目次

概要

このドキュメントでは、ゾーンベース ファイアウォール（ZBF）機能を使用して、Dynamic Host Control Protocol（DHCP）サーバまたは DHCP クライアントとして機能するルータの設定方法について説明します。 DHCP と ZBF を同時に有効にすることはよく行われることであり、以下の設定に関するヒントがこれらの機能を正しく動作させるのに役立ちます。

前提条件

要件

Cisco UCS® ソフトウェアのゾーンベース ファイアウォールについて理解しておくことをお勧めします。 詳細については、「ゾーンベース ポリシー ファイアウォールの設計と適用ガイド」を参照してください。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、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、クリアな（デフォルト）設定で作業を開始して

います。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

機能情報

IOS ルータ上で ZBF が有効になっている場合は、セルフ ゾーンへのトラフィック（つまり、ルータの管理プレーン宛てのトラフィック）がコードの IOS 15.x トレインでデフォルトで許可されます。

任意のゾーン（内部や外部など）からセルフ ゾーン方向のポリシー（out-to-self ポリシー）またはその逆方向のポリシー（self-to-out ポリシー）が作成されている場合は、それらのゾーンに適用するポリシーで許可トラフィックを明示的に定義する必要があります。 許可トラフィックを定義するには、検査またはパス アクションを使用します。

データ分析

DHCP では、ブロードキャスト User Datagram Protocol（UDP）パケットを使用して DHCP プロセスが実行されます。 このような UDP ブロードキャスト パケットに対して検査アクションが指定されたゾーンベース ファイアウォール設定では、このようなパケットがルータによってドロップされ、DHCP プロセスが失敗する可能性があります。 次のログ メッセージが表示されることもあります。

Cisco Bug ID CSCso53376「ブロードキャスト トラフィックに対して ZBF 検査が機能しない」に記載された問題を参照してください。

この問題を回避するには、検査アクションではなくパス アクションが DHCP トラフィックに適用されるようにゾーンベース ファイアウォール設定を変更します。

> **注** これが必要なのは、ポリシーがルータ上のセルフ ゾーンに適用されている場合だけです。

UDP トラフィックに対するパス アクションを使用した DHCP クライアントとしてのゾーンベース ファイアウォール

設定

この設定例では、ルータとの間でやり取りされるすべての UDP トラフィックに対するポリシーマップで検査アクションではなくパス アクション セットが使用されます。

確認

ルータが正常に DHCP アドレスを取得したかどうかを検証するには、Syslog を確認します。

out-to-self ポリシーと self-to-out ポリシーの両方が UDP トラフィックを通過させるように設定されている場合は、次の syslog のように、ルータが DHCP から IP アドレスを取得できます。

out-to-self ゾーン ポリシーだけが UDP トラフィックを通過させるように設定されている場合も、ルータは DHCP から IP アドレスを取得でき、次の syslog が作成されます。

self-to-out ゾーン ポリシーだけが UDP トラフィックを通過させるように設定されている場合も、ルータは DHCP から IP アドレスを取得でき、次の syslog が作成されます。

DHCP トラフィックに対するパス アクションを使用したゾーン ベース ファイアウォール

設定

この設定例では、特定のゾーンからルータのセルフ ゾーンへの DHCP パケット以外のすべての UDP トラフィックを禁止する方法を示します。 DHCP トラフィックのみを許可するには、特定のポートを含むアクセス リストを使用します。 この例では、UDP ポート 67 と UDP ポート 68 が一致するように指定されます。 アクセス リストを参照するクラス マップにパス アクションが適用されます。

```
access-list extended 111
 10 permit udp any any eq 67

access-list extended 112
 10 permit udp any any eq 68

class-map type inspect match-any self-to-out
match access-group 111
class-map type inspect match-any out-to-self
match access-group 112

zone security outside
zone security inside

interface Ethernet0/1
zone-member security outside
interface Ethernet0/2
zone-member security inside

policy-map type inspect out-to-self
class type inspect out-to-self
pass
class class-default
drop
policy-map type inspect self-to-out
class type inspect self-to-out
pass
class class-default
drop

zone-pair security out-to-self source outside destination self
service-policy type inspect out-to-self
zone-pair security self-to-out source self destination outside
service-policy type inspect self-to-out
```

確認

ルータがゾーン ファイアウォール経由の DHCP トラフィックを許可していることを確認するには、**show policy-map type inspect zone-pair sessions コマンド**の出力をチェックします。 この出力例では、強調表示されているカウンタが、パケットがゾーン ファイアウォールを通過していることを示しています。 これらのカウンタが 0 の場合は、設定に問題があるか、パケットが処理用のルータに到着していません。

```
router#show policy-map type inspect zone-pair sessions

policy exists on zp out-to-self
Zone-pair: out-to-self
Service-policy inspect : out-to-self
Class-map: out-to-self (match-any)
Match: access-group 112
3 packets, 924 bytes
30 second rate 0 bps
Pass
6 packets, 1848 bytes

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes

policy exists on zp self-to-out
Zone-pair: self-to-out
Service-policy inspect : self-to-out
Class-map: self-to-out (match-any)
Match: access-group 111
6 packets, 3504 bytes
30 second rate 0 bps
Pass
6 packets, 3504 bytes

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes
```

不正な設定のシナリオ

このサンプル シナリオでは、ルータが DHCP トラフィックに対して検査アクションを指定するように間違って設定されている場合の動作を示します。 このシナリオでは、ルータが DHCP クライアントとして設定されます。 ルータは、DHCP ディスカバリ メッセージを送出して IP アドレスを取得しようとします。 ゾーンベース ファイアウォールは、この DHCP トラフィックを検査するように設定されます。 ZBF の設定例を以下に示します。

```
router#show policy-map type inspect zone-pair sessions

policy exists on zp out-to-self
Zone-pair: out-to-self
Service-policy inspect : out-to-self
Class-map: out-to-self (match-any)
Match: access-group 112
3 packets, 924 bytes
30 second rate 0 bps
Pass
6 packets, 1848 bytes
```

```
Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes

policy exists on zp self-to-out
Zone-pair: self-to-out
Service-policy inspect : self-to-out
Class-map: self-to-out (match-any)
Match: access-group 111
6 packets, 3504 bytes
30 second rate 0 bps
Pass
6 packets, 3504 bytes

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes
```

self-to-out ポリシーが UDP トラフィックに対する検査アクション用に設定されている場合は、DHCP ディスカバリ パケットがドロップされ、次の syslog が作成されます。

```
router#show policy-map type inspect zone-pair sessions

policy exists on zp out-to-self
Zone-pair: out-to-self
Service-policy inspect : out-to-self
Class-map: out-to-self (match-any)
Match: access-group 112
3 packets, 924 bytes
30 second rate 0 bps
Pass
6 packets, 1848 bytes

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes

policy exists on zp self-to-out
Zone-pair: self-to-out
Service-policy inspect : self-to-out
Class-map: self-to-out (match-any)
Match: access-group 111
6 packets, 3504 bytes
30 second rate 0 bps
Pass
6 packets, 3504 bytes

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes
```

self-to-out ポリシーと out-to-self ポリシーの両方が UDP トラフィックに対する検査アクション用に設定されている場合は、DHCP ディスカバリ パケットがドロップされ、次の syslog が作成されます:

```
router#show policy-map type inspect zone-pair sessions

policy exists on zp out-to-self
Zone-pair: out-to-self
```

```
Service-policy inspect : out-to-self
Class-map: out-to-self (match-any)
Match: access-group 112
3 packets, 924 bytes
30 second rate 0 bps
Pass
6 packets, 1848 bytes

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes

policy exists on zp self-to-out
Zone-pair: self-to-out
Service-policy inspect : self-to-out
Class-map: self-to-out (match-any)
Match: access-group 111
6 packets, 3504 bytes
30 second rate 0 bps
Pass
6 packets, 3504 bytes

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes
```

out-to-self ポリシーで UDP トラフィックに対する検査アクションが有効になっており、self-to-out ポリシーで UDP トラフィックに対するパス アクションが有効になっている場合は、DHCP オファー パケットが DHCP ディスカバリ パケットの送信後にドロップされ、次の syslog が作成されます。

```
router#show policy-map type inspect zone-pair sessions

policy exists on zp out-to-self
Zone-pair: out-to-self
Service-policy inspect : out-to-self
Class-map: out-to-self (match-any)
Match: access-group 112
3 packets, 924 bytes
30 second rate 0 bps
Pass
6 packets, 1848 bytes

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes

policy exists on zp self-to-out
Zone-pair: self-to-out
Service-policy inspect : self-to-out
Class-map: self-to-out (match-any)
Match: access-group 111
6 packets, 3504 bytes
30 second rate 0 bps
Pass
6 packets, 3504 bytes

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes
```

DHCP サーバとしてのルータ

ルータの内部インターフェイスが DHCP サーバとして機能している場合と内部インターフェイスに接続されたクライアントが DHCP クライアントの場合は、inside-to-self または self-to-inside ゾーン ポリシーが存在しなければ、DHCP トラフィックがデフォルトで許可されます。

ただし、これらのポリシーのどちらかが存在する場合は、ゾーン ペア サービス ポリシーで対象のトラフィック (UDP ポート 67 または UDP ポート 68) に対するパス アクションを設定する必要があります。

トラブルシューティング

現在のところ、ここで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。