

Inspection des protocoles Internet de base

Les rubriques suivantes expliquent l'inspection des applications pour les protocoles Internet de base. Pour en savoir plus sur la raison pour laquelle vous devez utiliser l'inspection pour certains protocoles et sur les méthodes globales d'application de l'inspection, consultez Premiers pas avec l'inspection du protocole de la couche application.

- Inspection DCERPC, à la page 1
- Inspection DNS, à la page 4
- Inspection FTP, à la page 8
- Inspection HTTP, à la page 13
- Inspection ICMP, à la page 17
- Inspection des erreurs ICMP, à la page 18
- Inspection ILS, à la page 18
- Inspection de la messagerie instantanée, à la page 19
- Inspection des options IP, à la page 21
- Inspection IPsec Pass Through, à la page 23
- Inspection IPv6, à la page 24
- Inspection NetBIOS, à la page 26
- Inspection PPTP, à la page 27
- Inspection RSH, à la page 27
- Inspection SMTP et SMTP étendue, à la page 28
- Inspection SNMP, à la page 32
- Inspection SQL*Net, à la page 33
- Inspection Sun RPC, à la page 33
- Inspection TFTP, à la page 35
- Inspection XDMCP, à la page 35
- Inspection VXLAN, à la page 36
- Historique de l'inspection du protocole Internet de base, à la page 36

Inspection DCERPC

L'inspection DCERPC n'est pas activée dans la politique d'inspection par défaut, vous devez donc l'activer si vous avez besoin de cette inspection. Vous pouvez simplement modifier la politique d'inspection globale par défaut pour ajouter l'inspection DCERPC. Vous pouvez également créer une nouvelle politique de service comme vous le souhaitez, par exemple, une politique spécifique à l'interface.

Les sections suivantes décrivent le moteur d'inspection DCERPC.

Présentation de DCERPC

L'appel de procédure à distance de Microsoft (MSRPC), basé sur DCERPC, est un protocole très utilisé par les applications client et serveur distribuées de Microsoft qui permet aux clients logiciels d'exécuter des programmes sur un serveur à distance.

Cela implique généralement qu'un client interroge un serveur appelé mappeur de terminaux à l'écoute sur un numéro de port bien connu pour obtenir les informations réseau allouées dynamiquement d'un service requis. Le client établit ensuite une connexion secondaire avec l'instance de serveur qui fournit le service. Le périphérique de sécurité autorise le numéro de port et l'adresse réseau appropriés et applique également la NAT, le cas échéant, pour la connexion secondaire.

Le moteur d'inspection DCERPC inspecte la communication TCP native entre l'EPM et le client sur le port TCP 135 bien connu. Les opérations de mappage et de recherche d'EPM sont prises en charge pour les clients. Le client et le serveur peuvent se trouver dans n'importe quelle zone de sécurité. L'adresse IP du serveur intégré et le numéro de port sont reçus à partir des messages de réponse EPM applicables. Étant donné qu'un client peut tenter plusieurs connexions au port de serveur renvoyé par EPM, l'utilisation multiple de passages est autorisée, avec des délais d'expiration configurables.

L'inspection DCE prend en charge les identifiants universels uniques (UUID) et les messages suivants :

- UUID du mappeur de terminal (EPM). Tous les messages EPM sont pris en charge.
- UUID ISystemMapper (non EPM). Les messages pris en charge sont les suivants :
  - RemoteCreateInstance opnum4
  - RemoteGetClassObject opnum3
- UUID d'OxidResolver (non EPM). Le message pris en charge est :
  - ServerAlive2 opnum5
- Tout message qui ne contient pas d'adresse IP ou d'informations de port, car ces messages ne nécessitent pas d'inspection.

Configurer une liste des politiques d'inspection DCERPC

Pour spécifier des paramètres d'inspection DCERPC supplémentaires, créez une liste des politiques d'inspection DCERPC. Vous pouvez ensuite appliquer la liste des politiques d'inspection lorsque vous activez l'inspection DCERPC.

Lors de la définition des critères de correspondance du trafic, vous pouvez soit créer une carte de trafic, soit inclure les instructions de correspondance directement dans la liste des politiques. La différence entre la création d'une carte de trafic et la définition de la correspondance de trafic directement dans la liste des politiques d'inspection est que vous pouvez réutiliser les cartes de trafic. La procédure suivante couvre les listes des politiques d'inspection, mais explique également les critères de correspondance de trafic disponibles dans la carte de trafic. Pour créer une carte de trafic, sélectionnez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Class Maps (Cartes de trafic)** > **DCERPC (DCERPC**).

Astuces Vous pouvez configurer des listes d'inspection lors de la création de politiques de service, en plus de la procédure expliquée ci-dessous. Le contenu de la liste est le même, quelle que soit la façon dont vous la créez.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **DCERPC**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste pour afficher son contenu. Vous pouvez modifier le niveau de sécurité directement ou cliquer sur **Customize** (Personnaliser) pour modifier la liste. Le reste de la procédure suppose que vous personnalisez ou ajoutez une liste.

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de l'édition d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Dans l'affichage **Security Level** (Niveau de sécurité) de la boîte de dialogue DCERPC Inspect Map (Liste d'inspection DCERPC), sélectionnez le niveau qui correspond le mieux à la configuration souhaitée.

Si l'un des niveaux prédéfinis correspond à vos exigences, vous avez maintenant terminé. Cliquez simplement sur **OK**, ignorez le reste de cette procédure et utilisez la liste dans une règle de politique de service pour l'inspection DCERPC.

Si vous devez personnaliser davantage les paramètres, cliquez sur **Details** (Détails) et poursuivez la procédure.

Astuces
Le bouton **UUID Filtering** (filtrage UUID) est un raccourci pour configurer le filtrage des messages, qui est expliqué plus loin dans cette procédure.

Étape 5 Configurez les options souhaitées.

- **Pinhole Timeout** (Délai d'expiration du passage) : définit le délai d'expiration du passage. Comme un client peut utiliser les informations de serveur renvoyées par le mappeur de point de terminaison pour plusieurs connexions, la valeur du délai d'expiration est configurable en fonction de l'environnement de l'application client. La plage est comprise entre 0:0:1 et 1193:0:0.
- **Enforce endpoint-mapper service** (Appliquer le service de mappage de point de terminaison) : indique s'il faut appliquer le service de mappage de point de terminaison lors de la liaison afin que seul le trafic de service soit traité.
- **Enable endpoint-mapper service lookup** (Activer la recherche du service de mappage de point de terminaison) : indique s'il faut activer l'opération de recherche du service de mappage de point de terminaison. Vous pouvez également appliquer un délai d'expiration pour la recherche de service. Si vous ne configurez pas de délai d'expiration, le pinhole timeout est utilisé.

Étape 6 (Facultatif) Cliquez sur l'onglet **Inspections** et définissez les actions à entreprendre pour des types de messages particuliers.

Vous pouvez définir les critères de correspondance du trafic en fonction des cartes de trafic DCERPC, en configurant les correspondances directement dans la liste d'inspection, ou les deux.

a) Effectuez l'une des actions suivantes :
   - Cliquez sur **Add** (Ajouter) pour ajouter un nouveau critère.
   - Sélectionnez un critère existant et cliquez sur **Edit** (Modifier).

b) Choisissez **Single Match** (Correspondance unique) pour définir le critère directement, ou **Multiple Match** (Correspondance multiple), auquel cas vous sélectionnez la carte de trafic DCERPC qui définit les critères.
c) Si vous définissez le critère ici, choisissez le type de correspondance : **Match** (Correspondance) (le trafic doit correspondre au critère) ou **No Match** (Aucune correspondance) (le trafic ne doit pas correspondre au critère). Ensuite, sélectionnez l'UUID souhaité :
   - **ms-rpc-epm**: correspond aux messages EPM Microsoft RPC.
   - **ms-rpc-isystemactivator**: correspond aux messages ISystemMapper.
   - **ms-rpc-oxidresolver**: correspond aux messages OxidResolver.

d) Choisissez de réinitialiser ou de journaliser la connexion avec **Reset** (Réinitialiser) ou **Log** (Journaliser). Vous pouvez également activer la journalisation si vous choisissez de réinitialiser la connexion. La réinitialisation de la connexion abandonne le paquet, ferme la connexion et envoie une réinitialisation TCP au serveur ou au client.
e) Cliquez sur **OK** pour ajouter le critère. Répétez le processus au besoin.

Étape 7 Cliquez sur **OK**.

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection DCERPC.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application.

Inspection DNS

L'inspection DNS est activée par défaut. Vous ne devez le configurer que si vous souhaitez un traitement autre que celui par défaut. Les sections suivantes décrivent l'inspection des applications DNS.

Valeurs par défaut pour l'inspection DNS

L'inspection DNS est activée par défaut, à l'aide de la carte de trafic d'inspection preset_dns_map :

- La longueur maximale du message DNS est de 512 octets.
- L'inspection DNS sur TCP est désactivée.
- La longueur maximale du message DNS du client est automatiquement définie pour correspondre à l'enregistrement de ressource.

- La protection DNS est activée, de sorte que l'ASA supprime la session DNS associée à une requête DNS dès que la réponse DNS est transmise par l'ASA. L'ASA surveille également l'échange de messages pour s'assurer que l'ID de la réponse DNS correspond à l'ID de la requête DNS.
- La traduction de l'enregistrement DNS en fonction de la configuration NAT est activée.
- L'application du protocole est activée, ce qui permet la vérification du format du message DNS, y compris une longueur de nom de domaine d'au plus 255 caractères, une longueur d'étiquette de 63 caractères, la compression et la vérification des pointeurs en boucle.

Remarque Une utilisation élevée du processeur est susceptible de se produire dans Cisco ASA lorsqu'un grand nombre de paquets est inspecté par seconde. À mesure que le nombre de paquets traités augmente, en particulier lorsque le périphérique approche de son débit ou de sa capacité de connexion maximum, l'utilisation du processeur augmente également. En effet, l'ASA doit effectuer plus d'opérations par seconde, ce qui augmente la consommation des ressources du processeur.

Configurer la liste des politiques d'inspection DNS

Vous pouvez créer une liste des politiques d'inspection DNS pour personnaliser les actions d'inspection DNS si le comportement d'inspection par défaut n'est pas suffisant pour votre réseau.

Vous pouvez éventuellement créer une carte de trafic d'inspection DNS pour définir la classe de trafic pour l'inspection DNS. L'autre option consiste à définir les classes de trafic directement dans la liste des politiques d'inspection DNS. La différence entre la création d'une carte de trafic et la définition de la correspondance de trafic directement dans la liste d'inspection est que vous pouvez créer des critères de correspondance plus complexes et que vous pouvez réutiliser les cartes de trafic. Bien que cette procédure explique les listes d'inspection, les critères de correspondance utilisés dans les cartes de trafics sont les mêmes que ceux expliqués à l'étape relative à l'onglet **Inspection**. Vous pouvez configurer les cartes de trafics DNS en sélectionnant **Configuration** > **Firewall** > **Objects** > **Class Maps (Cartes de trafic)** > **DNS**, ou en les créant lors de la configuration de la liste d'inspection.

Astuces Vous pouvez configurer des listes d'inspection lors de la création de politiques de service, en plus de la procédure expliquée ci-dessous. Le contenu de la liste est le même, quelle que soit la façon dont vous la créez.

Avant de commencer

Certaines options de correspondance de trafic utilisent des expressions régulières à des fins de correspondance. Si vous avez l'intention d'utiliser l'une de ces techniques, créez d'abord l'expression régulière ou la carte de trafic d'expressions régulières.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Cartes d'inspection)** > **DNS** .

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste pour afficher son contenu. Vous pouvez modifier le niveau de sécurité directement ou cliquer sur **Customize** (Personnaliser) pour modifier la liste. Le reste de la procédure suppose que vous personnalisez ou ajoutez une liste.

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de la modification d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Dans l'affichage **Security Level** (Niveau de sécurité) de la boîte de dialogue DNS Inspect Map (Liste d'inspection DNS), sélectionnez le niveau qui correspond le mieux à la configuration souhaitée. Le niveau par défaut est Low (Bas).

Si l'un des niveaux prédéfinis correspond à vos exigences, vous avez maintenant terminé. Cliquez simplement sur **OK**, ignorez le reste de cette procédure et utilisez la liste dans une règle de politique de service pour l'inspection DNS.

Si vous devez personnaliser davantage les paramètres, cliquez sur **Details** (Détails) et poursuivez la procédure.

Étape 5 Cliquez sur l'onglet **Conformité du protocole** et choisissez les options souhaitées :

- **Enable DNS guard function (Activer la fonction de protection DNS)** : à l'aide de DNS Guard, l'ASA supprime la session DNS associée à une requête DNS dès que la réponse DNS est transmise par l'ASA. L'ASA surveille également l'échange de messages pour s'assurer que l'ID de la réponse DNS correspond à l'ID de la requête DNS.
- **Enable NAT re-write function** (Activer la fonction de réécriture de la NAT) : traduit l'enregistrement DNS en fonction de la configuration NAT.
- **Enable protocol enforcement** (Activer l'application du protocole) : active la vérification du format du message DNS, y compris la longueur du nom de domaine d'au plus 255 caractères, la longueur d'étiquette de 63 caractères, la compression et la vérification des pointeurs en boucle.
- **Randomiser l'identifiant DNS pour la requête DNS**.
- **Activer l'inspection TCP** : active l'inspection du trafic DNS sur TCP. Assurez-vous que le trafic DNS/TCP du port 53 fait partie de la carte de trafic à laquelle vous appliquez l'inspection DNS. La carte de trafic d'inspection par défaut comprend TCP/53.
- **Enforce TSIG resource record to be present in DNS message** (Appliquer la présence de l'enregistrement de ressource TSIG dans le message DNS) : vous pouvez abandonner ou journaliser les paquets non conformes, et éventuellement journaliser les paquets abandonnés.

Étape 6 Cliquez sur l'onglet **Filtering** (Filtrage) et choisissez les options souhaitées.

- Paramètres globaux : choisissez s'il faut abandonner les paquets qui dépassent la longueur maximale spécifiée, qu'ils proviennent du client ou du serveur, de 512 à 65535 octets.
- Paramètres du serveur : **abandon des paquets qui dépassent la longueur maximale spécifiée** et **abandon des paquets envoyés au serveur qui dépassent la longueur indiquée par le RR** : définit la longueur maximale du message DNS du serveur, de 512 à 65 535 octets, ou définit la longueur maximale à la valeur dans l'enregistrement de ressource. Si vous activez les deux paramètres, la valeur la plus basse est utilisée.

- Paramètres du client : **abandon des paquets qui dépassent la longueur maximale spécifiée** et **abandon des paquets envoyés au serveur qui dépassent la longueur indiquée par le RR** : définit la longueur maximale du message DNS du client, de 512 à 65 535 octets, ou définit la longueur maximale à la valeur dans l'enregistrement de ressource. Si vous activez les deux paramètres, la valeur la plus basse est utilisée.

Étape 7 Cliquez sur l'onglet **Mismatch Rate** (Taux de non-concordance) et choisissez d'activer la journalisation lorsque le taux de non-concordance de l'ID DNS dépasse le seuil spécifié. Par exemple, vous pouvez définir un seuil de 30 incompatibilités par 3 secondes.

Étape 8 Cliquez sur l'onglet **Inspections** et définissez les inspections spécifiques que vous souhaitez mettre en œuvre en fonction des caractéristiques du trafic.

Vous pouvez définir les critères de correspondance du trafic en fonction des cartes de trafic DNS, en configurant les correspondances directement dans la liste d'inspection, ou les deux.

a) Effectuez l'une des actions suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter un nouveau critère.
- Sélectionnez un critère existant et cliquez sur **Edit** (Modifier).

b) Choisissez **Single Match** (Correspondance unique) pour définir le critère directement, ou **Multiple Match** (Correspondance multiple), auquel cas vous sélectionnez la carte de trafic DNS qui définit les critères.

c) Si vous définissez le critère ici, choisissez le type de correspondance : **Match** (Correspondance) (le trafic doit correspondre au critère) ou **No Match** (Aucune correspondance) (le trafic ne doit pas correspondre au critère). Par exemple, si No Match est sélectionné sur la chaîne « example.com », tout trafic contenant « example.com » est exclu de la carte de trafic. Configurez ensuite le critère comme suit :

- Indicateur d'en-tête : sélectionnez si l'indicateur doit être égal ou contenir la valeur spécifiée, puis sélectionnez le nom de l'indicateur d'en-tête ou saisissez la valeur hexadécimale de l'en-tête (0x0 à 0xfff). Si vous sélectionnez plusieurs valeurs d'en-tête, « Égal » nécessite la présence de tous les indicateurs et « Contient » que l'un des indicateurs est présent, dans le paquet. Les noms d'indicateurs d'en-tête sont **AA** (réponse faisant autorité), **QR** (requête), **RA** (récursivité disponible), **RD** (récursivité souhaitée), **TC** (troncage).
- Type : nom ou valeur du champ Type de DNS dans le paquet. Les noms des champs sont **A** (adresse IPv4), **AXFR** (transfert de zone complet), **CNAME** (nom canonique), **IXFR** (transfert de zone supplémentaire), **NS** (serveur de nom faisant autorité), **SOA** (démarrage d'une zone d'autorité) ou **TSIG** (signature de transaction). Les valeurs sont des nombres quelconques dans le champ Type de DNS de 0 à 65535 : saisissez une valeur spécifique ou une plage de valeurs.
- Classe : nom ou valeur du champ Classe DNS dans le paquet. Internet est le seul nom de champ possible. Les valeurs sont des nombres quelconques dans le champ carte DNS de 0 à 65 535 : saisissez une valeur spécifique ou une plage de valeurs.
- Question : la partie question d'un message DNS.
- Enregistrement de ressource : enregistrement de la ressource DNS. Choisissez si vous souhaitez faire correspondre la section de l'enregistrement de ressource supplémentaire, de réponse ou d'autorité.

d) Choisissez l'action principale à effectuer pour le trafic correspondant : abandonner le paquet, abandonner la connexion, masquer (pour les correspondances d'indicateur d'en-tête uniquement) ou aucune.

e) Choisissez d'activer ou de désactiver la journalisation. Vous devez désactiver la journalisation si vous souhaitez appliquer TSIG.

f) Choisissez s'il faut appliquer la présence d'un enregistrement de ressource TSIG. Vous pouvez abandonner le paquet, le journaliser, ou l'abandonner et le journaliser. Généralement, vous devez sélectionner **Primary Action (Action principale) : None** (Aucun) et **Log (Journal) : Disable** (Désactiver) pour appliquer TSIG. Cependant, pour les correspondances d'indicateurs d'en-tête, vous pouvez appliquer TSIG avec l'action principale de masque.

g) Cliquez sur **OK** pour ajouter l'inspection. Répétez le processus au besoin.

Étape 9 Cliquez sur l'onglet **Cisco Umbrella Connections (connexions Cisco Umbrella)** et activez la connexion à Cisco Umbrella dans le nuage.

Les options de cet onglet ne fonctionnent que si vous configurez la connexion Cisco Umbrella sur la page **Configuration** > **Firewall** > **(Pare-feu)** > **Objects** > **(Objets)** > **Umbrella**. Vous devez ensuite configurer les options de cet onglet pour que l'appareil s'enregistre auprès de Cisco Umbrella, afin que l'appareil puisse rediriger les recherches DNS vers Cisco Umbrella. Cisco Umbrella peut ensuite appliquer vos politiques de sécurité basées sur FQDN. Pour en savoir plus, consultez Cisco Umbrella.

- **Umbrella** : active Cisco Umbrella. Vous pouvez éventuellement spécifier le nom de la politique Cisco Umbrella à appliquer au périphérique dans le champ **Umbrella Tag** (Balise Cisco Umbrella). Si vous ne spécifiez pas de politique, la politique par défaut est appliquée. Après l'enregistrement, l'ID de l'appareil Cisco Umbrella s'affiche à côté de la balise.
- **Enable DNScrypt** (Activer DNScrypt) : active DNScrypt pour chiffrer les connexions entre le périphérique et Cisco Umbrella. L'activation de DNScrypt démarre le fil d'échange de clés avec le résolveur Umbrella. Le fil d'échange de clés effectue l'établissement de liaison avec le résolveur toutes les heures et met à jour le périphérique avec une nouvelle clé secrète. Comme DNScrypt utilise UDP/443, vous devez vous assurer que la carte de trafic utilisée pour l'inspection DNS comprend ce port. Notez que la classe d'inspection par défaut comprend déjà UDP/443 pour l'inspection DNS.
- **Fail Open** (Autoriser en cas de défaillance) : activez cette option si vous souhaitez que la résolution DNS continue de fonctionner lorsque le serveur DNS Cisco Umbrella est indisponible. En cas d'échec de l'ouverture, si le serveur DNS Cisco Umbrella n'est pas disponible, Cisco Umbrella se désactive dans cette liste des politiques et permet aux demandes DNS d'accéder aux autres serveurs DNS configurés sur le système, le cas échéant. Lorsque les serveurs DNS Cisco Umbrella sont de nouveau disponibles, la liste des politiques reprend de leur utilisation. Si vous ne sélectionnez pas cette option, les requêtes DNS continuent d'être acheminées vers le résolveur Cisco Umbrella inaccessible, de sorte qu'elles ne recevront pas de réponse

Étape 10 Cliquez sur **OK** dans la boîte de dialogue de la liste d'inspection DNS.

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection DNS.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application.

Inspection FTP

L'inspection FTP est activée par défaut. Vous ne devez le configurer que si vous souhaitez un traitement autre que celui par défaut. Les sections suivantes décrivent le moteur d'inspection FTP.

Présentation de l'inspection FTP

L'inspection d'application FTP inspecte les sessions FTP et effectue quatre tâches :

- Prépare les canaux de connexion de données secondaires dynamiques pour le transfert de données FTP. Les ports pour ces canaux sont négociés au moyen de commandes PORT ou PASV. Les canaux sont alloués en réponse à un chargement de fichier, à un téléchargement de fichier ou à un événement de liste de répertoires
- Effectue le suivi de la séquence de commande-réponse FTP.
- Génère une trace d'audit.
  - L'enregistrement d'audit 303002 est généré pour chaque fichier récupéré ou chargé.
  - L'enregistrement d'audit 201005 est généré si la préparation du canal dynamique secondaire a échoué en raison d'un manque de mémoire.
- Traduit l'adresse IP intégrée.

Remarque Si vous désactivez l'inspection FTP, les utilisateurs sortants ne peuvent démarrer les connexions qu'en mode passif, et tous les FTP entrants sont désactivés.

FTP strict

Le protocole FTP strict augmente la sécurité des réseaux protégés en empêchant les navigateurs Web d'envoyer des commandes intégrées dans les demandes FTP. Pour activer un protocole FTP strict, cliquez sur le bouton **Configure** (Configurer) situé à côté de FTP dans Configuration > Firewall (Pare-feu) > Service Policy Rules (Règles de politique de service) > Edit Service Policy Rule (Modifier une règle de politique de service) > Rule Actions (Actions des règles) > Protocol Inspection (Inspection du protocole).

Lorsque vous utilisez un protocole FTP strict, vous pouvez éventuellement spécifier une liste des politiques d'inspection FTP pour préciser les commandes FTP qui ne sont pas autorisées à passer par l'ASA.

L'inspection FTP strict applique le comportement suivant :

- Une commande FTP doit être reconnue avant que l'ASA autorise une nouvelle commande.
- L'ASA abandonne les connexions qui envoient des commandes intégrées.
- Les commandes 227 et PORT sont vérifiées pour s'assurer qu'elles ne s'affichent pas dans une chaîne d'erreur.

Mise en garde L'utilisation de FTP strict peut entraîner des défaillances chez les clients FTP qui ne sont pas strictement conformes aux RFC FTP. En outre, vous devez vous assurer d'appliquer l'inspection à vos ports FTP uniquement (TCP/21 est le port FTP normal). Une inspection FTP stricte appliquée au trafic non FTP peut entraîner une perte de trafic inattendue, en particulier le trafic HTTP.

Grâce à une inspection FTP stricte, chaque commande et séquence de réponse FTP est suivie pour l'activité anormale suivante :

- Commande tronquée : le nombre de virgules dans la commande de réponse PORT et PASV est vérifié pour voir s'il est de cinq. S'il n'y a pas cinq, la commande PORT est considérée comme tronquée et la connexion TCP est fermée.
- Commande incorrecte : vérifie la commande FTP pour voir si elle se termine par <CR><LF> caractères, comme l'exige la RFC. Si ce n'est pas le cas, la connexion est fermée.
- Taille des commandes RETR et STOR : celles-ci sont vérifiées par rapport à une constante fixe. Si la taille est supérieure, un message d'erreur est enregistré et la connexion est fermée.
- Usurpation de commande : la commande PORT doit toujours être envoyée par le client. La connexion TCP est refusée si une commande PORT est envoyée à partir du serveur.
- Usurpation de réponse : la commande de réponse PASV (227) doit toujours être envoyée à partir du serveur. La connexion TCP est refusée si une commande de réponse PASV est envoyée par le client. Cela empêche le gouffre de sécurité lorsque l'utilisateur exécute « 227 xxxx a1, a2, a3, a4, p1, p2 ».
- Modification du flux TCP : l'ASA ferme la connexion s'il détecte une modification du flux TCP.
- Négociation de port non valide : la valeur de port dynamique négociée est vérifiée pour voir si elle est inférieure à 1024. Comme les numéros de port dans la plage de 1 à 1024 sont réservés aux connexions bien connues, si le port négocié se trouve dans cette plage, la connexion TCP est libérée.
- Filtrage de commande : le nombre de caractères présents après les numéros de port dans les commandes de réponse PORT et PASV est vérifié par recoupement avec une valeur constante de 8. S'il est supérieur à 8, la connexion TCP est fermée.
- L'ASA remplace la réponse du serveur FTP à la commande SYST par une série de X pour empêcher le serveur de révéler son type de système aux clients FTP. Pour remplacer ce comportement par défaut, utilisez la commande **no mask-syst-reply** dans la liste FTP.

Configurer une liste des politiques d'inspection FTP

Le filtrage des commandes FTP et les vérifications de sécurité sont fournis à l'aide de l'inspection FTP stricte pour améliorer la sécurité et le contrôle. La conformité au protocole comprend les vérifications de la longueur des paquets, les vérifications des délimiteurs et du format des paquets, les vérifications du terminateur de commande et la validation des commandes.

Le blocage de FTP en fonction des valeurs des utilisateurs est également pris en charge afin que les sites FTP puissent publier des fichiers à télécharger, tout en limitant l'accès à certains utilisateurs. Vous pouvez bloquer les connexions FTP en fonction du type de fichier, du nom du serveur et d'autres attributs. Des journaux de messages système sont générés si une connexion FTP est refusée après l'inspection.

Si vous souhaitez que l'inspection FTP permette aux serveurs FTP de révéler leur type de système aux clients FTP et limite les commandes FTP autorisées, créez et configurez une liste des politiques d'inspection FTP. Vous pouvez ensuite appliquer la liste lorsque vous activez l'inspection FTP.

Vous pouvez éventuellement créer une carte de trafic d'inspection FTP pour définir la carte de trafic pour l'inspection FTP. L'autre option consiste à définir les cartes de trafic directement dans la liste des politiques d'inspection FTP. La différence entre la création d'une carte de trafic et la définition de la correspondance de trafic directement dans la liste d'inspection est que vous pouvez créer des critères de correspondance plus complexes et que vous pouvez réutiliser les cartes de trafic. Bien que cette procédure explique les cartes

d'inspection, les critères de correspondance utilisés dans les cartes de trafics sont les mêmes que ceux expliqués à l'étape relative à l'onglet **Inspection**. Vous pouvez configurer les cartes de trafic FTP en sélectionnant **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Class Maps (Cartes de trafic)** > **FTP**, ou en les créant lors de la configuration de la liste d'inspection.

Astuces Vous pouvez configurer des listes d'inspection lors de la création de politiques de service, en plus de la procédure expliquée ci-dessous. Le contenu de la liste est le même, quelle que soit la façon dont vous la créez.

Avant de commencer

Certaines options de correspondance de trafic utilisent des expressions régulières à des fins de correspondance. Si vous avez l'intention d'utiliser l'une de ces techniques, créez d'abord l'expression régulière ou la carte de trafic d'expressions régulières.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Cartes d'inspection)** > **FTP** .

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste pour afficher son contenu. Vous pouvez modifier le niveau de sécurité directement ou cliquer sur **Customize** (Personnaliser) pour modifier la liste. Le reste de la procédure suppose que vous personnalisez ou ajoutez une liste.

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de la modification d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Dans l'affichage **Niveau de sécurité** de la boîte de dialogue de la liste d'inspection FTP sélectionnez le niveau qui correspond le mieux à la configuration souhaitée. La valeur par défaut est High (Élevé).

Si l'un des niveaux prédéfinis correspond à vos exigences, vous avez maintenant terminé. Cliquez simplement sur **OK**, ignorez le reste de cette procédure et utilisez la liste dans une règle de politique de service pour l'inspection FTP.

Si vous devez personnaliser davantage les paramètres, cliquez sur **Details** (Détails) et poursuivez la procédure.

Astuces
Le bouton **File Type Filtering** (Filtrage de type de fichier) est un raccourci pour configurer l'inspection du média de fichier ou du type MIME, qui est expliquée plus loin dans cette procédure.

Étape 5 Cliquez sur l'onglet **Parameters** (Paramètres) et choisissez de masquer la bannière de message d'accueil du serveur ou de masquer la réponse à la commande SYST.

Le masquage de ces éléments empêche le client de découvrir des informations sur le serveur qui pourraient être utiles lors d'une attaque.

Étape 6 Cliquez sur l'onglet **Inspections** et définissez les inspections spécifiques que vous souhaitez mettre en œuvre en fonction des caractéristiques du trafic.

Vous pouvez définir les critères de correspondance du trafic en fonction des cartes de trafic DNS, en configurant les correspondances directement dans la liste d'inspection, ou les deux.

a) Effectuez l'une des actions suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter un nouveau critère.
- Sélectionnez un critère existant et cliquez sur **Edit** (Modifier).

b) Choisissez **Single Match** (Correspondance unique) pour définir le critère directement, ou **Multiple Match** (Correspondance multiple), auquel cas vous sélectionnez la carte de trafic FTP qui définit les critères.

c) Si vous définissez le critère ici, choisissez le type de correspondance : **Match** (Correspondance) (le trafic doit correspondre au critère) ou **No Match** (Aucune correspondance) (le trafic ne doit pas correspondre au critère). Par exemple, si No Match (Aucune correspondance) est sélectionné pour la chaîne « example.com », tout trafic contenant « example.com » est exclu de la carte de trafic. Configurez ensuite le critère comme suit :

- Nom du fichier : correspond au nom du fichier transféré par rapport à l'expression régulière ou à la liste d'expressions régulières sélectionnée.
- Type de fichier : correspond au type MIME ou de média du fichier transféré par rapport à l'expression régulière ou à la liste d'expressions régulières sélectionnée.
- Serveur : fait correspondre le nom du serveur FTP avec l'expression régulière ou la liste d'expressions régulières sélectionnée.
- Utilisateur : fait correspondre le nom de l'utilisateur connecté à l'expression régulière ou à la liste d'expressions régulières sélectionnée.
- Commande de demande : commande FTP utilisée dans le paquet, toute combinaison des éléments suivants :
  - **APPE** : ajouter à un fichier.
  - **CDUP** : passe au répertoire parent du répertoire de travail actuel.
  - **DELE** : supprime un fichier sur le serveur.
  - **GET** : obtient un fichier du serveur.
  - **HELP** : fournit des renseignements d'aide.
  - **MKD** : crée un répertoire sur le serveur.
  - **PUT** : envoie un fichier au serveur.
  - **RMD** : supprime un répertoire sur le serveur.
  - **RNFR** : spécifie le nom de fichier « rename-from ».
  - **RNTO** : spécifie le nom de fichier « rename-to ».
  - **SITE** : utilisé pour spécifier une commande spécifique au serveur. Ceci est généralement utilisé pour l'administration à distance.
  - **STOU** : stocke un fichier en utilisant un nom de fichier unique.

d) Choisissez d'activer ou de désactiver la journalisation. L'action consiste toujours à réinitialiser la connexion, ce qui abandonne le paquet, ferme la connexion et envoie une réinitialisation TCP au serveur ou au client.
e) Cliquez sur **OK** pour ajouter l'inspection. Répétez le processus au besoin.

Étape 7 Cliquez sur **OK** dans la boîte de dialogue FTP Inspect Map (Liste d'inspection FTP).

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection FTP.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application.

Inspection HTTP

L'inspection HTTP n'est pas activée dans la politique d'inspection par défaut, vous devez donc l'activer si vous avez besoin de cette inspection. Cependant, la carte de trafic d'inspection par défaut comprend les ports HTTP par défaut, vous pouvez donc simplement modifier la politique d'inspection globale par défaut pour ajouter l'inspection HTTP. Vous pouvez également créer une nouvelle politique de service comme vous le souhaitez, par exemple, une politique spécifique à l'interface.

Les sections suivantes décrivent le moteur d'inspection HTTP.

Présentation de l'inspection HTTP

Utilisez le moteur d'inspection HTTP pour une protection contre les attaques spécifiques et d'autres menaces associées au trafic HTTP.

L'inspection des applications HTTP analyse les en-têtes et le corps HTTP et effectue diverses vérifications sur les données. Ces vérifications empêchent diverses constructions HTTP, types de contenu et protocoles de tunnellisation et de messagerie de traverser l'appareil de sécurité.

La fonctionnalité d'inspection HTTP améliorée, également connue sous le nom de pare-feu d'application et disponible lorsque vous configurez une liste des politiques d'inspection HTTP, peut aider à empêcher les attaquants d'utiliser les messages HTTP pour contourner la politique de sécurité du réseau.

L'inspection des applications HTTP peut bloquer les applications tunnellisées et les caractères non ASCII dans les demandes et réponses HTTP, ce qui empêche le contenu malveillant d'atteindre le serveur Web. La limitation de taille de divers éléments dans les en-têtes de demande et de réponse HTTP, le blocage d'URL et l'usurpation d'en-tête de serveur HTTP sont également pris en charge.

L'inspection HTTP améliorée vérifie les éléments suivants pour tous les messages HTTP :

- Conformité à la RFC 2616
- Utilisation uniquement des méthodes définies par la RFC.
- Conformité avec les critères supplémentaires.

Configurer une liste des politiques d'inspection HTTP

Pour préciser les actions lorsqu'un message enfreint un paramètre, créez une liste des politiques d'inspection HTTP. Vous pouvez ensuite appliquer la liste des politiques d'inspection lorsque vous activez l'inspection HTTP.

Vous pouvez éventuellement créer une carte de trafic d'inspection HTTP pour définir la classe de trafic pour l'inspection HTTP. L'autre option consiste à définir les classes de trafic directement dans la liste des politiques d'inspection HTTP. La différence entre la création d'une carte de trafic et la définition de la correspondance de trafic directement dans la liste d'inspection est que vous pouvez créer des critères de correspondance plus complexes et que vous pouvez réutiliser les cartes de trafics. Bien que cette procédure explique les cartes d'inspection, les critères de correspondance utilisés dans les cartes de trafics sont les mêmes que ceux expliqués à l'étape relative à l'onglet **Inspection**. Vous pouvez configurer les cartes de trafic HTTP en sélectionnant **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Class Maps (Cartes de trafic)** > **HTTP**, ou en les créant lors de la configuration de la liste d'inspection.

Astuces Vous pouvez configurer des listes d'inspection lors de la création de politiques de service, en plus de la procédure expliquée ci-dessous. Le contenu de la liste est le même, quelle que soit la façon dont vous la créez.

Avant de commencer

Certaines options de correspondance de trafic utilisent des expressions régulières à des fins de correspondance. Si vous avez l'intention d'utiliser l'une de ces techniques, créez d'abord l'expression régulière ou la carte de trafic d'expressions régulières.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **HTTP**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste pour afficher son contenu. Vous pouvez modifier le niveau de sécurité directement ou cliquer sur **Customize** (Personnaliser) pour modifier la liste. Le reste de la procédure suppose que vous personnalisez ou ajoutez une liste.

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de l'édition d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Dans l'affichage **Niveau de sécurité** de la boîte de dialogue de la liste d'inspection HTTP, sélectionnez le niveau qui correspond le mieux à la configuration souhaitée. Le niveau par défaut est Bas.

Si l'un des niveaux prédéfinis correspond à vos exigences, vous avez maintenant terminé. Cliquez simplement sur **OK**, ignorez le reste de cette procédure et utilisez la liste dans une règle de politique de service pour l'inspection HTTP.

Si vous devez personnaliser davantage les paramètres, cliquez sur **Details** (Détails) et poursuivez la procédure.

Astuces

Le bouton **URI Filtering** (Filtrage URI) est un raccourci pour configurer l'inspection Request URI (URI de demande), qui est expliquée plus loin dans cette procédure.

Étape 5 Cliquez sur l'onglet **Parameters** (Paramètres) et configurez les options souhaitées.

- **Body Match Maximum** (Nombre maximal de caractères pour la correspondance de corps) : nombre maximal de caractères dans le corps d'un message HTTP qui doivent être recherchés dans une correspondance de corps. La valeur par défaut est de 200 octets. Un grand nombre aura un impact considérable sur les performances.
- **Check for protocol violations** (Vérifier les violations de protocole) : indique s'il faut vérifier que les paquets sont conformes au protocole HTTP. En cas de non-conformité, vous pouvez abandonner la connexion, la réinitialiser ou la journaliser. Lors de l'abandon ou de la réinitialisation, vous pouvez également activer la journalisation.
- **Spoof server String (chaîne de serveur Spoof)** : remplace la valeur d'en-tête HTTP du serveur par la chaîne spécifiée, jusqu'à 82 caractères.

Étape 6 Cliquez sur l'onglet **Inspections** et définissez les inspections spécifiques que vous souhaitez mettre en œuvre en fonction des caractéristiques du trafic.

Vous pouvez définir les critères de correspondance du trafic en fonction des cartes de trafic HTTP, en configurant les correspondances directement dans la liste d'inspection, ou les deux.

a) Effectuez l'une des actions suivantes :
   - Cliquez sur **Add** (Ajouter) pour ajouter un nouveau critère.
   - Sélectionnez un critère existant et cliquez sur **Edit** (Modifier).

b) Choisissez **Single Match** (Correspondance unique) pour définir le critère directement, ou **Multiple Match** (Correspondance multiple), auquel cas vous sélectionnez la carte de trafic HTTP qui définit les critères.

c) Si vous définissez le critère ici, choisissez le type de correspondance : **Match** (Correspondance) (le trafic doit correspondre au critère) ou **No Match** (Aucune correspondance) (le trafic ne doit pas correspondre au critère). Par exemple, si No Match (Aucune correspondance) est sélectionné dans la chaîne « example.com », tout trafic contenant « example.com » est exclu de la carte de trafic. Configurez ensuite le critère comme suit :
   - Incompatibilité de type de contenu de la demande/de la réponse : correspond aux paquets dont le type de contenu dans la réponse ne correspond pas à l'un des types MIME dans le champ accept de la demande.
   - Arguments de la demande : faites correspondre les arguments de la demande à l'expression régulière ou à la liste d'expressions régulières sélectionnée.
   - Longueur du corps de la demande : correspond aux paquets dont le corps de la demande est supérieur au nombre d'octets spécifié.
   - Corps de la demande : faites correspondre le corps de la demande avec l'expression régulière ou la liste d'expressions régulières sélectionnée.
   - Nombre de champs d'en-tête de demande : correspond aux paquets dont le nombre de champs d'en-tête dans la demande est supérieur au nombre spécifié. Vous pouvez faire correspondre le type d'en-tête de champ à une expression régulière ou à un type prédéfini. Les types prédéfinis sont les suivants : accept, accept-charset, accept-encoding, accept-language, allow, authorization, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5,

content-range, content-type, cookie, date, expect, expires, from, host, if-match, if-modified-since, if-none-match, if-range, if-unmodified-since, last-modified, max-forwards, pragma, proxy-authorization, range, referer, te, trailer, transfer-encoding, upgrade, user-agent, via, warning.

- Longueur du champ d'en-tête de la demande : correspond aux paquets dont la longueur du champ d'en-tête dans la demande est supérieure aux octets spécifiés. Vous pouvez faire correspondre le type d'en-tête de champ à une expression régulière ou à un type prédéfini. Les types prédéfinis sont répertoriés ci-dessus pour le nombre de champs d'en-tête de demande.
- Champ d'en-tête de demande : faites correspondre le contenu du champ d'en-tête sélectionné dans la demande avec l'expression régulière ou la liste d'expressions régulières sélectionnée. Vous pouvez spécifier un type d'en-tête prédéfini ou utiliser une expression régulière pour sélectionner les en-têtes.
- Nombre d'en-têtes de demande : correspond aux paquets dont le nombre d'en-têtes dans la demande est supérieur au nombre spécifié.
- Longueur de l'en-tête de la demande : correspond aux paquets dont la longueur de l'en-tête dans la demande est supérieure aux octets spécifiés.
- Request Header Non-ASCII : correspond aux paquets dont l'en-tête de la demande contient des caractères non ASCII.
- Méthode de demande : correspond aux paquets dans lesquels la méthode de demande correspond au type prédéfini ou à l'expression régulière ou à la liste d'expressions régulières sélectionnée. Les types prédéfinis sont les suivants : bcopy, bdelete, bmove, bpropfind, bproppatch, connect, copy, delete, edit, get, getattribute, getattributenames, getproperties, head, index, lock, mkcol, mkdir, move, notify, options, poll, post, propfind, proppatch, put, revadd, revlabel, revlog, revnum, save, search, setattribute, startrev, stoprev, subscribe, trace, unedit, unlock, unsubscribe.
- Longueur de l'URI de la demande : correspond aux paquets dans lesquels la longueur de l'URI de la demande est supérieure aux octets spécifiés.
- URI de la demande : faites correspondre le contenu de l'URI de la demande à l'expression régulière ou à la liste d'expressions régulières sélectionnée.
- Corps de la demande : faites correspondre le corps de la demande à l'expression régulière ou à la liste d'expressions régulières sélectionnée, ou au contenu d'ActiveX ou de Java Applet.
- Longueur du corps de la réponse : correspond aux paquets dans lesquels la longueur du corps de la réponse est supérieure aux octets spécifiés.
- Nombre de champs d'en-tête de réponse : correspond aux paquets dont le nombre de champs d'en-tête dans la réponse est supérieur au nombre spécifié. Vous pouvez faire correspondre le type d'en-tête de champ à une expression régulière ou à un type prédéfini. Les types prédéfinis sont les suivants : accept-ranges, age, allow, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5, content-range, content-type, date, etag, expires, last-modified, location, pragma, proxy-authenticate, retry-after, server, set-cookie, trailer, transfer-encoding, upgrade, vary, via, warning, www-authenticate.
- Longueur du champ d'en-tête de la réponse : correspond aux paquets dont la longueur du champ d'en-tête dans la réponse est supérieure aux octets spécifiés. Vous pouvez faire correspondre le type d'en-tête de champ à une expression régulière ou à un type prédéfini. Les types prédéfinis sont répertoriés ci-dessus pour le nombre de champs d'en-tête de réponse.

- Champ d'en-tête de réponse : fait correspondre le contenu du champ d'en-tête sélectionné dans la réponse à l'expression régulière ou à la liste d'expressions régulières sélectionnée. Vous pouvez spécifier un type d'en-tête prédéfini ou utiliser une expression régulière pour sélectionner les en-têtes.
- Nombre d'en-têtes de réponse : correspond aux paquets dont le nombre d'en-têtes dans la réponse est supérieur au nombre spécifié.
- Longueur de l'en-tête de la réponse : correspond aux paquets dont la longueur de l'en-tête dans la réponse est supérieure aux octets spécifiés.
- En-tête de réponse non-ASCII : correspond aux paquets dont l'en-tête de la réponse contient des caractères non ASCII.
- Ligne d'état de la réponse : faites correspondre le contenu de la ligne d'état de la réponse à l'expression régulière ou à la liste d'expressions régulières sélectionnée.

d) Choisissez d'abandonner la connexion, de la réinitialiser ou de la journaliser. Pour abandonner la connexion et la réinitialisation, vous pouvez activer ou désactiver la journalisation.
e) Cliquez sur **OK** pour ajouter l'inspection. Répétez le processus au besoin.

Étape 7 Cliquez sur **OK** dans la boîte de dialogue de la liste d'inspection HTTP.

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection HTTP.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application.

Inspection ICMP

Le moteur d'inspection ICMP permet au trafic ICMP d'avoir une « session » afin qu'il puisse être inspecté comme le trafic TCP et UDP. Sans le moteur d'inspection ICMP, nous vous recommandons de ne pas autoriser ICMP par l'intermédiaire de l'ASA dans une liste de contrôle d'accès. Sans inspection dynamique, ICMP peut être utilisé pour attaquer votre réseau. Le moteur d'inspection ICMP garantit qu'il n'y a qu'une seule réponse à chaque demande et que le numéro de séquence est correct.

Cependant, le trafic ICMP dirigé vers une interface ASA n'est jamais inspecté, même si vous activez l'inspection ICMP. Ainsi, un ping (requête d'écho) à une interface peut échouer dans des circonstances spécifiques, comme lorsque la demande d'écho provient d'une source que l'ASA peut atteindre par une route de sauvegarde par défaut.

Remarque La NAT utilise l'inspection ICMP lors de la traduction des paquets, même si vous désactivez l'inspection ICMP.

Pour en savoir plus sur l'activation de l'inspection ICMP, consultez Configurer l'inspection du protocole de couche d'application.

Inspection des erreurs ICMP

Lorsque l'inspection des erreurs ICMP est activée, l'ASA crée des sessions de traduction pour les sauts intermédiaires qui envoient des messages d'erreur ICMP, en fonction de la configuration NAT. L'ASA remplace les adresses IP du paquet par les adresses IP traduites.

Lorsque cette option est désactivée, l'ASA ne crée pas de sessions de traduction pour les nœuds intermédiaires qui génèrent des messages d'erreur ICMP. Les messages d'erreur ICMP générés par les nœuds intermédiaires entre l'hôte interne et l'ASA atteignent l'hôte externe sans utiliser de ressource NAT supplémentaire. Cela n'est pas souhaité lorsqu'un hôte externe utilise la commande traceroute pour retracer les sauts jusqu'à la destination à l'intérieur de l'ASA. Lorsque l'ASA ne traduit pas les sauts intermédiaires, tous les sauts intermédiaires s'affichent avec l'adresse IP de destination mappée.



Remarque Vous devez toujours activer l'inspection d'erreur ICMP s'il est possible que la NAT soit utilisée sur les paquets ICMP. Comme la NAT utilise automatiquement l'inspection ICMP pour les paquets ICMP, même si l'inspection ICMP est désactivée, l'utilisation de l'adresse de destination mappée comme adresse source peut donner l'impression qu'un analyseur examine votre réseau. Par exemple, sans inspection d'erreur ICMP également activée, si le paquet de demande ECHO a sa destination traduite, lorsqu'il est intégré dans une réponse de délai ICMP dépassé, l'en-tête externe de la demande de délai dépassé utilise la destination traduite comme adresse source. Si vous activez l'inspection d'erreur ICMP, l'adresse source de dépassement sera définie à la valeur correcte.

Pour en savoir plus sur l'activation de l'inspection des erreurs ICMP, consultez Configurer l'inspection du protocole de couche d'application.

Inspection ILS

Le moteur d'inspection Internet Locator Service (ILS) prend en charge la NAT pour les produits Microsoft NetMeeting, SiteServer et Active Directory qui utilisent LDAP pour échanger des informations de répertoire avec un serveur ILS. Vous ne pouvez pas utiliser la PAT avec l'inspection ILS, car seules les adresses IP sont stockées par une base de données LDAP.

Pour les réponses de recherche, lorsque le serveur LDAP est situé à l'extérieur, considérez l'utilisation de la NAT pour permettre aux homologues internes de communiquer localement lorsqu'ils sont enregistrés sur des serveurs LDAP externes. Si vous n'avez pas besoin d'utiliser la NAT, nous vous recommandons de désactiver le moteur d'inspection pour obtenir de meilleures performances.

Une configuration supplémentaire peut être nécessaire lorsque le serveur ILS est situé à l'intérieur de la frontière ASA. Cela nécessiterait une ouverture pour que les clients externes accèdent au serveur LDAP sur le port spécifié, généralement TCP 389.



Remarque Comme le trafic ILS (signalisation d'appel H225) ne se produit que sur le canal UDP secondaire, la connexion TCP est déconnectée après l'intervalle d'inactivité TCP. Par défaut, cet intervalle est de 60 minutes et peut être ajusté à l'aide de la commande TCP **timeout**. Dans ASDM, cela se trouve dans le volet **Configuration > Firewall (Pare-feu) > Advanced (Avancé) > Global Timeouts (Délais d'expiration globaux)**.

L'inspection ILS a les limites suivantes :

- Les demandes de parrainage et les réponses ne sont pas prises en charge.
- Les utilisateurs de plusieurs répertoires ne sont pas unifiés.
- Les utilisateurs uniques ayant plusieurs identités dans plusieurs répertoires ne peuvent pas être reconnus par la NAT.

Pour en savoir plus sur l'activation de l'inspection ILS, consultez Configurer l'inspection du protocole de couche d'application.

Inspection de la messagerie instantanée

Le moteur d'inspection de messagerie instantanée (IM) vous permet de contrôler l'utilisation du réseau d'IM et d'arrêter la fuite de données confidentielles, la propagation des vers et d'autres menaces pour le réseau d'entreprise.

L'inspection IM n'est pas activée dans la politique d'inspection par défaut, vous devez donc l'activer si vous avez besoin de cette inspection. Cependant, la carte de trafic d'inspection par défaut comprend les ports IM par défaut, vous pouvez donc simplement modifier la politique d'inspection globale par défaut pour ajouter l'inspection IM. Vous pouvez également créer une nouvelle politique de service comme vous le souhaitez, par exemple, une politique spécifique à l'interface.

Si vous décidez de mettre en œuvre l'inspection IM, vous pouvez également configurer une liste des politiques d'inspection IM pour préciser les actions lorsqu'un message enfreint un paramètre. La procédure suivante explique les mappages de politiques d'inspection d'IM.

Vous pouvez également créer une carte de trafic d'inspection IM pour définir la carte de classes de trafic utilisée pour l'inspection IM. L'autre option consiste à définir les cartes de classes de trafic directement dans la liste des politiques d'inspection d'IM. La différence entre la création d'une carte de trafic et la définition de la correspondance du trafic directement dans la liste d'inspection est que vous pouvez créer des critères de correspondance plus complexes et réutiliser les cartes de trafic. Cette procédure explique les cartes d'inspection, mais les cartes de trafic sont essentiellement les mêmes, sauf que vous ne spécifiez pas les actions appliquées au trafic correspondant. Vous pouvez configurer les cartes de trafic IM en sélectionnant **Configuration > Firewall (Pare-feu) > Objects (Objets) > Class Maps (Cartes de trafic) > Instant Messaging (IM) [Messagerie instantanée]**.



Astuces Vous pouvez configurer des listes d'inspection lors de la création de politiques de service, en plus de la procédure expliquée ci-dessous. Le contenu de la liste est le même, quelle que soit la façon dont vous la créez.

Avant de commencer

Certaines options de correspondance de trafic utilisent des expressions régulières à des fins de correspondance. Si vous avez l'intention d'utiliser l'une de ces techniques, créez d'abord l'expression régulière ou la carte de trafic d'expressions régulières.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **Instant Messaging (IM)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste et cliquez sur **Edit** (Modifier).

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de l'édition d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Définissez les inspections spécifiques que vous souhaitez mettre en œuvre en fonction des caractéristiques du trafic.

Vous pouvez définir les critères de correspondance du trafic en fonction des cartes de trafic IM, en configurant les correspondances directement dans la liste d'inspection, ou les deux.

a) Effectuez l'une des actions suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter un nouveau critère.
- Sélectionnez un critère existant et cliquez sur **Edit** (Modifier).

b) Choisissez **Single Match** (Correspondance unique) pour définir directement le critère, ou **Multiple Match** (Correspondance multiple), puis sélectionnez la carte de trafic IM qui définit les critères. Cliquez sur **Manage** (Gérer) pour créer de nouvelles cartes de trafic.

c) Si vous définissez le critère ici, choisissez le type de correspondance pour les critères : **correspondance** (le trafic doit correspondre au critère) ou **aucune correspondance** (le trafic ne doit pas correspondre au critère). Par exemple, si Aucune correspondance est sélectionné dans la chaîne « example.com », tout trafic contenant « example.com » est exclu de la carte de trafic. Configurez ensuite le critère.

- Protocole : correspond au trafic d'un protocole IM spécifique, tel que Yahoo Messenger ou MSN Messenger.
- Service : correspond à un service de messagerie instantanée spécifique, tel que la conversation, le transfert de fichiers, la caméra Web, la conversation vocale, la conférence ou les jeux.
- Version : faites correspondre la version du message IM à l'expression régulière ou à la liste d'expressions régulières sélectionnée.
- Nom de connexion du client : faites correspondre le nom de connexion du client source du message IM avec l'expression régulière ou la liste d'expressions régulières sélectionnée.
- Nom de connexion de l'homologue du client : faites correspondre le nom de connexion de l'homologue de destination du message IM avec l'expression régulière ou la liste d'expressions régulières sélectionnée.
- Adresse IP source : faites correspondre l'adresse IP source et le masque.
- Adresse IP de destination : faites correspondre l'adresse IP de destination et le masque.
- Nom de fichier : faites correspondre le nom de fichier du message IM avec l'expression régulière ou la liste d'expressions régulières sélectionnée.

d) Choisissez d'abandonner la connexion, de la réinitialiser ou de la journaliser. Pour abandonner la connexion et la réinitialisation, vous pouvez activer ou désactiver la journalisation.
e) Cliquez sur **OK** pour ajouter l'inspection. Répétez le processus au besoin.

Étape 5 Cliquez sur **OK** dans la boîte de dialogue de la liste d'inspection IM.

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection IM.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application.

Inspection des options IP

Vous pouvez configurer l'inspection des options IP pour contrôler les paquets IP qui sont autorisés en fonction du contenu du champ Options IP dans l'en-tête du paquet. Vous pouvez abandonner les paquets qui ont des options indésirables, effacer les options (et autoriser le paquet) ou autoriser le paquet sans modification.

Les options IP fournissent des fonctions de contrôle nécessaires dans certaines situations, mais inutiles pour la plupart des communications courantes. En particulier, les options IP comprennent des dispositions pour les horodatages, la sécurité et le routage spécial. L'utilisation des options IP est facultative, et le champ peut contenir zéro, une ou plusieurs options.

Pour obtenir la liste des options IP, avec des références aux RFC pertinents, consultez la page IANA, http://www.iana.org/assignments/ip-paramètres/ip-paramètres.xhtml.

L'inspection des options IP est activée par défaut, mais pour le trafic RSVP uniquement. Vous ne devez le configurer que si vous souhaitez autoriser des options supplémentaires que la liste par défaut, ou si vous souhaitez l'appliquer à d'autres types de trafic à l'aide d'une carte de classe de trafic d'inspection autre que celle par défaut.

Remarque L'inspection des options IP ne fonctionne pas sur les paquets fragmentés. Par exemple, les options ne sont pas effacées des fragments.

Les sections suivantes décrivent l'inspection des options IP.

Valeurs par défaut pour l'inspection des options IP

L'inspection des options IP est activée par défaut pour le trafic RSVP uniquement, à l'aide de la liste des politiques d'inspection _default_ip_options_map.

- L'option Router Alert est autorisée.

  Cette option informe les routeurs de transit d'inspecter le contenu du paquet même lorsque le paquet n'est pas destiné à ce routeur. Cette inspection est utile lors de la mise en œuvre de RSVP et de protocoles similaires qui nécessitent un traitement plutôt complexe de la part des routeurs le long du chemin de livraison du paquet. L'abandon de paquets RSVP contenant l'option Router Alert peut entraîner des problèmes dans les implémentations VoIP.

- Les paquets qui contiennent d'autres options sont abandonnés.

  Chaque fois qu'un paquet est abandonné en raison d'une inspection, le journal système 106012 est émis. Le message indique quelle option a causé l'abandon. Utilisez la commande **show service-policy inspect ip-options** pour afficher les statistiques de chaque option.

Configurer une liste des politiques d'inspection des options IP

Si vous souhaitez effectuer une inspection d'options IP autres que celles par défaut, créez une liste des politiques d'inspection d'options IP pour préciser comment vous souhaitez gérer chaque type d'option.



Astuces Vous pouvez configurer des listes d'inspection lors de la création de politiques de service, en plus de la procédure expliquée ci-dessous. Le contenu de la liste est le même, quelle que soit la façon dont vous la créez.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Cartes d'inspection)** > **IP Options (Options IP)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste, puis cliquez sur **Edit** (Modifier).

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de la modification d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Choisissez les options que vous souhaitez autoriser en les déplaçant de la liste d'abandon vers la liste d'autorisation.

Tenez compte des conseils suivants :

- L'option « default » (défaut) définit le comportement par défaut pour les options non incluses dans la liste. Si vous le déplacez vers la liste Autorisé, même les options affichées dans la liste Abandon seront autorisées.
- Pour toute option que vous autorisez, vous pouvez cocher la case Clear (Effacer) pour supprimer l'option de l'en-tête du paquet avant de transmettre le paquet.
- Certaines options sont répertoriées par numéro de type d'option. Le nombre est l'octet complet du type d'option (copie, carte et numéro d'option), et pas seulement la partie numéro d'option de l'octet. Ces types d'options peuvent ne pas représenter des options réelles. Les options non standard doivent être au format type-longueur attendu défini dans le protocole Internet RFC 791, http://tools.ietf.org/html/rfc791.
- Si un paquet comprend plus d'un type d'option, il est abandonné tant que l'action pour l'un de ces types est d'abandonner le paquet.

Pour obtenir la liste des options IP, avec des références aux RFC pertinents, consultez la page IANA, http://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml.

Étape 5 Cliquez sur **OK**.

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection d'options IP.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application.

Inspection IPsec Pass Through

L'inspection IPsec Pass Through n'est pas activée dans la politique d'inspection par défaut. Vous devez donc l'activer si vous avez besoin de cette inspection. Cependant, la carte de trafic d'inspection par défaut comprend les ports IPsec par défaut, vous pouvez donc simplement modifier la politique d'inspection globale par défaut pour ajouter l'inspection IPsec. Vous pouvez également créer une nouvelle politique de service comme vous le souhaitez, par exemple, une politique spécifique à l'interface.

Les sections suivantes décrivent le moteur d'inspection IPsec Pass Through.

Aperçu de l'inspection de transmission directe IPsec

Internet Protocol Security (IPsec) est une suite de protocoles permettant de sécuriser les communications IP en authentifiant et en chiffrant chaque paquet IP d'un flux de données. IPsec comprend également des protocoles pour établir une authentification mutuelle entre les agents au début de la session et la négociation des clés cryptographiques à utiliser pendant la session. IPsec peut être utilisé pour protéger les flux de données entre une paire d'hôtes (par exemple, utilisateurs d'ordinateurs ou serveurs), entre une paire de passerelles de sécurité (comme les routeurs ou les pare-feu) ou entre une passerelle de sécurité et un hôte.

L'inspection applicative d'IPsec Pass Through (transmission directe IPsec) permet la traversée transparente du trafic ESP (protocole IP 50) et AH (protocole IP 51) associé à une connexion IKE sur le port UDP 500. Il évite une longue configuration d'ACL pour autoriser le trafic ESP et AH et offre également une sécurité à l'aide du délai d'expiration et du nombre maximal de connexions.

Configurez une liste des politiques pour la transmission directe IPsec afin de préciser les restrictions relatives au trafic ESP ou AH. Vous pouvez définir le nombre maximal de connexions par client et le délai d'inactivité.

Le trafic NAT et non NAT est autorisé. Cependant, la PAT n'est pas prise en charge.

Configurer une liste des politiques d'inspection de transmission directe IPsec

Une liste IPsec Passthrough vous permet de modifier les valeurs de configuration par défaut utilisées pour l'inspection de l'application IPsec Pass Through. Vous pouvez utiliser une liste IPsec Passthrough pour autoriser certains flux sans utiliser d'ACL.

La configuration comprend une liste par défaut, _default_ipsec_passthru_map, qui n'établit aucune limite maximale aux connexions ESP par client, et définit le délai d'inactivité ESP à 10 minutes. Vous ne devez configurer une liste des politiques d'inspection que si vous souhaitez des valeurs différentes ou si vous souhaitez définir des valeurs AH.

Astuces Vous pouvez configurer des listes d'inspection lors de la création de politiques de service, en plus de la procédure expliquée ci-dessous. Le contenu de la liste est le même, quelle que soit la façon dont vous la créez.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Listes d'inspection)** > **IPsec Pass Through (IPsec Pass Through)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste pour afficher son contenu. Vous pouvez modifier le niveau de sécurité directement ou cliquer sur **Customize** (Personnaliser) pour modifier la liste. Le reste de la procédure suppose que vous personnalisez ou ajoutez une liste.

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de l'édition d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Dans l'affichage **Security Level** (Niveau de sécurité) de la boîte de dialogue IPsec Pass Through Inspect Map (Liste d'inspection IPsec Pass Through), sélectionnez le niveau qui correspond le mieux à la configuration souhaitée.

Si l'un des niveaux prédéfinis correspond à vos exigences, vous avez maintenant terminé. Cliquez simplement sur **OK**, ignorez le reste de cette procédure et utilisez la liste dans une règle de politique de service pour l'inspection IPsec Pass Through.

Si vous devez personnaliser davantage les paramètres, cliquez sur **Details** (Détails) et poursuivez la procédure.

Étape 5 Choisissez d'autoriser les tunnels ESP et HA.

Pour chaque protocole, vous pouvez également définir le nombre maximal de connexions autorisées par client et le délai d'inactivité.

Étape 6 Cliquez sur **OK**.

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection IPsec Pass Through.

Inspection IPv6

L'inspection IPv6 vous permet de consigner ou d'abandonner sélectivement le trafic IPv6 en fonction de l'en-tête d'extension. En outre, l'inspection IPv6 peut vérifier la conformité à la RFC 2460 pour le type et l'ordre des en-têtes d'extension dans les paquets IPv6.

L'inspection IPv6 n'est pas activée dans la politique d'inspection par défaut, vous devez donc l'activer si vous avez besoin de cette inspection. Vous pouvez simplement modifier la politique d'inspection globale par défaut

pour ajouter l'inspection IPv6. Vous pouvez également créer une nouvelle politique de service comme vous le souhaitez, par exemple, une politique spécifique à l'interface.

Valeurs par défaut pour l'inspection IPv6

Si vous activez l'inspection IPv6 et que vous ne spécifiez pas de liste des politiques d'inspection, la liste des politiques d'inspection IPv6 par défaut est utilisée, et les actions suivantes sont effectuées :

- Autorise uniquement les en-têtes d'extension IPv6 connus. Les paquets non conformes sont abandonnés et journalisés.
- Applique l'ordre des en-têtes d'extension IPv6 tel que défini dans la spécification RFC 2460. Les paquets non conformes sont abandonnés et journalisés.
- Abandonne tout paquet avec un en-tête de type routage.

Configurer une liste des politiques d'inspection IPv6

Pour identifier les en-têtes d'extension à abandonner ou à journaliser, ou pour désactiver la vérification des paquets, créez une liste des politiques d'inspection IPv6 à utiliser par la politique de service.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Listes d'inspection)** > **IPv6**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste, puis cliquez sur **Edit** (Modifier).

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de l'édition d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Cliquez sur l'onglet **Enforcement** (Application) et choisissez d'autoriser uniquement les en-têtes d'extension IPv6 connus ou d'appliquer l'ordre des en-têtes d'extension IPv6 comme défini dans la RFC 2460. Les paquets non conformes sont abandonnés et journalisés.

Étape 5 (Facultatif) Cliquez sur l'onglet **Header Matches** (Correspondances d'en-têtes) pour identifier le trafic à abandonner ou à journaliser en fonction des en-têtes des messages IPv6.

a) Effectuez l'une des actions suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter un nouveau critère.
- Sélectionnez un critère existant et cliquez sur **Edit** (Modifier).

b) Choisissez l'en-tête d'extension IPv6 correspondant :

- En-tête d'authentification (HA).
- En-tête des options de destination.
- En-tête Encapsulating Security Payload (ESP).

- En-tête de fragment.
- En-tête Hop-by-hop Options.
- En-tête de routage : spécifiez un numéro de type d'en-tête unique ou une plage de numéros.
- Nombre d'en-têtes : spécifiez le nombre maximal d'en-têtes d'extension que vous autoriserez sans supprimer ni journaliser le paquet.
- Nombre d'adresses d'en-tête de routage : spécifiez le nombre maximal d'adresses dans l'en-tête de routage de type 0 que vous autoriserez sans supprimer ni journaliser le paquet.

c) Choisissez d'abandonner ou de consigner le paquet. Si vous abandonnez le paquet, vous pouvez également activer la journalisation.
d) Cliquez sur **OK** pour ajouter l'inspection. Répétez le processus au besoin.

Étape 6 Cliquez sur **OK** dans la boîte de dialogue IPv6 Inspect Map (Liste d'inspection IPv6).

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection IPv6.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application.

Inspection NetBIOS

L'inspection d'application NetBIOS effectue une NAT pour l'adresse IP intégrée dans les paquets du service de nom NetBIOS (NBNS) et les paquets des services de datagramme NetBIOS. Il applique également la conformité du protocole en vérifiant la cohérence des champs de nombre et de longueur.

L'inspection NetBIOS est activée par défaut. Vous pouvez éventuellement créer une liste des politique abandonner ou journaliser les violations du protocole NetBIOS. La procédure suivante explique comment configurer une liste des politiques d'inspection NetBIOS.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Cartes d'inspection)** > **NetBIOS**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste, puis cliquez sur **Edit** (Modifier).

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de l'édition d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Sélectionnez **Check for Protocol Violations** (Vérifier les violations de protocole). Il n'y a aucune raison de créer une liste si vous ne sélectionnez pas cette option.

Étape 5 Sélectionnez l'action à effectuer, soit abandonner le paquet, soit le consigner. Si vous abandonnez le paquet, vous pouvez également activer la journalisation.

Étape 6 Cliquez sur **OK**.

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection NetBIOS.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application.

Inspection PPTP

PPTP est un protocole de tunnellisation du trafic PPP. Une session PPTP est composée d'un canal TCP et généralement de deux tunnels GRE PPTP. Le canal TCP est le canal de contrôle utilisé pour négocier et gérer les tunnels PPTP GRE. Les tunnels GRE acheminent les sessions PPP entre les deux hôtes.

Lorsque cette option est activée, le moteur d'inspection PPTP inspecte les paquets du protocole PPTP et crée dynamiquement les connexions GRE et les xlates nécessaires pour autoriser le trafic PPTP.

Plus précisément, l'ASA inspecte les annonces de version PPTP et la séquence de demande/réponse d'appel sortant. Seul PPTP version 1, tel que défini dans la RFC 2637, est inspecté. L'inspection plus approfondie sur le canal de contrôle TCP est désactivée si la version annoncée par l'un ou l'autre des côtés n'est pas la version 1. En outre, la demande d'appel sortant et la séquence de réponse sont suivies. Les connexions et les xlates sont allouées dynamiquement selon les besoins pour permettre le trafic de données GRE secondaire subséquent.

Le moteur d'inspection PPTP doit être activé pour que le trafic PPTP soit traduit par PAT. En outre, la PAT n'est effectuée que pour une version modifiée de GRE (RFC2637) et uniquement si elle est négociée sur le canal de contrôle TCP PPTP. La PAT n'est pas effectuée pour la version non modifiée de GRE (RFC 1701 et RFC 1702).

Pour en savoir plus sur l'activation de l'inspection PPTP, consultez Configurer l'inspection du protocole de couche d'application.

Inspection RSH

L'inspection RSH est activée par défaut. Le protocole RSH utilise une connexion TCP du client RSH au serveur RSH sur le port TCP 514. Le client et le serveur négocient le numéro de port TCP où le client est à l'écoute du flux de sortie STDERR. L'inspection RSH prend en charge la NAT du numéro de port négocié, si nécessaire.

Pour en savoir plus sur l'activation de l'inspection RSH, consultez Configurer l'inspection du protocole de couche d'application.

Inspection SMTP et SMTP étendue

L'inspection ESMTP détecte les attaques, y compris les attaques de pourriels, d'hameçonnage, de messages malformés et les attaques de débordement ou d'insuffisance de la mémoire tampon. Elle prend également en charge la sécurité des applications et la conformité des protocoles, qui imposent la validité des messages ESMTP, bloquent les expéditeurs/récepteurs et bloquent le relais de messagerie.

L'inspection ESMTP est activée par défaut. Vous ne devez le configurer que si vous souhaitez un traitement différent de celui fourni par la liste d'inspection par défaut.

Les sections suivantes décrivent le moteur d'inspection ESMTP.

Aperçu de l'inspection SMTP et ESMTP

L'inspection des applications SMTP étendue (ESMTP) offre une protection améliorée contre les attaques basées sur SMTP en limitant les types de commandes SMTP qui peuvent passer par l'ASA et en ajoutant des fonctionnalités de surveillance. ESMTP est une amélioration du protocole SMTP et est similaire à SMTP à bien des égards.

L'inspection d'application ESMTP contrôle et réduit les commandes que l'utilisateur peut utiliser ainsi que les messages que le serveur renvoie. L'inspection ESMTP effectue trois tâches principales :

- Restreint les requêtes SMTP à sept commandes SMTP de base et à huit commandes étendues. Les commandes prises en charge sont les suivantes :
  - SMTP étendu : AUTH, EHLO, ETRN, HELP, SAML, SEND, SOML, STARTTLS et VRFY.
  - SMTP (RFC 821) : DATA, HELO, MAIL, NOOP, QUIT, RCPT, RSET.
- Surveille la séquence de commande-réponse SMTP.
- Génère une trace d'audit : l'enregistrement d'audit 108002 est généré lorsqu'un caractère non valide intégré dans l'adresse courriel est remplacé. Pour en savoir plus, consultez la RFC 821.

L'inspection ESMTP surveille la séquence de commande et de réponse pour les signatures anormales suivantes :

- Commandes tronquées.
- Fin de commande incorrecte (absence de terminaison par <CR> <LF>).
- Les commandes MAIL et RCPT précisent qui sont l'expéditeur et le destinataire du courriel. Les adresses de messagerie sont analysées pour détecter les caractères inconnus. Le caractère de routage (|) est supprimé (changé en espace vide) et « < » □« > » ne sont autorisés que s'ils sont utilisés pour définir une adresse de courriel (« > » doit être précédé de « < »).
- Transition inattendue du serveur SMTP. 3379
- Pour les commandes inconnues ou non prises en charge, le moteur d'inspection modifie tous les caractères du paquet en X, qui sont rejetés par le serveur interne. Il en résulte un message tel que « 500 Command unknown: « XXX » (Commande inconnue : « XXX »). Les commandes incomplètes sont rejetées

  Les commandes ESMTP non prises en charge sont ATRN, ONEX, VERB, CHUNKING et les extensions privées.
- Modification du flux TCP.

- Pipelining de commandes.

Remarque Lorsque l'inspection ESMTP est activée, une session Telnet utilisée pour le protocole SMTP interactif peut se bloquer si les règles suivantes ne sont pas respectées : les commandes SMTP doivent comporter au moins quatre caractères ; elles doivent se terminer par un retour chariot et un saut de ligne; et vous devez attendre une réponse avant d'envoyer la commande suivante.

Valeurs par défaut pour l'inspection ESMTP

L'inspection ESMTP est activée par défaut, à l'aide de la liste des politiques d'inspection _default_esmtp_map.

- La bannière du serveur est masquée. Le moteur d'inspection ESMTP remplace les caractères de la bannière SMTP du serveur par des astérisques, à l'exception des caractères « 2 », « 0 », « 0 ». Les caractères de retour chariot (CR) et de retour de ligne (LF) sont ignorés.
- Les connexions chiffrées sont autorisées, mais pas inspectées.
- Les caractères spéciaux dans les adresses de l'expéditeur et du destinataire ne sont pas détectés et aucune action n'est entreprise.
- Les connexions dont la longueur de ligne de commande est supérieure à 512 sont abandonnées et journalisées.
- Les connexions de plus de 100 destinataires sont abandonnées et journalisées.
- Les messages dont la longueur du corps est supérieure à 998 octets sont journalisés.
- Les connexions dont la longueur de ligne d'en-tête est supérieure à 998 sont abandonnées et journalisées.
- Les messages avec des noms de fichier MIME supérieurs à 255 caractères sont abandonnés et journalisés.
- Les paramètres de réponse EHLO correspondant à « autres » sont masqués.

Configurer une liste des politiques d'inspection ESMTP

Pour préciser les actions lorsqu'un message enfreint un paramètre, créez une liste des politiques d'inspection ESMTP. Vous pouvez ensuite appliquer la liste des politiques d'inspection lorsque vous activez l'inspection ESMTP.

Avant de commencer

Certaines options de correspondance de trafic utilisent des expressions régulières à des fins de correspondance. Si vous avez l'intention d'utiliser l'une de ces techniques, créez d'abord l'expression régulière ou la carte de trafic d'expressions régulières.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Cartes d'inspection)** > **ESMTP**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste pour afficher son contenu. Vous pouvez modifier le niveau de sécurité directement ou cliquer sur **Customize** (Personnaliser) pour modifier la liste. Le reste de la procédure suppose que vous personnalisez ou ajoutez une liste.

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de la modification d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Dans l'affichage **Security Level** (Niveau de sécurité) de la boîte de dialogue ESMTP Inspect Map (Liste d'inspection ESMTP), sélectionnez le niveau qui correspond le mieux à la configuration souhaitée.

Si l'un des niveaux prédéfinis correspond à vos exigences, vous avez maintenant terminé. Cliquez simplement sur **OK**, ignorez le reste de cette procédure et utilisez la liste dans une règle de politique de service pour l'inspection ESMTP.

Si vous devez personnaliser davantage les paramètres, cliquez sur **Details** (Détails) et poursuivez la procédure.

Astuces

Le bouton **MIME File Type Filtering** (Filtrage de type de fichier MIME) est un raccourci pour configurer l'inspection du type de fichier, qui est expliquée ultérieurement dans cette procédure.

Étape 5 Cliquez sur l'onglet **Parameters** (Paramètres) et configurez les options souhaitées.

- **Mask Server Banner** (Masquer la bannière du serveur) : indique s'il faut masquer la bannière du serveur ESMTP.
- **Encrypted Packet Inspection** (Inspection des paquets chiffrés) : indique s'il faut autoriser ESMTP sur TLS (connexions chiffrées) sans inspection. Vous pouvez éventuellement journaliser les connexions chiffrées. La valeur par défaut est d'autoriser les sessions TLS sans inspection. Si vous désélectionnez l'option, le système supprime l'indication STARTTLS de toute tentative de connexion de session chiffrée et force une connexion en texte brut.

Étape 6 Cliquez sur l'onglet **Filtering** (Filtrage) et configurez les options souhaitées.

- **Configure mail relay** (Configurer le relais de messagerie) : identifie un nom de domaine pour le relais de messagerie. Vous pouvez soit abandonner la connexion et éventuellement la journaliser, soit la journaliser.
- **Check for special characters** (Vérifier les caractères spéciaux) : identifie l'action à prendre pour les messages qui incluent les caractères spéciaux pipe (|), guillemet arrière et NUL dans les adresses courriel de l'expéditeur ou du destinataire. Vous pouvez soit abandonner la connexion et éventuellement la journaliser, soit la journaliser.

Étape 7 Cliquez sur l'onglet **Inspections** et définissez les inspections spécifiques que vous souhaitez mettre en œuvre en fonction des caractéristiques du trafic.

a) Effectuez l'une des actions suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter un nouveau critère.
- Sélectionnez un critère existant et cliquez sur **Edit** (Modifier).

b) Choisissez le type de correspondance pour les critères : **Match** (le trafic doit correspondre au critère) ou **No Match** (le trafic ne doit pas correspondre au critère). Par exemple, si No Match est sélectionné sur la chaîne « example.com », tout trafic contenant « example.com » est exclu de la carte de trafic. Configurez ensuite le critère :

- **Body Length** (Longueur du corps) : correspond aux messages où la longueur d'un message de corps ESMTP est supérieure au nombre d'octets spécifié.
- **Body Line Length** (Longueur de ligne du corps) : correspond aux messages où la longueur d'une ligne dans un message de corps ESMTP est supérieure au nombre d'octets spécifié.
- **Commands** (Commandes) : correspond au verbe de commande dans le message. Vous pouvez spécifier une ou plusieurs des commandes suivantes : auth, data, ehlo, etrn, helo, help, mail, noop, quit, rcpt, rset, saml, soml, vrfy.
- **Command Recipient Count** (Nombre de destinataires de commande) : correspond aux messages où le nombre de destinataires est supérieur au nombre spécifié.
- **Command Line Length** (Longueur de ligne de commande) : correspond aux messages où la longueur d'une ligne dans le verbe de commande est supérieure au nombre d'octets spécifié.
- **EHLO Reply Parameters** (Paramètres de réponse EHLO) : correspond aux paramètres de réponse EHLO ESMTP. Vous pouvez spécifier un ou plusieurs des paramètres suivants : 8bitmime, auth, binaryname, checkpoint, dsn, etrn, others, pipelining, size, vrfy.
- **Header Length** (Longueur de l'en-tête) : correspond aux messages où la longueur d'un en-tête ESMTP est supérieure au nombre d'octets spécifié.
- **Header Line Length** (Longueur de ligne de l'en-tête) : correspond aux messages où la longueur d'une ligne dans un en-tête ESMTP est supérieure au nombre d'octets spécifié.
- **Header To: Fields Count** (Nombre de champs To dans l'en-tête) : correspond aux messages où le nombre de champs To dans l'en-tête est supérieur au nombre spécifié.
- **Invalid Recipients Count** (Nombre de destinataires non valides) : correspond aux messages où le nombre de destinataires non valides est supérieur au nombre spécifié.
- **MIME File Type** (Type de fichier MIME) : correspond au type de fichier MIME ou média avec l'expression régulière ou la liste d'expressions régulières spécifiée.
- **MIME Filename Length** (Longueur du nom de fichier MIME) : correspond aux messages dans lesquels le nom de fichier est plus long que le nombre d'octets spécifié.
- **MIME Encoding** (Encodage MIME) : correspond au type d'encodage MIME. Vous pouvez spécifier un ou plusieurs des types suivants : 7bit, 8bit, base64, binary, others, quoted-printable.
- **Sender Address** (Adresse de l'expéditeur) : correspond à l'adresse courriel de l'expéditeur avec l'expression régulière ou la liste d'expressions régulières spécifiée.
- **Sender Address Length** (Longueur de l'adresse de l'expéditeur) : correspond aux messages dont l'adresse de l'expéditeur est supérieure au nombre d'octets spécifié.

c) Choisissez d'abandonner la connexion, de la réinitialiser ou de la journaliser. Pour abandonner la connexion et la réinitialisation, vous pouvez activer ou désactiver la journalisation. Pour la mise en correspondance de la commande et du paramètre de réponse EHLO, vous pouvez également masquer la commande. Pour la correspondance de commande, vous pouvez également appliquer une limite de débit en paquets par seconde.

d) Cliquez sur **OK** pour ajouter l'inspection. Répétez le processus au besoin.

Étape 8 Cliquez sur **OK** dans la boîte de dialogue de la liste d'inspection ESMTP.

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection ESMTP.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application.

Inspection SNMP

L'inspection des applications SNMP est appliquée à la fois au trafic vers le périphérique et au trafic traversant le périphérique. Cette inspection est nécessaire si vous configurez SNMP v3 où les utilisateurs sont limités à des hôtes SNMP spécifiques. Sans inspection, un utilisateur v3 défini peut interroger le périphérique à partir de n'importe quel hôte autorisé. L'inspection SNMP est activée par défaut pour les ports par défaut. Vous ne devez donc la configurer que si vous utilisez des ports autres que les ports par défaut. Les ports par défaut sont UDP/161, 162 (pour tous les types de périphériques) et UDP/4161 pour les périphériques qui exécutent également FXOS, car FXOS écoute sur UDP/161.

Par défaut, l'inspection SNMP limite l'interrogation à la version configurée.

Remarque Si vous configurez SNMP sur un périphérique qui exécute également FXOS, l'inspection SNMP est obligatoire et est réactivée si vous la désactivez. L'inspection SNMP est activée sur une classe de trafic qui comprend le port UDP/4161.

Vous pouvez également restreindre le trafic SNMP à une version particulière de SNMP. Les versions antérieures de SNMP sont moins sécurisées; par conséquent, le refus de certaines versions SNMP peut être requis par votre politique de sécurité. Le système peut refuser les versions SNMP 1, 2, 2c ou 3. Vous contrôlez les versions autorisées en créant une liste SNMP, comme expliqué ci-dessous. Si vous n'avez pas besoin de contrôler les versions, activez simplement l'inspection SNMP sans liste.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **SNMP**.

Étape 2 Cliquez sur **Add** (Ajouter), ou sélectionnez une liste et cliquez sur **Edit** (Modifier). Lors de l'ajout d'une liste, saisissez un nom de liste.

Étape 3 Sélectionnez les versions SNMP à refuser.

Étape 4 Cliquez sur **OK**.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application.

Inspection SQL*Net

L'inspection SQL*Net est activée par défaut. Le moteur d'inspection prend en charge les versions 1 et 2 de SQL*Net, mais uniquement le format Transparent Network Substrate (TNS). L'inspection ne prend pas en charge le format Tabular Data Stream (TDS). Les messages SQL*Net sont analysés pour rechercher les adresses et les ports intégrés, et la réécriture NAT est appliquée au besoin.

L'affectation de port par défaut pour SQL*Net est 1521. Il s'agit de la valeur utilisée par Oracle pour SQL*Net, mais cette valeur n'est pas conforme aux affectations de port IANA pour Structured Query Language (SQL). Si votre application utilise un port différent, appliquez l'inspection SQL*Net à une carte de trafic qui comprend ce port.

Désactiver l'inspection SQL*Net dans les cas suivants :

- Le transfert de données SQL se produit sur le même port que le port TCP de contrôle SQL 1521. Le périphérique de sécurité agit comme un serveur proxy lorsque l'inspection SQL*Net est activée et réduit la taille de la fenêtre client de 65 000 à environ 16 000, ce qui entraîne des problèmes de transfert de données.
- L'inspection de débits élevés de trafic SQL entraîne des pointes inacceptables dans l'utilisation du processeur.

Après avoir désactivé l'inspection SQL*Net, utilisez la commande **clear conn port 1521** pour que les connexions puissent être recréées sans inspection.

Pour en savoir plus sur l'activation de l'inspection SQL*Net, consultez Configurer l'inspection du protocole de couche d'application.

Inspection Sun RPC

Cette section décrit l'inspection des applications Sun RPC.

Aperçu de l'inspection Sun RPC

L'inspection du protocole Sun RPC est activée par défaut. Vous devez simplement gérer la table du serveur Sun RPC pour identifier les services autorisés à traverser le pare-feu. Cependant, l'ouverture dynamique de ports pour NFS est effectuée pour n'importe quel serveur, même sans configuration de la table du serveur.

Sun RPC est utilisé par NFS et NIS. Les services Sun RPC peuvent s'exécuter sur n'importe quel port. Lorsqu'un client tente d'accéder à un service Sun RPC sur un serveur, il doit connaître le port sur lequel le service est exécuté. Il le fait en interrogeant le processus de mappage de port, généralement rpcbind, sur le port bien connu de 111.

Le client envoie le numéro de programme Sun RPC du service et le processus de mappage de port répond en indiquant le numéro de port du service. Le client envoie ses requêtes Sun RPC au serveur, en précisant le port identifié par le processus de mappage de port. Lorsque le serveur répond, l'ASA intercepte ce paquet et ouvre les connexions TCP et UDP embryonnaires sur ce port.

La NAT ou la PAT des informations de charge utile Sun RPC n'est pas prise en charge.

Gérer les services Sun RPC

Utilisez la table des services Sun RPC pour contrôler le trafic de RPC en fonction des sessions de RPC établies.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **SUNRPC Server (Serveur SUNRPC)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter un nouveau serveur.
- Sélectionnez un serveur, puis cliquez sur **Edit** (Modifier).

Étape 3 Configurez les propriétés du service :

- **Interface Name** (Nom de l'interface) : interface par laquelle le trafic vers le serveur transite.
- **IP Address/Mask** (Adresse IP/Masque) : adresse du serveur Sun RPC.
- **Service ID (ID** de service) : type de service sur le serveur. Pour déterminer le type de service (par exemple, 100003), utilisez la commande **sunrpcinfo** dans la ligne de commande UNIX ou Linux sur la machine du serveur Sun RPC.
- **Protocol** (Protocole) : indique si le service utilise TCP ou UDP
- **Port/Port Range** (Port/Plage de ports) : port ou plage de ports utilisés par le service.
- **Timeout** (Délai d'expiration) : délai d'inactivité du passage ouvert pour la connexion par l'inspection Sun RPC.

Étape 4 Cliquez sur **OK**.

Étape 5 (Facultatif) Surveillez les passages créés pour ces services.

Pour afficher les passages ouverts pour les services Sun RPC, saisissez la commande **show sunrpc-server active**. Sélectionnez **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)** pour saisir la commande. Par exemple :

```
hostname# show sunrpc-server active
LOCAL FOREIGN SERVICE TIMEOUT
-----------------------------------------------
1 209.165.200.5/0 192.168.100.2/2049 100003 0:30:00
2 209.165.200.5/0 192.168.100.2/2049 100003 0:30:00
3 209.165.200.5/0 192.168.100.2/647 100005 0:30:00
4 209.165.200.5/0 192.168.100.2/650 100005 0:30:00
```

L'entrée dans la colonne LOCAL affiche l'adresse IP du client ou du serveur sur l'interface interne, tandis que la valeur dans la colonne FOREIGN affiche l'adresse IP du client ou du serveur sur l'interface externe.

Au besoin, vous pouvez effacer ces services à l'aide de **clear sunrpc-server active**

Inspection TFTP

L'inspection TFTP est activée par défaut.

TFTP, décrit dans la RFC 1350, est un protocole simple pour lire et écrire des fichiers entre un serveur TFTP et un client.

Le moteur d'inspection inspecte la demande de lecture (RRQ), la demande d'écriture (WRQ) et la notification d'erreur (ERROR) et crée dynamiquement des connexions et des traductions, au besoin, pour permettre le transfert de fichiers entre un client et un serveur TFTP.

Un canal secondaire dynamique et une traduction de PAT, le cas échéant, sont alloués lors de la réception d'une demande valide de lecture (RRQ) ou d'écriture (WRQ). Ce canal secondaire est ensuite utilisé par TFTP pour le transfert de fichiers ou la notification d'erreurs.

Seul le serveur TFTP peut initier le trafic sur le canal secondaire, et au plus un canal secondaire incomplet peut exister entre le client et le serveur TFTP. Une notification d'erreur du serveur ferme le canal secondaire.

L'inspection TFTP doit être activée si la PAT statique est utilisée pour rediriger le trafic TFTP.

Pour en savoir plus sur l'activation de l'inspection TFTP, consultez Configurer l'inspection du protocole de couche d'application.

Inspection XDMCP

XDMCP est un protocole qui utilise le port UDP 177 pour négocier les sessions X, qui utilisent TCP lorsqu'elles sont établies.

Pour une négociation réussie et le démarrage d'une session XWindows, l'ASA doit autoriser la connexion TCP de retour à partir de l'ordinateur hébergeant X. Pour autoriser la connexion de retour, vous pouvez utiliser des règles d'accès pour autoriser les ports TCP. Sinon, vous pouvez exécuter la commande **established** sur l'ASA. Une fois que XDMCP a négocié le port pour envoyer l'affichage, la commande **established** est consultée pour vérifier si cette connexion arrière doit être autorisée.

Pendant la session XWindows, le gestionnaire communique avec le serveur X d'affichage sur le port bien connu 6000 | n. Chaque affichage a une connexion distincte au serveur X, en raison du paramètre de terminal suivant.

```
setenv DISPLAY Xserver:n
```

où *n* est le numéro d'affichage.

Lorsque XDMCP est utilisé, l'affichage est négocié à l'aide d'adresses IP, sur lesquelles l'ASA peut appliquer la NAT si nécessaire. L'inspection XDMCP ne prend pas en charge la PAT.

Pour en savoir plus sur l'activation de l'inspection XDMCP, consultez Configurer l'inspection du protocole de couche d'application.

Inspection VXLAN

L'inspection du réseau local virtuel extensible (VXLAN) fonctionne sur le trafic encapsulé VXLAN qui passe par l'ASA. Il garantit que le format d'en-tête VXLAN est conforme aux normes, en abandonnant les paquets malformés. L'inspection VXLAN n'est pas effectuée sur le trafic pour lequel l'ASA agit comme point d'extrémité de tunnel VXLAN (VTEP) ou passerelle VXLAN, car ces vérifications sont effectuées dans le cadre normal de la désencapsulation des paquets VXLAN.

Les paquets VXLAN sont UDP, normalement sur le port 4789. Ce port fait partie de la classe par défaut-inspection-trafic, vous pouvez donc simplement ajouter l'inspection VXLAN à la règle de politique de service inspection_default. Vous pouvez également créer une carte de trafic pour celui-ci en utilisant la mise en correspondance de port ou d'ACL.

Historique de l'inspection du protocole Internet de base

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge de l'inspection DCERPC pour le message UUID ISystemMapper, RemoteGetClassObject opnum3.	9.4(1)	L'ASA a commencé à prendre en charge les messages DCERPC non EPM dans la version 8.3, en prenant en charge le message UUID ISystemMapper, RemoteCreateInstance opnum4. Cette modification étend la prise en charge au message RemoteGetClassObject opnum3. Nous n'avons pas modifié d'écrans ASDM.
Inspection des paquets VXLAN	9.4(1)	L'ASA peut inspecter l'en-tête VXLAN pour faire respecter le format standard. Nous avons modifié l'écran suivant : **Configuration > Firewall (Pare-feu) > Service Policy Rules (Règles de politique de service) > Add Service Policy Rule (Ajouter une règle de politique de service) > Rule Actions (Actions découlant d'une règle) > Protocol Inspection (Inspection de protocole)**
L'inspection ESMTP change de comportement par défaut pour les sessions TLS.	9.4(1)	La valeur par défaut pour l'inspection ESMTP a été modifiée pour autoriser les sessions TLS, qui ne sont pas inspectées. Cependant, cette valeur par défaut s'applique aux systèmes nouveaux ou recréés. Si vous mettez à niveau un système qui inclut **no allow-tls**, la commande n'est pas modifiée. Le changement de comportement par défaut a également été apporté dans ces anciennes versions : 8.4(7.25), 8.5(1.23), 8.6(1.16), 8.7(1.15), 9.0(4.28), 9.1(6.1), 9.2(3.2) 9.3(1.2), 9.3(2.2).

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Améliorations de l'inspection des options d'IP	9.5(1)	L'inspection des options IP prend désormais en charge toutes les options IP possibles. Vous pouvez régler l'inspection pour autoriser, effacer ou abandonner toutes les options standard ou expérimentales, y compris celles non encore définies. Vous pouvez également définir un comportement par défaut pour les options non définies explicitement dans une carte d'inspection des options IP. Nous avons modifié la boîte de dialogue IP Options Inspect Map (Liste d'inspection des options IP) afin d'inclure des options supplémentaires. Vous sélectionnez maintenant les options à autoriser et éventuellement à effacer.
Améliorations de l'inspection DCERPC et du filtrage des UUID	9.5(2)	L'inspection DCERPC prend désormais en charge la NAT pour les messages opnum5 d'OxidResolver ServerAlive2. Vous pouvez également filtrer les identifiants universels (UUID) des messages DCERPC pour réinitialiser ou enregistrer des types de messages particuliers. Il existe une nouvelle carte des classes d'inspection DCERPC pour le filtrage des UUID. Nous avons ajouté l'écran suivant : **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Class Maps (Cartes de trafic)** > **DCERPC**. Nous avons modifié l'écran suivant : **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Cartes d'inspection)** > **DCERPC**.
Inspection DNS sur TCP	9.6(2)	Vous pouvez désormais inspecter le trafic DNS sur TCP (TCP/53). Nous avons modifié la page suivante : **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspection Maps (Cartes d'inspection)** > **DNS** Add/Edit dialog box (Boîte de dialogue Ajouter/modifier)
Prise en charge de Cisco Umbrella	9.10(1)	Vous pouvez configurer le périphérique pour rediriger les requêtes DNS vers Cisco Umbrella, afin que votre politique de sécurité d'entreprise définie dans Cisco Umbrella puisse être appliquée aux connexions des utilisateurs. Vous pouvez autoriser ou bloquer les connexions en fonction du FQDN ou, pour les FQDN suspects, vous pouvez rediriger l'utilisateur vers le mandataire intelligent Cisco Umbrella, qui peut effectuer le filtrage d'URL. La configuration de Cisco Umbrella fait partie de la politique d'inspection DNS. Écrans nouveaux ou modifiés : **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Cisco Umbrella**, **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **DNS**.

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Améliorations de Cisco Umbrella.	9.12(1)	Vous pouvez maintenant identifier les noms de domaine locaux qui doivent contourner Cisco Umbrella. Les demandes DNS pour ces domaines sont directement transmises aux serveurs DNS sans passer par Cisco Umbrella. Vous pouvez également identifier les serveurs Cisco Umbrella à utiliser pour la résolution des demandes DNS. Enfin, vous pouvez définir la politique d'inspection de Cisco Umbrella pour qu'elle s'ouvre même en cas de non-conformité, afin que les demandes DNS ne soient pas bloquées si le serveur Cisco Umbrella n'est pas disponible. Nous avons modifié les écrans suivants : **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Cisco Umbrella**, **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **DNS**.
Inspection XDMCP désactivée par défaut dans les nouvelles installations.	9.15(1)	Auparavant, l'inspection XDMCP était activée par défaut pour tout le trafic. Désormais, sur les nouvelles installations, qui comprennent les nouveaux systèmes et les systèmes recréés, XDMCP est désactivé par défaut. Si vous avez besoin de cette inspection, veuillez l'activer. Notez que lors des mises à niveau, vos paramètres actuels pour l'inspection XDMCP sont conservés, même si vous les aviez simplement activés via les paramètres d'inspection par défaut.

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.