네이티브 FTP 트래픽을 리디렉션하기 위해 WCCP를 사용하여 투명 리디렉션 구성

목차

소개

이 문서에서는 WCCP(Web Cache Communication Protocol)를 사용하여 HTTP, HTTPS 및 네이티브 FTP 트래픽의 투명 리디렉션을 지원하기 위해 WSA(Web Security Appliance)/Cisco 라우터를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- AsyncOS 버전 6.0 이상을 실행하는 Cisco Web Security Appliance
- WSA에서 활성화된 네이티브 FTP 프록시
- WCCPv2 호환 Cisco 라우터/스위치 또는 ASA 방화벽

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

네이티브 FTP 트래픽이 WSA에 투명하게 리디렉션되면 WSA는 일반적으로 표준 FTP 포트 21에서 트래픽을 수신합니다. 따라서 WSA의 네이티브 FTP 프록시가 포트 21에서 수신해야 합니다(기본적으로 네이티브 FTP 프록시는 8021). GUI에서 **Security Services(보안 서비스) >FTP Proxy(FTP**

프록시를 선택하여 확인합니다.

WSA 컨피그레이션

1. FTP 트래픽에 대한 ID를 생성합니다.GUI에서 **Web Security Manager > Identities**를 선택하고 이 ID에 대한 인증이 비활성화되었는지 확인합니다.
2. 액세스 정책을 생성합니다.GUI에서 **Web Security Manager > Access Policies(액세스 정책)**를 선택합니다. 이 정책은 1단계에서 ID를 참조합니다.
3. FTP 프록시 설정에서 모든 포트가 단일 서비스 그룹에 맞는지 확인하기 위해 FTP Passive 포트를 11000-11006으로 수정합니다.
4. 다음 WCCP 서비스 ID를 생성합니다.

   이름 서비스 포트
   web-cache 0 80*(또는 여러 WSA를 사용하는 경우 98 custom-web-cache를 사용할 수 있음)*
   ftp-native 60 21,1100,11001,11002,11003,11004,11005,11006
   https-cache 70 443

이 예에서는 3개의 내부 서브넷을 리디렉션하는 동시에 모든 개인 주소 지정 대상 및 단일 내부 호스트에 대해 WCCP 리디렉션을 우회합니다.

샘플 ASA 컨피그레이션

```
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
```

샘플 스위치 구성(c3560)

대부분의 라우터에서도 작동해야 합니다.

```
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
```

참고:WCCP 기술 제한으로 인해 WCCP 서비스 ID당 최대 8개의 포트를 할당할 수 있습니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.