SDM : Exemple de configuration de filtrage d'URL sur routeur Cisco IOS

Contenu

Introduction

Ce document montre comment configurer le filtrage d'URL sur un routeur Cisco IOS. Le filtrage d'URL permet un meilleur contrôle du trafic qui traverse le routeur Cisco IOS. Le Filtrage URL est pris en charge dans des versions de Cisco IOS dans la version 12.2(11)YU et ultérieures.

Note: 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. Basé sur la vitesse de votre réseau et la capacité de votre serveur de Filtrage URL, la durée requise pour la connexion initiale peut être sensiblement plus lente quand le trafic est filtré avec un serveur de filtrage externe.

Conditions préalables

Restrictions pour le Filtrage URL de Websense de Pare-feu

Condition requise en matière de serveur de Websense : Afin d'activer cette caractéristique, vous devez avoir au moins un serveur de Websense ; , mais deux serveurs ou plus de Websense sont préférés. Bien qu'il n'y ait aucune limite au nombre de serveurs de Websense que vous pouvez avoir, et vous pouvez configurer autant de serveurs comme vous souhaitez, seulement un serveur

peut être en activité à un moment donné — le serveur primaire. Des demandes de consultation URL sont envoyées seulement au serveur primaire.

Restriction de support de Filtrage URL : Ce les prises en charge de fonctionnalité seulement un Filtrage URL actif complotent à la fois. (Avant que vous activiez le Filtrage URL de Websense, vous devez toujours s'assurer qu'il n'y a pas un autre schéma de Filtrage URL configuré, comme N2H2.)

Restriction de nom d'utilisateur : Cette caractéristique ne passe pas le nom d'utilisateur et l'information du groupe au serveur de Websense, mais le serveur de Websense peut travailler pour des stratégies utilisateur utilisateur parce qu'elle a un autre mécanisme pour permettre au nom d'utilisateur de correspondre à une adresse IP.

Composants utilisés

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

- Routeur de Cisco 2801 avec la version de logiciel 12.4(15)T de Cisco IOS®
- Cisco Security Device Manager (SDM) version 2.5

Note: Consultez Configuration de routeur de base à l'aide de SDM afin de permettre la configuration du routeur par SDM.

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

La caractéristique de Filtrage URL de Websense de Pare-feu permet à votre Pare-feu Cisco IOS (également connu sous le nom de logiciel intégré Cisco Secure [CSIS]) d'interagir avec le logiciel de Filtrage URL de Websense. Ceci te permet pour empêcher l'accès client aux sites Web spécifiés sur la base d'une certaine stratégie. Le Pare-feu Cisco IOS fonctionne avec le serveur de Websense pour savoir si un URL particulier peut être permis ou refusé (bloqué).

Configurez le routeur avec le CLI

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

Note: 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 le réseau intérieur. 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 terminées à la demande d'utilisateur du web server :

1. L'utilisateur final navigue sur une page sur le serveur Web et le navigateur envoie une demande HTTP.
2. Après que le Pare-feu Cisco IOS reçoive cette demande, il en avant la demande au web server. Il 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. Le Pare-feu de Cisco IOS® 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 d'**ip urlfilter server vendor**. Vous devez utiliser la forme appropriée de cette commande en fonction du type de serveur de filtrage que vous utilisez.

Note: 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.

La commande d'**ip urlfilter server vendor** indique le serveur qui exécute l'application de Filtrage URL N2H2 ou de Websense. Afin de configurer un serveur de constructeur pour le Filtrage URL, utilisez la commande d'**ip urlfilter server vendor** en mode de configuration globale. Afin de retirer

un serveur de votre configuration, utilisez le forme no de cette commande. C'est la syntaxe de la commande d'**ip urlfilter server vendor** :

```
hostname(config)# ip urlfilter server vendor
   {websense | n2h2} ip-address [port port-number]
[timeout seconds] [retransmit number] [outside] [vrf vrf-name]
```

Remplacez l'`IP address` par l'adresse IP du serveur de websense. Remplacez les `secondes` par le nombre de secondes que le pare-feu d'IOS doit continuer pour essayer de se connecter au serveur de filtrage.

Par exemple, afin de configurer un serveur de filtrage simple de Websense pour le Filtrage URL, émettez cette commande :

```
hostname(config)#
   ip urlfilter server vendor websense 192.168.15.15
```

Configurer la politique de filtrage

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

Tronquer des URL HTTP longues

Afin de permettre au filtre URL pour tronquer le long URLs au serveur, utilisez la commande tronquée d'urlfilter d'IP en mode de configuration globale. Afin de désactiver l'option tronquante, utilisez le forme no de cette commande. Cette commande est prise en charge dans la version 12.4(6)T et ultérieures de Cisco IOS.

`urlfilter d'IP tronqué {script-paramètres | l'adresse Internet}` est la syntaxe de cette commande.

script-paramètres : Seulement l'URL jusqu'aux options de script est envoyé. Par exemple, si l'URL entier est `http://www.cisco.com/dev/xxx.cgi?when=now`, seulement l'URL par `http://www.cisco.com/dev/xxx.cgi` est envoyé (si la longueur URL prise en charge par maximum n'est pas dépassée).

Adresse Internet : Seulement l'adresse Internet est envoyée. Par exemple, si l'URL entier est `http://www.cisco.com/dev/xxx.cgi?when=now`, seulement `http://www.cisco.com` est envoyé.

Si les script-paramètres et les mots clé chacun des deux d'adresse Internet sont configurés, le mot clé de script-paramètres a la priorité au-dessus du mot clé d'adresse Internet. Si les deux mots clé sont configurés et l'URL de paramètres de script est tronqué et la longueur URL prise en charge par maximum est dépassée, l'URL est tronqué jusqu'à l'adresse Internet.

Note: Si des script-paramètres et l'adresse Internet de mots clé sont configurés, ils doivent être sur les lignes distinctes comme affiché ci-dessous. Ils ne peuvent pas être combinés dans une ligne.

Note: `script-paramètres tronqués d'urlfilter d'IP`

Note: `adresse Internet tronquée d'urlfilter d'IP`

Configuration pour le routeur qui exécute la version 12.4 de Cisco IOS

Cette configuration inclut les commandes décrites dans ce document :

Configuration pour le routeur qui exécute la version 12.4 de Cisco IOS

```
R3#show running-config
: Saved
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
!
!--- username cisco123 privilege 15 password
   7 104D000A061843595F
!
aaa session-id common
ip subnet-zero
!
!
ip cef
!
!
ip ips sdf location flash://128MB.sdf
ip ips notify SDEE
ip ips po max-events 100

!--- use the ip inspect name command in global
configuration mode to define a set of inspection rules.
This Turns on HTTP inspection. The urlfilter keyword
associates URL filtering with HTTP inspection.

ip inspect name test http urlfilter


!--- use the ip urlfilter allow-mode command in global
configuration mode to turn on the default mode (allow
mode) of the filtering algorithm.

ip urlfilter allow-mode on


!--- use the ip urlfilter exclusive-domain command in
global configuration mode to add or remove a domain name
to or from the exclusive domain list so that the
firewall does not have to send lookup requests to the
vendor server. Here we have configured the IOS firewall
to permit the URL www.cisco.com without sending any
lookup requests to the vendor server.

ip urlfilter exclusive-domain permit www.cisco.com


!--- use the ip urlfilter audit-trail command in global
configuration mode to log messages into the syslog
server or router.
```

```
ip urlfilter audit-trail


!--- use the ip urlfilter urlf-server-log command in
global configuration mode to enable the logging of
system messages on the URL filtering server.

ip urlfilter urlf-server-log


!--- use the ip urlfilter server vendor command in
global configuration mode to configure a vendor server
for URL filtering. Here we have configured a websense
server for URL filtering ip urlfilter server vendor
websense 192.168.15.15
no ftp-server write-enable
!
!
!--- Below is the basic interface configuration on the
router interface FastEthernet0 ip address 192.168.5.10
255.255.255.0 ip virtual-reassembly !--- use the ip
inspect command in interface configuration mode to apply
a set of inspection rules to an interface. Here the
inspection name TEST is applied to the interface
FastEthernet0. ip inspect test in
 duplex auto
 speed auto
!
interface FastEthernet1
 ip address 192.168.15.1 255.255.255.0
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet2
 ip address 10.77.241.109 255.255.255.192
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet2
 no ip address
!

interface Vlan1
 ip address 10.77.241.111 255.255.255.192
 ip virtual-reassembly
!
ip classless
ip route 10.10.10.0 255.255.255.0 172.17.1.2
ip route 10.77.0.0 255.255.0.0 10.77.241.65
!
!
!--- Configure the below commands to enable SDM access
to the cisco routers ip http server
ip http authentication local
no ip http secure-server
!
!
line con 0
line aux 0
line vty 0 4
 privilege level 15
 transport input telnet ssh
```

```
!
end
```

Configurez le routeur avec SDM

Configuration SDM du routeur

Terminez-vous ces étapes afin de configurer le Filtrage URL sur le routeur Cisco IOS :

Note: Afin de configurer le Filtrage URL avec SDM, utilisez la commande d'**ip inspect name** en mode de configuration globale de définir un ensemble de règles d'inspection. Ceci active l'inspection de HTTP. Le mot clé d'urlfilter associe le Filtrage URL avec l'inspection de HTTP. Alors le nom d'inspection configuré peut être tracé à l'interface sur laquelle le filtrage doit être fait, par exemple :

```
R3#show running-config
: Saved
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
!
!--- username cisco123 privilege 15 password
   7 104D000A061843595F
!
aaa session-id common
ip subnet-zero
!
!
ip cef
!
!
ip ips sdf location flash://128MB.sdf
ip ips notify SDEE
ip ips po max-events 100

!--- use the ip inspect name command in global configuration mode to define a set of inspection
rules. This Turns on HTTP inspection. The urlfilter keyword associates URL filtering with HTTP
inspection.

ip inspect name test http urlfilter


!--- use the ip urlfilter allow-mode command in global configuration mode to turn on the default
mode (allow mode) of the filtering algorithm.

ip urlfilter allow-mode on


!--- use the ip urlfilter exclusive-domain command in global configuration mode to add or remove
a domain name to or from the exclusive domain list so that the firewall does not have to send
lookup requests to the vendor server. Here we have configured the IOS firewall to permit the URL
www.cisco.com without sending any lookup requests to the vendor server.

ip urlfilter exclusive-domain permit www.cisco.com
```

!--- use the **ip urlfilter audit-trail** command in global configuration mode to log messages into the syslog server or router.

ip urlfilter audit-trail

!--- use the **ip urlfilter urlf-server-log** command in global configuration mode to enable the logging of system messages on the URL filtering server.

ip urlfilter urlf-server-log

!--- use the ip urlfilter server vendor command in global configuration mode to configure a vendor server for URL filtering. Here we have configured a websense server for URL filtering **ip urlfilter server vendor websense 192.168.15.15**

```
no ftp-server write-enable
!
!
```

!--- Below is the basic interface configuration on the router interface FastEthernet0 ip address 192.168.5.10 255.255.255.0 ip virtual-reassembly *!--- use the ip inspect command in interface configuration mode to apply a set of inspection rules to an interface. Here the inspection name TEST is applied to the interface FastEthernet0.* **ip inspect test in**

```
 duplex auto
 speed auto
!
interface FastEthernet1
 ip address 192.168.15.1 255.255.255.0
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet2
 ip address 10.77.241.109 255.255.255.192
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet2
 no ip address
!

interface Vlan1
 ip address 10.77.241.111 255.255.255.192
 ip virtual-reassembly
!
ip classless
ip route 10.10.10.0 255.255.255.0 172.17.1.2
ip route 10.77.0.0 255.255.0.0 10.77.241.65
!
!
```

!--- Configure the below commands to enable SDM access to the cisco routers **ip http server**
ip http authentication local
no ip http secure-server

```
!
!
line con 0
line aux 0
line vty 0 4
 privilege level 15
 transport input telnet ssh
!
end
```

1. Ouvrez votre navigateur et entrez **https://<Adresse IP de l'interface du routeur qui a été configurée pour l'accès à SDM>** pour accéder au SDM sur le routeur.Veillez à autoriser tous les avertissements que votre navigateur vous donne lié à l'authenticité de certificat ssl. Le nom d'utilisateur par défaut et le mot de passe sont tous deux vides.Le routeur présente cette fenêtre pour permettre le téléchargement de l'application SDM. Cet exemple charge l'application sur l'ordinateur local et ne fonctionne pas dans une applet Java.
2. Le téléchargement de SDM commence alors. Une fois le lanceur de SDM téléchargé, exécutez les étapes stipulées par les invites afin d'installer le logiciel et d'exécuter le lanceur de Cisco SDM.
3. Écrivez le **nom d'utilisateur et mot de passe**, si vous spécifiiez un, et cliquez sur OK.Cet exemple utilise **cisco123** comme nom d'utilisateur et **cisco123** comme mot de passe.
4. Choisissez les **tâches de Configuration->Additional** et cliquez sur le **Filtrage URL** sur la page d'accueil SDM. Cliquez sur Edit alors les **paramètres généraux**, comme affiché ici :
5. Dans la nouvelle fenêtre qui apparaît, activez les paramètres requis pour le Filtrage URL, tel que le **journal du serveur d'alerte d'allow-mode, de filtre URL, d'Audit-essai** et de **Filtrage URL**. Vérifiez les cases à côté du chaque des paramètres comme affichés. Fournissez maintenant la **taille de mise en cache** et les **informations sur la mémoire tampon de HTTP**. Fournissez également l'**interface de source** et la méthode tronquée URL sous la section **avancée** comme affiché pour permettre au filtre URL pour tronquer le long URLs au serveur. (Ici le paramètre de troncation est choisi comme **adresse Internet**.) Cliquez sur OK maintenant.
6. Choisissez maintenant les **gens du pays que l'**option de **liste URL** située sous le **Filtrage URL** tableau cliquent sur Add afin d'ajouter le nom de domaine et configurer le Pare-feu pour permettre ou refuser le nom de domaine ajouté. Vous pouvez également choisir la **liste URL d'importation d'**option si la liste d'URLs requise sont présent comme fichier. Le choix est à vous pour choisir ou l'**URL d'ajouter** ou les options de **liste URL d'importation** basées sur la condition requise et la Disponibilité de l'URL les répertorient.
7. Dans cet exemple, cliquez sur Add pour ajouter l'URL et pour configurer le pare-feu d'IOS pour permettre ou refuser l'URL au besoin. Maintenant une nouvelle fenêtre autorisée **AJOUTENT des gens du pays que l'URL** s'ouvre dans ce que l'utilisateur doit fournir le nom de domaine et décider si permettre ou refuser l'URL. Cliquez sur la case d'option à côté de l'autorisation ou refusez l'option comme affichée. Ici le nom de domaine est **www.cisco.com**, et l'utilisateur **permet l'URL www.cisco.com**. De la même manière, vous pouvez cliquer sur Add, ajouter autant d'URLs comme nécessaire, et configurer le Pare-feu à l'autorisation ou les refuser a basé sur la condition requise.
8. Choisissez l'option de **serveurs de filtre URL** située sous l'onglet de **Filtrage URL**, comme affiché. Cliquez sur Add afin d'ajouter le nom du serveur de Filtrage URL qui remplit la fonction de Filtrage URL.
9. Après que vous cliquiez sur Add, choisissez le serveur de filtrage comme **Websense** comme affiché ci-dessous puisque le serveur de filtrage de Websense est utilisé dans cet exemple.
10. En cela **ajoutez la** fenêtre de **serveur de Websense**, fournissez l'**adresse IP du** serveur de Websense avec la **direction** dans laquelle le filtre fonctionne et **numéro de port,** (le numéro de port par défaut pour le serveur de Websense est **15868**). Fournissez également le **compte de retransmission** et les valeurs du dépassement de durée de **retransmission**, comme affiché. Cliquez sur OK, et ceci se termine la configuration de **Filtrage URL**.

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 ip urlfilter statistics — Expositions les informations et statistiques au sujet du serveur de filtrageExemple :

```
Router# show ip urlfilter statistics
URL filtering statistics
================
Current requests count:25
Current packet buffer count(in use):40
Current cache entry count:3100
Maxever request count:526
Maxever packet buffer count:120
Maxever cache entry count:5000
Total requests sent to
   URL Filter Server: 44765
Total responses received from
   URL Filter Server: 44550
Total requests allowed: 44320
Total requests blocked: 224
```

- show ip urlfilter cache — Affiche le nombre maximal d'entrées qui peuvent être cachées dans la table de cache, le nombre d'entrées, et les adresses IP de destination qui sont cachées dans la table de cache quand vous utilisez la commande de show ip urlfilter cache dans le mode d'exécution privilégié
- config de filtre d'urlfilter de show ip — Affiche la configuration de filtrageExemple :

```
hostname#show ip urlfilter config

URL filter is ENABLED
Primary Websense server configurations
======================================
Websense server IP address Or Host Name:
   192.168.15.15
Websense server port: 15868
Websense retransmission time out:
   6 (in seconds)
Websense number of retransmission: 2

Secondary Websense servers configurations
=========================================
None

Other configurations
====================
Allow Mode: ON
System Alert: ENABLED
Audit Trail: ENABLED
Log message on Websense server: ENABLED
Maximum number of cache entries: 5000
Maximum number of packet buffers: 200
Maximum outstanding requests: 1000
```

Dépannez

Messages d'erreur

`%URLF-3-SERVER_DOWN : La connexion au serveur 10.92.0.9 de filtre URL est en baisse` — des affichages de ce du niveau trois message de LOG_ERR-type quand un UFS configuré descend. Quand ceci se produit, le Pare-feu marquera le serveur configuré en tant que secondaire et essai pour amener un des autres serveurs secondaires et pour marquer ce serveur en tant que serveur primaire. S'il n'y a aucun autre serveur configuré, le Pare-feu entrera permettent le mode et affichent le message `URLF-3-ALLOW_MODE`.

`%URLF-3-ALLOW_MODE : La connexion à tous les serveurs de filtre URL sont en baisse et PERMETTENT LE MODE est éteinte` — les affichages de ce LOG_ERR message de type quand tout l'UFSs sont vers le bas, et le système entre permettent le mode.

Note: Toutes les fois que le système entre dans permettez le mode (tous les serveurs de filtre sont en panne), un temporisateur périodique de keep-alive est déclenché qui tente d'ouvrir une connexion TCP et d'amener un serveur.

`%URLF-5-SERVER_UP : Le rapport à un serveur 10.92.0.9 de filtre URL est établi ; le système retourne de PERMETTENT LE MODE` — des affichages de ce message de LOG_NOTICE-type quand l'UFSs sont détectés pendant que vers le haut de et les retours de système du mode d'autoriser.

`%URLF-4-URL_TOO_LONG:URL trop long (plus de 3072 octets), probablement un faux paquet ?` — Affichages de ce message de LOG_WARNING-type quand l'URL dans une demande de consultation est trop long ; n'importe quel URL plus long que 3K est lâché.

`%URLF-4-MAX_REQ : Le nombre de demande en suspens dépasse la limite maximum <1000>` — les affichages de ce message de LOG_WARNING-type quand le nombre de demandes en suspens dans le système dépasse la limite maximum, et tout demande en outre sont abandonnés.

Informations connexes

- Cisco IOS Firewall
- Filtrage URL de Websense de Pare-feu
- Guide de configuration de Cisco IOS Security, version 12.4-Support
- Support et documentation techniques - Cisco Systems