用WCCP配置透明重定向为了重定向本地FTP数据流

Contents

Introduction

本文描述如何配置Web安全工具(WSA) /Cisco路由器为了支持HTTP、HTTPS和本地FTP数据流透明重定向与WEB缓存通信协议(WCCP)。

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

本文档中的信息基于以下软件和硬件版本：

- Cisco Web运行AsyncOS版本6.0或以上的安全工具
- 在WSA启用的本地FTP代理
- WCCPv2兼容的Cisco路由器/交换机或者ASA防火墙

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

Configure

当本地FTP数据流重定向透明地对WSA时， WSA典型地收到在标准的FTP端口21的数据流。因此，在WSA的本地FTP代理在端口21应该监听(默认情况下本地FTP代理是8021)。在GUI中，请选择**安全服务**>验证的**FTP代理**。

WSA 配置

1. 创建FTP数据流的一个身份。在GUI中，请选择**Web安全经理>身份**并且保证认证为此ID被禁用。
2. 创建一个访问策略。在GUI中，请选择**Web安全经理>**Access**策略，**参考身份step1。
3. 在FTP代理设置下，请修改FTP被动端口是11000-11006为了保证所有端口适合到一个单路供电的组。
4. 创建这些WCCP服务ID ：

   域名服务端口
   web-cache 0 80 *(二者择一，您能使用98自定义Web高速缓冲存储器，如果使用多个WSAs)*
   ftp本地60 21,11000,11001,11002,11003,11004,11005,11006
   https高速缓冲存储器70 443

这些示例重定向三内部子网，当他们绕过所有私下寻址的目的地以及单个内部主机的时WCCP重定向。

示例ASA配置

```
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
```

示例交换机配置(c3560)

这应该在多数路由器也是运作。

```
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:由于WCCP技术限制，最多八个端口可以每个WCCP服务ID分配。

Verify

当前没有可用于此配置的验证过程。

Troubleshoot

目前没有针对此配置的故障排除信息。