

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 10
- Configurer les expressions régulières, à la page 17
- Surveillance des politiques d'inspection, à la page 20
- Historique de l'inspection des applications, à la page 22

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. Ensuite, vous l'ajoutez avec le nouveau nom de liste des politiques.

Par exemple, pour remplacer sip-map1 par sip-map2 dans l'inspection SIP, utilisez la séquence de commandes suivante :

```
hostname(config)# policy-map test
hostname(config-pmap)# class sip
hostname(config-pmap-c)# no inspect sip sip-map1
hostname(config-pmap-c)# inspect sip sip-map2
```

Comment plusieurs classes de trafic sont gérées

Vous pouvez spécifier plusieurs mappages de classes d'inspection ou correspondances directes dans la liste des politiques 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. Par exemple, les commandes de correspondance suivantes peuvent être saisies dans n'importe quel ordre, mais la commande **match request method get** est mise en correspondance en premier.

```
match request header host length gt 100
  reset
match request method get
  log
```

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. Par exemple, pour un paquet dont la longueur d'en-tête est 1001, il correspondra à la première commande ci-dessous et sera journalisé, puis correspondra à la deuxième commande et sera réinitialisé. Si vous inversez l'ordre des deux commandes **match**, le paquet sera abandonné et la connexion sera réinitialisée avant de pouvoir correspondre à la deuxième commande **dmatch** ; il ne sera jamais journalisé.

```
match request header length gt 100
  log
match request header length gt 1000
  reset
```

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. Par exemple, les trois cartes de trafics suivantes contiennent deux types de commandes **match** : **match request-cmd** (priorité supérieure) et **match filename** (priorité inférieure). La carte de trafic ftp3 comprend les deux commandes, mais elle est classée selon la commande de priorité la plus basse, **match filename**. La carte de trafic ftp1 comprend la commande de priorité la plus élevée, elle est donc mise en correspondance en premier, quel que soit l'ordre dans la liste des politiques. La carte de trafic ftp3 est classée comme étant de la même priorité que la carte de trafic ftp2, qui contient également la commande **match filename**. Elles sont mises en correspondance selon l'ordre dans la liste des politiques : ftp3 puis ftp2.

```
class-map type inspect ftp match-all ftp1
  match request-cmd get
class-map type inspect ftp match-all ftp2
  match filename regex abc
class-map type inspect ftp match-all ftp3
  match request-cmd get
  match filename regex abc

policy-map type inspect ftp ftp
  class ftp3
    log
  class ftp2
```

```
  log
class ftp1
  log
```

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 :

- Diameter
- 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

Lignes directrices 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.	—	—
Diameter	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	—
GTP	UDP/3386 (GTPv0) UDP/2123 (GTPv1+)	Pas de PAT étendue. Pas de NAT.	—	Nécessite la licence Carrier (exploitant).

Application	Protocole, port par défaut	Limites de la NAT	Normes	Commentaires
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).
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.	—	—

Application	Protocole, port par défaut	Limites de la NAT	Normes	Commentaires
Serveur de noms NetBIOS sur IP	UDP/133, 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.
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.

Application	Protocole, port par défaut	Limites de la NAT	Normes	Commentaires
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 Cisco 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.	—	—
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.	—	—

Application	Protocole, port par défaut	Limites de la NAT	Normes	Commentaires
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** .

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 Sauf si vous ajoutez une inspection à une carte de trafic existante, créez une carte de trafic L3/L4 pour identifier le trafic auquel vous souhaitez appliquer l'inspection.

```
class-map name
match parameter
```

Exemple :

```
hostname(config)# class-map dns_class_map
hostname(config-cmap)# match access-list dns
```

Dans la politique globale par défaut, la carte de trafic inspection_default est une carte de trafic spéciale qui comprend des ports par défaut pour tous les types d'inspection (**match default-inspection-traffic**). Vous pouvez appliquer plusieurs inspections uniquement à la carte de trafic inspection_default; il peut donc suffire

de modifier la politique globale existante qui applique les inspections par défaut. Si vous utilisez cette carte de trafic dans la politique par défaut ou pour une nouvelle politique de service, vous pouvez ignorer cette étape. Pour obtenir des renseignements détaillés sur le choix d'une carte de trafic, consultez Choix de la bonne classe de trafic pour l'inspection, à la page 15.

Pour en savoir plus sur la mise en correspondance des instructions, consultez Créer une carte de trafic de couche 3/4 pour le trafic de transit. Pour l'inspection de comptabilité RADIUS, qui utilise une carte de trafic de gestion de couche 3/4, consultez Configurer l'inspection de comptabilité RADIUS.

Étape 2 Ajoutez ou modifiez une liste des politiques de couche 3/4 qui définit les actions à appliquer au trafic de la carte de trafic : **policy-map** *name*

Exemple :

```
hostname(config)# policy-map global_policy
```

Dans la configuration par défaut, la liste des politiques global_policy est affectée globalement à toutes les interfaces. Si vous souhaitez modifier la liste global_policy, saisissez global_policy comme nom de politique.

Étape 3 Déterminez la carte de trafic L3/L4 que vous utilisez pour l'inspection : **class** *name*

Exemple :

```
hostname(config-pmap)# class inspection_default
```

Pour modifier la politique par défaut ou pour utiliser la carte de trafic spéciale inspection_default dans une nouvelle politique, spécifiez **inspection_default** comme *nom*. Sinon, vous spécifiez la carte que vous avez créée précédemment au cours de cette procédure.

Vous pouvez combiner plusieurs cartes de trafic dans la même politique si vous le souhaitez, de sorte que vous pouvez créer une carte de trafic pour faire correspondre un certain trafic et une autre pour faire correspondre un trafic différent. Toutefois, si le trafic correspond à une carte de trafic qui contient une commande d'inspection, puis correspond à une autre carte de trafic qui comporte également une commande d'inspection, seule la première carte correspondante est utilisée. Par exemple, SNMP correspond à la carte de trafic inspection_default. Pour activer l'inspection SNMP, activez l'inspection SNMP pour la carte par défaut. N'ajoutez pas d'autre carte qui correspond à SNMP.

Étape 4 Activez l'inspection des applications : **inspect** *protocol*

Le *protocole* est l'une des valeurs suivantes :

Tableau 2 : Mots-clés du protocole d'inspection

Mots-clés	Notes
ctiqbe	Consultez Inspection CTIQBE.
dcerpc [*map_name*]	Consultez Inspection DCERPC. Si vous avez ajouté une liste des politiques d'inspection DCERPC conformément à Configurer une liste des politiques d'inspection DCERPC, identifiez le nom de la liste dans cette commande.

Mots-clés	Notes
diameter [*map_name*] [**tls-proxy** *proxy_name*]	Consultez Inspection Diameter. Si vous avez ajouté une liste des politiques d'inspection Diameter conformément à Configurer une liste des politiques d'inspection Diameter, identifiez le nom de la liste dans cette commande. **tls-proxy** *proxy_name* identifie le serveur proxy TLS à utiliser pour cette inspection. Vous avez besoin d'un serveur proxy TLS uniquement si vous souhaitez activer l'inspection du trafic chiffré.
dns [*map_name*] [**dynamic-filter-snoop**]	Consultez Inspection DNS. Si vous avez ajouté une liste des politiques d'inspection DNS en fonction de Configurer la liste des politiques d'inspection DNS, identifiez le nom de la liste dans cette commande. Le nom de la liste des politiques d'inspection DNS par défaut est « preset_dns_map ». **dynamique-filtre-snoop** active la surveillance dynamique des filtres, utilisée exclusivement par le filtre de trafic de réseau de zombies. Incluez ce mot-clé uniquement si vous utilisez le filtrage du trafic de réseau de zombies. 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.
esmtp [*map_name*]	Consultez Inspection SMTP et SMTP étendue. Si vous avez ajouté une liste des politiques d'inspection ESMTP conformément à Configurer une liste des politiques d'inspection ESMTP, identifiez le nom de la liste dans cette commande.
ftp [**strict** [*map_name*]]	Consultez Inspection FTP. Utilisez le mot-clé **strict** pour renforcer la sécurité des réseaux protégés en empêchant les navigateurs Web d'envoyer des commandes intégrées dans les requêtes FTP. Consultez FTP strict pour de plus amples renseignements. Si vous avez ajouté une liste des politiques d'inspection FTP conformément à Configurer une liste des politiques d'inspection FTP, identifiez le nom de la liste dans cette commande.
gtp [*map_name*]	Consultez Aperçu de l'inspection GTP. Si vous avez ajouté une liste des politiques d'inspection GTP conformément à Configurer une liste des politiques d'inspection GTP, identifiez le nom de la liste dans cette commande.
h323 h225 [*map_name*]	Consultez Inspection H.323. Si vous avez ajouté une liste des politiques d'inspection H323 conformément à Configurer la liste des politiques d'inspection H.323, identifiez le nom de la liste dans cette commande.

Mots-clés	Notes
h323 ras [*map_name*]	Consultez Inspection H.323. Si vous avez ajouté une liste des politiques d'inspection H323 conformément à Configurer la liste des politiques d'inspection H.323, identifiez le nom de la liste dans cette commande.
http [*map_name*]	Consultez Inspection HTTP. Si vous avez ajouté une liste des politiques d'inspection HTTP conformément à Configurer une liste des politiques d'inspection HTTP, identifiez le nom de la liste dans cette commande.
ICMP	Consultez Inspection ICMP.
icmp error	Consultez Inspection des erreurs ICMP.
ils	Consultez Inspection ILS.
im [*map_name*]	Consultez Inspection de la messagerie instantanée. Si vous avez ajouté une liste des politiques d'inspection de messagerie instantanée, identifiez le nom de la liste dans cette commande.
ip-options [*map_name*]	Consultez Inspection des options IP. Si vous avez ajouté une liste des politiques d'inspection des options IP conformément à Configurer une liste des politiques d'inspection des options IP, identifiez le nom de la liste dans cette commande.
ipsec-pass-thru [*map_name*]	Consultez Inspection IPsec Pass Through. Si vous avez ajouté une liste des politiques d'inspection de transmission directe IPsec conformément à Configurer une liste des politiques d'inspection de transmission directe IPsec, identifiez le nom de la liste dans cette commande.
ipv6 [*map_name*]	Consultez Inspection IPv6. Si vous avez ajouté une liste des politiques d'inspection IPv6 conformément à Configurer une liste des politiques d'inspection IPv6, identifiez le nom de la liste dans cette commande.
lisp [*map_name*]	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. Si vous avez ajouté une liste des politiques d'inspection LISP, identifiez le nom de la liste dans cette commande.
m3ua [*map_name*]	Consultez Inspection M3UA. Si vous avez ajouté une liste des politiques d'inspection M3UA conformément à Configurer une liste des politiques d'inspection M3UA, identifiez le nom de la liste dans cette commande.

Mots-clés	Notes
mgcp [*map_name*]	Consultez Inspection MGCP. Si vous avez ajouté une liste des politiques d'inspection MGCP conformément à Configurer une liste des politiques d'inspection MGCP, identifiez le nom de la liste dans cette commande.
netbios [*map_name*]	Consultez Inspection NetBIOS. Si vous avez ajouté une liste des politiques d'inspection NetBIOS, identifiez le nom de la liste dans cette commande.
pptp	Consultez Inspection PPTP.
radius-accounting *map_name*	Consultez Aperçu de l'inspection de comptabilité RADIUS. Le mot-clé **radius-accounting** est uniquement disponible pour une carte de trafic de gestion. Vous devez spécifier une liste des politiques d'inspection de comptabilité RADIUS; voir Configurer une liste des politiques d'inspection de comptabilité RADIUS.
rsh	Consultez Inspection RSH.
rtsp [*map_name*]	Consultez Inspection RTSP. Si vous avez ajouté une liste des politiques d'inspection RTSP conformément à Configurer une liste des politiques d'inspection RTSP, identifiez le nom de la liste dans cette commande.
sctp [*map_name*]	Consultez Inspection de la couche application SCTP. Si vous avez ajouté une liste des politiques d'inspection SCTP conformément à Configurer une liste des politiques d'inspection SCTP, identifiez le nom de la liste dans cette commande.
sip [*map_name*] [**tls-proxy** *proxy_name*]	Consultez Inspection SIP. Si vous avez ajouté une liste des politiques d'inspection SIP conformément à Configurer une liste des politiques d'inspection SIP, identifiez le nom de la liste dans cette commande. **tls-proxy** *proxy_name* identifie le serveur proxy TLS à utiliser pour cette inspection. Vous avez besoin d'un serveur proxy TLS uniquement si vous souhaitez activer l'inspection du trafic chiffré.
Skinny [*map_name*]	Consultez Inspection Skinny (SCCP). Si vous avez ajouté une liste des politiques d'inspection Skinny conformément à Configurer une liste des politiques d'inspection Skinny (SCCP), identifiez le nom de la liste dans cette commande.
snmp [*map_name*]	Consultez Inspection SNMP. Si vous avez ajouté une liste des politiques d'inspection SNMP, identifiez le nom de la liste dans cette commande.
sqlnet	Consultez Inspection SQL*Net.

Mots-clés	Notes
stun	Consultez Inspection STUN.
sunrpc	Consultez Inspection Sun RPC. La carte de trafic par défaut comprend le port UDP 111; si vous souhaitez activer l'inspection Sun RPC 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 la commande **inspect sunrpc** à cette carte.
tftp	Consultez Inspection TFTP.
WAAS	Active l'analyse TCP de l'option 33. À utiliser lors du déploiement des produits de services d'applications pour zone étendue.
xdmcp	Consultez Inspection XDMCP.
vxlan	Consultez Inspection VXLAN.

Remarque
Si vous modifiez la politique globale par défaut (ou toute politique en cours d'utilisation) afin d'utiliser une liste des politiques d'inspection différente, vous devez supprimer l'ancienne inspection avec la commande **no inspect** *protocol*, puis la rajouter avec le nouveau nom de la liste des politiques d'inspection.

Exemple :

```
hostname(config-class)# no inspect sip
hostname(config-class)# inspect sip sip-map
```

Étape 5 Si vous modifiez une politique de service existante (comme la politique globale par défaut appelée global_policy), vous pouvez ignorer cette étape. Sinon, activez la liste des politiques sur une ou plusieurs interfaces.

service-policy *policymap_name* {**global** | **interface** *interface_name*}

Exemple :

```
hostname(config)# service-policy global_policy global
```

Le mot clé **global** applique la liste des politiques à toutes les interfaces et **interface** applique la politique à une interface. Une seule politique globale est autorisée. Vous pouvez remplacer la politique globale sur une interface en appliquant une politique de service à cette interface. Vous ne pouvez appliquer qu'une seule liste de politiques à chaque interface.

Choix de la bonne classe de trafic pour l'inspection

La carte de trafic par défaut de la couche 3/4 pour le trafic de transit est appelée « inspection_default ». Elle fait correspondre le trafic à l'aide d'une commande **match** spéciale, **match default-inspection-traffic**, pour faire correspondre les protocoles et les ports par défaut pour chaque protocole d'application. Cette classe de

trafic (ainsi que **match any**, qui n'est généralement pas utilisé pour l'inspection) correspond au trafic IPv4 et IPv6 pour les inspection qui prennent en charge IPv6. Consultez Lignes directrices relatives à l'inspection des applications, à la page 4 pour obtenir la liste des inspections activées pour IPv6.

Vous pouvez spécifier une commande **match access-list** avec la commande **match default-inspection-traffic** pour restreindre le trafic correspondant à des adresses IP spécifiques. Comme la commande **match default-inspection-traffic** spécifie les ports à mettre en correspondance, tous les ports dans l'ACL sont ignorés.

Astuces Nous vous suggérons d'inspecter le trafic uniquement sur les ports sur lesquels vous attendez un trafic d'application; si vous inspectez tout le trafic, par exemple à l'aide de **match any**, les performances de l'ASA peuvent être affectées.

Si vous souhaitez faire correspondre des ports non standard, créez une nouvelle carte de trafic 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 cartes de trafic dans la même politique si vous le souhaitez, de sorte que vous pouvez créer une carte de trafic pour faire correspondre un certain trafic et une autre pour faire correspondre un trafic différent. Toutefois, si le trafic correspond à une carte de trafic qui contient une commande d'inspection, puis correspond à une autre carte de trafic qui comporte également une commande d'inspection, seule la première carte correspondante est utilisée. Par exemple, SNMP correspond à la carte inspection_default. Pour activer l'inspection SNMP, activez l'inspection SNMP pour la carte par défaut. N'ajoutez pas d'autre carte qui correspond à SNMP.

Par exemple, pour limiter l'inspection au trafic de 10.1.1.0 à 192.168.1.0 à l'aide de la carte de trafic par défaut, saisissez les commandes suivantes :

```
hostname(config)# access-list inspect extended permit ip 10.1.1.0 255.255.255.0
192.168.1.0 255.255.255.0
hostname(config)# class-map inspection_default
hostname(config-cmap)# match access-list inspect
```

Affichez l'ensemble de la carte de trafic en utilisant la commande suivante :

```
hostname(config-cmap)# show running-config class-map inspection_default
!
class-map inspection_default
 match default-inspection-traffic
 match access-list inspect
!
```

Pour inspecter le trafic FTP sur le port 21 ainsi que sur le port 1056 (port non standard), créez une liste de contrôle d'accès qui spécifie les ports et affectez-la à une nouvelle carte de trafic :

```
hostname(config)# access-list ftp_inspect extended permit tcp any any eq 21
hostname(config)# access-list ftp_inspect extended permit tcp any any eq 1056
hostname(config)# class-map new_inspection
hostname(config-cmap)# match access-list ftp_inspect
```

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

Utilisez **Ctrl+V** pour échapper tous les caractères spéciaux de l'interface de ligne de commande, comme un point d'interrogation (?) ou un onglet. Par exemple, tapez **d[Ctrl+V]?g** pour saisir **d?g** dans la configuration.

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 À des fins d'optimisation, l'ASA effectue la recherche sur l'URL désobfusquée. La désobfuscation remplace plusieurs barres obliques (/) consécutives par une seule. 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.

Caractères	Description	Remarques
|	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.
[^*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.

Caractères	Description	Remarques
\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 Testez une expression régulière pour vous assurer qu'elle correspond à ce que vous pensez qu'elle correspondra : **test regex** *input_text regular_expression*

Où l'argument *input_text* est une chaîne que vous souhaitez mettre en correspondance à l'aide de l'expression régulière, jusqu'à 201 caractères de longueur. L'argument *regular_expression* peut comporter jusqu'à 100 caractères.

Utilisez **Ctrl+V** pour échapper tous les caractères spéciaux de l'interface de ligne de commande. Par exemple, pour saisir un onglet dans le texte d'entrée de la commande **test regex**, vous devez saisir **test regex «test[Ctrl+V Tab]» «test\t»**.

Si l'expression régulière correspond au texte d'entrée, le message suivant s'affiche :

```
INFO: Regular expression match succeeded.
```

Si l'expression régulière ne correspond pas au texte d'entrée, le message suivant s'affiche :

```
INFO: Regular expression match failed.
```

Étape 2 Pour ajouter une expression régulière après l'avoir testée, saisissez la commande suivante : **regex** *name regular_expression*

Où l'argument *name* peut comporter jusqu'à 40 caractères de longueur. L'argument *regular_expression* peut comporter jusqu'à 100 caractères.

Exemples

L'exemple suivant crée deux expressions régulières à utiliser dans une liste des politiques d'inspection :

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
```

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 Créez la carte de trafic d'expressions régulières : **class-map type regex match-any** *class_map_name*

Où *class_map_name* est une chaîne d'une longueur maximale de 40 caractères. Le nom « class-default » est réservé. Tous les types de cartes de trafic utilisent le même espace de nom, de sorte que vous ne pouvez pas réutiliser un nom déjà utilisé par un autre type de carte de trafic.

Le mot-clé **match-any** spécifie que le trafic correspond à la carte de classes s'il correspond à au moins une des expressions régulières.

Étape 2 (Facultatif) Ajoutez une description à la carte de trafic : **description** *string*

Étape 3 Déterminez les expressions régulières que vous souhaitez inclure en entrant la commande suivante pour chaque expression régulière : **match regex** *regex_name*

Exemples

L'exemple suivant crée deux expressions régulières et les ajoute à une carte de trafic d'expressions régulières. Le trafic correspond à la carte de trafic s'il comprend la chaîne « example.com » ou « example2.com ».

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
hostname(config)# class-map type regex match-any URLs
hostname(config-cmap)# match regex url_example
hostname(config-cmap)# match regex url_example2
```

Surveillance des politiques d'inspection

Pour surveiller les politiques de service d'inspection, entrez les commandes suivantes. 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**.
match any 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.

À propos de la traduction

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

À propos de la traduction

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

À propos de la traduction

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

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.