Exemple de configuration du filtrage d'URL PIX/ASA

Contenu

Introduction

Ce document explique comment configurer le filtrage URL sur une appliance de sécurité.

Filtrer le trafic a ces avantages :

- Cela peut aider à réduire les risques de sécurité et à empêcher une utilisation inadéquate.
- Cela peut fournir un plus grand contrôle du trafic qui passe par l'appliance de sécurité.

Remarque: Puisque le filtrage URL dépend du CPU, l'utilisation d'un serveur de filtrage externe assure que le débit de l'autre trafic n'est pas affecté. Cependant, en fonction de la vitesse de votre réseau et de la capacité de votre serveur de filtrage URL, le temps nécessaire à la connexion initiale peut être sensiblement plus important quand le trafic est filtré avec un serveur de filtrage externe.

Remarque: Implémenter un filtrage d'un niveau de sécurité plus bas à un plus élevé n'est pas pris en charge. Le filtrage URL fonctionne seulement pour le trafic sortant, par exemple, le trafic qui commence sur une interface de sécurité élevée destinée à un serveur sur une interface de sécurité basse.

Conditions préalables

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Dispositifs de sécurité de la gamme PIX 500 avec les versions 6.2 et ultérieures
- Appliance de sécurité de la gamme ASA 5500 avec versions 7.x et ultérieures
- Adaptive Security Device Manager (ASDM) 6.0

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Vous pouvez filtrer les demandes de connexion qui proviennent d'un réseau plus sécurisé à un réseau moins sécurisé. Bien que vous puissiez utiliser des listes de contrôle d'accès (ACL) afin d'empêcher l'accès sortant à des serveurs spécifiques, il est difficile de gérer l'utilisation de cette façon en raison de la taille et de la nature dynamique d'Internet. Vous pouvez simplifier la configuration et améliorer la performance d'appliance de sécurité avec l'utilisation d'un serveur distinct qui exécute un de ces produits de filtrage Internet :

- Websense Enterprise — filtres HTTP, HTTPS et FTP. Pris en charge par le pare-feu PIX versions 5.3 et ultérieures.
- Secure Computing SmartFilter, autrefois connu sous le nom de N2H2 - filtres HTTP, HTTPS, FTP et filtrage URL longues. Pris en charge par le pare-feu PIX versions 6.2 et ultérieures.

Comparé à l'utilisation des listes de contrôle d'accès, ceci réduit la tâche administrative et améliore l'efficacité du filtrage. En outre, parce que le filtrage URL est pris en charge sur une plate-forme distincte, les performances du pare-feu PIX sont beaucoup moins affectées. Cependant, les utilisateurs peuvent remarquer que les temps d'accès aux sites Web ou aux serveurs FTP sont plus longs quand le serveur de filtrage est éloigné de l'appliance de sécurité.

Le pare-feu PIX vérifie les demandes d'URL sortantes avec la politique définie sur le serveur de filtrage URL. Le pare-feu PIX permet ou refuse la connexion, selon la réponse du serveur de filtrage.

Quand le filtrage est autorisé et qu'une demande de contenu est dirigée par l'appliance de sécurité, la demande est envoyée au serveur de contenu et au serveur de filtrage en même temps. Si le serveur de filtrage permet la connexion, l'appliance de sécurité transfère la réponse du serveur de contenu au client qui a lancé la demande. Si le serveur de filtrage refuse la connexion, l'appliance de sécurité supprime la réponse et envoie un message ou un code retour qui indique que la connexion n'a pas réussi.

Si l'authentification des utilisateurs est autorisée sur l'appliance de sécurité, l'appliance de sécurité envoie également le nom de l'utilisateur au serveur de filtrage. Le serveur de filtrage peut utiliser les paramètres de filtrage d'un utilisateur spécifique ou fournir des rapports améliorés en ce qui concerne l'utilisation.

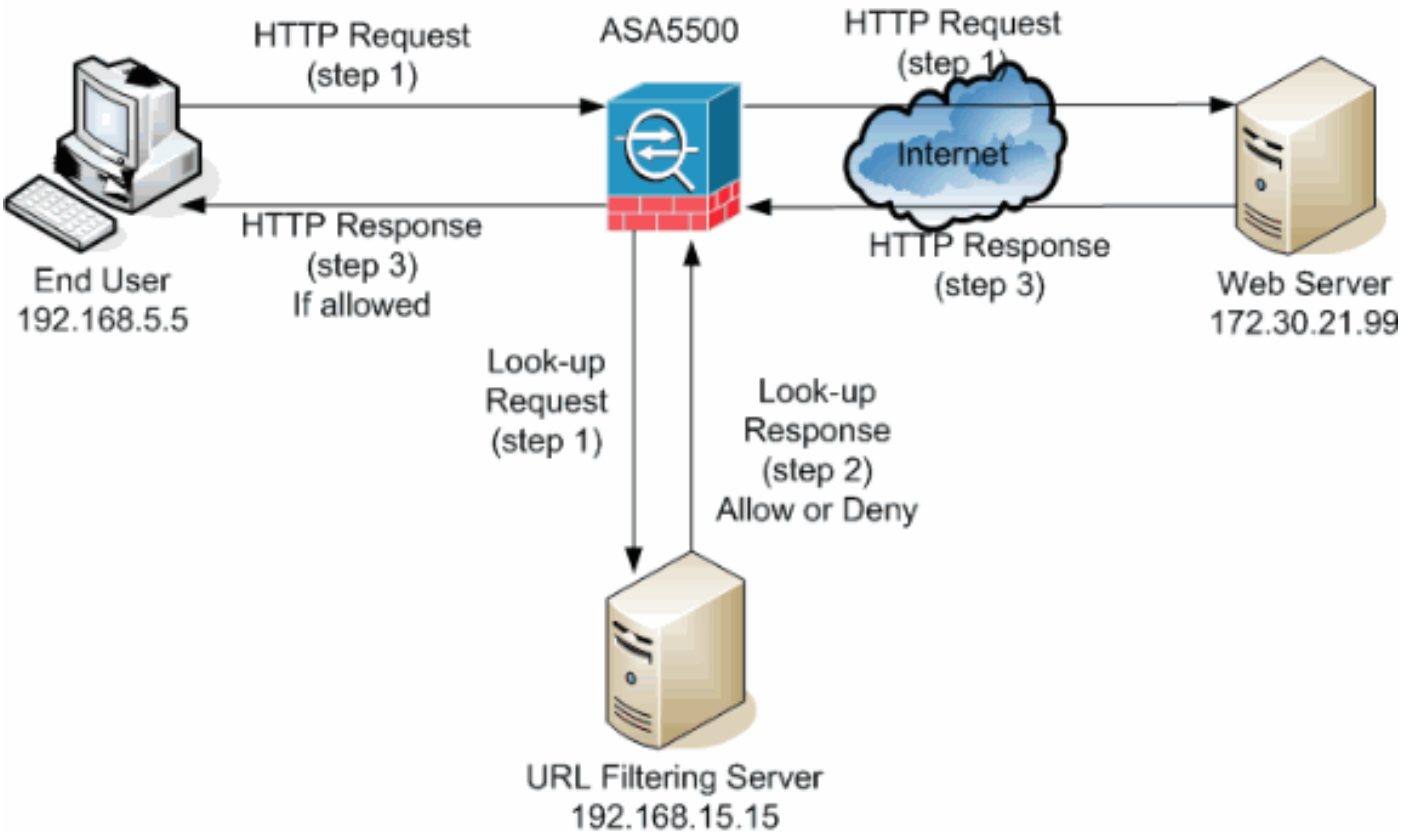
Configurer ASA/PIX avec CLI

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Dans cet exemple, le serveur de filtrage URL se trouve dans un réseau DMZ. Les utilisateurs finaux situés à l'intérieur du réseau essaient d'accéder le serveur Web situé en dehors du réseau sur Internet.

Ces étapes sont réalisées pendant la demande des utilisateurs pour le serveur Web :

1. L'utilisateur final navigue sur une page sur le serveur Web et le navigateur envoie une demande HTTP.
2. Après que l'appliance de sécurité a reçu cette demande, elle la fait suivre au serveur Web, extrait simultanément l'URL et envoie une demande de consultation au serveur de filtrage URL.

3. Après que le serveur de filtrage URL a reçu la demande de consultation, il vérifie sa base de données afin de déterminer si l'URL est autorisée ou non. Il renvoie un état d'autorisation ou de refus avec une réponse de consultation au pare-feu Cisco IOS®.
4. L'appliance de sécurité reçoit cette réponse de consultation et remplit une de ces fonctions :Si la réponse de consultation autorise l'URL, elle envoie la réponse HTTP à l'utilisateur final.Si la réponse de consultation refuse l'URL, le serveur de filtrage URL redirige l'utilisateur à son propre serveur Web interne, qui affiche un message décrivant la catégorie sous laquelle l'URL est bloquée. Ensuite, la connexion est réinitialisée sur les deux extrémités.

Identifier le serveur de filtrage

Vous devez identifier l'adresse du serveur de filtrage avec la commande **url-server**. Vous devez utiliser la forme appropriée de cette commande en fonction du type de serveur de filtrage que vous utilisez.

Remarque: Pour les versions 7.x et ultérieures du logiciel, vous pouvez identifier jusqu'à quatre serveurs de filtrage pour chaque contexte. L'appliance de sécurité utilise les serveurs dans l'ordre jusqu'à ce qu'un serveur réagisse. Vous pouvez configurer un seul type de serveur, Websense ou N2H2, dans votre configuration.

Websense

Websense est un logiciel de filtrage tiers qui peut filtrer les demandes HTTP sur la base de ces politiques :

- nom de l'hôte de destination
- adresse IP de destination
- mots clé
- nom de l'utilisateur

Le logiciel garde une base de données d'URL de plus de 20 millions de sites organisés en plus de 60 catégories et sous-catégories.

- Logiciel version 6.2 :
  `url-server [(if_name)] vendor websense host local_ip [timeout seconds] [protocol {TCP | UDP} version]` La commande **url-server** indique le serveur qui exécute l'application de filtrage URL N2H2 ou Websense. La limite est 16 serveurs d'URL. Cependant, vous pouvez utiliser seulement une application à la fois, N2H2 ou Websense. De plus, si vous modifiez votre configuration sur le pare-feu PIX, cela ne met pas à jour la configuration sur le serveur d'application. Ceci doit être fait séparément, en fonction des instructions du fournisseur individuel.
- Logiciel versions 7.x et ultérieures :
  `pix(config)# url-server (if_name) host local_ip [timeout seconds] [protocol TCP | UDP version 1|4 [connections num_conns] ]`

Remplacez if_name par le nom de l'interface d'appliance de sécurité qui est connectée au serveur de filtrage. La valeur par défaut est à l'intérieur. Remplacez local_ip par l'adresse IP du serveur de filtrage. Remplacez seconds par le nombre de secondes pendant lesquelles l'appliance de sécurité doit continuer d'essayer de se connecter au serveur de filtrage.

Utilisez l'option protocol afin de spécifier si vous voulez utiliser TCP ou UDP. Avec un serveur

Websense, vous pouvez également spécifier la version TCP que vous voulez utiliser. TCP version 1 est la valeur par défaut. TCP version 4 permet au pare-feu PIX d'envoyer des noms d'utilisateurs authentifiés et des informations de connexion URL au serveur Websense si le pare-feu PIX a déjà authentifié l'utilisateur.

Par exemple, afin d'identifier un unique serveur de filtrage Websense, lancez cette commande :

```
hostname(config)#url-server (DMZ) vendor websense host 192.168.15.15 protocol TCP version 4
```

Secure Computing SmartFilter

- PIX version 6.2 :`pix(config)#url-server [(if_name)] vendor n2h2 host local_ip[:port number] [timeout <seconds>] [protocol TCP | UDP]`
- Logiciel versions 7.0 et 7.1 :`hostname(config)#url-server (if_name) vendor n2h2 host local_ip[:port number] [timeout seconds] [protocol TCP connections number | UDP [connections num_conns]]`
- Logiciel versions 7.2 et ultérieures :`hostname(config)#url-server (if_name) vendor {secure-computing | n2h2} host <local_ip> [port <number>] [timeout <seconds>] [protocol {TCP [connections <number>]} | UDP]` Pour vendor {secure-computing | n2h2}, vous pouvez utiliser secure-computing comme chaîne de fournisseur. Cependant, n2h2 est acceptable pour la rétrocompatibilité. Quand les entrées de configuration sont générées, secure-computing est enregistré comme chaîne de fournisseur.

Remplacez if_name par le nom de l'interface d'appliance de sécurité qui est connectée au serveur de filtrage. La valeur par défaut est à l'intérieur. Remplacez local_ip par l'adresse IP du serveur de filtrage et port <number> avec le numéro de port désiré.

Remarque: Le port par défaut utilisé par le serveur Secure Computing SmartFilter pour communiquer avec l'appliance de sécurité avec TCP ou UDP est le port 4005.

Remplacez seconds par le nombre de secondes pendant lesquelles l'appliance de sécurité doit continuer d'essayer de se connecter au serveur de filtrage. Utilisez l'option protocol afin de spécifier si vous voulez utiliser TCP ou UDP.

connections <number> est le nombre de fois à essayer d'établir une connexion entre l'hôte et le serveur.

Par exemple, afin d'identifier un unique serveur de filtrage N2H2, lancez cette commande :

```
hostname(config)#url-server (DMZ) vendor n2h2 host 192.168.15.15 port 4444 timeout 45 protocol tcp connections 10
```

Ou, si vous voulez utiliser les valeurs par défaut, lancez cette commande :

```
hostname(config)#url-server (DMZ) vendor n2h2 host 192.168.15.15
```

Configurer la politique de filtrage

Remarque: Vous devez identifier et activer le serveur de filtrage URL avant d'activer le filtrage URL.

Activer le filtrage URL

Quand le serveur de filtrage approuve une demande de connexion HTTP, l'appliance de sécurité permet à la réponse du serveur Web d'atteindre le client qui a lancé la demande. Si le serveur de

filtrage refuse la demande, l'appliance de sécurité redirige l'utilisateur à une page bloquée qui indique que l'accès est refusé.

Lancez la commande **filter url** afin de configurer la politique utilisée pour filtrer les URL :

- PIX version 6.2 :
  filter url [http | port[-port] local_ip local_mask foreign_ip foreign_mask] [allow] [proxy-block] [longurl-truncate | longurl-deny] [cgi-truncate]
- Logiciel versions 7.x et ultérieures :
  filter url [http | port[-port] local_ip local_mask foreign_ip foreign_mask] [allow] [proxy-block] [longurl-truncate | longurl-deny] [cgi-truncate]

Remplacez port par le numéro de port sur lequel filtrer le trafic HTTP si un port autre que le port par défaut pour l'HTTP (80) est utilisé. Afin d'identifier une suite de numéros de port, entrez le début et la fin de la liste séparée par un tiret.

Lorsque le filtrage est activé, l'appliance de sécurité arrête le trafic HTTP sortant jusqu'à ce qu'un serveur de filtrage permette la connexion. Si le serveur de filtrage principal ne réagit pas, l'appliance de sécurité dirige la demande de filtrage vers le serveur de filtrage secondaire. L'option allow fait que l'appliance de sécurité transfère le trafic HTTP sans filtrage quand le serveur de filtrage principal est indisponible.

Lancez la commande **proxy-block** afin d'annuler toutes les demandes aux serveurs proxys.

Remarque: Le reste des paramètres sont utilisés afin de tronquer des URL longues.

Tronquer des URL HTTP longues

L'option longurl-truncate fait que l'appliance de sécurité envoie seulement le nom d'hôte ou la partie d'adresse IP de l'URL pour l'évaluation au serveur de filtrage quand l'URL est plus longue que la longueur maximale autorisée.

Utilisez l'option longurl-deny afin de refuser le trafic d'URL sortant si l'URL est plus longue que le maximum autorisé.

Utilisez l'option cgi-truncate afin de tronquer les URL CGI pour n'inclure que l'emplacement du script CGI et le nom du script sans aucun paramètre.

C'est un exemple de configuration de filtre général :

```
hostname(config)#filter url http 192.168.5.0 255.255.255.0 172.30.21.99 255.255.255.255 allow
proxy-block longurl-truncate cgi-truncate
```

Exempter le trafic de filtrage

Si vous voulez faire une exception à la politique générale de filtrage, lancez cette commande :

```
filter url except local_ip local_mask foreign_ip foreign_mask]
```

Remplacez local_ip et local_mask par l'adresse IP et le masque de sous-réseau d'un utilisateur ou d'un sous-réseau que vous voulez exempter des restrictions de filtrage.

Remplacez foreign_ip et foreign_mask par l'adresse IP et le masque de sous-réseau d'un serveur ou d'un sous-réseau que vous voulez exempter des restrictions de filtrage.

Par exemple, cette commande entraîne toutes les demandes HTTP à 172.30.21.99, des hôtes internes, à être transférées au serveur de filtrage sauf les requêtes de l'hôte 192.168.5.5 :

C'est un exemple de configuration pour une exception :

```
hostname(config)#filter url except 192.168.5.5 255.255.255.255 172.30.21.99 255.255.255.255
```

Filtrage URL avancé

Cette section fournit des informations au sujet des paramètres de filtrage avancé, incluant ces rubriques :

- bufferiser
- mise en antémémoire
- Support d'URL longues

Mettre en mémoire tampon les réponses du serveur Web

Quand un utilisateur émet une demande de connexion à un serveur de contenu, l'appliance de sécurité envoie la demande au serveur de contenu et au serveur de filtrage en même temps. Si le serveur de filtrage ne réagit pas avant le serveur de contenu, la réponse du serveur est suspendue. Ceci retarde la réponse du serveur Web du point de vue du client Web parce que le client doit relancer la demande.

Si vous activez la mise en mémoire tampon de réponse HTTP, des réponses des serveurs de contenu web sont mises en mémoire tampon et les réponses sont transférées au client qui fait la demande si le serveur de filtrage autorise la connexion. Ceci empêche le retard qui peut autrement se produire.

Afin de mettre en mémoire tampon les réponses aux demandes HTTP, suivez ces étapes :

1. Afin d'activer la mise en mémoire tampon des réponses pour les demandes HTTP qui sont en attente d'une réponse du serveur de filtrage, lancez cette commande :`hostname(config)#url-block block block-buffer-limit` Remplacez block-buffer-limit par le nombre maximal de blocs à mettre en mémoire tampon.
2. Afin de configurer la mémoire maximale disponible pour mettre en mémoire tampon les URL en attente et pour mettre en mémoire tampon des URL longues avec Websense, lancez cette commande :`hostname(config)#url-block url-mempool memory-pool-size` Remplacez memory-pool-size par une valeur de 2 à 10240 pour une mémoire maximale de 2 Ko à 10 Mo.

Mettre en cache les adresses du serveur

Après qu'un utilisateur accède à un site, le serveur de filtrage peut permettre à l'appliance de sécurité de cacher l'adresse de serveur pendant un certain temps, tant que chaque site hébergé à l'adresse est dans une catégorie qui est autorisée à tout moment. Puis, quand l'utilisateur accède de nouveau au serveur, ou si un autre utilisateur accède au serveur, l'appliance de sécurité n'a pas besoin de consulter le serveur de filtrage de nouveau.

Lancez la commande **url-cache** si nécessaire pour améliorer le débit :

```
hostname(config)#url-cache dst | src_dst size
```
Remplacez la taille par une valeur avec la taille de mise en cache comprise entre 1 et 128 (Ko).

Utilisez le mot clé dst afin de mettre en cache les entrées basées sur l'adresse URL de destination. Sélectionnez ce mode si tous les utilisateurs partagent la même politique de filtrage URL sur le serveur Websense.

Utilisez le mot clé src_dst afin de mettre en cache l'adresse source qui lance la demande d'URL aussi bien que l'adresse URL de destination. Sélectionnez ce mode si les utilisateurs ne partagent pas la même politique de filtrage URL sur le serveur Websense.

Activer le filtrage d'URL longues

Par défaut, l'appliance de sécurité considère une URL HTTP comme étant une longue URL si elle dépasse 1159 caractères. Vous pouvez augmenter la longueur maximale autorisée pour une URL simple avec cette commande :

```
hostname(config)#url-block url-size long-url-size
```
Remplacez long-url-size par la taille maximale en Ko pour que chaque URL longue soit mise en mémoire tampon.

Par exemple, ces commandes configurent l'appliance de sécurité pour le filtrage URL avancé :

```
hostname(config)#url-block block 10 hostname(config)#url-block url-mempool 2
hostname(config)#url-cache dst 100 hostname(config)#url-block url-size 2
```

Configuration

Cette configuration inclut les commandes décrites dans ce document :

Configuration ASA 8.0

```
ciscoasa#show running-config : Saved : ASA Version
8.0(2) ! hostname ciscoasa domain-name Security.lab.com
enable password 2kxsYuz/BehvglCF encrypted no names dns-
guard ! interface GigabitEthernet0/0 speed 100 duplex
full nameif outside security-level 0 ip address
172.30.21.222 255.255.255.0 ! interface
GigabitEthernet0/1 description INSIDE nameif inside
security-level 100 ip address 192.168.5.11 255.255.255.0
! interface GigabitEthernet0/2 description LAN/STATE
Failover Interface shutdown ! interface
GigabitEthernet0/3 description DMZ nameif DMZ security-
level 50 ip address 192.168.15.1 255.255.255.0 !
interface Management0/0 no nameif no security-level no
ip address ! passwd 2KFQnbNIdI.2KYOU encrypted boot
system disk0:/asa802-k8.bin ftp mode passive clock
timezone CST -6 clock summer-time CDT recurring dns
server-group DefaultDNS domain-name Security.lab.com
same-security-traffic permit intra-interface pager lines
20 logging enable logging buffer-size 40000 logging
asdm-buffer-size 200 logging monitor debugging logging
buffered informational logging trap warnings logging
asdm informational logging mail debugging logging from-
address aaa@cisco.com mtu outside 1500 mtu inside 1500
mtu DMZ 1500 no failover failover lan unit primary
failover lan interface interface GigabitEthernet0/2
failover link interface GigabitEthernet0/2 no monitor-
```

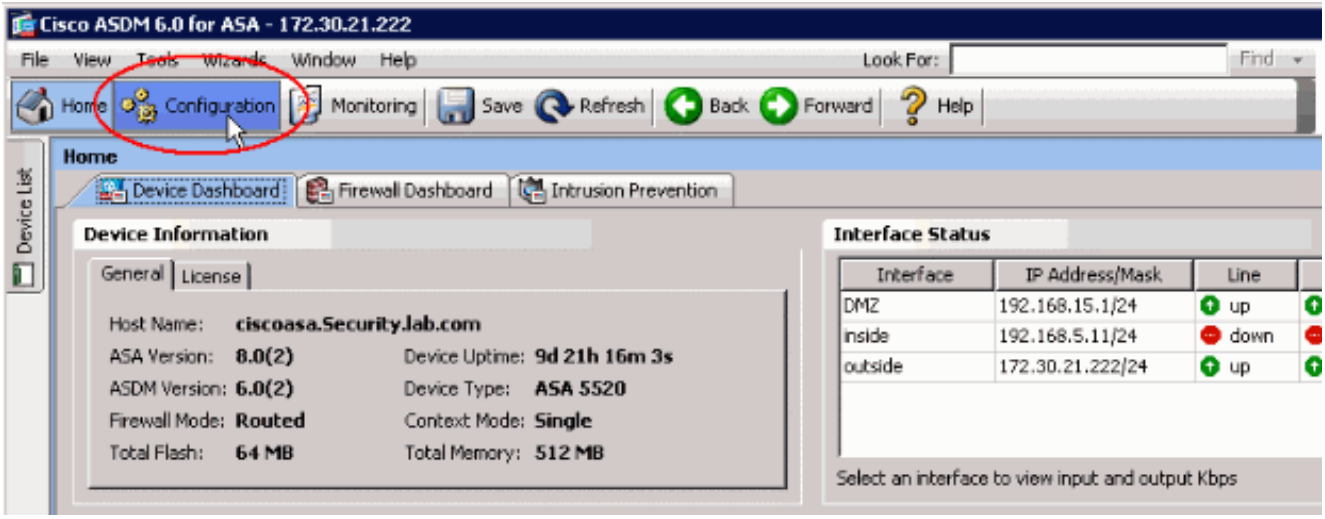
```
interface outside icmp unreachable rate-limit 1 burst-
size 1 asdm image disk0:/asdm-602.bin asdm history
enable arp timeout 14400 global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0 route outside 0.0.0.0
0.0.0.0 172.30.21.244 1 timeout xlate 3:00:00 timeout
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp
0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00
mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00
sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect
0:02:00 timeout uauth 0:05:00 absolute ldap attribute-
map tomtom dynamic-access-policy-record DfltAccessPolicy
url-server (DMZ) vendor websense host 192.168.15.15
timeout 30 protocol TCP version 1 connections 5 url-
cache dst 100 aaa authentication ssh console LOCAL aaa
authentication enable console LOCAL aaa authentication
telnet console LOCAL filter url except 192.168.5.5
255.255.255.255 172.30.21.99 255.255.255.255 filter url
http 192.168.5.0 255.255.255.0 172.30.21.99
255.255.255.255 allow proxy-block longurl-truncate cgi-
truncate http server enable http 172.30.0.0 255.255.0.0
outside no snmp-server location no snmp-server contact
telnet 0.0.0.0 0.0.0.0 inside telnet timeout 5 ssh
0.0.0.0 0.0.0.0 inside ssh timeout 60 console timeout 0
management-access inside dhcpd address 192.168.5.12-
192.168.5.20 inside dhcpd enable inside ! threat-
detection basic-threat threat-detection statistics
access-list ! class-map inspection_default match
default-inspection-traffic ! ! policy-map global_policy
class inspection_default inspect ftp inspect h323 h225
inspect h323 ras inspect rsh inspect sqlnet inspect
skinny inspect sunrpc inspect xdmcp inspect sip inspect
netbios inspect tftp inspect icmp ! service-policy
global_policy global url-block url-mempool 2 url-block
url-size 2 url-block block 10 username fwadmin password
aDRVKThrSs46pTjG encrypted privilege 15 prompt hostname
context Cryptochecksum:db208a243faa71f9b3e92491a6ed2105
: end
```

Configurer ASA/PIX avec ASDM

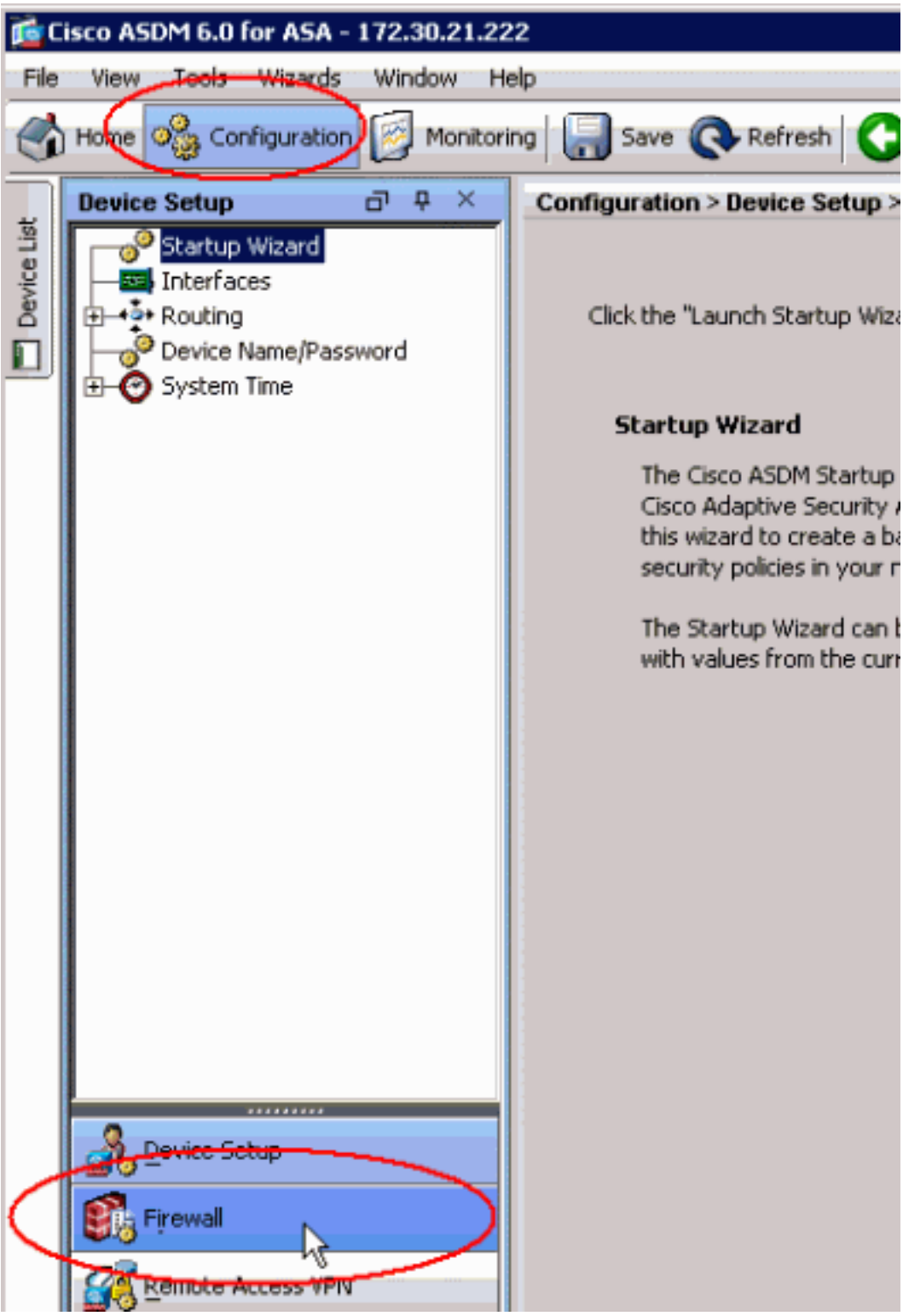
Cette section explique comment configurer le filtrage URL pour l'appliance de sécurité avec l'Adaptive Security Device Manager (ASDM).

Après avoir lancé l'ASDM, suivez ces étapes :

1. Choisissez le volet **Configuration**.

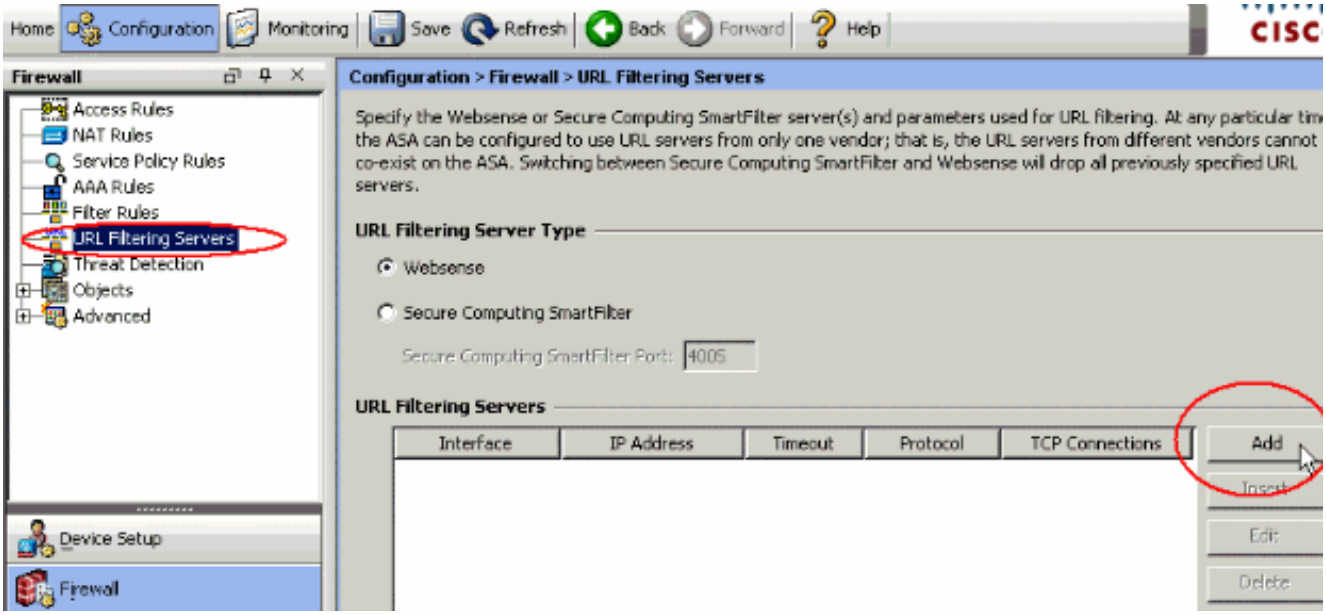


2. Cliquez sur **Firewall** dans la liste montrée dans le volet

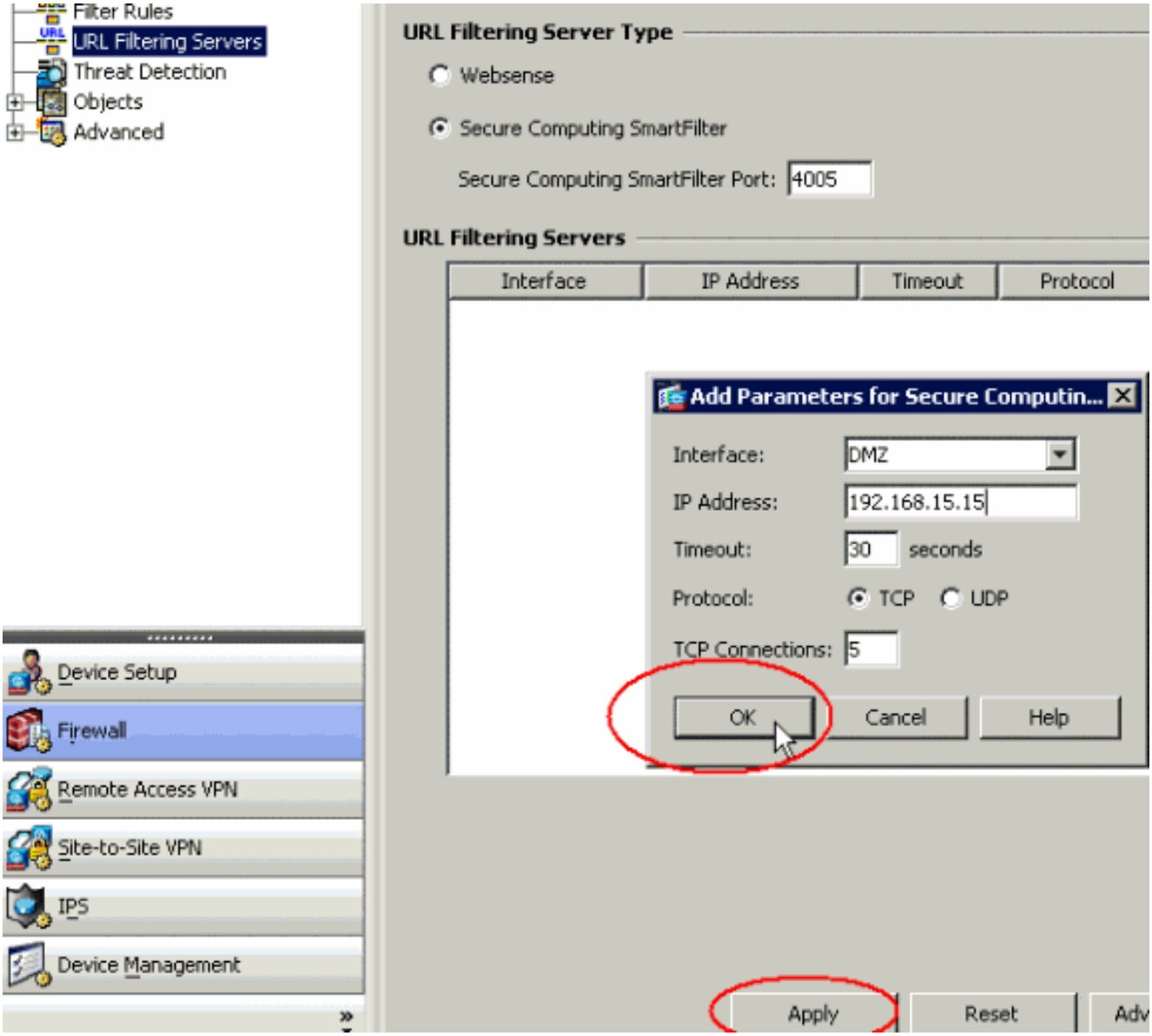


Configuration.

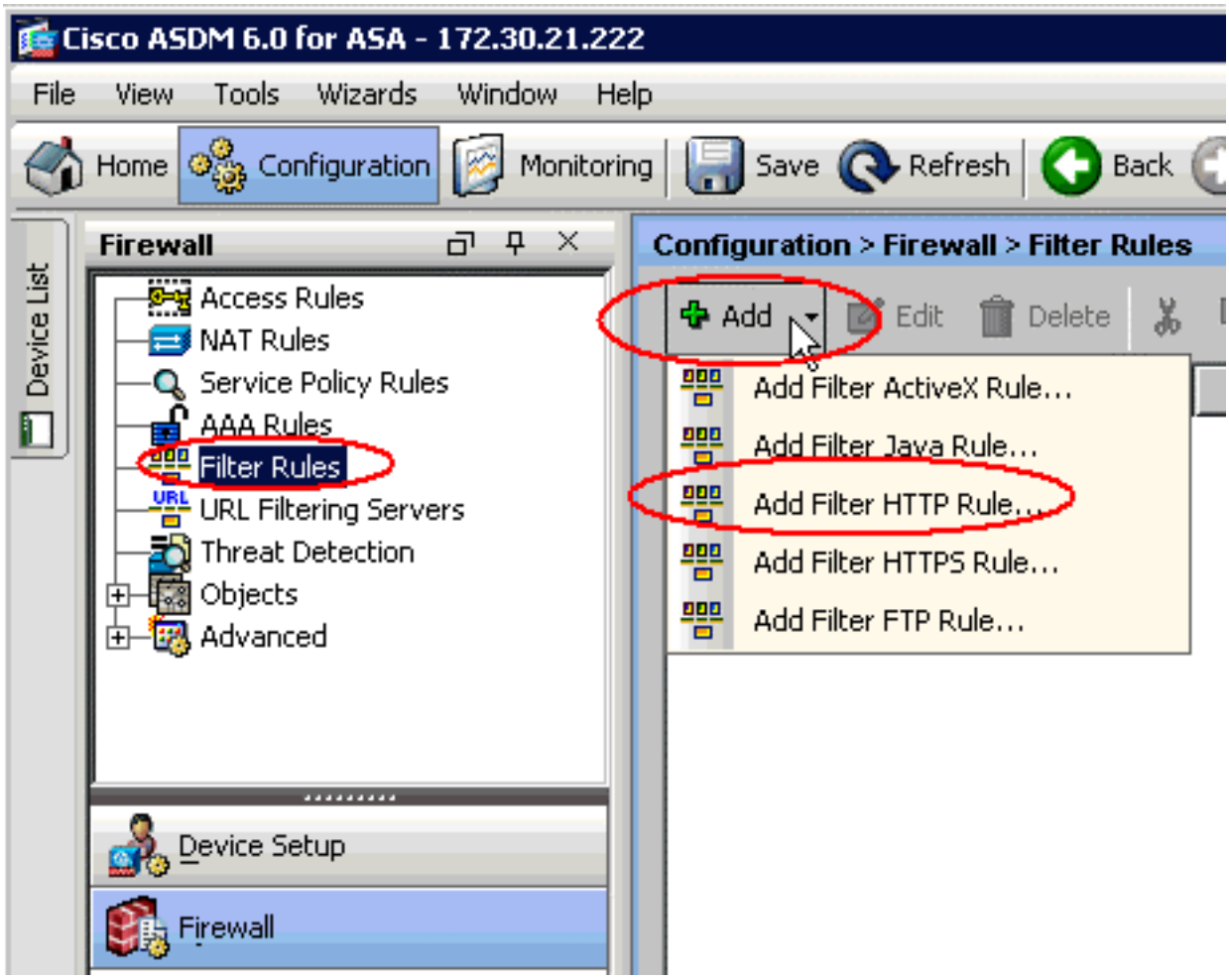
3. De la liste déroulante **Firewall**, choisissez **URL Filtering Servers**. Choisissez le type de serveur de filtrage URL que vous voulez utiliser et cliquez sur **Add** pour configurer ses paramètres.**Remarque:** Vous devez ajouter le serveur de filtrage avant de pouvoir configurer les règles de filtrage pour HTTP, HTTPS, ou
FTP.



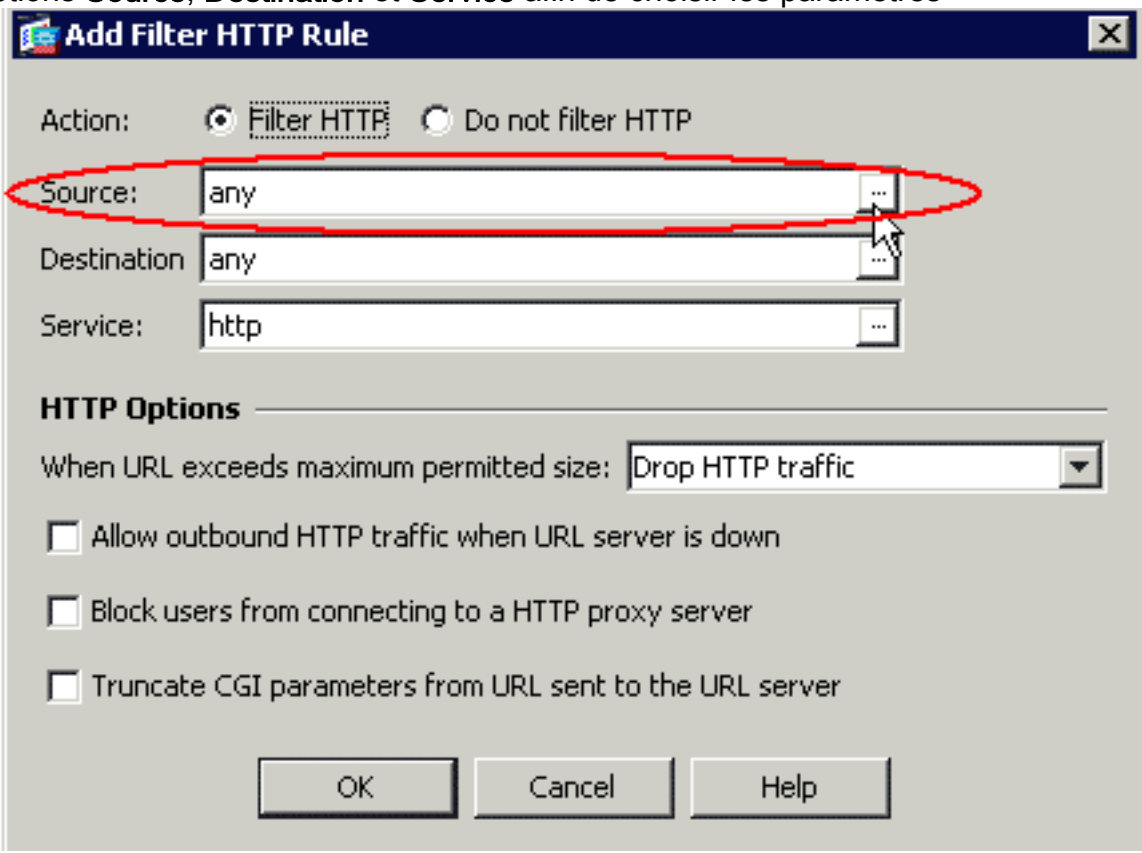
4. Choisissez les paramètres appropriés dans la fenêtre externe :Interface - Affiche l'interface connectée au serveur de filtrageIP Address - Affiche l'adresse IP du serveur de filtrageTimeout - Affiche le nombre de secondes après quoi la demande au serveur de filtrage expireProtocol - Affiche le protocole utilisé pour communiquer avec le serveur de filtrage. TCP version 1 est la valeur par défaut. TCP version 4 permet au pare-feu PIX d'envoyer des noms d'utilisateurs authentifiés et des informations de connexion URL au serveur Websense si le pare-feu PIX a déjà authentifié l'utilisateur.TCP Connections - Affiche le nombre maximal de connexions TCP autorisées à communiquer avec le serveur de filtrage URLAprès avoir entré les paramètres, cliquez sur **OK** dans la fenêtre externe et sur **Apply** dans la fenêtre
principale.



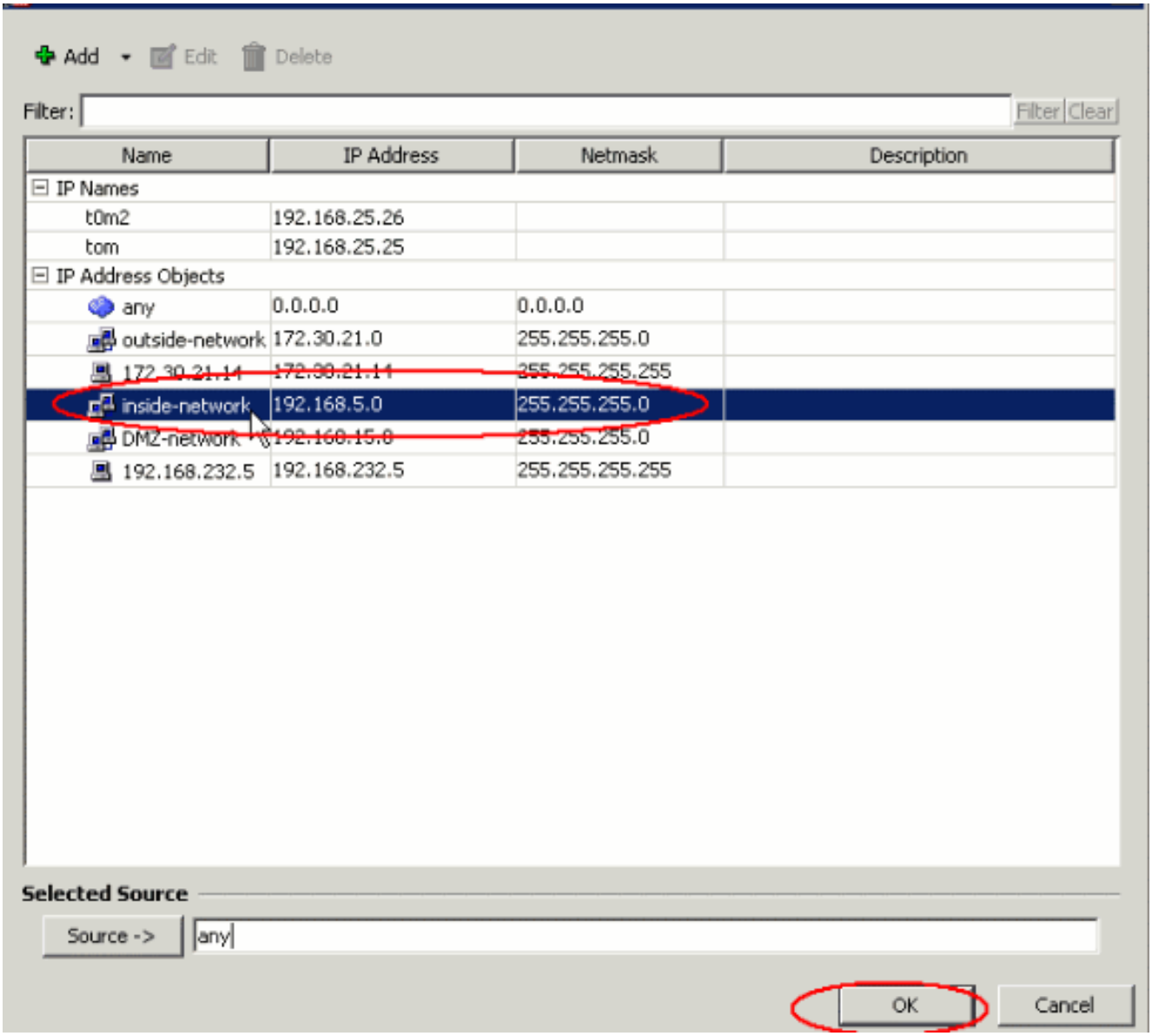
5. De la liste déroulante **Firewall**, choisissez **Filter Rules**. Cliquez sur le bouton **Add** dans la fenêtre principale et choisissez le type de règle que vous voulez ajouter. Dans cet exemple, **Add Filter HTTP Rule** est
choisi.



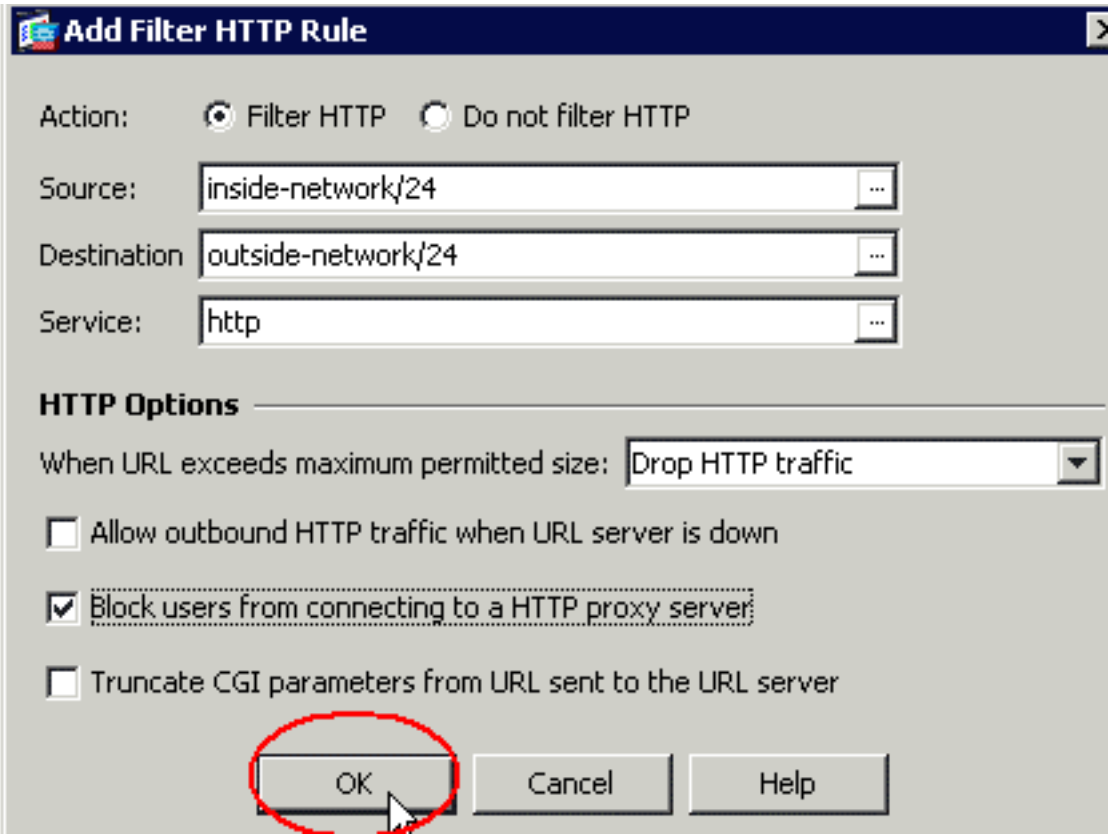
6. Une fois que la fenêtre externe apparaît, vous pouvez cliquer sur les boutons de navigation pour des options **Source**, **Destination** et **Service** afin de choisir les paramètres appropriés.



7. Ceci montre la fenêtre de navigation pour l'option **Source**. Faites votre sélection et cliquez sur **OK**.

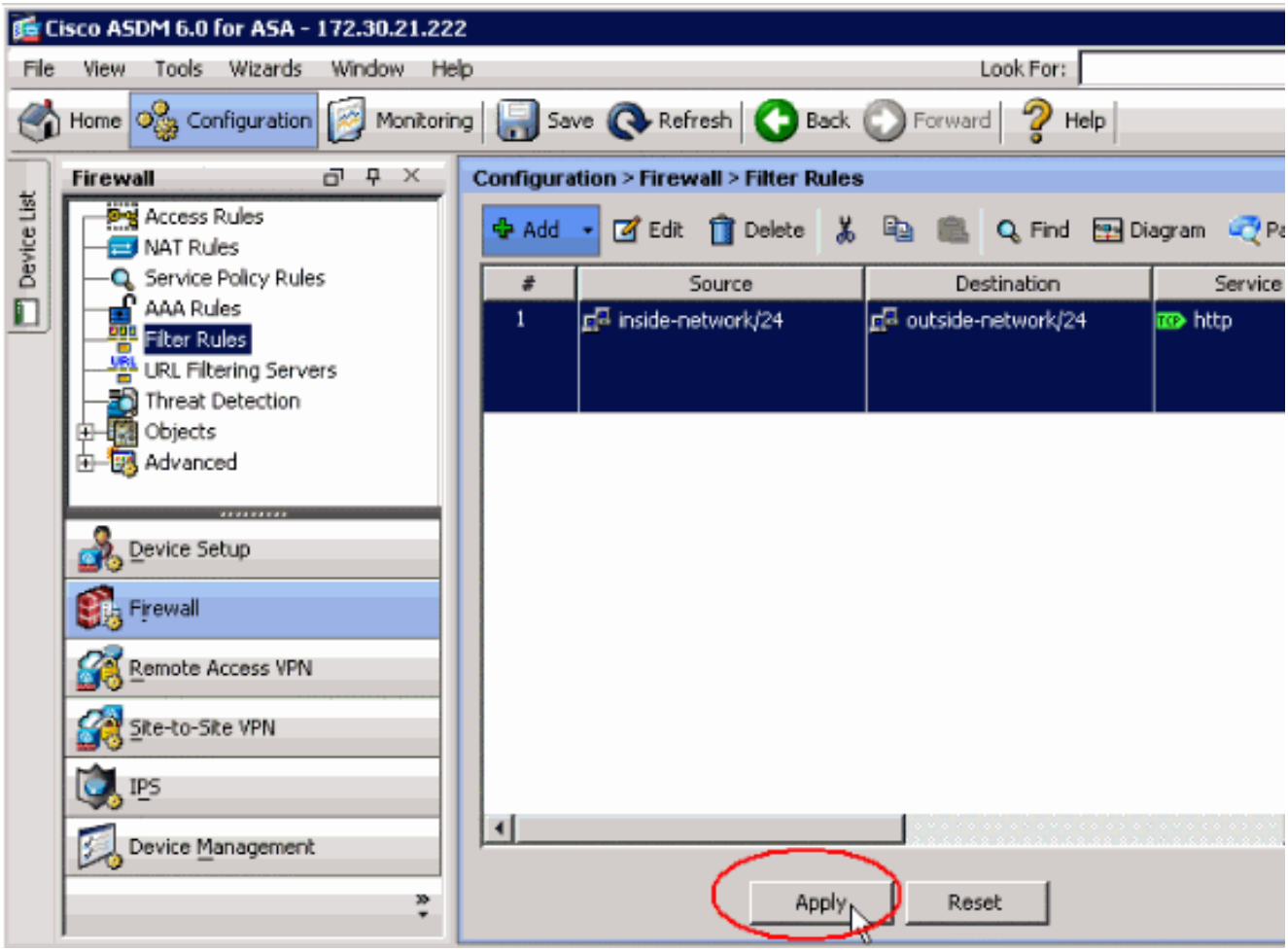


8. Après avoir fini la sélection de tous les paramètres, cliquez sur **OK** pour



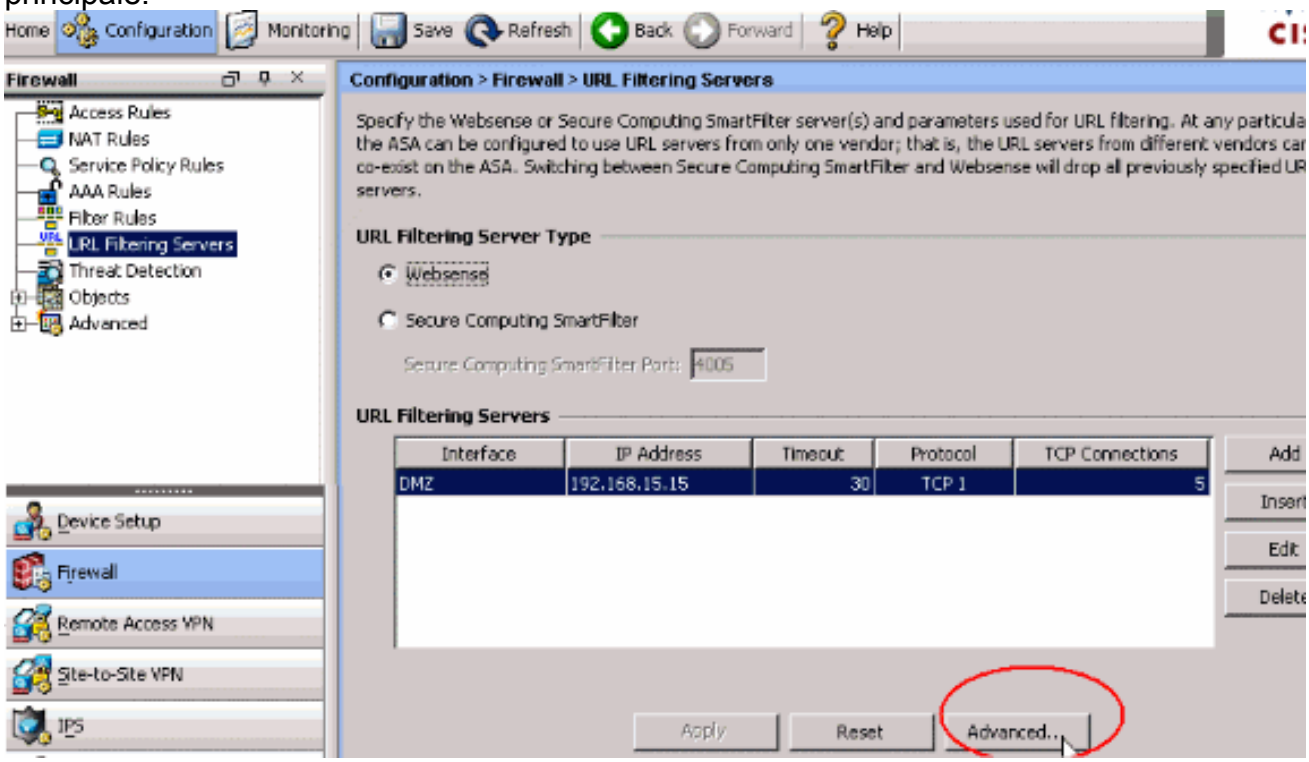
continuer.

9. Une fois que les paramètres appropriés sont configurés, cliquez sur **Apply** afin de soumettre les
modifications.

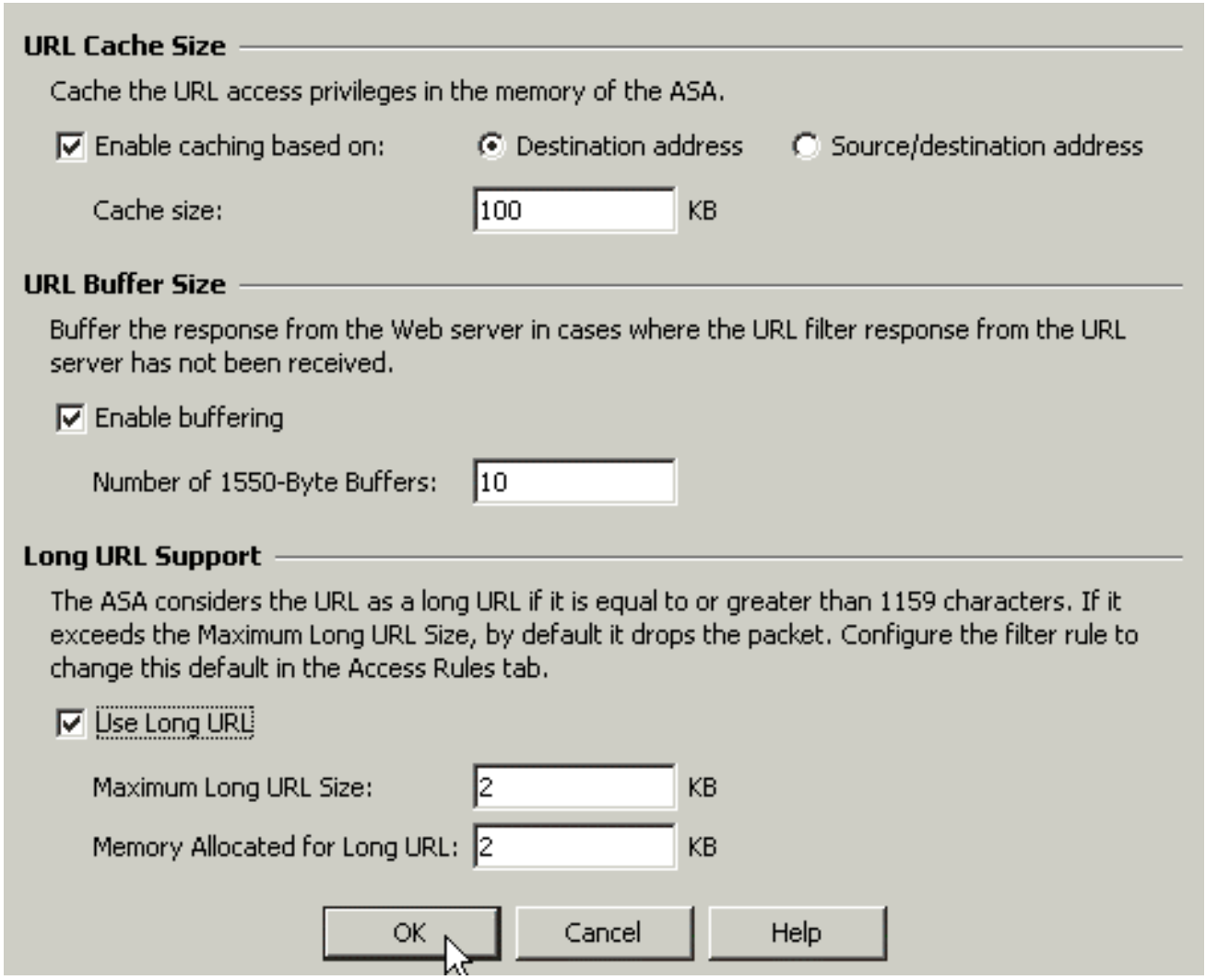


10. Pour des options de filtrage URL avancé, choisissez de nouveau **URL Filtering Servers** dans la liste déroulante **Firewall** et cliquez sur le **bouton Advanced** dans la fenêtre

principale.



11. Configurez les paramètres, tels que la taille de mise en cache d'URL, la taille de mise en mémoire tampon d'URL et le support d'URL longues, dans la fenêtre externe. Cliquez sur **OK** dans la fenêtre externe et cliquez sur **Apply** dans la fenêtre principale afin de continuer.



12. Enfin, assurez-vous que vous sauvegardez les modifications que vous apportez avant de terminer la session ASDM.

Vérifiez

Utilisez les commandes dans cette section afin d'afficher les informations de filtrage URL. Vous pouvez utiliser ces commandes afin de vérifier votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Employez l'OIT afin d'afficher une analyse de la sortie de la commande show.

- **show url-server** — Montre des informations sur le serveur de filtrageExemple :`hostname#show url-server url-server (DMZ) vendor n2h2 host 192.168.15.15 port 4444 timeout 45 protocol tcp connections 10` Dans les versions 7.2 et ultérieures du logiciel, lancez la forme **show running-config url-server** de cette commande.
- **show url-server stats** — Montre les informations et les statistiques au sujet du serveur de filtragePour la version 7.2 du logiciel, lancez la forme **show running-config url-server statistics** de cette commande.Dans les versions 8.0 et ultérieures du logiciel, lancez la forme **show url-server statistics** de cette commande.Exemple :`hostname#show url-server statistics Global Statistics: ---------- URLs total/allowed/denied 13/3/10 URLs allowed by cache/server 0/3 URLs denied by cache/server 0/10 HTTPSs total/allowed/denied 138/137/1 HTTPSs allowed by cache/server 0/137 HTTPSs denied by cache/server 0/1 FTPs total/allowed/denied 0/0/0 FTPs allowed by cache/server 0/0 FTPs denied by cache/server 0/0 Requests dropped 0 Server timeouts/retries 0/0 Processed rate average 60s/300s 0/0 requests/second Denied rate average 60s/300s 0/0 requests/second Dropped rate average 60s/300s 0/0 requests/second Server Statistics: ---------- 192.168.15.15 UP Vendor websense Port 15868 Requests total/allowed/denied 151/140/11 Server timeouts/retries 0/0 Responses received 151 Response time average 60s/300s 0/0 URL Packets Sent and Received Stats: ---------- Message Sent Received STATUS_REQUEST 1609 1601 LOOKUP_REQUEST 1526 1526 LOG_REQUEST 0 NA Errors: ------- RFC noncompliant GET method 0 URL buffer update failure 0`
- **show url-block** — Montre la configuration de la mise en mémoire tampon de blocage d'URLExemple :`hostname#show url-block url-block url-mempool 128 url-block url-size 4 url-block block 128` Dans les versions 7.2 et ultérieures du logiciel, lancez la forme **show running-config url-block** de cette commande.
- **show url-block block statistic** - Montre les statistiques de blocage d'URLExemple :`hostname#show url-block block statistics URL Pending Packet Buffer Stats with max block 128 ---------- Cumulative number of packets held: 896 Maximum number of packets held (per URL): 3 Current number of packets held (global): 38 Packets dropped due to exceeding url-block buffer limit: 7546 HTTP server retransmission: 10 Number of packets released back to client: 0` Pour la version 7.2 du logiciel, lancez la forme **show running-config url-block block statistics** de cette commande.
- **show url-cache stats** - Montre comment la mise en cache est utiliséeExemple :`hostname#show url-cache stats URL Filter Cache Stats ---------- Size : 128KB Entries : 1724 In Use : 456 Lookups : 45 Hits : 8` Dans la version 8.0 du logiciel, lancez la forme **show url-cache statistics** de cette commande.
- **show perform** - Montre les statistiques de performance de filtrage URL, avec d'autres statistiques de performance. Les statistiques de filtrage sont montrées des lignes URL Access et URL Server.Exemple :`hostname#show perfmon PERFMON STATS: Current Average Xlates 0/s 0/s Connections 0/s 2/s TCP Conns 0/s 2/s UDP Conns 0/s 0/s URL Access 0/s 2/s URL Server Req 0/s 3/s TCP Fixup 0/s 0/s TCPIntercept 0/s 0/s HTTP Fixup 0/s 3/s FTP Fixup 0/s 0/s AAA Authen 0/s 0/s AAA Author 0/s 0/s AAA Account 0/s 0/s`
- **show filter** - Montre la configuration du filtrageExemple :`hostname#show filter filter url http`

`192.168.5.5 255.255.255.255 172.30.21.99 255.255.255.255 allow proxy-block longurl-truncate cgi-truncate` Dans les versions 7.2 et ultérieures du logiciel, lancez la forme **show running-config filter** de cette commande.

Dépannez

Cette section fournit des informations sur la façon dont dépanner votre configuration.

Erreur : "%ASA-3-304009 : A manqué de blocs de mémoire tampon spécifiés par commande d'URL-bloc »

Les passages de Pare-feu hors de l'URL cachent qui est censé pour tenir des réponses de serveur quand le Pare-feu attend d'obtenir la confirmation du serveur URL.

Solution

La question est fondamentalement liée à une latence entre l'ASA et le serveur de Websense. Afin de résoudre cet essai de question ces contournements.

- Essayez de changer le protocole qui est utilisé sur l'ASA à l'UDP afin de communiquer avec le Websense.Il y a une question avec la latence entre le serveur de Websense et le Pare-feu, en lesquels les réponses du serveur de Websense prennent un longtemps de retourner au Pare-feu, ainsi ceci fait remplir la mémoire tampon URL tandis qu'il attend une réponse.Vous pouvez utiliser l'UDP au lieu du TCP pour la transmission entre le serveur de Websense et le Pare-feu. C'est parce que quand vous utilisez le TCP pour le Filtrage URL, pour chaque nouvelle demande URL, l'ASA doit établir une connexion TCP avec le serveur de Websense. Puisque l'UDP est un protocole sans connexions, l'ASA n'est pas forcée pour établir la connexion pour recevoir la réponse du serveur. Ceci devrait améliorer la représentation du serveur.`ASA(config)#`**`url-server (inside) vendor websense host X.X.X.X timeout 30`** `protocol UDP version 4 connections 5`
- Veillez à augmenter le bloc d'URL-bloc à la valeur la plus élevée possible, qui est 128. Ceci peut être vérifié avec la commande d'URL-**bloc d'exposition**.S'il affiche 128, prenez en compte l'amélioration de l'ID de bogue Cisco CSCta27415 **(clients enregistrés seulement)**.

Informations connexes

- Assistance produit des dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500
- Assistance produit des dispositifs de sécurité de la gamme Cisco PIX 500
- Assistance produit de Cisco Adaptive Security Device Manager
- PIX/ASA : Établir et dépanner les problèmes de connexion dans le dispositif de sécurité Cisco
- Dépannage des connexions via PIX et ASA
- Support et documentation techniques - Cisco Systems