ネイティブ FTP トラフィックをリダイレクトするために WCCP での透過的リダイレクトを設定する

目次

概要

この資料記述しますどのように設定するため Web セキュリティ アプライアンス（WSA）/Ciscoルータ Web Cache Communication Protocol （WCCP）の HTTP、HTTPS および FTP ネイティブ トラフィックの透過的なリダイレクションをサポートするため。

前提条件

要件

このドキュメントに関しては個別の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- AsyncOS バージョン 6.0 または それ 以降を実行する Cisco Web セキュリティ アプライアンス
- WSA で有効に なる FTP ネイティブ プロキシ
- WCCPv2 互換性のある Ciscoルータ/スイッチまたは ASA ファイアウォール

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

設定

FTP ネイティブ トラフィックが WSA に透過的にリダイレクトされるとき、WSA は一般的に FTP 標準ポート 21 のトラフィックを受信します。 それ故に、WSA の FTP ネイティブ プロキシはポート 21 で受信する必要があります (FTP ネイティブ プロキシは 8021) デフォルトであります。 GUI で、**サービス** > 確認のための **FTP プロキシを**『Security』 を選択 して下さい。

WSA の設定

1. FTP トラフィックのための識別を作成して下さい。 GUI で、**Web セキュリティ マネージャ > 識別を**選択し、認証がこの ID のために無効に なったことを確認して下さい。
2. アクセスポリシーを作成して下さい。 GUI で、ステップ 1.で識別を参照する**アクセスポリシー**選択して下さい、**> Web セキュリティ マネージャを**。
3. FTP プロキシ設定の下で、11000-11006 であるために FTP 受動ポートをそれにシングル サービス グループに合うすべてのポートを確認するために修正して下さい。
4. これらの WCCP サービス ID を作成して下さい:

   ネーム・サービス ポート
   多重 WSAs を使用する場合 web-cache 0 80 *(代わりに、カスタム Web キャッシュを 98 使用できます)*
   ftp ネイティブ 60 21,11000,11001,11002,11003,11004,11005,11006
   https キャッシュ 70 443

それらがすべての個人的に 当たった 宛先、また単一 内部 ホストのための WCCP リダイレクションをバイパスする間、これらのリダイレクト例 3 つの内部サブネット。

ASA の設定例

```
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
```

サンプル スイッチ設定（c3560）

これはほとんどのルータで動作するも必要があります。

```
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
```

> **注:** WCCP 技術的な制限が原因で、最大 8 つのポートは WCCP サービス ID ごとに割り当てることができます。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。