

Premiers pas avec l'inspection du protocole de la couche application

Les rubriques suivantes décrivent comment configurer l'inspection du protocole de couche d'application.

- Inspection des protocoles de la couche applicative, à la page 1
- Configurer l'inspection du protocole de couche d'application, à la page 9
- Configurer les expressions régulières, à la page 13
- Surveillance des politiques d'inspection, à la page 18
- Historique de l'inspection des applications, à la page 19

Inspection des protocoles de la couche applicative

Des plateformes d'inspection sont nécessaires pour les services qui intègrent des renseignements d'adressage IP dans le paquet de données des utilisateurs ou qui ouvrent des canaux secondaires sur des ports attribués de manière dynamique. Ces protocoles obligent l'ASA à effectuer une inspection approfondie des paquets au lieu de transmettre le paquet par le chemin rapide. Par conséquent, les moteurs d'inspection peuvent avoir une incidence sur le débit global. Plusieurs moteurs d'inspection courants sont activés sur l'ASA par défaut, mais vous devrez peut-être en activer d'autres en fonction de votre réseau.

Les rubriques suivantes expliquent l'inspection des applications plus en détail.

Quand utiliser l'inspection du protocole d'application

Lorsqu'un utilisateur établit une connexion, l'ASA vérifie le paquet par rapport aux ACL, crée une traduction d'adresses et crée une entrée pour la session dans le chemin rapide, afin que d'autres paquets puissent contourner les vérifications chronophages. Cependant, le chemin rapide repose sur des numéros de port prévisibles et n'effectue pas de traduction d'adresses dans un paquet.

De nombreux protocoles ouvrent des ports TCP ou UDP secondaires. La session initiale sur un port bien connu est utilisée pour négocier les numéros de port attribués dynamiquement.

D'autres applications intègrent une adresse IP dans le paquet qui doit correspondre à l'adresse source normalement traduite lorsqu'elle passe par l'ASA.

Si vous utilisez des applications comme celles-ci, vous devez activer l'inspection des applications.

Lorsque vous activez l'inspection des applications pour un service qui intègre les adresses IP, l'ASA traduit les adresses intégrées et met à jour la somme de contrôle ou les autres champs affectés par la traduction.

Lorsque vous activez l'inspection des applications pour un service qui utilise des ports affectés dynamiquement, l'ASA surveille les sessions pour identifier les affectations de ports dynamiques et permet l'échange de données sur ces ports pour la durée de la session spécifique.

Listes des politiques d'inspection

Vous pouvez configurer des actions spéciales pour de nombreuses inspection d'application à l'aide d'une *liste des politiques d'inspection*. Ces listes sont facultatives : vous pouvez activer l'inspection pour un protocole qui prend en charge les listes des politiques d'inspection sans configurer de liste. Ces listes sont nécessaires uniquement si vous souhaitez autre chose que les actions d'inspection par défaut.

Une liste des politiques d'inspection comprend un ou plusieurs des éléments suivants. Les options exactes disponibles pour une liste des politiques d'inspection dépendent de l'application.

- Critères de correspondance du trafic : vous faites correspondre le trafic d'application à des critères spécifiques à l'application, tels qu'une chaîne d'URL, pour laquelle vous activez ensuite les actions.

  Pour certains critères de correspondance de trafic, vous utilisez des expressions régulières pour faire correspondre le texte à l'intérieur d'un paquet. Assurez-vous de créer et de tester les expressions régulières avant de configurer la liste des politiques, qu'elles soient uniques ou regroupées dans une carte de trafic d'expression régulière.

- Carte de trafic d'inspection : certaines listes des politiques d'inspection vous permettent d'utiliser une carte de trafic d'inspection pour inclure plusieurs critères de correspondance de trafic. Vous identifiez ensuite la carte de trafic d'inspection dans la liste des politiques d'inspection et activez les actions pour la carte dans son ensemble. 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 créer des critères de correspondance plus complexes et que vous pouvez réutiliser les cartes de trafic. Cependant, vous ne pouvez pas définir différentes actions pour différentes correspondances.

- Paramètres : les paramètres affectent le comportement du moteur d'inspection.

Pour plus d'informations, consultez les rubriques suivantes.

Remplacement d'une liste des politiques d'inspection en cours d'utilisation

Si une inspection est activée avec une liste des politiques dans une politique de service, le remplacement de la liste des politiques est un processus en deux étapes. Vous devez d'abord supprimer l'inspection de la politique de service et appliquer les modifications. Ensuite, vous le rajoutez, sélectionnez le nouveau nom de liste des politiques et appliquez à nouveau les modifications.

Comment plusieurs classes de trafic sont gérées

Vous pouvez spécifier plusieurs mappages de classes d'inspection ou correspondances directes dans la carte de politique d'inspection.

Si un paquet correspond à plusieurs classes différentes ou correspondances directes, l'ordre dans lequel l'ASA applique les actions est déterminé par les règles ASA internes, et non par l'ordre dans lequel elles sont ajoutées à la carte des politiques d'inspection. Les règles internes sont déterminées par le type d'application et la progression logique de l'analyse d'un paquet, et ne sont pas configurables par l'utilisateur. Par exemple, pour le trafic HTTP, l'analyse d'un champ méthode de requête précède l'analyse du champ Longueur de l'hôte d'en-tête ; une action pour le champ méthode de requête se produit avant l'action pour le champ Longueur de l'hôte d'en-tête.

Si une action abandonne un paquet, aucune autre action n'est effectuée dans la liste des politiques d'inspection. Par exemple, si la première action est de réinitialiser la connexion, elle ne correspondra jamais à d'autres critères de correspondance. Si la première action consiste à journaliser le paquet, une deuxième action, telle que la réinitialisation de la connexion, peut se produire.

Si un paquet correspond à plusieurs critères de correspondance qui sont identiques, ils sont mis en correspondance dans l'ordre dans lequel ils apparaissent dans la liste des politiques.

Une carte de trafic est déterminée comme étant du même type qu'une autre carte de trafic ou une correspondance directe en fonction de l'option de correspondance de priorité la plus basse dans la carte de trafic (la priorité est basée sur les règles internes). Si une carte de trafic a le même type d'option de correspondance de priorité la plus basse qu'une autre carte de trafic, les cartes de trafic sont mises en correspondance en fonction de l'ordre dans lequel elles sont ajoutées à la liste des politiques. Si la correspondance de priorité la plus basse pour chaque mappage de carte est différente, la carte de trafic avec l'option de correspondance de priorité la plus élevée est mise en correspondance en premier.

Lignes directrices relatives à l'inspection des applications

Basculement

Les informations d'état pour les sessions multimédias qui nécessitent une inspection ne sont pas transmises sur la liaison d'état pour le basculement dynamique. Les exceptions sont GTP, M3UA et SIP, qui sont répliquées sur la liaison d'état. Vous devez configurer la vérification stricte de l'état du processus de serveur d'applications (ASP) dans l'inspection M3UA pour obtenir un basculement dynamique.

Mise en grappes

Les inspections suivantes ne sont pas prises en charge dans le regroupement :

- CTIQBE
- H323, H225 et RAS
- Intercommunication IPsec
- MGCP
- MMP
- RTSP
- SCCP (Skinny)
- WAAS

IPv6

Prend en charge IPv6 pour les inspections suivantes :

- Diamètre
- DNS sur UDP
- FTP
- GTP

- HTTP
- ICMP
- Intercommunication IPsec
- IPv6
- M3UA
- SCCP (Skinny)
- SCTP
- SIP
- SMTP
- VXLAN

Prend en charge NAT64 pour les inspections suivantes :

- DNS sur UDP
- FTP
- HTTP
- ICMP
- SCTP

Directives supplémentaires

- Certains moteurs d'inspection ne prennent pas en charge la PAT, la NAT, la NAT externe ou la NAT entre les mêmes interfaces de sécurité. Pour plus d'informations sur la prise en charge de la NAT, consultez Inspections par défaut et limites de la NAT, à la page 5.
- Pour toutes les inspections d'application, l'ASA limite le nombre de connexions de données actives simultanées à 200 connexions. Par exemple, si un client FTP ouvre plusieurs connexions secondaires, le moteur d'inspection FTP n'autorise que 200 connexions actives et la connexion 201 est abandonnée et l'appliance de sécurité adaptative génère un message d'erreur du système.
- Les protocoles inspectés sont soumis à un suivi avancé de l'état TCP, et l'état TCP de ces connexions n'est pas automatiquement répliqué. Pendant que ces connexions sont répliquées sur l'unité de secours, il y a une tentative au mieux pour rétablir un état TCP.
- Si le système détermine qu'une connexion TCP nécessite une inspection, le système efface toutes les options TCP, à l'exception des options MSS et de réception sélective (SACK) sur les paquets avant de les inspecter. Les autres options sont effacées même si vous les autorisez dans une liste TCP appliquée aux connexions.
- Le trafic TCP/UDP dirigé vers l'ASA (vers une interface) est inspecté par défaut. Cependant, le trafic ICMP dirigé vers une interface 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.

Valeurs par défaut pour l'inspection des applications

Les rubriques suivantes expliquent les opérations par défaut pour l'inspection des applications.

Inspections par défaut et limites de la NAT

Par défaut, la configuration comprend une politique qui correspond à tout le trafic d'inspection d'application par défaut et applique l'inspection au trafic sur toutes les interfaces (politique globale). Le trafic d'inspection des applications par défaut comprend le trafic vers les ports par défaut pour chaque protocole. Vous ne pouvez appliquer qu'une seule politique globale. Par conséquent, si vous souhaitez modifier la politique globale, par exemple, pour appliquer une inspection aux ports non standard ou pour ajouter des inspections qui ne sont pas activées par défaut, vous devez modifier la politique par défaut, ou désactivez-le et appliquez-en un nouveau.

Le tableau suivant répertorie toutes les inspections prises en charge, les ports par défaut utilisés dans la carte de trafic par défaut et les moteurs d'inspection qui sont activés par défaut, qui sont en gras. Ce tableau indique également toutes les limites de la NAT. Dans ce tableau :

- Les moteurs d'inspection activés par défaut pour le port par défaut sont en gras.
- L'ASA est conforme aux normes indiquées, mais il n'applique pas la conformité aux paquets inspectés. Par exemple, les commandes FTP sont censées être dans un ordre particulier, mais l'ASA ne fait pas respecter l'ordre.

Tableau 1 : Moteurs d'inspection d'applications pris en charge

Application	Protocole, port par défaut	Limites de la NAT	Normes	Commentaires
CTIQBE	TCP/2748	Pas de PAT étendue. No NAT64. (Mise en grappe) Pas de PAT statique.	—	—
DCERPC	TCP/135	No NAT64.	—	—
Diamètre	TCP/3868 TCP/5868 (pour TCP/TLS) SCTP/3868	Pas de NAT / PAT.	RFC 6733	Nécessite la licence Carrier (exploitant).
DNS sur UDP DNS sur TCP	UDP/53 UDP/443 TCP/53	Aucune prise en charge de NAT n'est disponible pour la résolution de nom par le biais de WINS.	RFC 1123	Vous devez activer l'inspection DNS/TCP dans la liste des politiques d'inspection DNS pour inspecter le DNS sur TCP. UDP/443 est utilisé uniquement pour les sessions DNScrypt de Cisco Umbrella.
FTP	TCP/21	(Mise en grappe) Pas de PAT statique.	RFC 959	—

Application	Protocole, port par défaut	Limites de la NAT	Normes	Commentaires
GTP	UDP/3386 (GTPv0) UDP/2123 (GTPv1+)	Pas de PAT étendue. Pas de NAT.	—	Nécessite la licence Carrier (exploitant).
H.323 H.225 et **RAS**	TCP/1720 UDP/1718 UDP (RAS) 1718-1719	(Mise en grappe) Pas de PAT statique. Pas de PAT étendue. Pas de NAT sur les mêmes interfaces de sécurité. No NAT64.	ITU-T H.323, H.245, H225.0, Q.931, Q.932	—
HTTP	TCP/80	—	RFC 2616	Méfiez-vous des limites de la MTU en supprimant ActiveX et Java. Si la MTU est trop faible pour permettre à la balise Java ou ActiveX d'être incluse dans un paquet, il se peut que le stripping (suppression) ne se produise pas.
ICMP	ICMP	—	—	Le trafic ICMP dirigé vers une interface ASA n'est jamais inspecté.
ERREUR ICMP	ICMP	—	—	—
ILS (LDAP)	TCP/389	Pas de PAT étendue. No NAT64.	—	—
Messagerie instantanée (IM)	Varie selon le client	Pas de PAT étendue. No NAT64.	RFC 3860	—
Options d'adresse IP	RSVP	No NAT64.	RFC 791, RFC 2113	—
Intercommunication IPsec	UDP/500	Pas de PAT No NAT64.	—	—
IPv6	—	No NAT64.	RFC 2460	—
LISP	—	Pas de NAT ou PAT.	—	—
M3UA	SCTP/2905	Pas de NAT ou PAT pour les adresses intégrées.	RFC 4666	Nécessite la licence Carrier (exploitant).

Application	Protocole, port par défaut	Limites de la NAT	Normes	Commentaires
MGCP	UDP/2427, 2727	Pas de PAT étendue. No NAT64. (Mise en grappe) Pas de PAT statique.	RFC 2705bis-05	—
MMP	TCP/5443	Pas de PAT étendue. No NAT64.	—	—
Serveur de noms NetBIOS sur IP	UDP/137, 138 (ports sources)	Pas de PAT étendue. No NAT64.	—	NetBIOS est pris en charge par l'exécution de la NAT des paquets pour le port UDP 138 du service NBNS et le port UDP 138.
PPTP	TCP/1723	No NAT64. (Mise en grappe) Pas de PAT statique.	RFC 2637	—
Gestion des comptes RADIUS	UDP/1646	No NAT64.	RFC 2865	—
RSH	TCP/514	Pas de PAT No NAT64. (Mise en grappe) Pas de PAT statique.	Berkeley UNIX	—
RTSP	TCP/554	Pas de PAT étendue. No NAT64. (Mise en grappe) Pas de PAT statique.	RFC 2326, 2327, 1889	Aucun traitement pour le masquage HTTP.
SCTP	SCTP	—	RFC 4960	Nécessite la licence Carrier (exploitant). Bien que vous puissiez effectuer une NAT d'objet réseau statique sur le trafic SCTP (sans NAT ni PAT dynamique), le moteur d'inspection n'est pas utilisé pour la NAT.

Application	Protocole, port par défaut	Limites de la NAT	Normes	Commentaires
SIP	TCP/5060 UDP/5060	Pas de NAT/PAT sur les interfaces avec des niveaux de sécurité identiques ou inférieurs ou supérieurs. Pas de PAT étendue. Pas de NAT64 ou NAT46. (Mise en grappe) Pas de PAT statique.	RFC 2543	Ne gère pas les configurations de téléphones IP Cisco téléchargées par TFTP dans certaines circonstances.
SKINNY (SCCP)	TCP/2000	Pas de NAT sur les mêmes interfaces de sécurité. Pas de PAT étendue. Pas de NAT64, NAT46 ou NAT66. (Mise en grappe) Pas de PAT statique.	—	Ne gère pas les configurations de téléphones IP Cisco téléchargées par TFTP dans certaines circonstances.
SMTP et **ESMTP**	TCP/25	No NAT64.	RFC 821, 1123	—
SNMP	UDP/161, 162 UDP/4161 sur les plateformes qui exécutent également Secure Firewall eXtensible Operating System (FXOS).	Pas de NAT ou PAT.	RFC 1155, 1157, 1212, 1213, 1215	v.2 RFC 1902-1908; v.3 RFC 2570-2580. Sur les plateformes FXOS, si vous configurez SNMP, cette inspection est activée automatiquement et vous ne pouvez pas la désactiver.
SQL*Net	TCP/1521	Pas de PAT étendue. No NAT64. (Mise en grappe) Pas de PAT statique.	—	v.1 et v.2.
STUN	TCP/3478 UDP/3478	(WebRTC) NAT statique/PAT44 uniquement. (Cisco Spark) NAT/PAT 44 et 64 statiques; et NAT/PAT dynamique.	RFC 5245, 5389	—
Sun RPC	TCP/111 UDP/111	Pas de PAT étendue. No NAT64.	—	—

Application	Protocole, port par défaut	Limites de la NAT	Normes	Commentaires
TFTP	UDP/69	No NAT64. (Mise en grappe) Pas de PAT statique.	RFC 1350	Les adresses IP de charge utile ne sont pas traduites.
WAAS	TCP/1- 65535	Pas de PAT étendue. No NAT64.	—	—
XDMCP	UDP/177	Pas de PAT étendue. No NAT64. (Mise en grappe) Pas de PAT statique.	—	—
VXLAN	UDP/4789	Sans objet	RFC 7348	Réseau local extensible virtuel.

Listes des politiques d'inspection par défaut

Certains types d'inspection utilisent des listes des politiques par défaut masquées. Par exemple, si vous activez l'inspection ESMTP sans préciser de liste, _default_esmtp_map est utilisé.

L'inspection par défaut est décrite dans les sections qui expliquent chaque type d'inspection. Vous pouvez afficher ces listes par défaut à l'aide de la commande **show running-config all policy-map** ; utilisez **Tools (Outils) > Command Line Interface (Interface de ligne de commande)**.

L'inspection DNS est la seule à utiliser une liste par défaut configurée explicitement, preset_dns_map.

Configurer l'inspection du protocole de couche d'application

Vous configurez l'inspection des applications dans les politiques de service.

L'inspection est activée par défaut globalement sur toutes les interfaces pour certaines applications sur leurs ports et protocoles standard. Consultez Inspections par défaut et limites de la NAT, à la page 5 pour obtenir plus d'informations sur les inspections par défaut. Une méthode courante pour personnaliser la configuration d'inspection consiste à personnaliser la politique globale par défaut. Vous pouvez également créer une nouvelle politique de service comme vous le souhaitez, par exemple, une politique spécifique à l'interface.

Avant de commencer

Pour certaines applications, vous pouvez effectuer des actions particulières lorsque vous activez l'inspection en configurant des listes des politiques d'inspection. Le tableau présenté plus loin dans cette procédure indique les protocoles qui prennent en charge les listes des politiques d'inspection et renvoie aux instructions permettant de les configurer. Si vous souhaitez configurer ces fonctionnalités avancées, créez la liste avant de configurer l'inspection.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)**.

Étape 2 Ouvrez une règle.

- Pour modifier la politique globale par défaut, sélectionnez la règle « inspection_default » dans le dossier Global, puis cliquez sur **« Edit »** (Modifier).
- Pour créer une nouvelle règle, cliquez sur **Add (Ajouter) > Add Service Policy Rule (Ajouter une règle de politique de service)**. Passez par l'assistant jusqu'à la page Rules (Règles).
- Si vous avez une autre règle d'inspection ou une règle à laquelle vous ajoutez une inspection, sélectionnez-la et cliquez sur **Edit** (Modifier).

Si vous souhaitez faire correspondre des ports non standard, créez une nouvelle règle pour les ports non standard. Consultez Inspections par défaut et limites de la NAT, à la page 5 pour connaître les ports standard de chaque moteur d'inspection.

Vous pouvez combiner plusieurs règles dans la même politique de service si vous le souhaitez, de sorte que vous pouvez créer une règle pour faire correspondre un certain trafic et une autre pour faire correspondre un trafic différent. Toutefois, si le trafic correspond à une règle qui contient une action d'inspection, puis correspond à une autre règle qui a également une action d'inspection, seule la première règle correspondante est utilisée.

Si vous mettez en œuvre l'inspection de comptabilité RADIUS, créez plutôt une règle de politique de service de gestion. Consultez Configurer l'inspection de comptabilité RADIUS.

Étape 3 Sur la page ou l'onglet de l'assistant Rule Actions (Actions de règle), sélectionnez l'onglet Protocol Inspection **(Inspection du protocole)** .

Étape 4 (Pour modifier une politique en cours d'utilisation) Si vous modifiez une politique en cours d'utilisation pour utiliser une liste des politiques d'inspection différente, vous devez désactiver l'inspection, puis la réactiver avec le nouveau nom de liste des politiques d'inspection :

a) Décochez la case du protocole.
b) Cliquez sur **OK** .
c) Cliquez sur **Apply** (Appliquer).
d) Répétez ces étapes pour revenir à l'onglet **Protocol Inspection** (Inspection de protocole).

Étape 5 Sélectionnez le type d'inspection que vous souhaitez appliquer.

Vous pouvez sélectionner plusieurs options dans la classes de trafic d'inspection par défaut uniquement.

Certains moteurs d'inspection vous permettent de contrôler des paramètres supplémentaires lorsque vous appliquez l'inspection au trafic. Cliquez sur (Configure) (**Configurer**) pour le type d'inspection afin de configurer une liste des politiques d'inspection et d'autres options. Vous pouvez choisir une liste des politiques d'inspection existante ou en créer une nouvelle. Vous pouvez prédéfinir des listes des politiques d'inspection à partir de **Configuration > Firewall > Objects > Inspect Maps** (Configuration > Pare-feu > Objets > Listes d'inspection).

Le tableau suivant répertorie les protocoles que vous pouvez inspecter, qu'ils autorisent l'inspection des listes des politiques ou des cartes de trafics d'inspection, et un pointeur vers des informations détaillées sur l'inspection.

Tableau 2 : Protocoles d'inspection

Protocole	Prend en charge les listes des politiques d'inspection	Prend en charge les cartes de trafics d'inspection	Notes
CTIQBE	Non	Non	Consultez Inspection CTIQBE .
DCERPC	Oui	Oui	Consultez Inspection DCERPC .
Diamètre	Oui	Oui	Consultez Inspection Diameter. Si vous souhaitez inspecter le trafic Diameter chiffré, choisissez **Enable encrypted traffic inspection** (Activer l'inspection du trafic chiffré) et sélectionnez un proxy TLS (cliquez sur **Manage** (Gérer) pour en créer un si nécessaire).
DNS	Oui	Oui	Consultez Inspection DNS . Si vous utilisez le filtre de trafic de réseau de zombies, choisissez **Enable DNS snooping** (Activer la surveillance DNS). Nous vous suggérons d'activer la surveillance DNS uniquement sur les interfaces vers lesquelles des demandes DNS externes sont transmises. L'activation de la surveillance DNS sur tout le trafic DNS UDP, y compris celui vers un serveur DNS interne, crée une charge inutile sur l'ASA. Par exemple, si le serveur DNS se trouve sur l'interface externe, vous devez activer l'inspection DNS avec surveillance pour tout le trafic DNS UDP sur l'interface externe.
ESMTP	Oui	Non	Consultez Inspection SMTP et SMTP étendue .
FTP	Oui	Oui	Consultez Inspection FTP . Sélectionnez **Use Strict FTP** (Utiliser le protocole FTP strict) pour sélectionner une liste des politiques d'inspection. Le protocole FTP strict augmente la sécurité des réseaux protégés en empêchant les navigateurs Web d'envoyer des commandes intégrées dans les demandes FTP.
GTP	Oui	Non	Consultez Présentation de l'inspection GTP.
H.323 H.225	Oui	Oui	Consultez Inspection H.323 .
H.323 RAS	Oui	Oui	Consultez Inspection H.323 .
HTTP	Oui	Oui	Consultez Inspection HTTP .
ICMP	Non	Non	Consultez Inspection ICMP .

Protocole	Prend en charge les listes des politiques d'inspection	Prend en charge les cartes de trafics d'inspection	Notes
Erreur ICMP	Non	Non	Consultez Inspection des erreurs ICMP .
ILS	Non	Non	Consultez Inspection ILS .
IM	Oui	Oui	Consultez Inspection de la messagerie instantanée .
IP-Options	Oui	Non	Consultez Inspection des options IP .
IPSec Pass Thru	Oui	Non	Consultez Inspection IPsec Pass Through .
IPv6	Oui	Non	Consultez Inspection IPv6 .
LISP	Oui	Non	Pour des informations détaillées sur la configuration de LISP, y compris l'inspection, consultez le chapitre sur la mise en grappe dans le guide de configuration général.
M3UA	Oui	Non	Consultez Inspection M3UA.
MGCP	Oui	Non	Consultez Inspection MGCP .
NetBIOS	Oui	Non	Consultez Inspection NetBIOS .
PPTP	Non	Non	Consultez Inspection PPTP .
Gestion des comptes RADIUS	Oui	Non	Consultez Aperçu de l'inspection de comptabilité RADIUS. L'inspection de comptabilité RADIUS est disponible pour une politique de service de gestion uniquement. Vous devez sélectionner une liste des politiques pour mettre en œuvre cette inspection.
RSH	Non	Non	Consultez Inspection RSH .
RTSP	Oui	Non	Consultez Inspection RTSP .
SCCP (Skinny)	Oui	Non	Consultez Inspection Skinny (SCCP) .
SCTP	Oui	Non	Consultez Inspection de la couche application SCTP .
SIP	Oui	Oui	Consultez Inspection SIP . Si vous souhaitez inspecter le trafic SIP chiffré, choisissez **Enable encrypted traffic inspection** (Activer l'inspection du trafic chiffré) et sélectionnez un proxy TLS (cliquez sur **Manage** (Gérer) pour en créer un, le cas échéant).
SNMP	Oui	Non	Consultez Inspection SNMP .

Protocole	Prend en charge les listes des politiques d'inspection	Prend en charge les cartes de trafics d'inspection	Notes
SQLNET	Non	Non	Consultez Inspection SQL*Net .
STUN	Non	Non	Consultez Inspection STUN.
SunRPC	Non	Non	Consultez Inspection Sun RPC . La carte de trafic par défaut comprend le port UDP 111 ; Si vous souhaitez activer l'inspection SUNRPC pour le port TCP 111, vous devez créer une nouvelle carte de trafic qui correspond au port TCP 111, ajouter la carte à la politique, puis appliquer l'inspection SUNRPC à cette carte.
TFTP	Non	Non	Consultez Inspection TFTP .
WAAS	Non	Non	Active l'analyse TCP de l'option 33. À utiliser lors du déploiement des produits de services d'applications pour zone étendue.
XDMCP	Non	Non	Consultez Inspection XDMCP .
VXLAN	Non	Non	Consultez Inspection VXLAN .

Étape 6 Cliquez sur **OK** ou **Finish** (Terminer) pour enregistrer la règle de politique de service.

Configurer les expressions régulières

Les expressions régulières définissent la mise en correspondance de modèles pour les chaînes de texte. Vous pouvez utiliser ces expressions dans certaines listes d'inspection de protocoles pour faire correspondre les paquets en fonction de chaînes telles que les URL ou le contenu de champs d'en-tête particuliers.

Créer une expression régulière

Une expression régulière correspond aux chaînes de texte soit littéralement en tant que chaînes exacte, soit en utilisant des *métacaractères* afin que vous puissiez mettre en correspondance plusieurs variantes d'une chaîne de texte. Vous pouvez utiliser une expression régulière pour mettre en correspondance le contenu de certains trafics d'application; par exemple, vous pouvez mettre en correspondance une chaîne d'URL dans un paquet HTTP.

Avant de commencer

Consultez la commande **regex** dans la référence de commande pour obtenir des renseignements sur l'incidence sur les performances lors de la mise en correspondance d'une expression régulière et de paquets. En général,

la mise en correspondance avec de longues chaînes d'entrée ou la tentative de mise en correspondance d'un grand nombre d'expressions régulières réduira les performances du système.

Remarque En tant qu'optimisation, l'ASA recherche sur l'URL désobfusquée. La désobfuscation compresse plusieurs barres obliques (/) en une seule barre oblique. Pour les chaînes qui utilisent couramment des barres obliques doubles, comme « http:// », veillez à rechercher « http:/ » à la place.

Le tableau suivant répertorie les métacaractères qui ont des significations particulières.

Tableau 3 : Métacaractères d'expressions régulières

Caractères	Description	Remarques
.	Point	Correspond à un caractère unique. Par exemple, **d.g** correspond à dog, dag, dtg et à tout mot qui contient ces caractères, tel que doggonnit.
(*exp*)	Sous-expression	Une sous-expression sépare les caractères des caractères environnants, afin que vous puissiez utiliser d'autres métacaractères sur la sous-expression. Par exemple, **d(o|a)g** correspond à dog et dag, mais **do|ag** correspond à do et ag. Une sous-expression peut également être utilisée avec des quantificateurs de répétition pour différencier les caractères destinés à la répétition. Par exemple, **ab(xy){3}z** correspond à abxyxyxyz.
|	Alternance	Correspond à l'une ou l'autre des expressions qu'il sépare. Par exemple, **dog|cat** correspond à dog ou cat.
?	Point d'interrogation	Un quantificateur qui indique qu'il y a 0 ou 1 de l'expression précédente. Par exemple, **lo?se** correspond à lse ou lose.
*	Astérisque	Un quantificateur qui indique qu'il y a 0, 1 ou n'importe quel nombre de l'expression précédente. Par exemple, **lo*se** correspond à lse, lose, loose, etc.
+	Plus	Un quantificateur qui indique qu'il y a au moins 1 de l'expression précédente. Par exemple, **lo+se** correspond à lose et loose, mais pas à lse.
{*x*} ou {*x*,}	Quantificateur de répétition minimal	Répétez au moins *x* fois. Par exemple, **ab(xy){2,}z** correspond à abxyxyz, abxyxyxyz, etc.
[*abc*]	Classe de caractères	Correspond à l'un des caractères entre crochets. Par exemple, **[abc]** correspond à a, b ou c.

Caractères	Description	Remarques
[^*abc*]	Classe de caractère négative	Correspond à un seul caractère qui n'est pas contenu dans les crochets. Par exemple, **[^abc]** correspond à tout caractère autre que a, b ou c. **[^A-Z]** correspond à tout caractère qui n'est pas une lettre majuscule.
[*a-c*]	Classe de plage de caractères	Correspond à n'importe quel caractère dans la plage. **[a-z]** correspond à n'importe quelle lettre minuscule. Vous pouvez combiner les caractères et les plages : **[abcq-z]** correspond à a, b, c, q, r, s, t, u, v, w, x, y, z, de même que [**a-cq-z]**. Le caractère de tiret (-) est littéral uniquement s'il s'agit du dernier ou du premier caractère entre crochets : **[abc-]** ou **[-abc]**.
""	Guillemets	Préserve les espaces de fin ou de début dans la chaîne. Par exemple, **« test »** conserve l'espace de début lorsqu'il recherche une correspondance.
^	Caret	Spécifie le début d'une ligne.
\	Caractère d'échappement	Lorsqu'il est utilisé avec un metacaractère, correspond à un caractère littéral. Par exemple, **\[** correspond au crochet gauche.
char	Caractères	Lorsque le caractère n'est pas un métacaractère, correspond au caractère littéral.
\r	Retour chariot	Correspond à un retour chariot 0x0d.
\n	Nouvelle ligne	Correspond à une nouvelle ligne 0x0a.
\t	Onglet	Correspond à une tabulation 0x09.
\f	Saut de page	Correspond à un saut de page 0x0c.
\x*NN*	Nombre hexadécimal échappé	Correspond à un caractère ASCII au moyen de l'hexadécimal (exactement deux chiffres).
NNN	Nombre octal échappé	Correspond à un caractère ASCII comme octal (exactement trois chiffres). Par exemple, le caractère 040 représente un espace.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Regular Expressions (Expressions régulières)**.

Étape 2 Dans la zone des expressions régulières, effectuez l'une des opérations suivantes :

- Choisissez **Add** (Ajouter) pour ajouter un nouvel objet. Saisissez un nom et éventuellement, une description.
- Choisissez un objet existant et cliquez sur **Edit** (Modifier).

Étape 3 Saisissez l'expression régulière dans le champ **Value** (Valeur) ou cliquez sur **Build** (Créer) pour obtenir de l'aide pour créer l'expression.

L'expression régulière est limitée à 100 caractères de longueur.

Si vous cliquez sur **Build** (Créer), utilisez le processus suivant pour créer l'expression :

a) Dans la zone Build Snippet (Créer un fragment), créez un composant de l'expression en utilisant les options suivantes. Consultez la zone d'aperçu du fragment de code à la fin de cette section pour voir l'expression que vous créez.

- Commence au début de la ligne (^) : indique que le fragment de code doit commencer au début d'une ligne, en utilisant le métacaractère (^). Veillez à insérer tout fragment de code avec cette option au début de l'expression régulière.
- Spécifier une chaîne de caractères : si vous essayez de faire correspondre une chaîne en particulier, comme un mot ou une expression, saisissez la chaîne.

  S'il y a des métacaractères dans votre chaîne de texte que vous souhaitez utiliser littéralement, choisissez **Escape Special Characters** (Échapper les caractères spéciaux) pour ajouter le caractère d'échappement de barre oblique inverse avant eux. Par exemple, si vous saisissez « example.com », cette option le convertit en « example.com ».

  Si vous souhaitez faire correspondre les majuscules et les minuscules, choisissez **Ignore Case** (Ignorer la casse). Par exemple, « cats » est converti en « [cC][aA][tT][sS] ».
- Préciser le caractère : si vous essayez de mettre en correspondance un type de caractère ou un ensemble de caractères spécifique, plutôt qu'une phrase particulière, sélectionnez cette option et identifiez les caractères à l'aide de ces options :
  - **Négation du caractère** : spécifie ne pas correspondre au caractère que vous identifiez.
  - **Tout caractère (.)** : insère le metacaractère du point (.) pour correspondre à n'importe quel caractère. Par exemple, **d.g** correspond à dog, dag, dtg et à tout mot qui contient ces caractères, tel que doggonnit.
  - **Ensemble de caractères** : insère un ensemble de caractères. Le texte peut correspondre à n'importe quel caractère dans l'ensemble. Par exemple, si vous spécifiez [0-9A-Za-z], ce fragment de code correspondra à tout caractère de A à Z (majuscules ou minuscules) ou à tout chiffre de 0 à 9. L'ensemble [\n\f\r\t] correspond à une nouvelle ligne, à un saut de page, à un retour chariot ou à une tabulation.
  - **Caractère spécial** : insère un caractère qui nécessite un échappement, y compris , ?, *, +, |, ., [, (, ou ^. Le caractère d'échappement est la barre oblique inverse , qui est automatiquement saisie lorsque vous choisissez cette option.
  - **Caractère d'espacement** : les caractères d'espacement comprennent \n (nouvelle ligne), \f (saut de page), \r (retour chariot) ou \t (tabulation).
  - **Nombre octal à trois chiffres** : correspond à un caractère ASCII sous forme octale (jusqu'à trois chiffres). Par exemple, le caractère \040 représente un espace. La barre oblique inverse (\) est saisie automatiquement.

- **Nombre hexadécimal à deux chiffres** : correspond à un caractère ASCII en utilisant l'hexadécimal (exactement deux chiffres). La barre oblique inverse (\) est saisie automatiquement.
- **Caractère précisé** : saisissez un seul caractère.

b) Ajoutez le fragment de code à la zone d'expression régulière en utilisant l'un des boutons suivants. Notez que vous pouvez également taper directement dans l'expression régulière.

- **Ajouter le fragment** : ajoute le fragment à la fin de l'expression régulière.
- **Ajouter le fragment comme variante** : ajoute le fragment de code à la fin de l'expression régulière séparé par une barre verticale (|), qui correspond à l'une ou l'autre des expressions qu'elle sépare. Par exemple, **dog|cat** correspond à dog ou cat.
- **Insérer le fragment au curseur)** : insère le fragment au curseur.

c) Répétez le processus pour ajouter des fragments jusqu'à ce que l'expression soit terminée.

d) (Facultatif) Dans **Occurrences de sélection**, sélectionnez la fréquence à laquelle l'expression ou des parties de celle-ci doivent correspondre au texte pour être considérées comme une correspondance. Sélectionnez du texte dans le champ Expression régulière, cliquez sur l'une des options suivantes, puis cliquez sur **Appliquer à la sélection**. Par exemple, si l'expression régulière est « test me » et que vous sélectionnez « me » et appliquez **Une ou plusieurs fois**, l'expression régulière passe à « test (me)+ ».

- **Zéro ou une fois (?)** : Il y a 0 ou 1 de l'expression précédente. Par exemple, **lo?se** correspond à lse ou lose.
- **Une ou plusieurs fois (+)** : il y a au moins 1 de l'expression précédente. Par exemple, **lo+se** correspond à lose et loose, mais pas à lse.
- **Un nombre quelconque de fois (*)** : il y a 0, 1 ou un nombre quelconque de l'expression précédente. Par exemple, **lo*se** correspond à lse, lose, loose, etc.
- **Au moins :**répétez au moins *x* fois. Par exemple, **ab(xy){2,}z** correspond à abxyxyz, abxyxyxyz, etc.
- **Exactement** : répétez exactement *x* fois. Par exemple, **ab(xy){3}z** correspond à abxyxyxyz.

e) Cliquez sur **Test** (Tester) pour vérifier que votre expression correspondra au texte prévu. Si le test échoue, vous pouvez essayer de le modifier dans la boîte de dialogue de test ou revenir au générateur d'expression. Si vous modifiez l'expression dans la boîte de dialogue de texte et que vous cliquez sur **OK**, les modifications sont enregistrées et répercutées dans le générateur d'expression.

f) Cliquez sur **OK** .

Créer une carte de trafic d'expression régulière

Une carte de trafic d'expression régulière identifie une ou plusieurs expressions régulières. Il s'agit simplement d'un ensemble d'objets d'expression régulière. Vous pouvez utiliser une carte de trafic d'expression régulière dans de nombreux cas pour remplacer un objet d'expression régulière.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Regular Expressions (Expressions régulières)**.

Étape 2 Dans la zone Regular Expressions Classes (Listes d'expressions régulières), effectuez l'une des opérations suivantes :

- Choisissez **Ajouter** (Ajouter) pour ajouter une nouvelle carte de trafic. Saisissez un nom et éventuellement, une description.
- Choisissez une carte de trafic existante et cliquez sur **Edit** (Modifier).

Étape 3 Sélectionnez les expressions que vous souhaitez dans la liste et cliquez sur **Add** (Ajouter). Supprimez tout ce que vous ne souhaitez pas.

Étape 4 Cliquez sur **OK**.

Surveillance des politiques d'inspection

Pour surveiller les politiques de service d'inspection, entrez les commandes suivantes. Sélectionnez **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)** pour entrer ces commandes. Consultez la référence de commande sur Cisco.com pour obtenir une syntaxe détaillée et des exemples.

- **show service-policy inspect** *protocol*

  Affiche les statistiques pour les politiques de service d'inspection. Le *protocole* est le protocole de la commande inspect, par exemple **dns**. Cependant, tous les protocoles d'inspection n'affichent pas de statistiques avec cette commande. Par exemple :

```
asa# show service-policy inspect dns

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0
        message-length maximum client auto, drop 0
        message-length maximum 512, drop 0
        dns-guard, count 0
        protocol-enforcement, drop 0
        nat-rewrite, count 0
asa#
```

- **show conn**

  Affiche les connexions actuelles pour le trafic passant par le périphérique. Cette commande dispose d'un large éventail de mots-clés afin que vous puissiez obtenir des informations sur les différents protocoles.

- Commandes supplémentaires pour des protocoles inspectés spécifiques :
  - **show ctiqbe**

Affiche les renseignements sur les connexions de support attribuées par le moteur d'inspection CTIQBE

- **show h225**

  Affiche les informations sur les sessions H.225.

- **show h245**

  Affiche les informations sur les sessions H.245 établies par les terminaux à l'aide du démarrage lent.

- **show h323 ras**

  Affiche les informations de connexion pour les sessions RAS H.323 établies entre un portier et son terminal H.323.

- **show mgcp** {**commands** | **sessions**}

  Affiche le nombre de commandes MGCP dans la file d'attente de commandes ou le nombre de sessions MGCP existantes.

- **show sip**

  Affiche les informations pour les sessions SIP.

- **show skinny**

  Affiche les informations pour les sessions Skinny (SCCP).

- **show sunrpc-server active**

  Affiche les passages ouverts pour les services Sun RPC.

Historique de l'inspection des applications

Nom de la caractéristique	Versions	Description
listes des politiques d'inspection	7.2(1)	La liste des politiques d'inspection a été introduite. La commande suivante a été introduite : **class-map type inspect**.
Expressions régulières et listes des politiques	7.2(1)	Les expressions régulières et les listes des politiques ont été introduites pour être utilisées dans les listes des politiques d'inspection. Les commandes suivantes ont été introduites : **class-map type regex**, **regex**, **match regex**.
Correspondance de n'importe quel pour les listes des politiques d'inspection	8.0(2)	Le mot-clé **match any** a été introduit pour une utilisation avec des listes des politiques d'inspection : le trafic peut correspondre à un ou plusieurs critères pour correspondre à la carte de trafic. Auparavant, uniquement **match all** était disponible.

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.