous permet de regrouper logiquement deux périphériques ou plus et de répartir équitablement les sessions VPN d'accès à distance entre les périphériques. L'équilibrage de charge VPN partage des sessions VPN Secure Client (services client sécurisés) entre les périphériques d'un groupe d'équilibrage de charge.

L'équilibrage de charge VPN est basé sur une répartition simple du trafic sans prendre en compte le débit ou d'autres facteurs. Un groupe d'équilibrage de la charge VPN se compose d'au moins deux défense contre les menaces . L'un des périphériques sert de directeur et les autres périphériques sont des périphériques membres. Il n'est pas nécessaire que les périphériques d'un groupe soient exactement du même type ou aient des versions de logiciels ou des configurations identiques. Tout périphérique défense contre les menaces qui prend en charge le VPN d'accès à distance peut participer à un groupe d'équilibrage de la charge. Défense contre les menaces prend en charge l'équilibrage de la charge VPN avec l'authentification SAML Secure Client.

Tous les périphériques actifs dans un groupe d'équilibrage de la charge VPN transportent des charges de session. L'équilibrage de charge VPN dirige le trafic vers le périphérique le moins chargé du groupe, distribuant la charge sur tous les périphériques. Il utilise efficacement les ressources système et offre des performances accrues et une disponibilité élevée.

Composants de l'équilibrage de la charge VPN

Voici les composants de l'équilibrage de charge VPN :

- **Groupe d'équilibrage de la charge** : groupe virtuel de deux périphériques défense contre les menaces ou plus pour partager les sessions VPN.

  Un groupe d'équilibrage de la charge VPN peut comprendre des périphériques défense contre les menaces de la même version ou de versions mixtes; mais le périphérique doit prendre en charge la configuration VPN d'accès à distance.

  Consultez Configurer les paramètres de groupe pour l'équilibrage de la charge VPN, à la page 54 et Configurer des paramètres supplémentaires pour l'équilibrage de la charge, à la page 55.

- **Directeur** : un périphérique du groupe fait fonction de directeur. Il répartit la charge entre les autres membres du groupe et la participation sert les sessions VPN.

  Le directeur surveille tous les périphériques du groupe, suit le niveau de charge de chaque appareil et répartit la charge de session en conséquence. Le rôle de directeur n'est pas lié à un appareil physique; il peut se déplacer entre les périphériques. Par exemple, si le directeur actuel tombe en panne, l'un des périphériques membres du groupe assume ce rôle et devient immédiatement le nouveau directeur.

- **Membres** : les périphériques autres que le directeur dans un groupe sont appelés membres. Ils participent à l'équilibrage de la charge et partagent les connexions VPN d'accès à distance.

  Configurer les paramètres des périphériques participants, à la page 55.

Conditions préalables à l'équilibrage de la charge VPN

- **Certificats** : le certificat de défense contre les menaces doit contenir les adresses IP ou le nom de domaine complet du directeur et des membres vers lesquels la connexion est redirigée. Sinon, le certificat sera considéré comme non fiable. Le certificat doit utiliser un autre nom de sujet (SAN) ou un certificat à caractère générique
- **URL du groupe** : ajoutez l'URL du groupe pour l'adresse IP du groupe d'équilibrage de charge VPN aux profils de connexion. Spécifiez une URL de groupe pour éliminer la nécessité pour l'utilisateur de sélectionner un groupe lors de la connexion.
- **Ensemble d'adresses IPl** : choisissez un ensemble d'adresses IP unique pour les périphériques membres et remplacez l'ensemble d'adresses IP dans centre de gestion pour chacun des périphériques membres.
- Les périphériques qui se trouvent derrière la traduction d'adresses réseau (NAT) peuvent également faire partie d'un groupe d'équilibrage de la charge.

Directives et limites pour l'équilibrage de charge VPN

- L'équilibrage de charge VPN est désactivé par défaut. Vous devez activer explicitement l'équilibrage de charge VPN.
- Seuls les périphériques défense contre les menaces qui sont co-détenus peuvent être ajoutés à un groupe d'équilibrage de la charge.
- Un groupe d'équilibrage de la charge doit compter au moins deux défense contre les menaces .
- Les périphériques en défense contre les menaces haute disponibilité peuvent participer à un groupe d'équilibrage de la charge.
- Les périphériques qui se trouvent derrière la traduction d'adresses réseau (NAT) peuvent également faire partie d'un groupe d'équilibrage de la charge.
- Lorsqu'un périphérique membre ou directeur tombe en panne, les connexions VPN d'accès à distance qui sont desservies par ce périphérique sont abandonnées. Vous devez relancer la connexion VPN.
- Le certificat d'identité sur chaque périphérique doit avoir un autre nom de sujet (SAN) ou un caractère générique.

Configurer les paramètres de groupe pour l'équilibrage de la charge VPN

Vous pouvez activer l'équilibrage de charge VPN et configurer les paramètres de groupe qui s'appliquent à tous les membres du groupe d'équilibrage de charge. Lorsque vous créez le groupe, vous pouvez configurer les paramètres de participation pour l'équilibrage de la charge.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Cliquez sur **Edit** (Modifier) dans la politique VPN d'accès à distance que vous souhaitez mettre à jour.

Étape 3 Cliquez sur **Advanced (Avancé)** > **Load Balancing (Équilibrage de charge)**.

Étape 4 Cliquez sur le bouton à bascule **Enable Load balancing between member devices** (Activer l'équilibrage de la charge entre les périphériques membres) pour activer l'équilibrage de la charge.
La page **Edit Group Configuration** (modifier la configuration de groupe) s'ouvre. Les paramètres de groupe s'appliquent à tous les périphériques sous la configuration d'équilibrage de charge.

Étape 5 Précisez l'**adresse IPv4 de groupe** et l'**adresse IPv6 de groupe**, le cas échéant.

L'adresse IP que vous spécifiez ici s'applique à l'ensemble du groupe d'équilibrage de la charge et le directeur CDO ouvre cette adresse IP pour les connexions VPN entrantes.

Étape 6 Sélectionnez l' **communication interface** (interface de communication) pour le groupe d'équilibrage de la charge. Cliquez sur **Add** (ajouter) pour ajouter un groupe d'interfaces ou une zone de sécurité.

L'interface de communication est une interface privée par l'intermédiaire de laquelle le directeur et les membres échangent des renseignements concernant leur charge.

Étape 7 Saisissez le **port UDP** pour la communication entre le directeur et les membres d'un groupe. La valeur du port par défaut est 9023.

Étape 8 Activez le bouton à bascule **IPsec Encryption** (chiffrement IPsec) pour activer le chiffrement IPsec pour la communication entre le directeur et les membres.

L'activation du chiffrement établit un tunnel IKEv1/IPsec entre le directeur et les membres à l'aide d'une clé prépartagée.

Étape 9 Saisissez la **clé de chiffrement** pour le chiffrement IPsec et confirmez la clé de chiffrement.

Étape 10 Cliquez sur **OK**.

Configurer des paramètres supplémentaires pour l'équilibrage de la charge

Les paramètres supplémentaires pour l'équilibrage de charge VPN comprennent la redirection du nom de domaine complet (FQDN) et IKEv2.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Cliquez sur **Edit** (Modifier) dans la politique VPN d'accès à distance que vous souhaitez mettre à jour.

Étape 3 Cliquez sur **Advanced (Avancé)** > **Load Balancing (Équilibrage de charge)**.

Étape 4 Activez le bouton à bascule **Enable Load balancing between member devices** (Activer l'équilibrage de la charge entre les périphériques membres) pour activer l'équilibrage de la charge, si ce n'est déjà fait.

Étape 5 Cliquez sur **Settings** (Paramètres).

Étape 6 Activez le bouton à bascule **Send FQDN to peer devices instead of IP**(Envoyer le nom de domaine complet aux périphériques homologues au lieu de l'adresse IP) pour activer la redirection à l'aide d'un nom de domaine complet.

Par défaut, défense contre les menaces envoie uniquement les adresses IP dans la redirection de l'équilibrage de charge VPN à un client.

Étape 7 Sélectionnez l'une des phases de **redirection IKEv2** :

- **Rediriger pendant l'authentification du SA**
- **Redirect during SA initialization** (Rediriger pendant l'initialisation de la SA)

Étape 8 Cliquez sur **OK**.

Étape 9 Enregistrez vos modifications.

Configurer les paramètres des périphériques participants

Les paramètres de participation des périphériques déterminent la façon dont les périphériques se partagent la charge dans l'équilibrage de charge VPN. Configurez un appareil participant en activant l'équilibrage de charge VPN sur le périphérique et en définissant les propriétés spécifiques au périphérique. Ces valeurs varient d'un appareil à l'autre. Vous pouvez fournir un numéro de priorité pour les périphériques participant à l'équilibrage de charge. Un numéro de priorité plus élevée donne au périphérique une meilleure chance de devenir directeur sur les autres périphériques. Mais vous ne pouvez pas sélectionner un périphérique comme directeur du groupe.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Cliquez sur **Edit** (Modifier) à côté de la politique VPN d'accès à distance que vous souhaitez modifier.

Étape 3 Cliquez sur **Advanced (Avancé)** > **Load Balancing (Équilibrage de charge)**.

Étape 4 Activez le bouton à bascule **Activer l'équilibrage de la charge entre les périphériques membres** pour activer l'équilibrage de la charge si vous ne l'avez pas déjà activé.

Étape 5 Configurez les paramètres de **participation du périphérique** :

La section **Participation du périphérique** répertorie tous les périphériques cibles de la configuration VPN d'accès à distance sélectionnée. Vous pouvez configurer ces périphériques pour partager la charge des sessions VPN entrantes.

a) Activez le bouton à bascule **Load balancing** pour activer l'équilibrage de la charge pour un périphérique, puis cliquez sur **Edit** (Modifier) .

b) Saisissez la **priorité** du périphérique.

Par défaut, la priorité du périphérique est fixée à 5. Vous pouvez choisir un nombre de 1 à 10.

c) Spécifiez l'**adresse NAT IPv4** ou **IPv6** pour l'adresse IP de l'interface VPN si le périphérique se trouve derrière la NAT.

d) Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** pour enregistrer les paramètres de politique VPN d'accès à distance.

Configuration des paramètres IPsec pour les VPN d'accès à distance

Les paramètres IPsec ne s'appliquent que si vous avez sélectionné IPsec comme protocole VPN lors de la configuration de votre politique VPN d'accès à distance. Sinon, vous pouvez activer IKEv2 à l'aide de la boîte de dialogue Edit Access Interface. Consultez Configurer les interfaces d'accès pour le VPN d'accès à distance, à la page 44 pour obtenir de plus amples renseignements.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Dans la liste des politiques VPN disponibles, sélectionnez la politique dont vous souhaitez modifier les paramètres.

Étape 3 Cliquez sur **Advanced** (Avancé).

La liste des paramètres IPsec s'affiche dans un volet de navigation à gauche de l'écran.

Étape 4 Utilisez le volet de navigation pour modifier les options IPsec suivantes :

a) **Crypto Maps** : la page Crypto Maps répertorie les groupes d'interfaces sur lesquels le protocole IKEv2 est activé. Les cartes de chiffrement sont générées automatiquement pour les interfaces sur lesquelles le protocole IPsec-IKEv2 est activé. Pour modifier une carte de chiffrement, consultez Configurer les cartes de chiffrement du VPN d'accès à distance, à la page 57. Vous pouvez ajouter ou supprimer des groupes d'interface à la politique VPN sélectionnée dans **Access Interface** (interface d'accès). Consultez Configurer les interfaces d'accès pour le VPN d'accès à distance, à la page 44 pour obtenir de plus amples renseignements.

b) **Politique IKE** : la page de politique IKE répertorie tous les objets de politique IKE applicables à la politique VPN sélectionnée lorsque les points terminaux Secure Client se connectent à l'aide du protocole IPsec. Consultez Politiques IKE dans les VPN d'accès à distance, à la page 59 pour obtenir de plus amples renseignements. Pour ajouter une nouvelle politique IKE, consultez Configurer des objets de politique IKEv2. Défense contre les menaces ne prend en charge que les clients Secure Client IKEv2. Les clients IKEv2 standard tiers ne sont pas pris en charge.

c) **Paramètres IPsec/IKEv2** : la page IPsec/IKEv2 Parameters vous permet de modifier les paramètres de session IKEv2, les paramètres d'association de sécurité IKEv2, les paramètres IPsec et les paramètres de transparence NAT. Consultez Configurer les paramètres du VPN d'accès à distance IPsec/IKEv2, à la page 60 pour obtenir de plus amples renseignements.

Étape 5 Cliquez sur **Save** (enregistrer).

Configurer les cartes de chiffrement du VPN d'accès à distance

Les cartes de chiffrement sont générées automatiquement pour les interfaces sur lesquelles le protocole IPsec-IKEv2 est activé. Vous pouvez ajouter ou supprimer des groupes d'interface à la politique VPN sélectionnée dans **Access Interface** (interface d'accès). Consultez Configurer les interfaces d'accès pour le VPN d'accès à distance, à la page 44 pour obtenir de plus amples renseignements.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Dans la liste des politiques VPN disponibles, sélectionnez la politique dont vous souhaitez modifier les paramètres.

Étape 3 Cliquez sur **Advanced** (Avancé) > **Crypto Maps** (cartes de chiffrement), sélectionnez une ligne dans le tableau et cliquez sur **Edit** (modifier) pour modifier les options de la carte de chiffrement.

Étape 4 Sélectionnez **IKEv2 IPsec Proposals** et sélectionnez les ensembles de transformations pour spécifier quels algorithmes d'authentification et de chiffrement seront utilisés pour sécuriser le trafic dans le tunnel.

Étape 5 Sélectionnez **Enable Reverse Route Injection** (activer l'insertion de route inverse) pour permettre l'insertion automatique des routes statiques dans le processus de routage pour les réseaux et les hôtes protégés par un point terminal de tunnel distant).

Étape 6 Sélectionnez **Enable Client Services** (activer les services client) et précisez le numéro de port.

Le serveur de services au client fournit un accès HTTPS (SSL) pour permettre au téléchargeur Secure Client de recevoir les mises à jour logicielles, les profils, les fichiers de localisation et de personnalisation, les CSD, les SCEP et les autres téléchargements de fichiers requis par le client. Si vous sélectionnez cette option, précisez le numéro de port des services client. Si vous n'activez pas le serveur de services client, les utilisateurs ne pourront pas télécharger les fichiers dont Secure Client pourrait avoir besoin.

Remarque Vous pouvez utiliser le même port que celui que vous utilisez pour le VPN SSL sur le même périphérique. Même si vous avez configuré un VPN SSL, vous devez sélectionner cette option pour activer les téléchargements de fichiers sur SSL pour les clients IPsec-IKEv2.

Étape 7 Sélectionnez **EnablePerfect Forward Secrecy** (activer la confidentialité de transmission parfaite), puis le **groupe Module (module)**.

Utilisez le protocole PFS (Perfect Forward Secrecy) pour générer et utiliser une clé de session unique pour chaque échange chiffré. La clé de session unique protège l'échange du déchiffrement ultérieur, même si

l'échange en entier a été enregistré et que l'agresseur a obtenu les clés prépartagées ou privées utilisées par les terminaux. Si vous sélectionnez cette option, sélectionnez également l'algorithme de dérivation de clé Diffie-Hellman à utiliser lors de la génération de la clé de session PFS dans la liste **Modulus group** (groupe de modules).

Le groupe Module est le groupe Diffie-Hellman à utiliser pour extraire un secret partagé entre les deux homologues IPsec sans le transmettre. Un module plus élevé offre une sécurité supérieure, mais nécessite plus de temps de traitement. Les deux homologues doivent avoir un groupe de module correspondant. Sélectionnez le groupe de module que vous souhaitez autoriser dans la configuration du VPN d'accès à distance :

- 1 : Groupe Diffie-Hellman 1 (module de 768 bits).
- 2 : Groupe Diffie-Hellman 2 (module de 1024 bits).
- 5 : Groupe Diffie-Hellman 5 (module de 1536 bits, considéré comme une bonne protection pour les clés de 128 bits, mais le groupe 14 est meilleur). Si vous utilisez le chiffrement AES, utilisez ce groupe (ou un groupe supérieur).
- 14 : Groupe Diffie-Hellman 14 (module de 2048 bits, considéré comme une bonne protection pour les clés de 128 bits).
- 19 : Groupe Diffie-Hellman 19 (taille de champ de courbe elliptique de 256 bits)
- 20 : Groupe Diffie-Hellman 20 (taille du champ de courbe elliptique 384 bits)
- 21 : Groupe Diffie-Hellman 21 (taille du champ de courbe elliptique 521 bits).
- 24 : Groupe Diffie-Hellman 24 (module de 2048 bits et sous-groupe de premier ordre de 256 bits).

Étape 8 Précisez la **durée de vie (en secondes)**

Durée de vie de l'association de sécurité (SA), en secondes. Lorsque la durée de vie est dépassée, l'association de sécurité expire et doit être renégociée entre les deux homologues. En général, plus la durée de vie est courte (jusqu'à un certain point), plus vos négociations IKE seront sécurisées. Cependant, avec des durées de vie plus longues, les futures associations de sécurité IPsec peuvent être configurées plus rapidement qu'avec des durées de vie plus courtes.

Vous pouvez spécifier une valeur comprise entre 120 et 2147483647 secondes. La valeur par défaut est de 28800 secondes.

Étape 9 Précisez la **taille de la durée de vie (kocets)**.

Le volume de trafic (en kilo-octets) qui peut passer entre les homologues IPsec à l'aide d'une association de sécurité donnée avant son expiration.

Vous pouvez spécifier une valeur comprise entre 10 et 2 147 483 3647 koctets. La valeur par défaut est de 4 608 000 kilo-octets. Aucune spécification n'autorise des données infinies.

Étape 10 Sélectionnez les **paramètres ESPv3** suivants :

- **Valider les messages d'erreur ICMP entrants** : choisissez s'il faut valider les messages d'erreur ICMP reçus dans un tunnel IPsec et destinés à un hôte intérieur sur le réseau privé.
- **Activer la politique « Ne pas fragmenter » :**Définissez la façon dont le sous-système IPsec gère les paquets volumineux dont le bit ne pas fragmenter (DF) est défini dans l'en-tête IP et sélectionnez l'une des options suivantes dans la liste **Policy** (Politique) :
  - Copy (copie) : Maintient le bit DF.

- Clear (effacer) : Ignore le bit DF.
- Set : Définit et utilise le bit DF.

- Sélectionnez **Enable Traffic Flow Confidentiality (TFC) Packets** (activer les paquets TFC de confidentialité du flux de trafic) pour activer des paquets TFC factices qui masquent le profil de trafic qui traverse le tunnel. Utilisez les paramètres **Burst** (Rafale), **Payload Size** (Taille de la charge utile) et **Timeout** (Expiration) pour générer des paquets de longueur aléatoire à des intervalles aléatoires sur le SA spécifié.

  Remarque L'activation de la confidentialité du flux de trafic (TFC) empêche le tunnel VPN d'être inactif. Par conséquent, le délai d'inactivité VPN configuré dans la politique de groupe ne fonctionne pas comme prévu lorsque vous activez les paquets TFC. Consultez Options avancées de la politique de groupe.

  - Rafale : spécifiez une valeur comprise entre 1 et 16 octets.
  - Payload Size (taille de la charge utile) : spécifiez une valeur comprise entre 64 et 1024 octets.
  - Timeout (délai d'expiration) : spécifiez une valeur comprise entre 10 et 60 secondes.

Étape 11 Cliquez sur **OK**.

Sujets connexes

Interface

Politiques IKE dans les VPN d'accès à distance

L'Internet Key Exchange (IKE ou l'échange de clé Internet) est un protocole de gestion de clés utilisé pour authentifier les pairs IPsec, négocier et distribuer les clés de chiffrement IPsec et établir automatiquement des associations de sécurité IPsec. La négociation IKE comprend deux phases. La phase 1 négocie une association de sécurité entre deux homologues IKE, ce qui permet aux homologues de communiquer de manière sécurisée pendant la phase 2. Pendant la négociation de la phase 2, IKE établit les associations de sécurité pour d'autres applications, telles qu'IPsec. Les deux phases utilisent des propositions lorsqu'elles négocient une connexion. Une proposition IKE est un ensemble d'algorithmes que deux homologues utilisent pour sécuriser la négociation entre eux. La négociation IKE commence lorsque chaque homologue s'accorde sur une politique IKE commune (partagée). Cette politique énonce les paramètres de sécurité utilisés pour protéger les négociations IKE ultérieures.

Remarque défense contre les menaces prend uniquement en charge IKEv2 pour les VPN d'accès à distance.

Contrairement à IKEv1, dans une proposition IKEv2, vous pouvez sélectionner plusieurs algorithmes et groupes de modules dans une politique. Étant donné que les homologues font leur choix au cours de la phase 1 de négociation, il est possible de créer une seule proposition IKE, mais envisagez de créer plusieurs propositions différentes afin de donner une plus grande priorité aux options que vous souhaitez privilégier. Pour IKEv2, l'objet de politique ne spécifie pas l'authentification, les autres politiques doivent définir les exigences d'authentification.

Une politique IKE est requise lorsque vous configurez un VPN IPsec d'accès à distance.

Configuration des politiques IKE du VPN d'accès à distance

Le tableau de politique IKE précise tous les objets de politique IKE applicables à la configuration VPN sélectionnée lorsque les points terminaux Secure Client se connectent à l'aide du protocole IPsec. Pour en savoir plus, consultez Politiques IKE dans les VPN d'accès à distance, à la page 59.

Remarque défense contre les menaces prend uniquement en charge IKEv2 pour les VPN d'accès à distance.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Dans la liste des politiques VPN disponibles, sélectionnez la politique dont vous souhaitez modifier les paramètres.

Étape 3 Cliquez sur **Advanced** (Avancé) > **IKE Policy** (politique IKE).

Étape 4 Cliquez sur **Add** (Ajouter) pour sélectionner une des politiques IKEv2 disponibles, ou ajoutez une nouvelle politique IKEv2 et spécifiez les éléments suivants :

- **Name** : nom de la politique IKEv2.
- **Description** : description facultative de la politique IKEv2
- **Priority** : la valeur de priorité détermine l'ordre de la politique IKE par rapport aux deux homologues à la négociation lors de la tentative de recherche d'une association de sécurité (SA).
- **Lifetime** : durée de vie de l'association de sécurité (SA), en secondes.
- **Integrity** : la partie algorithmes d'intégrité de l'algorithme de hachage utilisé dans la politique IKEv2.
- **Encryption** : l'algorithme de chiffrement utilisé pour établir le SA de phase 1 afin de protéger les négociations de phase 2.
- **PRF Hash** : la partie fonction pseudo-aléatoire (PRF) de l'algorithme de hachage utilisé dans la politique IKE. Dans IKEv2, vous pouvez spécifier différents algorithmes pour ces éléments.
- **DH Group** : le groupe Diffie-Hellman utilisé pour le chiffrement.

Étape 5 Cliquez sur **Save** (enregistrer).

Configurer les paramètres du VPN d'accès à distance IPsec/IKEv2

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Dans la liste des politiques VPN disponibles, sélectionnez la politique dont vous souhaitez modifier les paramètres.

Étape 3 Cliquez sur **Advanced** > **IPsec**> **IPsec/IKEv2 Parameters** (Avancé > IPSec > Paramètres IPSec/IKEv2).

Étape 4 Sélectionnez les éléments suivants pour les **paramètres de session IKEv2** :

- **Identity Sent to Peers**(identité envoyée aux homologues) : choisissez l'identité que les homologues utiliseront pour s'identifier pendant les négociations IKE :
  - **Auto** : détermine la négociation IKE par type de connexion : adresse IP pour la clé prépartagée ou DN de certificat pour l'authentification de certificat (non pris en charge).
  - **IP address** : utilise les adresses IP des hôtes qui échangent des informations d'identité ISAKMP.
  - **Hostname** : utilise le nom de domaine complet (FQDN) des hôtes échangeant des informations d'identité ISAKMP. Ce nom comprend le nom d'hôte et le nom de domaine.
- **Enable Notification on Tunnel Disconnect** (activer la notification lors de la déconnexion du tunnel) : permet à un administrateur d'activer ou de désactiver l'envoi d'une notification IKE à l'homologue lorsqu'un paquet entrant reçu sur un SA ne correspond pas aux sélecteurs de trafic de ce SA. L'envoi de cette notification est désactivé par défaut.
- **Ne pas autoriser le redémarrage du périphérique jusqu'à ce que toutes les sessions soient terminées** : cochez cette option pour activer l'attente que toutes les sessions actives se terminent volontairement avant le redémarrage du système. Le paramètre par défaut est Désactivé.

Étape 5 Sélectionnez les éléments suivants pour les **paramètres d'association de sécurité (SA) IKEv2** :

- **Défi relatif aux témoins** : s'il faut envoyer des défis liés aux témoins à des périphériques homologues en réponse aux paquets initiés par SA, qui peuvent aider à déjouer les attaques par déni de service (DoS). La valeur par défaut est d'utiliser les défis liés aux témoins lorsque 50 % des SA disponibles sont en négociation. Sélectionnez une des options :
  - **Personnalisé** : spécifiez le **seuil de défi des témoins entrants**, le pourcentage du total des SA autorisés qui sont en cours de négociation. Cela déclenche la contestation des témoins pour les futures négociations d'un SA. La plage va de zéro à 100 %. La valeur par défaut est de 50 %.
  - Toujours : sélectionnez cette option pour envoyer toujours des défis liés aux témoins aux périphériques homologues.
  - Jamais : sélectionnez cette option pour ne jamais envoyer de défis liés aux témoins aux périphériques homologues.
- **Nombre de SA autorisées dans la négociation** : limite le nombre maximal de SA qui peuvent être en négociation à tout moment. S'il est utilisé avec le Défi des témoins, configurez le seuil de défi pour les témoins sur une valeur inférieure à cette limite pour une vérification par recoupement efficace. La valeur par défaut est de 100 %.
- **Nombre maximal de associations de sécurité autorisées** : limite le nombre de connexions IKEv2 autorisées.

Étape 6 Sélectionnez les options suivantes pour **les paramètres IPsec** :

- **Enable Fragmentation Before Encryption** (activer la fragmentation avant le chiffrement) : cette option permet au trafic de circuler sur les périphériques NAT qui ne prennent pas en charge la fragmentation IP. Cela n'affecte pas le fonctionnement des périphériques NAT qui prennent en charge la fragmentation IP.

- **Path Maximum Transmission Unit Aging** (vieillissement maximal de l'unité de transmission) : cochez cette case pour activer le vieillissement de la PMTU (Path Maximum Transmission Unit), l'intervalle pour réinitialiser la PMTU d'une SA (association de sécurité).
- **Value Reset Interval** (intervalle de réinitialisation de la valeur) : saisissez le nombre de minutes pendant lesquelles la valeur de PMTU d'une SA (Security Association) est réinitialisée à sa valeur d'origine. La plage valide est de 10 à 30 minutes, la valeur par défaut est illimitée.

Étape 7 Sélectionnez les options suivantes pour **les paramètres NAT** :

- **Traversée des messages Keepalive** – Sélectionnez s'il faut activer la traversée des messages Keepalive de la NAT. La traversée de la NAT Keepalive est utilisée pour la transmission de messages Keepalive lorsqu'un périphérique (le périphérique du milieu) est situé entre un concentrateur connecté au VPN et en étoile, et que cet appareil effectue une NAT sur le flux IPsec. Si vous sélectionnez cette option, configurez l'intervalle, en secondes, entre les signaux Keepalive envoyés entre le périphérique en étoile et le périphérique du milieu pour indiquer que la session est active. La valeur peut être comprise entre 10 et 3600 secondes. La valeur par défaut est de 20 secondes.
- **Intervalle** : définit l'intervalle Keepalive de la NAT, de 10 à 3600 secondes. La valeur par défaut est de 20 secondes.

Étape 8 Cliquez sur **Save** (enregistrer).

Configurer le tunnel VPN de gestion Secure Client

Un tunnel VPN de gestion assure la connectivité au réseau d'entreprise chaque fois qu'un système client est mis sous tension, sans que les utilisateurs du VPN aient à s'y connecter. Cela aide les entreprises à maintenir leurs points d'accès à jour grâce à des correctifs et à des mises à jour logiciels. Le tunnel de gestion se déconnecte lorsque le tunnel VPN lancé par l'utilisateur est établi.

Cette section fournit des informations sur la configuration du tunnel VPN de gestion Secure Client sur défense contre les menaces . La configuration du tunnel de gestion Secure Client sur défense contre les menaces à l'aide de l'interface Web centre de gestion nécessite les paramètres suivants :

- Un **profil de connection** avec authentification par certificat et une URL de groupe
- Un fichier de profil VPN de gestion **Secure Client** , configuré avec un serveur doté d'URL du groupe et des serveurs de secours si nécessaire.
- Une **politique de groupe** avec le profil VPN de gestion, la tunnellisation fractionnée avec des réseaux explicitement inclus, le protocole de contournement du client et aucune bannière.

Pour des instructions détaillées sur la configuration du tunnel VPN de gestion Secure Client, consultez Configuration de Secure Client du tunnel VPN de gestion sur Défense contre les menaces, à la page 63.

Exigences et conditions préalables au tunnel VPN Management Secure Client

Logiciels requis et exigences de configuration

Vérifiez que vous disposez des éléments suivants avant de configurer le tunnel de gestion Secure Client dans l'utilisation de défense contre les menaces à l'aide de l'interface Web centre de gestion :

- Assurez-vous d'utiliser défense contre les menaces et centre de gestion en version 6.7.0 ou version ultérieure.
- Téléchargez le paquet logiciel Webdeploy de Secure ClientSecure Client VPN version 4.7 ou ultérieure et téléchargez-le sur le VPN d'accès à distance défense contre les menaces .
- Assurez-vous que l'authentification du certificat est configurée dans le profil de connexion.
- Assurez-vous qu'aucune bannière n'est configurée dans la politique de groupe.
- Vérifiez la configuration de la tunnellisation fractionnée dans la politique de groupe de tunnels de gestion.

Exigences du certificat

- Défense contre les menaces doit avoir un certificat d'identité valide pour le VPN d'accès à distance et le certificat racine de l'autorité de certification locale doit être présent sur défense contre les menaces .
- Les points terminaux qui se connectent au tunnel VPN de gestion doivent avoir un certificat d'identité valide.
- Un certificat de l'autorité de certification pour les certificats d'identité défense contre les menaces doit être installé sur les points d' extrémité et le certificat de l' autorité de certification pour les points d' extrémité doit être installé sur défense contre les menaces .
- Le certificat d'identité émis par la même autorité de certification locale doit être présent dans le magasin de la machine.

  Certificate Store (pour Windows) ou dans la chaîne de clé système (pour macOS).

Limites du tunnel VPN de gestion Secure Client

- Le tunnel VPN de gestion Secure Client prend uniquement en charge l'authentification de certificat, il ne prend pas en charge l'authentification basée sur AAA.
- Les paramètres de serveurs mandataires publics ou privés ne sont pas pris en charge.
- La mise à niveau de Secure Client et le téléchargement du module AnyConnect ne sont pas pris en charge lorsque le tunnel VPN de gestion est connecté.

Configuration de Secure Client du tunnel VPN de gestion sur Défense contre les menaces

Procédure

Étape 1 **Créez une configuration de politique VPN d'accès à distance à l'aide de l'assistant** :

Pour en savoir plus sur la configuration d'un VPN d'accès à distance, consultez Configuration d'une nouvelle connexion de VPN d'accès à distance, à la page 12.

Étape 2 **Configurez les paramètres de profil de connexion pour le tunnel VPN de gestion** :

Remarque Il est conseillé de créer un nouveau profil de connexion à utiliser uniquement pour le tunnel VPN de gestion Secure Client.

a) Modifiez la politique VPN d'accès à distance que vous avez créée.

b) Sélectionnez et modifiez le profil de connexion qui sera utilisé pour le tunnel VPN de gestion.
c) Cliquez sur **AAA** > **Authentication Méthode** (Méthode d'authentification) et sélectionnez **Client Certificate Only** (Certificat client uniquement). Configurer les paramètres d'autorisation et de traçabilité le cas échéant.
d) Cliquez sur l'onglet **Aliases** (alias) du profil de connexion.
e) Cliquez sur **Add (+)** sous URL Aliases et **URL Alias** (Alias de l'URL) pour le profil de connexion.
f) Cliquez sur **Enabled** pour activer l'URL.
g) Cliquez sur **OK**, puis sur **Save** (Enregistrer) pour enregistrer les paramètres du profil de connexion.

Pour en savoir plus sur les paramètres de profils de connexion, consultez Configurer les paramètres du profil de connexion, à la page 24.

Étape 3 **Créez un profil de tunnel de gestion à l'aide de l'éditeur de profil Secure Client** :

a) Téléchargez l'**éditeur de profil autonome de tunnel de gestion VPN** Secure Client à partir du Centre de téléchargement de logiciels Cisco si vous ne l'avez pas encore fait.
b) Créez un profil de tunnel de gestion avec les paramètres requis pour vos utilisateurs VPN, puis enregistrez le fichier.
c) Configurez un serveur dans la liste des serveurs avec l'URL de groupe que vous avez configurée dans le profil de connexion.

Pour en savoir plus sur la création d'un profil de gestion à l'aide de l'Éditeur de profils, consultez le *Guide de l'administrateur de Cisco Secure Client (incluant AnyConnect)*.

Étape 4 **Créez un objet de tunnel de gestion** :

a) Sur votre interface Web Cisco Secure Firewall Management Center, accédez à **Object** > **Object Management** > **VPN** > **Secure Client File**
b) Cliquez sur **Add Secure Client** (Ajouter un fichier AnyConnect > Ajouter un fichier Secure Client).
c) Précisez le **nom** du fichier Secure Client.
d) Cliquez sur **Parcourir** et sélectionnez le fichier de profil de tunnel de gestion que vous avez enregistré.
e) Cliquez sur la liste déroulante **File Type** (Type de fichier) et sélectionnez **Secure Client Management VPN Profile**. (Profil de VPN de gestion AnyConnect > Profil de VPN de gestion Secure Client).
f) Cliquez sur **Save** (enregistrer).

Remarque Vous pouvez également créer l'objet de tunnel de gestion lorsque vous créez ou mettez à jour les paramètres Secure Client pour une politique de groupe. Consultez Options de politique de groupe Secure Client (services client sécurisés).

Étape 5 **Associer un profil de gestion à une politique de groupe et configurer les paramètres de politique de groupe** :

Vous devez ajouter le profil VPN de gestion à la politique de groupe associée au profil de connexion utilisée pour la connexion VPN du tunnel de gestion. Lorsque l'utilisateur se connecte, le profil VPN de gestion est téléchargé avec le profil VPN de l'utilisateur déjà mappé à la politique de groupe, activant la fonctionnalité de tunnel VPN de gestion.

Mise en garde **Aucune bannière** : vérifiez qu'aucune bannière n'est configurée dans les paramètres de politique de groupe. Vous pouvez vérifier les paramètres de la bannière sous **Group Policy (Politique de groupe)** > **General Settings (Paramètres généraux)** > **Banner (Bannière)**.

a) Modifiez le profil de connexion que vous avez créé pour le tunnel VPN de gestion.
b) Cliquez sur **Edit Group Policy** > **Secure Client** > **Management Profile**.

c) Cliquez sur le menu déroulant **Management VPN Profile** (Profil de VPN de gestion) et sélectionnez l'objet de fichier de profil de gestion que vous avez créé.

Remarque Vous pouvez également cliquer sur le signe plus (+) et ajouter un nouvel objet de profil VPN de gestion Secure Client.

d) Cliquez sur **Save** (enregistrer).

Étape 6 **Configurer la tunnellisation fractionnée dans la politique de groupe** :

a) Cliquez sur **Edit Group Policy (Modifier la politique de groupe)** > **General (Général)** > **Split Tunneling** (Tunnelisation fractionnée).

b) Dans la liste déroulante Tunnelisation fractionnée IPv4 or IPv6, sélectionnez **Tunnel Networks specified below** (Réseaux de tunnels spécifiés ci-dessous).

c) Sélectionnez le type de liste de réseaux de tunnels fractionnés : **Standard Access List** ou **Extended Access List**, puis sélectionnez la liste d'accès requise (standard ou étendue) pour autoriser le trafic sur le tunnel VPN de gestion.

d) Cliquez sur **Save** (Enregistrer) pour enregistrer les paramètres de tunnel fractionné.

personnalisé de Secure Client

Le tunnel VPN de gestion Secure Client nécessite une configuration de tunnellisation fractionnée par défaut. Si vous configurez l'attribut personnalisé Secure Client dans la politique de groupe pour déployer le tunnel VPN de gestion avec la tunnellisation fractionnée pour tout inclure dans un tunnel, vous pouvez le faire à l'aide de FlexConfig, car l'interface Web centre de gestion 6.7 ne prend pas en charge l'attribut personnalisé Secure Client.

Voici un exemple de commande pour l'attribut personnalisé Secure Client :

```
webvpn
 anyconnect-custom-attr ManagementTunnelAllAllowed description ManagementTunnelAllAllowed
anyconnect-custom-data ManagementTunnelAllAllowed true true
group-policy MGMT_Tunnel attributes
 anyconnect-custom ManagementTunnelAllAllowed value true
```

Étape 7 **Déployer, vérifier et surveiller la politique VPN d'accès à distance** :

a) Déployez la configuration du tunnel VPN de gestion sur défense contre les menaces .

Remarque Les systèmes clients doivent se connecter une fois au VPN d'accès à distance défense contre les menaces pour télécharger le profil VPN du tunnel de gestion sur les ordinateurs clients.

b) Vous pouvez vérifier le tunnel de VPN de gestion Secure Client à pour**les** > **statistiques** > **.**

Vous pouvez également vérifier les détails de la session VPN de gestion à l'invite de commande défense contre les menaces à l'aide de la commande **show vpn-sessiondb anyconnect**.

c) Sur votre interface Web centre de gestion, cliquez sur **Analyse** pour afficher les informations de session du tunnel de gestion.

Sujets connexes

Configurer les paramètres du profil de connexion, à la page 24
Objets politique de groupe Défense contre les menaces

Authentification de plusieurs certificats

L'authentification basée sur les certificats multiples permet à défense contre les menaces de valider le périphérique ou le certificat de périphérique, pour s'assurer que le périphérique est émis par l'entreprise, en plus d'authentifier le certificat d'identité de l'utilisateur pour permettre l'accès au VPN à l'aide de Secure Client (services client sécurisés) pendant SSL ou IKEv2 Phase du programme EAP.

L'option de certificats multiples permet l'authentification de certificat de la machine et de l'utilisateur au moyen de certificats. Sans cette option, vous ne pourriez effectuer que l'authentification de certificat de la machine ou de l'utilisateur, mais pas les deux.

Directives et limites de l'authentification par certificat multiple

Remarque Lorsque vous configurez l'authentification par certificats multiples, veillez à définir la valeur de **AutomaticCertSélection** sur « true » dans les paramètres du profil Cisco Secure Client (services client sécurisés).

- L'authentification par certificats multiples limite actuellement le nombre de certificats à deux.
- Secure Client (services client sécurisés) doit indiquer la prise en charge de l'authentification par certificats multiples. Si ce n'est pas le cas, la passerelle utilise l'une des méthodes d'authentification existantes ou échoue à se connecter. La version 4.4.04030 ou ultérieure de Secure Client prend en charge l'authentification basée sur plusieurs certificats.
- Secure Client prend en charge uniquement les certificats codés en RAS.
- Seuls les certificats basés sur SHA256, SHA384 et SHA512 sont pris en charge lors de l'authentification agrégée Secure Client.
- L'authentification de certificat ne peut pas être combinée à l'authentification SAML.

Configuration de l'authentification de plusieurs certificats

Avant de commencer

Avant de configurer l'authentification par certificat multiple, assurez-vous d'avoir configuré l'objet d'inscription de certificat utilisé pour obtenir le certificat d'identité pour chaque défense contre les menaces . Pour en savoir plus, consultez Objets carte de certificat.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Sélectionnez la politique VPN d'accès à distance et cliquez sur **Edit** (Modifier).

Remarque Si vous n'avez pas configuré de VPN d'accès à distance, cliquez sur **Add** (Ajouter)pour créer une nouvelle politique de VPN d'accès à distance.

Étape 3 Sélectionnez et **modifiez** un profil de connexion pour configurer l'authentification à certificats multiples.

Étape 4 Cliquez sur **AAA Settings** (Paramètres AAA) et sélectionnez **Authentication Méthode** (Méthode d'authentification) > **Client Certificate Only** ou **Client Certificate & AAA** (Certificat client uniquement ou Certificat client et AAA).

Remarque Sélectionnez le **serveur d'authentification** si vous avez sélectionné la méthode d'authentification Certificat client et AAA

Étape 5 Cochez la case **Activer l'authentification de plusieurs certificats**.

Étape 6 Choisissez l'un des certificats pour **mapper le nom d'utilisateur à partir du certificat client** :

- **First Certificate (premier certificat)** : sélectionnez cette option pour mapper le nom d'utilisateur du certificat de la machine envoyé par le client VPN.
- **Second Certificate (second certificat)** : sélectionnez cette option pour mapper le nom d'utilisateur du certificat utilisateur envoyé par le client.

Le nom d'utilisateur envoyé par le client est utilisé comme nom d'utilisateur de session VPN lorsque l'authentification par certificat uniquement est activée. Lorsque l'authentification AAA et par certificat est activée, le nom d'utilisateur de session VPN sera basé sur l'option de préremplissage.

Remarque Si vous sélectionnez l'option **Mapper un champ spécifique**, qui comprend le nom d'utilisateur du certificat client, les champs **principal** et **secondaire** affichent les valeurs par défaut : **CN (nom commun)** et **OU (unité organisationnelle)** , respectivement.

Si vous sélectionnez l'option **Use entire DN (Distinguished Name) (Utiliser le Nom distinctif complet DN) comme nom d'utilisateur**, le système récupère automatiquement l'identité de l'utilisateur. Un nom distinctif (DN) est une identification unique, composée de champs individuels qui peuvent être utilisés comme identifiant lors de la mise en correspondance des utilisateurs avec les règles d'un DN de profil de connexion utilisées pour l'authentification de certificat améliorée.

Si vous avez sélectionné l'option Certificat client et authentification AAA, sélectionnez l'option **Pré-remplir le nom d'utilisateur à partir du certificat dans la fenêtre de connexion de l'utilisateur** pour pré-remplir le nom d'utilisateur secondaire à partir du certificat client lorsque l'utilisateur se connecte via le module AnyConnect VPN de Cisco Secure Client.

- **Masquer le nom d'utilisateur dans la fenêtre de connexion** : le nom d'utilisateur secondaire est prérempli à partir du certificat client, mais masqué pour l'utilisateur afin que ce dernier ne modifie pas le nom d'utilisateur prérempli.

Étape 7 Configurez les paramètres AAA et les paramètres de profil de connexion requis pour le VPN d'accès à distance.

Étape 8 Enregistrez le profil de connexion et la configuration VPN d'accès à distance, puis déployez-les sur votre périphérique défense contre les menaces .

Sujets connexes

Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 26

Personnalisation des paramètres AAA du VPN d'accès à distance

Cette section fournit des informations sur la personnalisation de vos préférences AAA pour les VPN d'accès à distance. Pour en savoir plus, consultez Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 26.

Authentifier les utilisateurs VPN à l'aide de certificats clients

Vous pouvez configurer l'authentification VPN d'accès à distance à l'aide d'un certificat client lorsque vous créez une nouvelle politique de VPN d'accès à distance à l'aide de l'assistant ou en modifiant la politique ultérieurement.

Avant de commencer

Configurez l'objet d'inscription de certificat utilisé pour obtenir le certificat d'identité pour chaque périphérique défense contre les menaces qui sert de passerelle VPN.

Procédure

Étape 1 Sur l'interface Web Cisco Secure Firewall Management Center, choisissez **Devices** (périphériques) > **VPN** > **Remote Access** (accès à distance).

Étape 2 Sélectionnez une politique d'accès à distance et cliquez sur **Edit** (Modifier); ou cliquez sur **Add** (Ajouter) pour créer une nouvelle politique VPN d'accès à distance.

Étape 3 Pour une nouvelle politique VPN d'accès à distance, configurez l'authentification tout en sélectionnant les paramètres de profil de connexion. Pour une configuration existante, sélectionnez le profil de connexion qui comprend le profil client, puis cliquez sur **Edit** (Modifier).

Étape 4 Cliquez sur **AAA** > **Authentication** > **Certificate Client Only** (certificat client uniquement de la méthode d'authentification AAA).

Avec cette méthode d'authentification, l'utilisateur est authentifié à l'aide d'un certificat client. Vous devez configurer le certificat client sur les points terminaux clients VPN. Par défaut, le nom d'utilisateur est dérivé des champs de certificat client CN et OU respectivement. Si le nom d'utilisateur est spécifié dans d'autres champs du certificat client, utilisez les champs « Principal » et « Secondaire » pour mapper les champs appropriés.

Si vous sélectionnez l'option **Map specific field** (Mapper un champ spécifique), qui comprend le nom d'utilisateur du certificat client. Les champs **principal** et **secondaire** affichent les valeurs par défaut suivantes, respectivement : **CN (Common Name, Nom commun)** et **OU (Organisational Unit, Unité organisationnelle)**. Si vous sélectionnez l'option **Use entire DN as username** (Utiliser le DN entier comme nom d'utilisateur), le système récupère automatiquement l'identité de l'utilisateur. Un nom distinctif (DN) est une identification unique, composée de champs individuels, qui peut être utilisée comme identifiant lors de la mise en correspondance des utilisateurs avec un profil de connexion. Les règles de nom distinctif sont utilisées pour l'authentification améliorée des certificats.

- Les champs principal et secondaire appartenant à l'option de **Map specific field** (Mapper un champ spécifique) contiennent les valeurs communes suivantes :

- C (Pays)
- CN (Nom courant)
- DNQ (Qualificatif du DN))
- EA (Adresse courriel)
- GENQ (Qualificatif générationnel)
- GN (Prénom)
- I (Initial)
- L (Localité)
- N (Nom)
- O (Organisation)
- OU (Unité organisationnelle)
- SER (Numéro de série)
- SN (Nom de famille)
- SP (État ou province)
- T (Titre)
- UID (Identifiant de l'utilisateur)
- UPN (Nom principal de l'utilisateur)

- Quelle que soit la méthode d'authentification que vous choisissez, cochez ou décochez la case **Allow connection only if user Existing in authentication database** (Autoriser la connexion uniquement si l'utilisateur existe dans la base de données d'authentification).

Pour en savoir plus, consultez Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 26.

Étape 5 Enregistrez vos modifications.

Sujets connexes

Configurer les paramètres du profil de connexion, à la page 24
Ajout d'objets d'Inscription du certificat

Configurer l'authentification des utilisateurs VPN à l'aide du certificat client et du serveur AAA

Lorsque vous configurez l'authentification VPN d'accès à distance pour utiliser à la fois le certificat client et le serveur d'authentification, l'authentification du client VPN est effectuée à l'aide de la validation du certificat client et du serveur AAA.

Avant de commencer

- Configurez l'objet d'inscription de certificat que vous utilisez pour obtenir le certificat d'identité pour chaque défense contre les menaces périphérique qui sert de passerelle VPN.
- Configurez l'objet de groupe de serveurs RADIUS et les domaines AD ou LDAP à utiliser dans la configuration de la politique de VPN d'accès à distance.
- Assurez-vous que le serveur AAA est accessible à partir du périphérique Cisco Secure Firewall Threat Defense pour que la configuration VPN d'accès à distance fonctionne.

Procédure

Étape 1 Sur l'interface Web Cisco Secure Firewall Management Center, choisissez **Devices** (périphériques) – **Remote Access** (accès à distance).

Étape 2 Cliquez sur **Edit** dans la politique VPN d'accès à distance dont vous souhaitez mettre à jour l'authentification ou cliquez sur **Add** pour en créer une nouvelle.

Étape 3 Si vous choisissez de créer une nouvelle politique VPN d'accès à distance, configurez l'authentification tout en sélectionnant les paramètres du profil de connexion. Pour une configuration existante, sélectionnez le profil de connexion qui comprend le profil client, puis cliquez sur **Edit** (Modifier).

Étape 4 Rendez-vous sur **AAA** et dans la liste déroulante **Authentication Méthode** (méthode d'authentification), choisissez **Client Certificate and AAA** (certificat client et AAA).

- Lorsque vous sélectionnez la **méthode d'authentification** :

  Certificat client et AAA : les deux types d'authentification sont effectués.

  - **AAA** : Si vous sélectionnez le **serveur d'authentification RADIUS**, par défaut la même valeur est attribuée au serveur d'autorisation. Sélectionnez le **Accounting Server** (Serveur de comptabilité) dans la liste déroulante. Chaque fois que vous sélectionnez **AD** et **LDAP** dans la liste déroulante Authentication Server, (Serveur d'authentification) vous devez sélectionner manuellement le **serveur d'autorisation** et le **serveur de comptabilité**, respectivement.
  - **Certificat client** : authentifie l'utilisateur à l'aide du certificat client. Vous devez configurer le certificat client sur les points terminaux clients VPN. Par défaut, le nom d'utilisateur est dérivé des champs de certificat client CN et OU respectivement. Si vous utilisez un autre champ du profil client pour spécifier le nom d'utilisateur, utilisez **le champ principal** et le champ **secondaire** pour mapper les champs appropriés.

    Si vous sélectionnez l'option **Map specific field** (Mapper un champ spécifique), qui comprend le nom d'utilisateur du certificat client. Les champs **principal** et **secondaire** affichent les valeurs par défaut : **NC (nom commun)** et **OU (unité organisationnelle)**, respectivement. Si vous sélectionnez l'option **Use entire DN as username** (Utiliser le DN entier comme nom d'utilisateur), le système récupère automatiquement l'identité de l'utilisateur. Un nom distinctif (DN) est une identification unique, composée de champs individuels qui peuvent être utilisés comme identifiant lors de la mise en correspondance des utilisateurs avec un profil de connexion. Les règles de nom distinctif sont utilisées pour l'authentification améliorée des certificats.

    Les champs principal et secondaire appartenant à l'option **de champ spécifique à la carte** contiennent les valeurs communes suivantes :

    - C (Pays)
    - CN (Nom courant)

- DNQ (Qualificatif du DN))
- EA (Adresse courriel)
- GENQ (Qualificatif générationnel)
- GN (Prénom)
- I (Initial)
- L (Localité)
- N (Nom)
- O (Organisation)
- OU (Unité organisationnelle)
- SER (Numéro de série)
- SN (Nom de famille)
- SP (État ou province)
- T (Titre)
- UID (Identifiant de l'utilisateur)
- UPN (Nom principal de l'utilisateur)

- Quelle que soit la méthode d'authentification que vous choisissez, cochez ou décochez la case **Allow connection only if user Existing in authentication database** (Autoriser la connexion uniquement si l'utilisateur existe dans la base de données d'authentification).

Pour en savoir plus, consultez Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 26.

Étape 5 Enregistrez vos modifications.

Sujets connexes

Configurer les paramètres du profil de connexion, à la page 24
Ajout d'objets d'Inscription du certificat

Gérer les modifications de mot de passe sur les sessions VPN

La gestion des mots de passe permet à l'administrateur de la politique de VPN d'accès à distance de configurer les paramètres de notification pour les utilisateurs du VPN d'accès à distance à l'expiration de leur mot de passe. La gestion des mots de passe est disponible dans les paramètres AAA avec les méthodes d'authentification AAA uniquement et les certificats client et AAA. Pour en savoir plus, consultez Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 26.

Procédure

Étape 1 Sur l'interface Web Cisco Secure Firewall Management Center, choisissez **Devices** (périphériques) – **Remote Access** (accès à distance).

Étape 2 Cliquez sur **Edit** (Modifier) dans la politique VPN d'accès à distance que vous souhaitez mettre à jour.

Étape 3 Cliquez sur **Edit** (Modifier) dans le profil de connexion qui comprend les paramètres AAA.

Étape 4 Choisissez **AAA** > **Paramètres avancés** >.

Étape 5 Cochez la case **Enable Password Management** (activer la gestion des mots de passe) et sélectionnez l'une des options suivantes :

- Aviser l'utilisateur : plusieurs jours avant l'expiration du mot de passe et spécifiez le nombre de jours dans la zone.
- Avertir l'utilisateur le jour de l'expiration du mot de passe.

Étape 6 Enregistrez vos modifications.

Sujets connexes

Configurer les paramètres du profil de connexion, à la page 24

Envoyer des enregistrements de comptabilité au serveur RADIUS

Les enregistrements comptables dans le VPN d'accès à distance aident l'administrateur VPN à suivre les services auxquels les utilisateurs accèdent et la quantité de ressources réseau qu'ils consomment. Les renseignements de comptabilité comprennent le début et la fin de la session utilisateur, le nom d'utilisateur, le nombre d'octets qui passent par le périphérique pour chaque session, le service utilisé et la durée de chaque session.

Vous pouvez utiliser la comptabilité seule ou conjointement avec l'authentification et l'autorisation. Lorsque vous activez la comptabilité AAA, le serveur d'accès au réseau signale l'activité de l'utilisateur au serveur de comptabilité configuré. Vous pouvez configurer un serveur RADIUS comme serveur de gestion de comptes de sorte que le centre de gestion envoie toutes les informations sur les activités de l'utilisateur au serveur RADIUS.

Remarque Vous pouvez utiliser le même serveur RADIUS ou des serveurs RADIUS distincts pour l'authentification, l'autorisation et la comptabilité dans les paramètres AAA du VPN d'accès à distance.

Avant de commencer

- Configurez un objet de groupe RADIUS avec les serveurs RADIUS pour recevoir les demandes d'authentification ou les enregistrements de comptabilité. Pour en savoir plus, consultez Options de groupe de serveurs RADIUS.
- Assurez-vous que le serveur RADIUS est accessible à partir du périphérique défense contre les menaces . Configurez le routage sur votre Cisco Secure Firewall Management Center dans **Devices** – **Device Management (gestion des périphériques)** – **Edit Device** – **Routing** (modifier le périphérique – routage) pour assurer la connectivité au serveur RADIUS.

Procédure

Étape 1 Sur l'interface Web Cisco Secure Firewall Management Center, choisissez **Devices** (périphériques) – **Remote Access** (accès à distance).

Étape 2 Cliquez sur **Edit** (Modifier) dans la politique d'accès à distance pour laquelle vous souhaitez configurer le serveur RADIUS, ou créez une nouvelle politique d'accès VPN à distance.

Étape 3 Cliquez sur **Edit** (Modifier) dans le profil de connexion qui comprend les paramètres AAA et sélectionnez **AAA**.

Étape 4 Sélectionnez le serveur RADIUS dans la liste déroulante du serveur de **comptabilité**.

Étape 5 Enregistrez vos modifications.

Sujets connexes

Configurer les paramètres du profil de connexion, à la page 24
Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 26

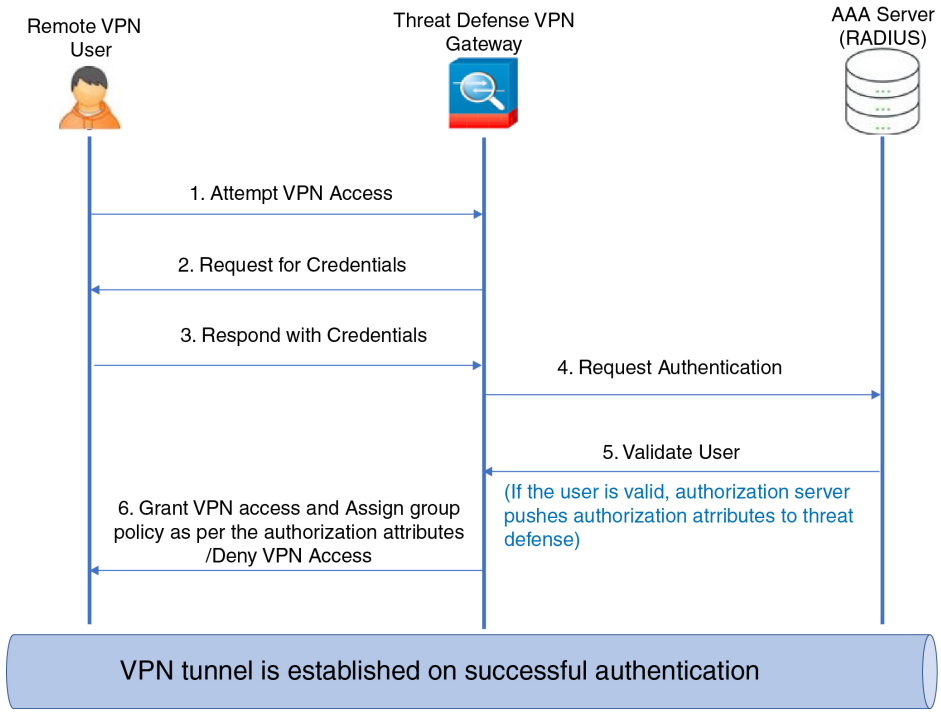
Délégation de la sélection de politiques de groupe au serveur d'autorisation

La politique de groupe appliquée à un utilisateur est déterminée lors de l'établissement du tunnel VPN. Vous pouvez sélectionner une politique de groupe pour un profil de connexion lors de la création d'une politique VPN d'accès à distance à l'aide de l'assistant ou mettre à jour la politique de connexion des profils de connexion ultérieurement. Cependant, vous pouvez configurer le serveur AAA (RADIUS) pour attribuer la politique de groupe ou elle est obtenue à partir du profil de connexion actuel. Si le périphérique défense contre les menaces reçoit des attributs du serveur AAA externe qui sont en conflit avec ceux configurés sur le profil de connexion, les attributs du serveur AAA ont toujours la priorité.

Vous pouvez configurer ISE ou le serveur RADIUS pour définir le profil d'autorisation pour un utilisateur ou un groupe d'utilisateurs en envoyant l'attribut RADIUS IETF 25 et en le mappant au nom de politique de groupe correspondant. Vous pouvez configurer une politique de groupe spécifique pour un utilisateur ou un groupe d'utilisateurs pour pousser une ACL téléchargeable, définir une bannière, restreindre le réseau VLAN et configurer l'option avancée consistant à appliquer une balise SGT à la session. Ces attributs sont appliqués à tous les utilisateurs qui font partie de ce groupe lorsque la connexion VPN est établie.

Pour plus d'informations, voir la section Configurer les politiques d'autorisation standard du Guide de l'administrateur du Service Cisco de vérification des identités et Attributs du serveur RADIUS pour Cisco Secure Firewall Threat Defense, à la page 33.

Illustration 1 : Sélection de politique de groupe VPN d'accès à distance par le serveur AAA



Sujets connexes

Configurer les objets de politique de groupe

Configurer les paramètres du profil de connexion, à la page 24

Remplacez la sélection de politique de groupe ou d'autres attributs par le serveur d'autorisation

Lorsqu'un utilisateur de VPN d'accès à distance se connecte au VPN, la politique de groupe et les autres attributs configurés dans le profil de connexion sont affectés à l'utilisateur. Cependant, l'administrateur du système VPN d'accès à distance peut déléguer la sélection de la politique de groupe et d'autres attributs au serveur d'autorisation en configurant ISE ou le serveur RADIUS pour définir le profil d'autorisation pour un utilisateur ou un groupe d'utilisateurs. Une fois les utilisateurs authentifiés, ces attributs d'autorisation spécifiques sont transmis au périphérique défense contre les menaces .

Avant de commencer

Assurez-vous de configurer une politique de VPN d'accès à distance avec RADIUS comme serveur d'authentification.

Procédure

Étape 1 Sur l'interface Web Cisco Secure Firewall Management Center, choisissez **Devices** (périphériques) > **VPN** > **Remote Access** (accès à distance).

Étape 2 Sélectionnez une politique d'accès à distance et cliquez sur **Edit** (Modifier).

Étape 3 Sélectionnez RADIUS ou ISE comme serveur d'autorisation s'il n'est pas déjà configuré.

Étape 4 Sélectionnez **Advanced** > **Group Policies** (Avancé > politiques de groupe) et ajoutez la politique de groupe requise. Pour des informations détaillées sur un objet de politique de groupe, consultez Configurer les objets de politique de groupe.

Vous ne pouvez mapper qu'une seule politique de groupe à un profil de connexion; mais vous pouvez créer plusieurs politiques de groupe dans une politique VPN d'accès à distance. Ces politiques de groupe peuvent être référencées dans ISE ou le serveur RADIUS et configurées pour remplacer la politique de groupe configurée dans le profil de connexion en affectant les attributs d'autorisation sur le serveur d'autorisations.

Étape 5 Déployez la configuration sur le périphérique.défense contre les menaces cible.

Étape 6 Sur le serveur d'autorisation, créez un profil d'autorisation avec les attributs RADIUS pour l'adresse IP et les listes de contrôle d'accès téléchargeables.

Lorsque la politique de groupe est configurée dans le serveur d'autorisation sélectionné pour le VPN d'accès à distance, cette dernière remplace la politique de groupe configurée dans le profil de connexion pour l'utilisateur du VPN d'accès à distance une fois que l'utilisateur est authentifié.

Sujets connexes

Configurer les objets de politique de groupe

Refuser l'accès VPN à un groupe d'utilisateurs

Lorsque vous ne souhaitez pas qu'un utilisateur ou groupe d'utilisateurs authentifiés puisse utiliser le VPN, vous pouvez configurer une politique de groupe pour refuser l'accès au VPN. Vous pouvez configurer une politique de groupe dans une politique VPN d'accès à distance et y faire référence dans la configuration du serveur ISE ou RADIUS pour l'autorisation.

Avant de commencer

Assurez-vous d'avoir configuré le VPN d'accès à distance à l'aide de l'assistant de politique d'accès à distance et les paramètres d'authentification pour la politique de VPN d'accès à distance.

Procédure

Étape 1 Sur l'interface Web Cisco Secure Firewall Management Center, choisissez **Devices** (périphériques) > **VPN** > **Remote Access** (accès à distance).

Étape 2 Sélectionnez une politique d'accès à distance et cliquez sur **Edit** (Modifier).

Étape 3 Sélectionnez **Advanced** (Avancé) > **Group Policies** (Politiques de groupe).

Étape 4 Sélectionnez une politique de groupe et cliquez sur **Edit** (Modifier) ou ajoutez une nouvelle politique de groupe.

Étape 5 Sélectionnez **Advanced** (Avancé) > **Session Settings** (Paramètres de session) et réglez **Simultaneous Login Per User** (Connexion simultanée par utilisateur) sur 0 (zéro).
Cela empêche l'utilisateur ou le groupe d'utilisateurs de se connecter au VPN même une seule fois.

Étape 6 Cliquez sur **Save** pour enregistrer la politique de groupe, puis enregistrez la configuration du VPN d'accès à distance.

Étape 7 Configurez le serveur ISE ou RADIUS pour définir le profil d'autorisation de cet utilisateur/groupe d'utilisateurs afin d'envoyer l'attribut RADIUS IETF 25 et de l'associer au nom de la politique de groupe correspondante.

Étape 8 Configurez le serveur ISE ou RADIUS comme serveur d'autorisation dans la politique VPN d'accès à distance.

Étape 9 Enregistrez et déployez la politique VPN d'accès à distance.

Sujets connexes

Configurer les paramètres du profil de connexion, à la page 24

Restreindre la sélection de profil de connexion pour un groupe d'utilisateurs

Lorsque vous souhaitez appliquer un profil de connexion unique à un utilisateur ou un groupe d'utilisateurs, vous pouvez choisir de désactiver le profil de connexion de sorte que l'alias de groupe ou les URL ne soient pas disponibles pour que les utilisateurs puissent les sélectionner lorsqu'ils se connectent à l'aide du module VPN AnyConnect client du AnyConnect de Cisco Secure Client .

Par exemple, si votre entreprise souhaite utiliser des configurations spécifiques pour différents groupes d'utilisateurs VPN, comme les utilisateurs mobiles, les utilisateurs d'ordinateurs portables d'entreprise ou les utilisateurs d'ordinateurs portables personnels, vous pouvez configurer de connexion un profil spécifique à chacun de ces groupes d'utilisateurs et appliquer la connexion appropriée. profil lorsque l'utilisateur se connecte au VPN.

Le Module VPN AnyConnect de Cisco Secure Client affiche par défaut une liste des profils de connexion (par nom de profil de connexion, alias ou URL d'alias) configurés dans centre de gestion et déployés sur défense contre les menaces . Si des profils de connexion personnalisés ne sont pas configurés, le module VPN Module AnyConnect de Cisco Secure Client affiche le profil de connexion par défaut *WEBVPNGroup*. Utilisez la procédure suivante pour appliquer un profil de connexion unique pour un groupe d'utilisateurs.

Avant de commencer

- Sur votre interface Web Cisco Secure Firewall Management Center, configurez le VPN d'accès à distance à l'aide de l'assistant de politique de VPN d'accès à distance en utilisant la méthode d'authentification « Client Certificate Only » ou « Client Certificate + AAA » (Certificat client uniquement ou certificat client + AAA). Choisissez les champs de nom d'utilisateur dans le certificat.
- Configurez le serveur ISE ou RADIUS pour l'autorisation et associez la politique de groupe au serveur d'autorisation.

Procédure

Étape 1 Sur l'interface Web Cisco Secure Firewall Management Center, choisissez **Devices** (périphériques) > **VPN** > **Remote Access** (accès à distance).

Étape 2 Sélectionnez une politique d'accès à distance et cliquez sur **Edit** (Modifier).

Étape 3 Sélectionnez **Access Interfaces** (Accès aux interfaces) et désactivez **Allow users to select connection profile while logging in** (Permettre aux utilisateurs de sélectionner un profil de connexion lors de l'ouverture de session).

Étape 4 Cliquez sur **Advanced** > **Certificate Maps** (Avancé > Carte de certificats).

Étape 5 Sélectionnez **Use the configured rules to match a certificate to a Connection Profile** (Utilisez les règles configurées pour faire correspondre un certificat à un profil de connexion).

Étape 6 Sélectionnez le **nom de la carte de certificats** ou cliquez sur l'icône **Ajouter** pour ajouter une règle de certificat.

Étape 7 Sélectionnez le **profil de connexion**, puis cliquez sur **OK**.

Avec cette configuration, lorsqu'un utilisateur se connecte à partir du module VPN AnyConnect de Cisco Secure Client, l'utilisateur aura le profil de connexion mappé et sera authentifié pour utiliser le VPN.

Sujets connexes

Configurer les objets de politique de groupe

Configurer les paramètres du profil de connexion, à la page 24

Mettre à jour le profil Secure Client (services client sécurisés) pour les clients VPN d'accès à distance

Le profilSecure Client (services client sécurisés) est un fichier XML qui contient les exigences de l'utilisateur final et les politiques d'authentification définies par l'administrateur. Il doit être déployé sur un système client VPN dans le cadre de Secure Client. Il met les profils réseau préconfigurés à la disposition des utilisateurs finaux.

Vous pouvez utiliser l'interface graphique Secure Client Profile Editor, un outil de configuration indépendant, pour le créer. Un éditeur de profil autonome peut être utilisé pour créer un nouveau profil ou modifier un profil existant Secure Client. Vous pouvez télécharger l'éditeur de profil à partir du Centre de téléchargement de logiciels Cisco.

Consultez le chapitre Secure Client Profile Editor de la version appropriée du Guide de l'administrateur de Cisco Secure Client (y compris AnyConnect) pour en savoir plus.

Avant de commencer

- Assurez-vous d'avoir configuré le VPN d'accès à distance à l'aide de l'assistant de politique d'accès à distance et de déployer la configuration sur le périphérique défense contre les menaces . Consultez Créer une nouvelle politique VPN d'accès à distance, à la page 14.
- Sur votre interface Web Cisco Secure Firewall Management Center, accédez à **Objects** (Objets) > **Object Management** (Gestion des objets) > **VPN** > **Secure Client File** (Fichier client sécurisé) et ajoutez la nouvelle image Secure Client (services client sécurisés).

Procédure

Étape 1 Sur l'interface Web Cisco Secure Firewall Management Center, choisissez **Devices** (périphériques) > **VPN** > **Remote Access** (accès à distance).

Étape 2 Sélectionnez une politique VPN d'accès à distance et cliquez sur **Edit** (Modifier).

Étape 3 Sélectionnez le profil de connexion qui comprend le profil client à modifier, puis cliquez sur **Edit** (Modifier).

Étape 4 Cliquez sur **Edit Group Policy (modifier la politique de groupe)** > **Secure Client** > **Profiles** (Profils).

Étape 5 Sélectionnez le fichier XML de profil client dans la liste ou cliquez sur **Add** pour ajouter un nouveau profil client.

Étape 6 Enregistrez la politique de groupe, le profil de connexion, puis la politique VPN d'accès à distance.

Étape 7 Déployez les modifications.
Les modifications apportées au profil du client sont mises à jour sur les clients VPN lorsqu'ils se connectent à la passerelle d'accès VPN à distance.

Sujets connexes

Configurer les objets de politique de groupe

Autorisation dynamique RADIUS

Cisco Secure Firewall Threat Defense a la capacité d'utiliser des serveurs RADIUS pour l'autorisation des utilisateurs d'accès à distance VPN et des sessions de proxy direct de pare-feu à l'aide de listes de contrôle d'accès dynamiques, ou de noms d'ACL par utilisateur. Pour mettre en œuvre des listes de contrôle d'accès dynamiques pour une autorisation dynamique ou RADIUS Change of Authorization (RADIUS CoA), vous devez configurer le serveur RADIUS pour les prendre en charge. Lorsque l'utilisateur tente de s'authentifier, le serveur RADIUS envoie une liste de contrôle d'accès téléchargeable ou un nom à défense contre les menaces . L'accès à un service donné est autorisé ou refusé par la liste de contrôle d'accès. Cisco Secure Firewall Threat Defense supprime la liste de contrôle d'accès à l'expiration de la session d'authentification.

Sujets connexes

Ajouter un groupe de serveurs RADIUS

Interface

Configuration de l'autorisation dynamique RADIUS, à la page 78

Attributs du serveur RADIUS pour Cisco Secure Firewall Threat Defense, à la page 33

Configuration de l'autorisation dynamique RADIUS

Avant de commencer :

- Une seule interface peut être configurée dans la zone de sécurité ou le groupe d'interfaces si elle est référencée dans un serveur RADIUS.
- Un serveur RADIUS pour lequel l'autorisation dynamique est activée nécessite Cisco Secure Firewall Threat Defense 6.3 ou une version ultérieure pour que l'autorisation dynamique fonctionne.
- La sélection d'interface dans le serveur RADIUS n'est pas prise en charge dans les versions Cisco Secure Firewall Threat Defense 6.2.3 ou antérieures. L'option d'interface sera ignorée lors du déploiement.
- Le VPN de posture Défense contre les menaces ne prend pas en charge la modification de politique de groupe par le biais de l'autorisation dynamique ou du changement d'autorisation RADIUS (CoA).

Tableau 5 : Procédure

	Faire ceci	Plus d'informations
Étape 1	Connectez-vous à votre interface Web Cisco Secure Firewall Management Center.	
Étape 2	Configurer un objet serveur RADIUS avec une autorisation dynamique.	Options de groupe de serveurs RADIUS

	Faire ceci	Plus d'informations
Étape 3	Configurez un routage vers le serveur ISE par une interface activée pour les changements d'autorisation (CoA) afin d'établir la connectivité de défense contre les menaces au serveur RADIUS par le biais du routage ou d'une interface spécifique.	Options de groupe de serveurs RADIUS Configurer ISE/ISE-PIC pour le contrôle utilisateur
Étape 4	Configurez une politique VPN d'accès à distance et sélectionnez l'objet de groupe de serveurs RADIUS que vous avez créé avec une autorisation dynamique.	Créer une nouvelle politique VPN d'accès à distance, à la page 14
Étape 5	Configurez les détails du serveur DNS et les interfaces de recherche de domaine en utilisant les paramètres de la plateforme.	Configurer le DNS, à la page 18 Groupe de serveurs DNS
Étape 6	Configurez une tunnelisation fractionnée dans la politique de groupe pour autoriser le trafic DNS à travers le tunnel VPN d'accès à distance si le serveur DNS est accessible par le réseau VNP.	Configurer les objets de politique de groupe
Étape 7	Déployer les modifications de configuration.	Déployer les modifications de configuration

Authentification à deux facteurs

Vous pouvez configurer l'authentification à deux facteurs pour le VPN d'accès à distance. Avec l'authentification à deux facteurs, l'utilisateur doit fournir un nom d'utilisateur et un mot de passe statiques, ainsi qu'un élément supplémentaire comme un jeton RSA ou un code d'accès. L'authentification à deux facteurs diffère de l'utilisation d'une deuxième source d'authentification en ce sens que l'authentification à deux facteurs est configurée sur une source d'authentification unique, la relation avec le serveur RSA étant liée à la source d'authentification principale.

Cisco Secure Firewall Threat Defense prend en charge les jetons RSA et les demandes d'authentification Duo Push à Duo Mobile pour le deuxième facteur, conjointement avec tout serveur RADIUS ou AD comme premier facteur dans le processus d'authentification à deux facteurs.

Configuration de l'authentification à deux facteurs RSA

À propos de cette tâche :

Vous pouvez configurer le serveur RADIUS ou AD comme agent d'authentification dans le serveur RSA et utiliser le serveur dans Cisco Secure Firewall Management Center comme source d'authentification principale dans le VPN d'accès à distance.

Lorsqu'il utilise cette approche, l'utilisateur doit s'authentifier à l'aide d'un nom d'utilisateur configuré sur le serveur RADIUS ou AD, et concaténer le mot de passe avec le jeton RSA à usage unique temporaire, en séparant le mot de passe et le jeton par une virgule : *password*,*token*.

Dans cette configuration, il est courant d'utiliser un serveur RADIUS distinct (comme celui fourni dans Cisco ISE) pour fournir les services d'autorisation. Vous devez configurer le deuxième serveur RADIUS en tant qu'autorisation et, éventuellement, serveur de comptabilité.

Avant de commencer :

Assurez-vous que les configurations suivantes sont terminées avant de configurer l'authentification à deux facteurs RADIUS sur Cisco Secure Firewall Threat Defense :

Sur le serveur RSA

- Configurez le serveur RADIUS ou Active Directory en tant qu'agent d'authentification.
- Générez et téléchargez le fichier de configuration (*sdconf.rec*).
- Créez un profil de jeton, attribuez le jeton à l'utilisateur et distribuez le jeton à l'utilisateur. Téléchargez et installez le jeton sur le système client VPN d'accès à distance.

Pour en savoir plus, consultez la documentation de RSA SecureID Suite.

Sur le serveur ISE

- Importez le fichier de configuration (*sdconf.rec*) généré sur le serveur RSA.
- Ajoutez le serveur RSA comme source d'identité externe et spécifiez le code secret partagé.

Tableau 6 : Procédure

	Faire ceci	Plus d'informations
Étape 1	Connectez-vous à votre interface Web Cisco Secure Firewall Management Center.	
Étape 2	Créer un groupe de serveurs RADIUS	Options de groupe de serveurs RADIUS
Étape 3	Créez un objet serveur RADIUS dans le nouveau groupe de serveurs RADIUS, avec un serveur RADIUS ou AD comme hôte et avec un délai d'expiration de 60 secondes ou plus.	Options de groupe de serveurs RADIUS **Remarque** Le serveur RADIUS ou AD doit être le même serveur configuré comme agent d'authentification dans le serveur RSA. Pour l'authentification à deux facteurs, assurez-vous que le délai d'expiration est également mis à jour à 60 secondes ou plus dans le fichier XML Secure Client Profile.
Étape 4	Configurez une nouvelle politique VPN d'accès à distance à l'aide de l'assistant ou modifiez une politique VPN d'accès à distance existante.	Créer une nouvelle politique VPN d'accès à distance, à la page 14
Étape 5	Sélectionnez RADIUS comme serveur d'authentification, puis sélectionnez le groupe de serveurs RADIUS nouvellement créé comme serveur d'authentification.	Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 26

	Faire ceci	Plus d'informations
Étape 7	Déployer les modifications de configuration.	Déployer les modifications de configuration

Configuration de l'authentification à deux facteurs Duo

À propos de cette tâche :

Vous pouvez configurer le serveur RADIUS Duo comme source d'authentification principale. Cette approche utilise le serveur mandataire d'authentification RADIUS Duo. (Vous ne pouvez pas utiliser de connexion directe avec le service en nuage Duo sur LDAPS.)

Pour connaître les étapes détaillées de la configuration de Duo, consultez https://duo.com/docs/cisco-firepower.

Vous devez ensuite configurer Duo pour transférer les demandes d'authentification dirigées vers le serveur mandataire pour utiliser un autre serveur RADIUS, ou un serveur AD, comme premier facteur d'authentification et le service en nuage Duo comme deuxième facteur.

Lorsqu'il utilise cette approche, l'utilisateur doit s'authentifier à l'aide d'un nom d'utilisateur configuré à la fois sur Duo Cloud ou le serveur Web et sur le serveur RADIUS associé. L'utilisateur doit saisir le mot de passe configuré dans le serveur RADIUS, suivi de l'un des codes Duo suivants :

- **Mot de passe duo**. Par exemple, *mon-motdepasse*,123456.
- **push**. Par exemple, *mon-motdepasse*,**push**. Utilisez la commande push pour demander à Duo d'envoyer une authentification poussée à l'application Duo Mobile, que l'utilisateur doit déjà avoir installée et enregistrée.
- **sms**. Par exemple, *mon-motdepasse*,**sms**. Utilisez **sms** pour demander à Duo d'envoyer un message SMS avec un nouveau lot de codes d'authentification au périphérique mobile de l'utilisateur. La tentative d'authentification de l'utilisateur échouera lors de l'utilisation de **sms**. L'utilisateur doit ensuite s'authentifier de nouveau et saisir le nouveau mot de passe comme facteur secondaire.
- **phone**. Par exemple, *mon-motdepasse*,**phone**. Utilisez **phone** pour s'authentifier à l'aide du rappel téléphonique.

Pour en savoir plus sur les options de connexion et consulter des exemples, consultez https://guide.duo.com/anyconnect.

Avant de commencer :

Avant de configurer l'authentification à deux facteurs avec le mandataire d'authentification Duo sur défense contre les menaces , assurez-vous d'effectuer les configurations suivantes :

- Configurez une authentification principale qui fonctionne (RADIUS ou AD) pour vos utilisateurs d'accès à distance VPN avant de commencer à déployer Duo.
- Installez le service proxy Duo sur un ordinateur Windows ou Linux de votre réseau pour intégrer Duo au VPN d'accès à distance Cisco Secure Firewall Threat Defense. Ce serveur mandataire Duo agit également comme serveur RADIUS.

  Téléchargez et installez le plus récent mandataire d'authentification Duo à partir de l'emplacement suivant :

  - **Windows** : https://dl.duosecurity.com/duoauthproxy-latest.exe

- **Linux** : https://dl.duosecurity.com/duoauthproxy-latest-src.tgz
- Vérifiez la somme de contrôle sur https://duo.com/docs/checksums#duo-authentication-proxy.

- Configurez le fichier d'authentification Duo `authproxy.cfg`. Suivez les instructions de la page https://duo.com/docs/cisco-firepower#configure-the-proxy pour configurer les paramètres de configuration de l'authentification.

  Le fichier de configuration `authproxy.cfg` doit contenir les détails du serveur RADIUS ou ISE, du périphérique défense contre les menaces , des détails du serveur mandataire Duo, de la clé d'intégration, de la clé secrète et de l'hôte d'API.

- Assurez-vous d'avoir les bonnes informations sur l'hôte d'API dans le fichier `authproxy.cfg`.
- Configurez les autres paramètres requis tels que le facteur d'authentification secondaire dans le serveur mandataire Duo nouvellement installé **Duo Security Server** (Serveur de sécurité Duo) > **Duo Admin Panel** (Volet d'administration Duo) > **Applications** > **VPN CISCO RADIUS**.

Tableau 7 : Procédure

	Faire ceci	Plus d'informations
Étape1	Connectez-vous à votre interface Web Cisco Secure Firewall Management Center.	
Étape2	Créer un groupe de serveurs RADIUS	Options de groupe de serveurs RADIUS
Étape3	Créer un objet serveur RADIUS dans le nouveau groupe de serveurs RADIUS avec le serveur mandataire Duo comme hôte avec un délai d'expiration de 60 secondes ou plus.	Options de serveurs RADIUS **Remarque** Pour l'authentification à deux facteurs, assurez-vous que le délai d'expiration est également mis à jour à 60 secondes ou plus dans le fichier XML Secure Client Profile.
Étape4	Configurez une nouvelle politique VPN d'accès à distance à l'aide de l'assistant ou modifiez une politique VPN d'accès à distance existante.	Créer une nouvelle politique VPN d'accès à distance, à la page 14
Étape5	Sélectionnez RADIUS comme serveur d'authentification, puis sélectionnez le groupe de serveurs RADIUS créé avec le serveur mandataire Duo comme serveur d'authentification.	Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 26
Étape7	Déployer les modifications de configuration.	Déployer les modifications de configuration

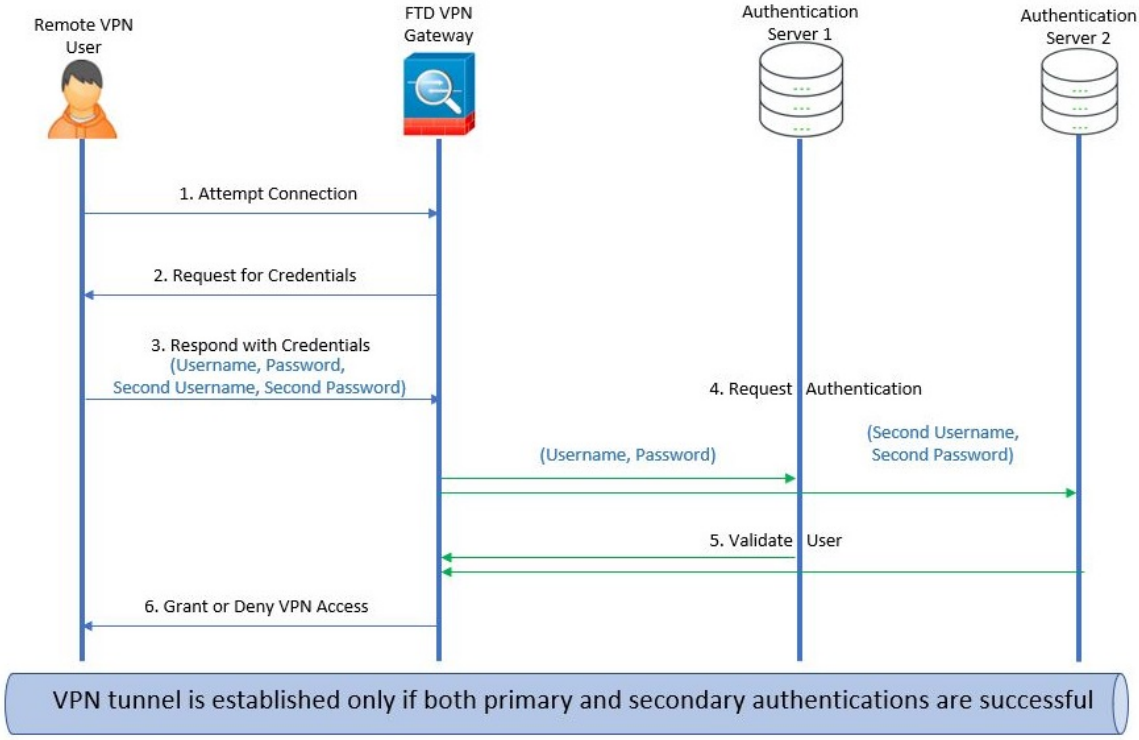
Authentification secondaire

L'authentification secondaire ou la double authentification de Cisco Secure Firewall Threat Defense ajoute une couche de sécurité supplémentaire aux connexions VPN d'accès à distance grâce à l'utilisation de deux serveurs d'authentification différents. Lorsque l'authentification secondaire est activée, les utilisateurs de

VPN Secure Client doivent fournir deux ensembles d'informations d'authentification pour se connecter à la passerelle VPN.

Le VPN d'accès à distance Cisco Secure Firewall Threat Defense prend en charge l'authentification secondaire dans les méthodes d'authentification AAA uniquement et certificat client et AAA.

Illustration 2 : Authentification VPN secondaire d'accès à distance ou double



Sujets connexes

Configurer l'authentification secondaire du VPN d'accès à distance, à la page 83

Configurer l'authentification secondaire du VPN d'accès à distance

Lorsque l'authentification VPN d'accès à distance est configurée pour utiliser à la fois un certificat client et un serveur d'authentification, l'authentification du client VPN est effectuée à l'aide de la validation du certificat client et du serveur AAA.

Avant de commencer

- Configurez deux serveurs d'authentification (AAA), les serveurs d'authentification principal et secondaire, et les certificats d'identité requis. Les serveurs d'authentification peuvent être un serveur RADIUS et les domaines AD ou LDAP.
- Assurez-vous que les serveurs AAA sont accessibles à partir du périphérique Cisco Secure Firewall Threat Defense pour que la configuration VPN d'accès à distance fonctionne. Configurez le routage (sous **Devices > Device Management > Edit Device > Routing**) (Périphériques > Gestion des périphériques > Modifier un périphérique > Routage) pour assurer la connectivité avec les serveurs AAA.

Procédure

Étape 1 Sur l'interface Web Cisco Secure Firewall Management Center, choisissez **Devices** (périphériques) > **VPN** > **Remote Access** (accès à distance).

Étape 2 Sélectionnez une politique d'accès à distance et cliquez sur **Edit** (Modifier); ou cliquez sur **Add** (Ajouter) pour créer une nouvelle politique VPN d'accès à distance.

Étape 3 Pour une nouvelle politique VPN d'accès à distance, configurez l'authentification tout en sélectionnant les paramètres de profil de connexion. Pour une configuration existante, sélectionnez le profil de connexion qui comprend le profil client, puis cliquez sur **Edit** (Modifier).

Étape 4 Cliquez sur **AAA** > **Authentication Méthode**(Méthode d'authentification AAA), **AAA** ou **Client Certificate & AAA**(certificat client et AAA).

- Lorsque vous sélectionnez la **méthode d'authentification** :

  Certificat client et AAA : l'authentification est effectuée à l'aide d'un certificat client et d'un serveur AAA.

  - **AAA** : Si vous sélectionnez le **serveur d'authentification RADIUS**, par défaut la même valeur est attribuée au serveur d'autorisation. Sélectionnez le **Accounting Server** (Serveur de comptabilité) dans la liste déroulante. Chaque fois que vous sélectionnez **AD** et **LDAP** dans la liste déroulante Authentication Server, (Serveur d'authentification) vous devez sélectionner manuellement le **serveur d'autorisation** et le **serveur de comptabilité**, respectivement.
  - Quelle que soit la méthode d'authentification que vous choisissez, cochez ou décochez la case **Allow connection only if user Existing in authentication database** (Autoriser la connexion uniquement si l'utilisateur existe dans la base de données d'authentification).

- **Utilisez l'authentification secondaire** : l'authentification secondaire est configurée en complément de l'authentification principale pour fournir une sécurité supplémentaire pour les sessions VPN. L'authentification secondaire s'applique uniquement aux méthodes d'authentification **AAA uniquement** et par **certificat client et AAA**.

  L'authentification secondaire est une fonctionnalité facultative qui oblige un utilisateur VPN à saisir deux ensembles de nom d'utilisateur et de mot de passe sur l'écran de connexion Secure Client. Vous pouvez également configurer le système pour préremplir le nom d'utilisateur secondaire à partir du serveur d'authentification ou du certificat client. L'authentification VPN de l'accès à distance est accordée uniquement si les authentifications principale et secondaire réussissent. L'authentification VPN est refusée si l'un des serveurs d'authentification n'est pas accessible ou si une authentification échoue.

  Vous devez configurer un groupe de serveurs d'authentification secondaire (serveur AAA) pour le deuxième nom d'utilisateur et mot de passe avant de configurer l'authentification secondaire. Par exemple, vous pouvez définir le serveur d'authentification principal sur un domaine LDAP ou Active Directory et l'authentification secondaire sur un serveur RADIUS.

  Remarque Par défaut, l'authentification secondaire n'est pas requise.

  Authentication Server(serveur d'authentification) : le serveur d'authentification secondaire fournit un nom d'utilisateur et un mot de passe secondaires aux utilisateurs de VPN.

  Sélectionnez les éléments suivants sous **Username for secondary authentication** (Nom d'utilisateur pour l'authentification secondaire) :

  - **Invite** : Invite les utilisateurs à saisir le nom d'utilisateur et le mot de passe lors de la connexion à la passerelle VPN.

- **Utiliser le nom d'utilisateur de l'authentification principale** : le nom d'utilisateur provient du serveur d'authentification principal pour l'authentification principale et secondaire. vous devez saisir deux mots de passe.
- **Mapper le nom d'utilisateur du certificat client** : préremplit le nom d'utilisateur secondaire du certificat client.
  - Si vous sélectionnez l'option **Map specific field** (Mapper un champ spécifique), qui comprend le nom d'utilisateur du certificat client. Les champs **principal** et **secondaire** affichent les valeurs par défaut : **NC (nom commun)** et **OU (unité organisationnelle)**, respectivement. Si vous sélectionnez l'option **Use entire DN (Distinguished Name) (Utiliser le Nom distinctif complet DN) comme nom d'utilisateur**, le système récupère automatiquement l'identité de l'utilisateur.

    Consultez la section Descriptions des **méthodes d'authentification** pour de plus amples renseignements sur le mappage des champs principal et secondaire.
  - **Préremplir le nom d'utilisateur à partir du certificat sur la fenêtre de connexion** : préremplit le nom d'utilisateur secondaire à partir du certificat client lorsque l'utilisateur se connecte avec Secure Client.
    - **Masquer le nom d'utilisateur dans la fenêtre de connexion** : le nom d'utilisateur secondaire est prérempli à partir du certificat client, mais masqué pour l'utilisateur afin que ce dernier ne modifie pas le nom d'utilisateur prérempli.
- **Utilisez le nom d'utilisateur secondaire pour la session VPN** : le nom d'utilisateur secondaire est utilisé pour signaler l'activité de l'utilisateur au cours d'une session VPN.

Pour en savoir plus, consultez Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 26.

Sujets connexes

Configurer les paramètres du profil de connexion, à la page 24

Authentification de connexion unique Single Sign-On avec SAML 2.0

À propos de l'authentification de connexion unique SAML

SAML (Security Assertion Markup Language) est une norme ouverte pour la connexion des utilisateurs aux applications en utilisant leurs sessions dans un autre contexte. Les entreprises connaissent déjà l'identité des utilisateurs lorsque ces derniers se connectent à leur domaine Active Directory (AD) ou à l'intranet. Elles utilisent ces renseignements d'identité pour connecter les utilisateurs à d'autres applications, telles que les applications Web utilisant SAML. Les applications individuelles n'ont pas besoin de stocker les informations d'authentification et les utilisateurs n'ont pas à se souvenir et à gérer différents ensembles d'informations d'authentification pour les applications individuelles. L'authentification unique (SSO) SAML consiste à transférer l'identité de l'utilisateur d'un emplacement (le fournisseur d'identité) à un autre (le fournisseur de service).

Authentification de connexion unique SAML avec Cisco Secure Firewall Threat Defense

Le périphérique Cisco Secure Firewall Threat Defense prend en charge l'authentification de connexion unique (SSO) SAML 2.0 pour les connexions VPN d'accès à distance qui utilisent Secure Client. Vous avez besoin

des éléments suivants pour configurer l'authentification unique de SAML 2.0 sur Cisco Secure Firewall Threat Defense :

- **Fournisseur d'identité** : la passerelle d'accès Duo agit comme fournisseur d'identité pour effectuer l'authentification des utilisateurs et émet des assertions.
- **Fournisseur de services** : le périphérique défense contre les menaces agit en tant que fournisseur de services et obtient l'assertion d'authentification du fournisseur d'identité.
- **Client VPN** : Secure Client effectue l'authentification SAML 2.0 à l'aide du navigateur intégré.

Vous pouvez appliquer une politique d'accès à un utilisateur authentifié par SAML si vous avez une politique d'identité associée à un domaine AD correspondant au domaine SAML.

Directives et limites relatives à SAML 2.0

- Défense contre les menaces prend en charge les signatures suivantes pour l'authentification SAML :
  - SHA1 avec RSA et HMAC
  - SHA2 avec RSA et HMAC
- Défense contre les menaces prend en charge la liaison Redirect-POST SAML 2.0, qui est prise en charge par tous les fournisseurs d'identité SAML.
- Défense contre les menaces fonctionne uniquement comme fournisseur de service SAML. Il ne peut pas servir de fournisseur d'identité en mode passerelle ou en mode homologue.
- Vous pouvez appliquer une politique d'accès à un utilisateur authentifié par SAML si vous avez une politique d'identité associée à un domaine AD correspondant au domaine SAML.
- Le fait d'avoir des attributs d'authentification SAML disponibles dans l'évaluation DAP (semblables aux attributs RADIUS envoyés dans la réponse d'authentification RADIUS par le serveur AAA) n'est pas pris en charge. Défense contre les menaces prend en charge la politique de groupe activée par SAML sur la politique DAP; cependant, vous ne pouvez pas vérifier l'attribut de nom d'utilisateur lorsque vous utilisez l'authentification SAML, car l'attribut de nom d'utilisateur est masqué par le fournisseur d'identité SAML.
- Les administrateursDéfense contre les menaces doivent assurer la synchronisation de l'horloge entre défense contre les menaces et le fournisseur d'identité SAML pour une gestion appropriée des déclarations d'authentification et un comportement correct du délai d'expiration.
- Les administrateurs de Défense contre les menaces sont responsables de maintenir un certificat de signature valide sur défense contre les menaces et sur le fournisseur d'identité en tenant compte des éléments suivants :
  - Le certificat de signature du fournisseur d'identité est obligatoire lors de la configuration d'un fournisseur d'identité sur défense contre les menaces .
  - défense contre les menaces n'effectue pas de vérification de révocation sur le certificat de signature reçu du fournisseur d'identité.
- Dans les assertions SAML, il existe des conditions NotBefore et NotOnOrAfter . Le délai d'expiration configuré pour le SAML défense contre les menaces interagit avec ces conditions comme suit :
  - Le délai d'expiration remplace NotOnOrAfter si la somme de NotBefore et du délai d'expiration est antérieure à NotOnOrAfter.

- Si NotBefore + le délai d'expiration est postérieur à NotOnOrWith, NotOnOrAfter prend effet.
- Si l'attribut NotBefore est absent, défense contre les menaces refuse la demande de connexion. Si l'attribut NotOnOrAfter est absent et que le délai d'expiration SAML n'est pas défini, défense contre les menaces refuse la demande de connexion.

- Défense contre les menaces ne fonctionne pas avec Duo dans un déploiement utilisant SAML interne, ce qui oblige défense contre les menaces à passer par le mandataire pour que le client s'authentifie, en raison du changement de nom de domaine complet qui se produit lors de la demande/réponse pour l'authentification à deux facteurs (push, code, mot de passe).
- Lorsque vous utilisez SAML avec Secure Client, suivez ces instructions :
  - Les certificats de serveur non fiable ne sont pas autorisés dans le navigateur intégré.
  - L'intégration SAML au navigateur intégré n'est pas prise en charge en modes CLI ou SBL.
  - L'authentification SAML établie dans un navigateur Web n'est pas partagée avec Secure Client, et inversement.
  - Selon la configuration, diverses méthodes sont utilisées lors de la connexion à la tête de réseau avec le navigateur intégré. Par exemple, alors que Secure Client peut préférez une connexion IPv4 à une connexion IPv6, le navigateur intégré peut préférez IPv6, ou inversement. De même, Secure Client peut avoir recours à l'absence de serveur mandataire après avoir essayé de passer par un mandataire et obtenu un échec, tandis que le navigateur intégré peut arrêter la navigation après avoir essayé de passer par un mandataire et obtenu un échec.
  - Vous devez synchroniser le serveur NTP (Network Time Protocol) de votre défense contre les menaces avec le serveur NTP du fournisseur d'identité pour utiliser la fonctionnalité SAML.
  - Vous ne pouvez pas accéder aux serveurs internes avec la SSO après vous être connecté à l'aide d'un fournisseur d'identité interne.
  - L'attribut NameID du fournisseur d'identité SAML détermine le nom d'utilisateur de l'utilisateur et est utilisé pour l'autorisation, la comptabilité et la base de données des sessions VPN.

Configuration de l'authentification de la connexion unique SAML

Avant de commencer

Assurez-vous d'avoir effectué les étapes suivantes avant de configurer la connexion unique SAML avec le VPN d'accès à distance défense contre les menaces :

- Créez un compte avec Duo
- Téléchargez et installez la passerelle duo Access Gateway.
- Obtenez les éléments suivants auprès de votre fournisseur d'identité SAML (Duo).
  - URL de l'identifiant d'entité du fournisseur d'identité (IDP)
  - URL de connexion
  - URL de déconnexion
  - Certificat du fournisseur d'identité

- Créez un objet serveur de connexion unique SAML. Pour en savoir plus, consultez Ajouter un serveur de connexion unique (SSO).

Remarque Vous pouvez créer un objet de serveur d'authentification unique dans les paramètres de **profil de connexion** lorsque vous créez une politique à l'aide de l'assistant de politique VPN d'accès à distance.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Cliquez sur **Edit** (Modifier) à côté de la politique VPN d'accès à distance pour laquelle vous souhaitez configurer l'authentification SAML. Si vous souhaitez créer une nouvelle politique, cliquez sur **Add** (Ajouter).

Étape 3 Cliquez sur **Edit** (Modifier) sur le profil de connexion que vous souhaitez modifier.

Étape 4 Choisissez les paramètres **AAA** et sélectionnez **SAML** dans la liste déroulante **Méthode d'authentification**.

Étape 5 Choisissez le serveur de connexion unique SAML requis comme serveur d'**authentification**.

Étape 6 Configurez les paramètres requis pour le VPN d'accès à distance.

Étape 7 Enregistrez et déployez la politique VPN d'accès à distance sur votre périphériquedéfense contre les menaces .

Sujets connexes

Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 26

Configuration de l'autorisation SAML

À propos de l'autorisation SAML

L'autorisation SAML prend en charge les attributs utilisateur fournis dans les énoncés SAML dans les cadres AAA et DAP (Dynamic Access Policy). Vous pouvez configurer les attributs d'assertion SAML sur le fournisseur d'identité en tant que paires nom-valeur, qui seront ensuite analysées comme des chaînes. Les attributs reçus sont mis à la disposition de DAP de sorte qu'ils peuvent être utilisés lors de la définition des critères de sélection dans un enregistrement DAP. L'assertion SAML *cisco_group_policy* est utilisée pour déterminer la politique de groupe à appliquer à la session VPN.

Représentation dynamique des attributs de la politique d'accès

Dans le tableau DAP, les attributs DAP sont représentés au format suivant :

```
aaa.saml.name = "value"
```

Exemple, *aaa.saml.department = "finance"*

Cet attribut peut être utilisé dans la sélection DAP comme suit :

```
<attr>
<name>aaa.saml.department</name>
<value>finance</value>
<operation>EQ</operation>
</attr>
```

Attributs à valeurs multiples

Les attributs à valeurs multiples sont également pris en charge dans DAP et la table DAP est indexée :

```
aaa.saml.name.1 = "value"
aaa.saml.name.2 = "value"
```

Attributs memberOf pour Active Directory

L'attribut memberOf d'Active Directory (AD) reçoit un traitement spécial cohérent avec la façon dont il est géré par une requête LDAP.

Les noms de groupe sont représentés par l'attribut CN du DN.

Exemple d'attributs reçus du serveur d'autorisation :

```
memberOf = "CN=FTD-VPN-Group,OU=Users,OU=TechspotUsers,DC=techspot,DC=us"
 memberOf = "CN=Domain Admins,OU=Users,DC=techspot,DC=us"
```

Attributs de la politique d'accès dynamique :

```
aaa.saml.memberOf.1 = "FTD-VPN-Group"
aaa.saml.memberOf.2 = "Domain Admins"
```

Interprétation de l'attribut cisco_group_policy

Une politique de groupe peut être spécifiée par un attribut d'assertion SAML. Lorsqu'un attribut « cisco_group_policy » est reçu par le défense contre les menaces , la valeur correspondante est utilisée pour sélectionner la politique de groupe de connexion

Configurer l'autorisation SAML

Avant de commencer

Assurez-vous d'avoir configuré un serveur d'authentification unique comme DUO et d'avoir défini les paramètres de fournisseur d'identité et de fournisseur de services requis.

Pour en savoir plus, consultez Authentification de connexion unique Single Sign-On avec SAML 2.0, à la page 85.

Procédure

Étape 1 Configurez un objet serveur d'authentification unique s'il n'est pas déjà configuré.

a) Choisissez **Object** > **Object Management** > **AAA Server** > **Single Sign-on Server** (Objet > Gestion des objets > serveur AAA > Serveur de connexion unique).
b) Cliquez sur **Ajouter un serveur de connexion unique**
c) Saisissez les détails du serveur de connexion unique et cliquez sur **Save**(Enregistrer).

Pour en savoir plus, consultez Ajouter un serveur de connexion unique (SSO).

Étape 2 Configurez l'authentification SAML dans le profil de connexion VPN d'accès à distance.

a) Choisissez **Devices** > **Remote Access (accès à distance aux périphériques)** .
b) Cliquez sur **Edit** (Modifier) dans la politique VPN d'accès à distance pour laquelle vous souhaitez configurer l'autorisation SAML ou créer une nouvelle politique.
c) Modifiez le profil de connexion requis et sélectionnez **AAA**.

d) Sélectionnez l'objet serveur de connexion unique dans la liste déroulante **Authentication Server** (serveur d'authentification).
e) Enregistrez la configuration VPN d'accès à distance

Étape 3 Correspondance de critères SAML dans la politique DAP.

a) Choisissez **Devices (Périphériques)** > **Dynamic Access Policy (Politique d'accès dynamique)**.
b) Créez une nouvelle DAP ou modifiez une DAP existante.
c) Créer un enregistrement DAP on modifiez un enregistrement DAP existant.
d) Cliquez sur **AAA Criteria** > **SAML Criteria** > **Add SAML Criteria**.
e) Créez des critères SAML en fonction des assertions SAML retournées par le serveur SSO.

Étape 4 Déployez la configuration VPN d'accès à distance

Sujets connexes

Configurer les paramètres du profil de connexion, à la page 24
Objets politique de groupe Défense contre les menaces

Configurations avancées Secure Client (services client sécurisés)

Configurer les modules Secure Client (services client sécurisés) sur un Défense contre les menaces

Secure Client (services client sécurisés) peut s'intégrer à diverses solutions de sécurité des points terminaux de Cisco et offrir une sécurité améliorée à l'aide de différents modules Secure Client (services client sécurisés).

Vous pouvez utiliser la tête de réseau gérée défense contre les menaces pour distribuer et gérer les modules Secure Client (services client sécurisés) sur les points terminaux. Lorsqu'un utilisateur se connecte à défense contre les menaces , il télécharge et installe Secure Client (services client sécurisés) et les modules requis sur le point terminal.

Dans les versions 6.7 ou ultérieures, vous pouvez utiliser la tête de réseau défense contre les menaces , gérée par un centre de gestion, pour distribuer et gérer les modules Secure Client (services client sécurisés) sur les points terminaux. Ces modules s'intègrent ensuite à la solution de sécurité des points terminaux Cisco correspondante.

Dans les versions 6.4 à 6.6, vous pouvez activer ces modules et ces profils sur un défense contre les menaces à l'aide de FlexConfig. Pour en savoir plus, consultez Configurer les modules et profils AnyConnect à l'aide de FlexConfig.

Avantages

Si vous utilisez un défense contre les menaces pour distribuer et gérer les modules Secure Client (services client sécurisés) sur les points d'extrémité, vous pouvez facilement effectuer les tâches suivantes :

- Distribuer et gérer les modules et les profils Secure Client (services client sécurisés) sur chaque terminal.
- Mise à niveau Secure Client (services client sécurisés) sur chaque point terminal.

Types de modules Secure Client (services client sécurisés)

Activateur de Cisco Advanced Malware Protection

Utilisez ce module pour déployer Cisco Secure Endpoint, anciennement AMP pour Endpoints, sur les points terminaux. Le module transmet Cisco Secure Endpoint aux points terminaux à partir d'un serveur hébergé localement dans l'entreprise. Ce module fournit un agent de sécurité supplémentaire qui détecte les menaces potentielles de programmes malveillants sur le réseau, supprime ces menaces et protège l'entreprise.

Dans Cisco Secure Client 5.0, l'activateur AMP est uniquement destiné à macOS. Cisco Secure Client pour Windows s'intègre entièrement à Cisco Secure Endpoint.

ISE Posture

Utilisez ce module pour effectuer des vérifications de la posture des points terminaux concernant un antivirus, un anti logiciel-espion, le système d'exploitation, etc. à l'aide de Cisco Identity Services Engine (ISE) et évaluer la conformité des points terminaux. Cisco ISE fournit des politiques de contrôle d'accès et d'identité de nouvelle génération. ISE Posture effectue une évaluation côté client. Le client reçoit la politique d'exigences de posture de la tête de réseau, effectue la collecte des données de posture, compare les résultats à la politique et renvoie les résultats de l'évaluation à la tête de réseau.

Visibilité du réseau

Utilisez ce module pour surveiller l'utilisation des applications de point terminal à l'aide du module de visibilité du réseau. Vous pouvez découvrir d'éventuelles anomalies de comportement et prendre des décisions éclairées en matière de conception de réseau. Il améliore la capacité de l'administrateur de l'entreprise à effectuer la planification de la capacité et des services, l'audit, la conformité et l'analyse de sécurité. Vous pouvez partager les données d'utilisation avec les outils d'analyse NetFlow tels que Cisco Stealthwatch.

Sécurité itinérante Cisco Umbrella

Utilisez ce module pour une sécurité de couche DNS utilisant le service Cisco Umbrella Itinérance Security. Cisco Umbrella offre un filtrage de contenu, plusieurs politiques, des rapports robustes, une intégration Active Directory et bien plus encore.

sécurité Web

Utilisez ce module pour activer Cisco Web Security Appliance (WSA), alimenté par Cisco Talos. Ce module protège le terminal en bloquant les sites à risque et en analysant les sites inconnus avant d'autoriser les utilisateurs à y accéder. Il peut déployer la sécurité Web par l'intermédiaire du WSA sur site ou de Cisco Cloud Web Security en nuage. Ce module ne fait pas partie de l'ensemble AnyConnect de la version 4.5 et de Secure Client 5.0.

Gestionnaire d'accès réseau

Ce module fournit un réseau de couche 2 sécurisé et effectue l'authentification du périphérique pour accéder aux réseaux câblés et sans fil. Le gestionnaire d'accès réseau gère l'identité des utilisateurs et des périphériques, ainsi que les protocoles d'accès réseau requis pour un accès sécurisé.

Le gestionnaire d'accès du réseau n'est pas pris en charge sur macOS ou Linux.

Commencer avant la connexion

Le démarrage avant la connexion (SBL) permet aux utilisateurs d'établir leur connexion VPN avec l'infrastructure de l'entreprise avant de se connecter à Windows. Après l'installation du module SBL, vous devez activer SBL dans le profil VPN Secure Client (services client sécurisés) et l'ajouter à la politique de groupe VPN d'accès à distance.

DART

L'outil de dépistage et de rapport DART (Diagnostics and Reporting Tool) rassemble les journaux système et d'autres informations de dépistage pour dépanner les problèmes d'installation et de connexion d'AnyConnect. Vous pouvez envoyer ces données à Cisco TAC pour le dépannage.

Par défaut, DART n'est pas activé dans les nouvelles politiques de groupe de VPN d'accès à distance pour les versions 6.7 et ultérieures. Dans les versions 6.6 et antérieures, DART est activé par défaut.

Commentaires

Le module de Commentaires sur l'expérience client (CES) fournit des informations sur les fonctionnalités et les modules que vous utilisez et avez activés. Ces renseignements donnent un aperçu de l'expérience de l'utilisateur afin que Cisco puisse continuer à améliorer la qualité, la fiabilité, les performances et l'expérience utilisateur du Secure Client (services client sécurisés). Secure Client (services client sécurisés) ne télécharge pas le module de commentaires sur le point terminal. Les données de commentaires sont envoyées au serveur de commentaires Cisco.

Conditions préalables à la configuration des modules Secure Client (services client sécurisés)

- Configurez les produits associés selon le module que vous allez utiliser.
- Téléchargez les progiciels associés aux Secure Client (services client sécurisés) suivants à partir du centre de téléchargement de logiciels Cisco sur votre hôte local.
  - Ensemble de déploiement de tête de réseau Cisco Secure Client (services client sécurisés)pour les plateformes requises.

    Ce paquet est pour la tête de réseau et contient tous les modules Secure Client (services client sécurisés). Pour Windows, le nom de fichier est cisco-secure-client-win-5.0.03076-webdeploy-k9.pkg.
  - Éditeur de profils : créez des profils pour les modules qui nécessitent des profils.

    Secure Client (services client sécurisés) a besoin d'un profil Secure Client (services client sécurisés) pour certains modules. Un profil contient des configurations pour activer les modules et se connecter aux services de sécurité correspondants. L'éditeur de profils ne prend en charge que Windows.

    Le tableau suivant indique si les modules nécessitent un profil client :

Module Secure Client	Nécessite un profil client
Activateur de Cisco Advanced Malware Protection	Oui
ISE Posture	Oui
Gestionnaire d'accès réseau	Oui
Network Visibility Module	Oui

Module Secure Client	Nécessite un profil client
Module sécurisé d'itinérance Umbrella	Oui
Commentaires	Oui
sécurité Web	Oui
DART	Non
Commencer avant la connexion	Non

- Licence
  - Vous avez besoin de l'une des licences Secure Client suivantes : Secure Client Premier, Secure Client Advantage ou VPN client sécurisé uniquement
  - Votre licence centre de gestion Essentielle doit autoriser la fonctionnalité dont l'exportation est contrôlée.

    Choisissez **System > Licenses > Smart Licenses** (Système > Licences > Licences Smart) pour vérifier cette fonctionnalité dans le centre de gestion.

Directives pour la configuration des modules Secure Client (services client sécurisés)

- Tous les modules Secure Client (services client sécurisés) sont pris en charge par les versions 4.8 et ultérieures d'AnyConnect et de Secure Client 5.0.
- Plusieurs modules prennent en charge des profils avec différentes extensions de fichier. Le tableau suivant répertorie les modules et les extensions de fichier prises en charge pour leurs profils :

Tableau 8 : Extensions de fichier de profils prises en charge

Module	Extension de fichier
Activateur de Cisco Advanced Malware Protection	*.xml, *.asp
Commentaires	*.xml
ISE Posture	*.xml, *.isp
Gestionnaire d'accès réseau	*.xml, *.nsp
Visibilité du réseau	*.xml, *.nsp
Sécurité itinérante Cisco Umbrella	*.xml, *.json
sécurité Web	*.xml, *.wsp, *.wso

- Vous ne pouvez ajouter qu'une seule entrée par module client. Vous pouvez modifier ou supprimer une entrée pour un module.

- Si vous prévoyez utiliser les modules de posture ISE et de Network Access Manager sur un système d'exploitation Windows, vous devez installer Network Access Manager avant d'utiliser le module de posture ISE.
- Si vous activez le module de sécurité Umbrella itinérante, assurez-vous de désactiver l'option **Toujours envoyer les requêtes DNS sur le tunnel** sous la tunnelisation fractionnée dans la politique de groupe VPN.
- Si vous souhaitez utiliser SBL, vous devez l'activer dans le profil VPN Secure Client (services client sécurisés).

Installer les modules Secure Client (services client sécurisés) à l'aide d'un Défense contre les menaces

Avant de commencer

Assurez-vous d'avoir consulté les rubriques Conditions préalables à la configuration des modules Secure Client (services client sécurisés), à la page 92 et Directives pour la configuration des modules Secure Client (services client sécurisés), à la page 93.

Procédure

Étape 1 L'administrateur crée des profils, au besoin, pour les modules Secure Client (services client sécurisés) requis.

Étape 2 L'administrateur utilise centre de gestion pour :

a) Configurer les modules et ajouter les profils dans la politique de groupe VPN d'accès à distance.

b) Déployer la configuration sur le défense contre les menaces .

Étape 3 L'utilisateur utilise Secure Client (services client sécurisés) pour établir une connexion VPN avec défense contre les menaces .

Étape 4 Le défense contre les menaces authentifie l'utilisateur.

Étape 5 Le Secure Client (services client sécurisés) vérifie les mises à jour.

Étape 6 Le défense contre les menaces distribue les modules Secure Client (services client sécurisés) et les profils sur le point terminal.

Prochaine étape

Configurez une politique de groupe VPN d'accès à distance avec les modules Secure Client (services client sécurisés), à la page 94.

Configurez une politique de groupe VPN d'accès à distance avec les modules Secure Client (services client sécurisés)

Pour installer et mettre à jour les modules Secure Client (services client sécurisés) sur le point terminal en utilisant un défense contre les menaces géré par un centre de gestion, vous devez mettre à jour la politique de groupe du VPN d'accès à distance avec les configurations des modules Secure Client (services client sécurisés).

Avant de commencer

Assurez-vous d'avoir configuré une politique VPN d'accès à distance danscentre de gestion.

Procédure

Étape 1 Choisissez **Devices > Remote Access** (Périphériques > Accès à distance).

Étape 2 Sélectionnez une politique VPN d'accès à distance et cliquez sur **Edit** (Modifier).

Étape 3 Sélectionnez un profil de connexion et cliquez sur **Edit** (Modifier).

Étape 4 Cliquez sur **Edit Group POlicy** (Modifier la politique de groupe).

Étape 5 Cliquez sur l'onglet de **Secure Client**.

Étape 6 Cliquez sur **Client Modules** (Modules clients).

Étape 7 Cliquez +.

Étape 8 Choisissez une valeur dans la liste déroulante **Modules clients**.

Étape 9 Choisissez un profil pour le module dans la liste déroulante **Profil à télécharger** ou cliquez sur le signe plus + pour ajouter un profil.

Étape 10 Cochez la case **Enable module download** (activer le téléchargement de module) pour télécharger le module sur le point terminal.

Étape 11 Cliquez sur **Add** (ajouter).

Étape 12 Répétez les étapes 7 à 11 si vous souhaitez ajouter d'autres modules.

Étape 13 Cliquez sur **Save** (enregistrer).

Prochaine étape

1. Déployer la configuration sur défense contre les menaces
2. Lancez Secure Client (services client sécurisés), sélectionnez le profil VPN et connectez-vous au VPN. Secure Client (services client sécurisés) installe les modules configurés dessus.
3. Vérifiez la configuration. Pour en savoir plus, consultez Vérifier la configuration des modules Secure Client (services client sécurisés), à la page 95.

Vérifier la configuration des modules Secure Client (services client sécurisés)

Sur Défense contre les menaces

Utilisez les commandes suivantes sur le défense contre les menaces pour afficher les profils et la configuration des modules Secure Client (services client sécurisés) :

- **show disk0:** : affichez les profils et leur configuration.
- **show run webvpn** : affichez les détails des configurations de Secure Client.
- **show run group-policy <ravpn_group_policy_name>** : affichez les détails de la politique de groupe de VPN d'accès à distance pour Secure Client.
- **show vpn-sessiondb anyconnect** : affichez les détails des sessions VPN actives de Secure Client.

sur le point terminal

1. Utilisez la Secure Client (services client sécurisés) pour établir une connexion VPN avec défense contre les menaces .
2. Vérifiez si les modules configurés sont téléchargés et installés dans le cadre de Secure Client (services client sécurisés).
3. Vérifiez si les profils configurés, le cas échéant, sont disponibles aux emplacements documentés dans le document Emplacement des profils pour tous les systèmes d'exploitation.

Sur Centre de gestion

Vous pouvez surveiller les sessions actives du VPN d'accès à distance sur le centre de gestion à l'aide du tableau de bord du VPN d'accès à distance (**Présentation > VPN d'accès à distance**). Vous pouvez identifier rapidement les problèmes liés aux sessions utilisateur et atténuer les problèmes pour votre réseau et vos utilisateurs.

Configurer le VPN d'accès à distance basé sur les applications (VPN par application) sur les périphériques mobiles

Lorsque vous utilisez Secure Client (services client sécurisés) pour établir une connexion VPN à partir d'un appareil mobile, tout le trafic, y compris le trafic des applications personnelles, est acheminé par le VPN.

Pour les périphériques mobiles qui fonctionnent sous Android ou iOS, vous pouvez restreindre les applications qui utilisent le tunnel VPN. Ce VPN d'accès à distance basé sur les applications s'appelle Per App VPN (VPN par application). Pour utiliser Per App VPN, vous devez installer et configurer une application tierce Mobile Device Manager (MDM). Vous devez définir la liste des applications approuvées qui peuvent être utilisées sur le tunnel VPN dans le MDM. Vous pouvez activer le VPN par application sur la tête de réseau défense contre les menaces pour que votre MDM puisse appliquer vos politiques sur les périphériques mobiles.

Avantages

Avantages de la restriction du VPN d'accès à distance aux applications approuvées :

- Rendement : limite le trafic VPN sur le réseau d'entreprise et libère les ressources de la tête de réseau VPN.
- Protection : protège le tunnel VPN de l'entreprise contre les applications malveillantes non approuvées sur le périphérique mobile.

Conditions préalables et licence pour la configuration des tunnels VPN par application

Prérequis

- Installer et configurer un gestionnaire de périphériques mobiles (MDM) tiers

  Vous devez configurer les applications qui seront autorisées dans le VPN sur le MDM, et non sur le périphérique de tête défense contre les menaces .
- Téléchargez le sélecteur d'applications Cisco AnyConnect Enterprise depuis le centre de téléchargement de logiciels Cisco.

Vous avez besoin de cet outil pour définir la politique VPN par application.

Licence

- Secure Client Premier, ou Secure Client Advantage .
- La licence Essentielle doit permettre l'utilisation de fonctionnalités contrôlées par l'exportation.

  Pour vérifier cette fonctionnalité dans centre de gestion, choisissez **System > Licenses > Smart Licenses** (Système > Licences > Licences Smart).

Déterminer les ID d'application des applications mobiles

Avant de configurer la tête de réseau défense contre les menaces pour autoriser le VPN basé sur les applications à partir de périphériques mobiles, vous devez déterminer quelles applications doivent être autorisées dans le tunnel.

Nous vous recommandons fortement de configurer la politique par application dans le gestionnaire de périphérique mobile (MDM) sur le périphérique mobile de l'utilisateur. Cela simplifie la configuration de la tête de réseau. Si vous décidez de configurer la liste des applications autorisées sur la tête de réseau, vous devez déterminer les ID d'application pour chaque application sur chaque type de terminal.

L'ID de l'application, appelé ID de lot dans iOS, est un nom DNS inversé. Vous pouvez utiliser un astérisque comme caractère générique. Par exemple, *.* indique toutes les applications et com.cisco.* indique toutes les applications Cisco.

Pour déterminer les ID d'application :

- **Android** : accédez à Google Play dans un navigateur Web et sélectionnez la catégorie Apps. Cliquez (ou passez le curseur sur) une application que vous souhaitez autoriser, puis regardez l'URL. L'ID de l'application se trouve dans l'URL, dans le paramètre **id=**. Par exemple, l'URL suivante concerne Facebook Messenger, donc l'ID de l'application est com.facebook.orca.

  https://play.google.com/store/apps/details?id=com.facebook.orca

  Pour les applications qui ne sont pas disponibles sur Google Play, comme les vôtres, téléchargez une application de visualisation de nom de paquet pour extraire l'ID de l'application. Plusieurs de ces applications sont disponibles, l'une d'entre elles devrait fournir ce dont vous avez besoin, mais Cisco n'approuve aucune d'entre elles.

- **iOS** : Il n'y a aucun moyen simple d'obtenir l'ID d'offre groupée. Voici une façon de le déterminer :

  1. Utilisez un navigateur Web de poste de travail tel que Chrome pour rechercher le nom de l'application.
  2. Dans les résultats de la recherche, cherchez le lien pour télécharger l'application sur l'App Store d'Apple. Par exemple, Facebook Messager ressemblerait à :

     https://apps.apple.com/us/app/messenger/id454638411
  3. Copiez le numéro après la chaîne d' **id**. Dans cet exemple, **454638411**.
  4. Ouvrez une nouvelle fenêtre de navigateur et ajoutez le numéro à la fin de l'URL suivante :

     https://itunes.apple.com/lookup?id=

     Pour cet exemple : https://itunes.Apple.com/lookup?id=454638411
  5. Vous serez invité à télécharger un fichier texte, généralement nommé 1.txt. Téléchargez le fichier.

6. Ouvrez le fichier dans un éditeur de texte tel que Wordpad et recherchez le bundleid. Par exemple :

   "bundleId":"com.facebook.Messenger",

   Dans cet exemple, l'ID de lot est com.facebook.Messenger. Utilisez-le comme ID d'application.

Une fois que vous avez votre liste d'ID d'application, vous pouvez configurer la politique comme expliqué dans la section.

Configurer les tunnels VPN basés sur les applications

Après avoir installé et configuré votre logiciel MDM, vous pouvez activer le VPN par application sur le périphérique de tête de réseau défense contre les menaces . Une fois activé sur la tête de réseau, votre logiciel MDM contrôlera quelles applications sont acheminées par tunnellisation du VPN vers le réseau d'entreprise.

Avant de commencer

- Assurez-vous d'avoir une politique VPN d'accès à distance dans centre de gestion.
- Configurez le VPN par application à l'aide de MDM et inscrivez chaque périphérique sur le serveur MDM.
- Téléchargez le sélecteur d'applications Cisco AnyConnect Enterprise

Procédure

Étape 1 Utilisez le sélecteur d'application d'entreprise Cisco AnyConnect pour définir la politique VPN par application.

Nous vous recommandons de créer une politique **Tout autoriser** simple et de définir les applications autorisées dans le MDM. Cependant, vous pouvez spécifier une liste d'applications à autoriser et contrôler la liste à partir de la tête de réseau. Si vous souhaitez inclure des applications spécifiques, créez une règle distincte pour chaque application en utilisant un nom unique et l'ID d'application de l'application. Pour en savoir plus sur l'obtention des ID d'application, consultez Déterminer les ID d'application des applications mobiles.

Pour créer une politique **Tout autoriser** qui prend en charge les plateformes Android et iOS à l'aide du sélecteur d'applications d'entreprise AnyConnect :

a) Choisissez **Android** dans la liste déroulante comme type de plateforme et configurez les options suivantes :

- **Nom convivial** : saisissez un nom pour la politique. Par exemple, Tout_autoriser.
- **ID de l'application** : saisissez *.* pour correspondre à toutes les applications possibles.
- Laissez les autres options inchangées.

b) Choisissez **iOS** dans la liste déroulante comme type de plateforme et configurez les options suivantes :

- **Nom convivial** : saisissez un nom pour la politique. Par exemple, Tout_autoriser.
- **ID de l'application** : saisissez *.* pour correspondre à toutes les applications possibles.
- Laissez les autres options inchangées.

c) Choisissez **Politique > Afficher la politique** pour obtenir la chaîne codée en base64 pour la politique.

Cette chaîne contient un fichier XML chiffré qui permet à défense contre les menaces de voir les politiques. Copiez cette valeur. Vous avez besoin de cette chaîne lorsque vous configurez le VPN par application sur défense contre les menaces .

Étape 2 Utilisez les centre de gestion pour activer Par application sur le périphérique de tête de réseau défense contre les menaces .

a) Choisissez **Devices > Remote Access** (Périphériques > Accès à distance).
b) Sélectionnez une politique VPN d'accès à distance et cliquez sur **Edit** (Modifier).
c) Sélectionnez un profil de connexion et cliquez sur **Edit** (Modifier).
d) Cliquez sur **Edit Group POlicy** (Modifier la politique de groupe).
e) Cliquez sur l'onglet de **Secure Client**.
f) Cliquez sur **Attributs personnalisés**, puis sur **+**.
g) Choisissez **VPN par application** dans la liste déroulante **Attribute** de **Secure Client** .
h) Choisissez un objet dans la liste déroulante d'**objets d'attribut personnalisé** ou cliquez sur le signe plus **+** pour ajouter un objet.

   Lorsque vous ajoutez un nouvel objet d'attribut personnalisé pour le VPN par application, saisissez le nom, la description et la chaîne de politique codée en base64 à partir du sélecteur d'applications Cisco AnyConnect Enterprise.

i) Cliquez sur **Save** (enregistrer).
j) Cliquez sur **Add** (ajouter), puis sur **Save**(Enregistrer).

Étape 3 Déployez vos modifications sur centre de gestion.

Prochaine étape

1. Lancez Secure Client (services client sécurisés), sélectionnez le profil VPN et connectez-vous au VPN.
2. Vérifiez la configuration. Pour en savoir plus, consultez Vérifier la configuration par application, à la page 99.

Vérifier la configuration par application

Sur Défense contre les menaces

Utilisez les commandes suivantes sur le défense contre les menaces pour afficher la configuration par application :

- **show run webvpn**
- **show run group-policy <ravpn_group_policy_name>**
- **show run anyconnect-custom-data**

sur le point terminal

Une fois que le point terminal a établi une connexion VPN avec défense contre les menaces :

1. Cliquez sur l'icône **Statistics** (Statistiques) dans le champ Secure Client (services client sécurisés).
2. **Le mode de tunnel** sera Tunnel d'application » au lieu de « Tunnel tout le trafic ».

3. **Applications tunnelisées** répertorie les applications que vous avez activées pour la tunnellisation dans le gestionnaire de périphérique mobile MDM.

Exemples de VPN d'accès à distance

Limiter la bande passante Secure Client par utilisateur

Cette section fournit des instructions pour limiter la bande passante maximale utilisée par les utilisateurs du VPN lorsqu'ils se connectent à l'aide de la passerelle d'accès VPN à distance Secure Client (services client sécurisés) à Cisco Secure Firewall Threat Defense. Vous pouvez limiter la bande passante maximale en utilisant une politique de qualité de service (QoS) dans défense contre les menaces , pour éviter qu'un seul utilisateur ou groupe d'utilisateurs ne s'accapare la totalité de la ressource. Cette configuration vous permet de donner la priorité au trafic critique, d'éviter l'utilisation de la bande passante et de gérer le réseau. Lorsque le trafic dépasse le débit maximal, le défense contre les menaces abandonne le trafic excédentaire.

Étape	Faire ceci	Plus d'informations
1	Créer et configurer un domaine	Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine
2	Créez une politique QoS et une règle QoS pour l'utilisateur ou le groupe disponible dans le domaine nouvellement créé.	• Consultez Création d'une politique de qualité de service (QoS) pour créer une politique de QoS. • Consultez Configuration des règles QoS pour créer une règle de QoS.
3	Configurez la politique VPN d'accès à distance et sélectionnez le domaine nouvellement créé pour l'authentification de l'utilisateur.	Créer une nouvelle politique VPN d'accès à distance, à la page 14
4	Déployez la politique VPN d'accès à distance.	Déployer les modifications de configuration

Utiliser l'identité du VPN pour les règles de contrôle d'accès basées sur l'identifiant de l'utilisateur

Étape	Faire ceci	Plus d'informations
1	Créer et configurer un domaine	Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine.
2	Créez une politique d'identité et ajoutez une règle d'identité.	• Consultez Créer une politique d'identité pour créer une politique d'identité. • Consultez Créer une règle d'identité pour créer une règle d'identité.

Étape	Faire ceci	Plus d'informations
3	Associez la politique d'identité à une politique de contrôle d'accès.	Association d'autres politiques au contrôle d'accès
4	Configurez la politique VPN d'accès à distance et sélectionnez le domaine nouvellement créé pour l'authentification de l'utilisateur.	Créer une nouvelle politique VPN d'accès à distance, à la page 14
5	Déployez la politique VPN d'accès à distance.	Déployer les modifications de configuration

Configurer l'authentification par certificats multiples Défense contre les menaces

Authentification basée sur plusieurs certificats

L'authentification basée sur plusieurs certificats permet au défense contre les menaces de valider le certificat de la machine ou du périphérique. Plusieurs certificats peuvent être activés pour l'authentification par certificat dans le profil de connexion VPN d'accès à distance. Elle peut être combinée à l'authentification AAA. L'option plusieurs certificats dans le profil de connexion VPN d'accès à distance permet l'authentification de certificats de la machine et de l'utilisateur au moyen de certificats. Cela garantit que le périphérique est un appareil émis par l'entreprise, en plus d'authentifier le certificat d'identité de l'utilisateur pour permettre l'accès de VPN d'accès à distance. L'administrateur peut choisir si le nom d'utilisateur pour la session doit provenir du certificat de la machine ou du certificat utilisateur.

Lorsque l'authentification basée sur les certificats multiples est configurée, deux certificats sont obtenus à partir du client VPN :

- **First Certificate** (premier certificat) : certificat de machine pour authentifier le point terminal
- **Second Certificat** : Certificat utilisateur pour authentifier l'utilisateur VPN.

Pour de plus amples renseignements sur les certificats défense contre les menaces , voir Gestion des certificats Défense contre les menaces.

Restrictions

- L'authentification par certificats multiples limite actuellement le nombre de certificats à deux.
- Secure Client prend en charge uniquement les certificats codés en RAS.
- Seuls les certificats basés sur SHA256, SHA384 et SHA512 sont pris en charge lors de l'authentification agrégée Secure Client.
- L'authentification de certificat ne peut pas être combinée à l'authentification SAML.

Préremplir le nom d'utilisateur à partir du certificat

L'option Pré-remplir le nom d'utilisateur permet à un champ des certificats d'être analysé et utilisé pour l'authentification AAA ultérieure (principale et secondaire). Lorsque deux certificats sont utilisés pour

l'authentification, l'administrateur peut choisir le certificat à partir duquel le nom d'utilisateur doit être dérivé pour la fonctionnalité de préremplissage. Par défaut, le nom d'utilisateur pour le préremplissage est extrait du certificat d'utilisateur (deuxième certificat reçu de Secure Client). Le nom d'utilisateur prérempli est utilisé comme nom d'utilisateur de session VPN lorsque la méthode d'authentification par certificat uniquement est activée. Lorsque l'authentification AAA et par certificat est activée, le nom d'utilisateur de session VPN sera basé sur l'option de pré-remplissage.

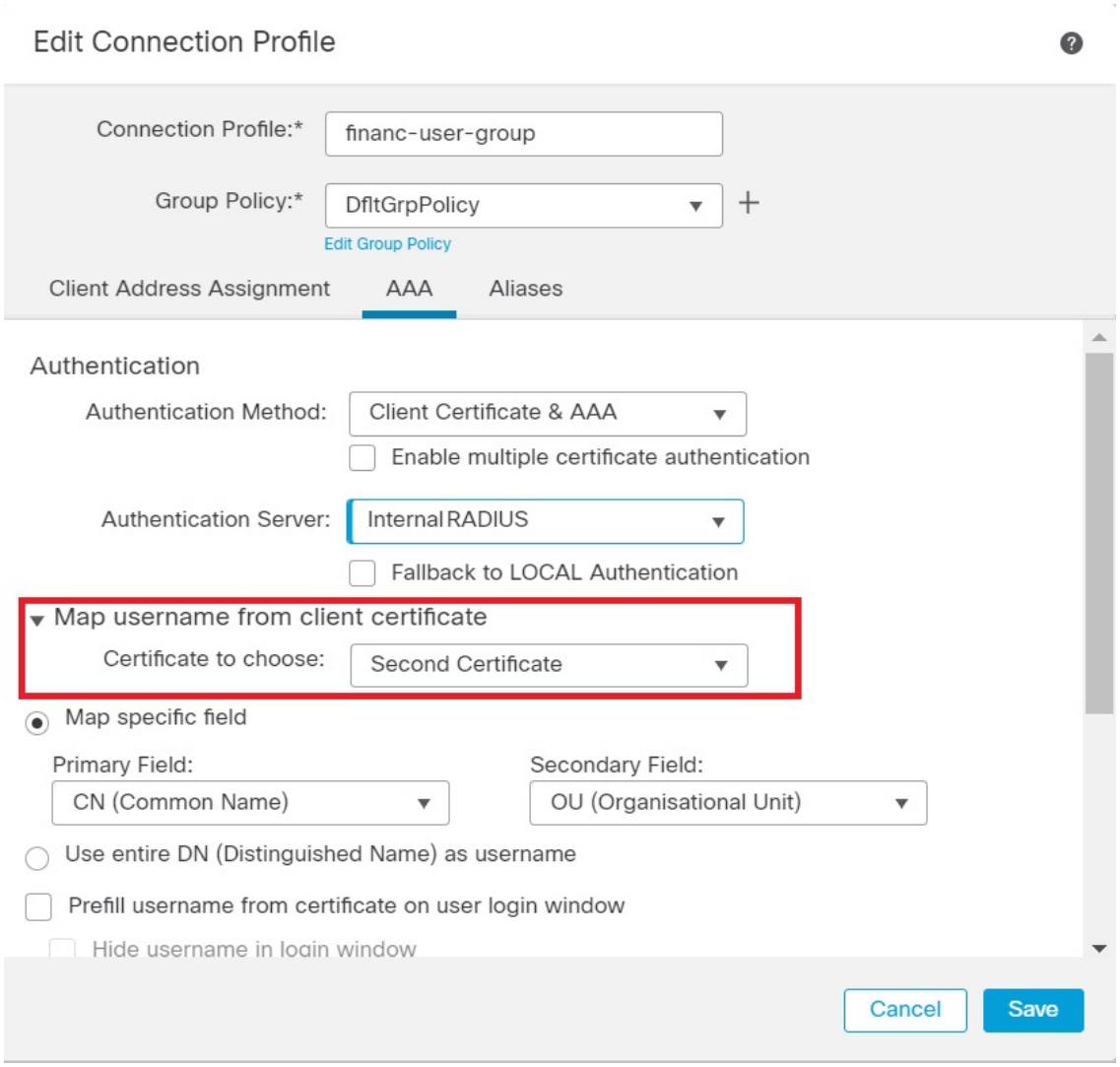
Configurer l'authentification de plusieurs certificats pour le VPN d'accès à distance

1. Sur l'interface Web Cisco Secure Firewall Management Center, choisissez **Devices** (périphériques) > **VPN** > **Remote Access** (accès à distance).
2. Modifiez une politique d'accès à distance existante, ou créez-en une nouvelle et modifiez-la.

   Consultez Créer une nouvelle politique VPN d'accès à distance, à la page 14.
3. Sélectionnez le profil de connexion pour configurer l'authentification à certificats multiples, puis cliquez sur **Edit** (Modifier).

   Consultez Configurer les paramètres du profil de connexion, à la page 24.
4. Choisissez **AAA**, puis sélectionnez une **méthode d'authentification** :

Illustration 3 :



- **Client Certificate Only** : l'utilisateur est authentifié à l'aide d'un certificat client. Le certificat client doit être configuré sur les points terminaux clients VPN. Par défaut, le nom d'utilisateur est dérivé des champs de certificat client CN et OU respectivement. Si le nom d'utilisateur est spécifié dans d'autres champs du certificat client, utilisez les champs « principal » et « secondaire » pour mapper les champs appropriés.
- **Certificat client et AAA** : l'utilisateur est authentifié à l'aide des deux types d'authentification, AAA et certificat client.

5. Sélectionnez **Activer l'authentification de plusieurs certificats**.
6. Sélectionnez **Mapper le nom d'utilisateur du certificat client** et sélectionnez un certificat dans la liste déroulante **Choix du certificat** pour choisir le nom d'utilisateur de la session VPN dans le certificat du périphérique ou l'utilisateur.
   - **First Certificate** (premier certificat) : mappez le nom d'utilisateur du certificat de la machine.

- **Second Certificate**(second certificat) : mappez le nom d'utilisateur du certificat d'utilisateur pour authentifier l'utilisateur VPN.

7. Configurez les paramètres de profil de connexion requis et les paramètres VPN d'accès à distance.
8. Enregistrez le profil de connexion et la politique VPN d'accès à distance. Déployez le VPN d'accès à distance sur défense contre les menaces .

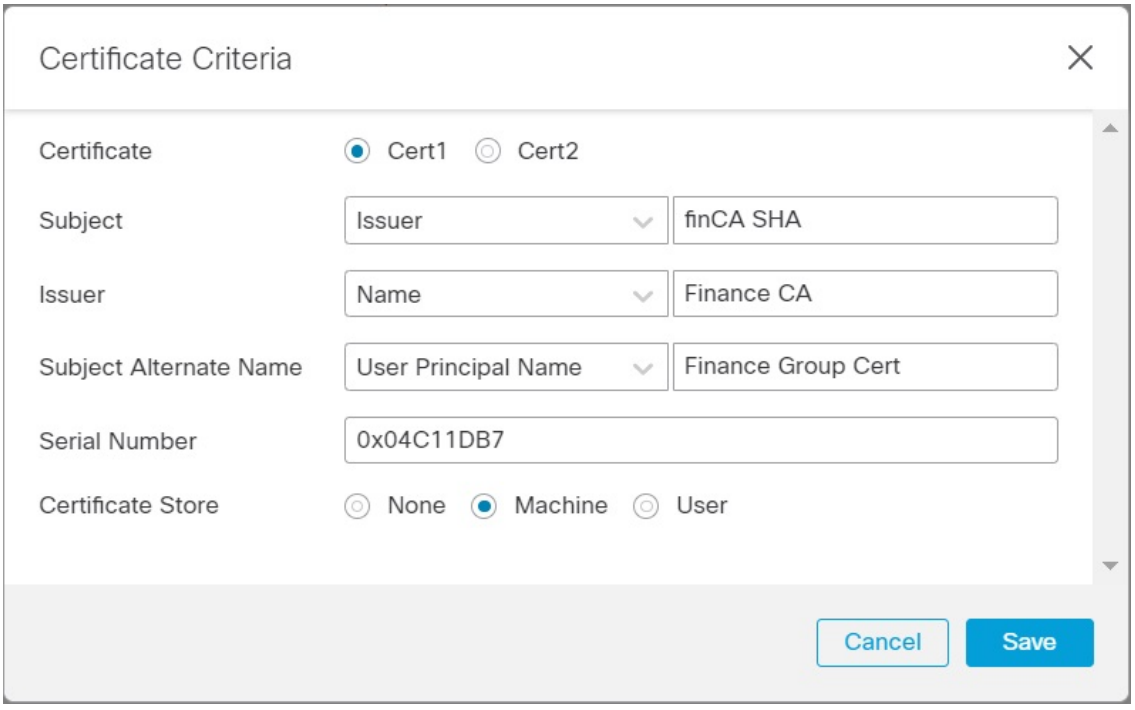
Pour en savoir plus sur les paramètres du VPN d'accès à distance AAA, consultez Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 26.

Configuration du certificat dans DAP

Vous pouvez également configurer les attributs de critères de certificat dans un enregistrement DAP. Les certificats d'utilisateur et de machine reçus du client VPN lors de l'authentification plusieurs certificats sont chargés dans la politique d'accès dynamique (DAP) pour permettre la configuration des politiques en fonction du champ du certificat. Vous pouvez prendre des décisions politiques en fonction des champs d'un certificat utilisés pour authentifier cette tentative de connexion.

1. Choisissez **Devices (Périphériques)** > **Dynamic Access Policy (Politique d'accès dynamique)**.
2. Modifiez une politique DAP existante ou créez-en une nouvelle, puis modifiez la politique.
3. Choisissez un enregistrement DAP existant ou créez-en un nouveau, puis modifiez l'enregistrement.
4. Sélectionnez**Critères de point terminal** > **Certificat**.
5. Sélectionnez les critères de correspondance **All** (Tous) ou **Any** (N'importe lequel).
6. Cliquez sur **Add** (Ajouter) pour ajouter des attributs de certificat.

Illustration 4 :



7. Sélectionnez le certificat, **Cert1** ou **Cert2**.
8. Sélectionnez l' **Objet** et précisez la valeur d'objet du certificat.
9. Sélectionnez l'**émetteur** et précisez le nom de l'émetteur du certificat.
10. Sélectionnez **Autre nom du sujet** et précisez l'autre nom du sujet.
11. Précisez le **numéro de série**.
12. Sélectionnez le **Magasin de certificats** : Aucun, Machine ou Utilisateur.

    Cette option ajoute une condition pour vérifier le magasin à partir duquel le certificat est extrait sur le point terminal.
13. Cliquez sur **Save** (Enregistrer) pour configurer les paramètres des critères de certificat.

    Configurez les paramètres d'enregistrement DAP requis, puis associez le DAP au VPN d'accès à distance.

Pour en savoir plus sur DAP, consultez Politiques d'accès dynamique.

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.