Configurez la redirection transparente avec le WCCP afin de réorienter le trafic FTP indigène

Contenu

Introduction

Ce document décrit comment configurer l'appliance de sécurité Web (WSA)/routeur de Cisco afin de prendre en charge la redirection transparente du HTTP, du HTTPS, et du trafic FTP indigène avec le Web Cache Communication Protocol (WCCP).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- Appliance de sécurité Web de Cisco qui exécute la version 6.0 ou ultérieures d'AsyncOS
- Proxy indigène de FTP activé sur WSA
- Routeur WCCPv2 Cisco/commutateur ou Pare-feu compatible ASA

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.

Configurez

Quand le trafic FTP indigène est réorienté d'une manière transparente au WSA, le WSA reçoit

typiquement le trafic sur le port standard 21 de FTP. Par conséquent, le proxy indigène de FTP sur le WSA devrait écouter sur le port 21 (par défaut le proxy indigène de FTP est 8021). Dans le GUI, choisissez les **Services de sécurité >** le **proxy de FTP** pour la vérification.

Configuration WSA

1. Créez une identité pour le trafic FTP. Dans le GUI, choisissez le **gestionnaire >** les **identités de sécurité Web** et assurez-vous que l'authentification a été désactivée pour cet ID.
2. Créez une stratégie d'accès. Dans le GUI, choisissez le **gestionnaire de sécurité Web >** les **stratégies d'Access,** qui met en référence l'identité dans l'étape 1.
3. Sous des paramètres de proxy de FTP, modifiez les ports passifs de FTP pour être 11000-11006 afin d'assurer à cela tous les ports insérés dans un groupe à usage unique.
4. Créez ces id de service WCCP :

   Ports de service de nom
   Web-cache 0 80 *(alternativement, vous pouvez utiliser le coutume-Web-cache 98 si vous utilisez plusieurs WSAs)*
   60 21,11000,11001,11002,11003,11004,11005,11006 FTP-indigènes
   https-cache 70 443

Ces exemples réorientent trois sous-réseaux internes tandis qu'ils sautent la redirection WCCP pour toutes les destinations en privé adressées aussi bien qu'un hôte interne simple.

Configuration de l'échantillon ASA

```
wccp web-cache redirect-list web-cache group-list group_acl
wccp 60 redirect-list ftp-native group-list group_acl
wccp 70 redirect-list https-cache group-list group_acl

wccp interface inside web-cache redirect in
wccp interface inside 60 redirect in
wccp interface inside 70 redirect in

access-list group_acl extended permit ip host 10.1.1.160 any

access-list ftp-native extended deny ip any 10.0.0.0 255.0.0.0
access-list ftp-native extended deny ip any 172.16.0.0 255.240.0.0
access-list ftp-native extended deny ip any 192.168.0.0 255.255.0.0
access-list ftp-native extended deny ip host 192.168.42.120 any
access-list ftp-native extended permit tcp 192.168.42.0 255.255.255.0 any eq ftp
access-list ftp-native extended permit tcp 192.168.42.0 255.255.255.0 any range 11000
11006
access-list ftp-native extended permit tcp 192.168.99.0 255.255.255.0 any eq ftp
access-list ftp-native extended permit tcp 192.168.99.0 255.255.255.0 any range 11000
11006
access-list ftp-native extended permit tcp 192.168.100.0 255.255.255.0 any eq ftp
access-list ftp-native extended permit tcp 192.168.100.0 255.255.255.0 any range 11000
11006

access-list https-cache extended deny ip any 10.0.0.0 255.0.0.0
access-list https-cache extended deny ip any 172.16.0.0 255.240.0.0
access-list https-cache extended deny ip any 192.168.0.0 255.255.0.0
access-list https-cache extended deny ip host 192.168.42.120 any
access-list https-cache extended permit tcp 192.168.42.0 255.255.255.0 any eq https
access-list https-cache extended permit tcp 192.168.99.0 255.255.255.0 any eq https
```

```
access-list https-cache extended permit tcp 192.168.100.0 255.255.255.0 any eq https

access-list web-cache extended deny ip any 10.0.0.0 255.0.0.0
access-list web-cache extended deny ip any 172.16.0.0 255.240.0.0
access-list web-cache extended deny ip any 192.168.0.0 255.255.0.0
access-list web-cache extended deny ip host 192.168.42.120 any
access-list web-cache extended permit tcp 192.168.42.0 255.255.255.0 any eq www
access-list web-cache extended permit tcp 192.168.99.0 255.255.255.0 any eq www
access-list web-cache extended permit tcp 192.168.100.0 255.255.255.0 any eq www
```

Configuration de commutateur témoin (c3560)

Ceci devrait travailler à la plupart des Routeurs aussi.

```
ip wccp web-cache redirect-list web-cache group-list group_acl
ip wccp 60 redirect-list ftp-native group-list group_acl
ip wccp 70 redirect-list https-cache group-list group_acl

interface Vlan99
ip address 192.168.99.1 255.255.255.0
ip wccp web-cache redirect in
ip wccp 60 redirect in
ip wccp 70 redirect in

interface Vlan100
ip address 192.168.100.1 255.255.255.0
ip wccp web-cache redirect in
ip wccp 60 redirect in
ip wccp 70 redirect in

interface Vlan420
ip address 192.168.42.1 255.255.255.0
ip helper-address 192.168.100.20
ip wccp web-cache redirect in
ip wccp 60 redirect in
ip wccp 70 redirect in

ip access-list extended ftp-native
deny   ip any 10.0.0.0 0.255.255.255
deny   ip any 172.16.0.0 0.15.255.255
deny   ip any 192.168.0.0 0.0.255.255
deny   ip host 192.168.42.120 any
permit tcp 192.168.42.0 0.0.0.255 any eq ftp
permit tcp 192.168.42.0 0.0.0.255 any range 11000 11006
permit tcp 192.168.99.0 0.0.0.255 any eq ftp
permit tcp 192.168.99.0 0.0.0.255 any range 11000 11006
permit tcp 192.168.100.0 0.0.0.255 any eq ftp
permit tcp 192.168.100.0 0.0.0.255 any range 11000 11006

ip access-list extended https-cache
deny   ip any 10.0.0.0 0.255.255.255
deny   ip any 172.16.0.0 0.15.255.255
deny   ip any 192.168.0.0 0.0.255.255
deny   ip host 192.168.42.120 any
permit tcp 192.168.42.0 0.0.0.255 any eq 443
permit tcp 192.168.99.0 0.0.0.255 any eq 443
permit tcp 192.168.100.0 0.0.0.255 any eq 443

ip access-list extended web-cache
deny   ip any 10.0.0.0 0.255.255.255
deny   ip any 172.16.0.0 0.15.255.255
deny   ip any 192.168.0.0 0.0.255.255
```

```
deny   ip host 192.168.42.120 any
permit tcp 192.168.42.0 0.0.0.255 any eq www
permit tcp 192.168.99.0 0.0.0.255 any eq www
permit tcp 192.168.100.0 0.0.0.255 any eq www

ip access-list standard group_acl
permit 10.1.1.160
```

> **Note**: En raison d'une limite de technologie WCCP, un maximum de huit ports peut être assigné par ID de service WCCP.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.