コンテキストベース アクセス制御: 概要と設定

目次

概要

Cisco IOS® ファイアウォール フィーチャ セットの Context-Based Access Control（CBAC; コンテキストベース アクセス制御）機能を使用すると、ファイアウォールの背後で行われるアクティビティを検査できます。 CBAC では、（Cisco IOS がアクセス リストを使用するのと同じ方法で）アクセス リストを使用して、着信する必要があるトラフィックと発信する必要があるトラフィックを指定します。 ただし、CBAC アクセス リストには ip inspect 文が含まれており、プロトコルを検査して、ファイアウォールの背後にあるシステムにプロトコルが到達するまでにプロトコルが改ざんされていないことを確認できます。

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。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

CBAC は Network Address Translation（NAT; ネットワーク アドレス変換）と共に使用することもできますが、このドキュメントでは、純粋に検査目的の設定を主に扱います。 NAT を実行する場合は、アクセス リストが実際のアドレスではなくグローバル アドレスを反映する必要があります。

設定に先立ち、次の項目について検討します。

- どのトラフィックを発信させたいですか。
- どのトラフィックに着信させたいですか。
- どのトラフィックについて調査したいですか。

どのトラフィックを発信させたいですか。

発信するトラフィックはサイトのセキュリティ ポリシーによって異なりますが、この一般的な例では、すべての発信が許可されます。 アクセス リストがすべてを拒否した場合、トラフィックは一切発信できません。 次の拡張アクセス リストで、発信トラフィックを指定します。

```
access-list 101 permit ip [source-network] [source-mask] any
access-list 101 deny ip any any
```

どのトラフィックに着信させたいですか。

着信するトラフィックは、サイトのセキュリティ ポリシーによって異なります。 ただし、論理的には、ネットワークに損傷を与えないものになります。

この例では、論理的に着信を許可できると考えられるトラフィックのリストを使用します。 Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）は一般に着信可能ですが、DoS 攻撃を受ける可能性があります。 着信トラフィックのアクセス リストのサンプルを、次に示します。

拡張 IP アクセス リスト 101

```
permit tcp 10.10.10.0 0.0.0.255 any (84 matches)
permit udp 10.10.10.0 0.0.0.255 any
permit icmp 10.10.10.0 0.0.0.255 any (3 matches)
deny ip any any
```

拡張 IP アクセス リスト 102

```
permit eigrp any any (486 matches)
permit icmp any 10.10.10.0 0.0.0.255 echo-reply (1 match)
permit icmp any 10.10.10.0 0.0.0.255 unreachable
permit icmp any 10.10.10.0 0.0.0.255 administratively-prohibited
permit icmp any 10.10.10.0 0.0.0.255 packet-too-big
permit icmp any 10.10.10.0 0.0.0.255 echo (1 match)
permit icmp any 10.10.10.0 0.0.0.255 time-exceeded
deny ip any any (62 matches)
```

```
access-list 101 permit tcp 10.10.10.0 0.0.0.255 any
access-list 101 permit udp 10.10.10.0 0.0.0.255 any
access-list 101 permit icmp 10.10.10.0 0.0.0.255 any
access-list 101 deny ip any any

access-list 102 permit eigrp any any
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 echo-reply
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 unreachable
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 administratively-prohibited
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 packet-too-big
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 echo
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 time-exceeded
access-list 102 deny ip any any
```

アクセス リスト 101 は発信トラフィック用です。 アクセス リスト 102 は着信トラフィック用です。 アクセス リストでは、ルーティング プロトコル、Enhanced Interior Gateway Routing Protocol（EIGRP）、および特定の ICMP 着信トラフィックだけを許可しています。

この例では、ルータのイーサネット側のサーバに、インターネットからアクセスできません。 アクセス リストは、セッションを確立し、これをブロックします。 アクセスできるようにするには、アクセス リストを変更してやり取りを許可する必要があります。 アクセス リストを変更するには、アクセス リストを削除し、編集し、更新されたアクセス リストを再適用します。

注: 編集して再適用する前にアクセス リスト 102 を削除するのは、アクセス リストの末尾に「deny ip any any」が指定されているためです。 この場合、アクセス リストを削除する前に新しいエントリを追加すると、新しいエントリが「deny」の後に指定されます。 したがって、そのエントリがチェックされることはありません。

次の例では、10.10.10.1 に対して Simple Mail Transfer Protocol（SMTP）だけを追加しています。

拡張 IP アクセス リスト 102

```
permit eigrp any any (385 matches)
permit icmp any 10.10.10.0 0.0.0.255 echo-reply
permit icmp any 10.10.10.0 0.0.0.255 unreachable
permit icmp any 10.10.10.0 0.0.0.255 administratively-prohibited
permit icmp any 10.10.10.0 0.0.0.255 packet-too-big
permit icmp any 10.10.10.0 0.0.0.255 echo
permit icmp any 10.10.10.0 0.0.0.255 time-exceeded
permit tcp any host 10.10.10.1 eq smtp (142 matches)
!--- In this example, you inspect traffic that has been !--- initiated from the inside network.
```

どのトラフィックについて調査したいですか。

Cisco IOS 内の CBAC は、次のものをサポートしています。

キーワード名	プロトコル
cuseeme	CUSeeMe プロトコル
ftp	File Transfer Protocol（FTP）
h323	H.323 プロトコル（例：Microsoft NetMeeting または sIntel Video Phone）
HTTP	HTTP プロトコル
rcmd	R コマンド（r-exec、r-login、r-sh）

realaudio	Real Audio プロトコル
rpc	リモート プロシージャ コール プロトコル
SMTP	Simple Mail Transfer Protocol（SMTP）
sqlnet	SQL Net プロトコル
streamworks	StreamWorks プロトコル
tcp	Transmission Control Protocol（TCP; 伝送制御プロトコル）
tftp	TFTP プロトコル
udp	User Datagram Protocol（UDP; ユーザ データグラム プロトコル）
vdolive	VDOLive プロトコル

各プロトコルにはキーワード名が対応しています。 検査するインターフェイスにキーワードを適用します。 たとえば、次の設定では、FTP、SMTP、および Telnet を検査します。

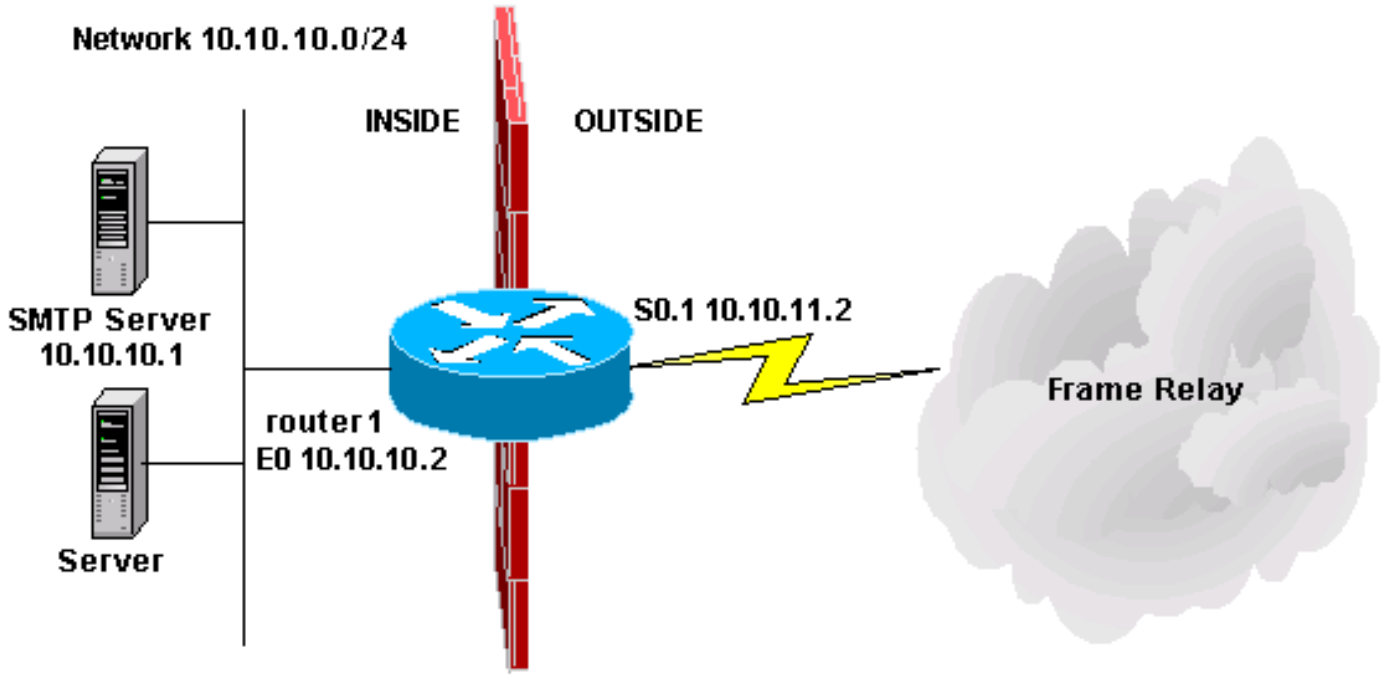
```
router1#configure
Configuring from terminal, memory, or network [terminal]? Enter configuration
commands, one per line. End with CNTL/Z.
router1(config)#ip inspect name mysite ftp
router1(config)#ip inspect name mysite smtp
router1(config)#ip inspect name mysite tcp
router1#show ip inspect config
Session audit trail is disabled
one-minute (sampling period) thresholds are [400:500]connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50.
Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
Inspection name mysite

ftp timeout 3600
smtp timeout 3600
tcp timeout 3600
```

このドキュメントでは、発信するトラフィック、着信するトラフィック、および検査するトラフィックについて説明しました。 次に、CBAC を設定する手順を示します。

1. 設定を適用します。
2. 上記で設定したようなアクセス リストを入力する。
3. 調査文を設定する。
4. アクセス リストをインターフェイスに適用します。

この手順を実行すると、次の図と設定に示される状態になります。



コンテキストベース アクセス制御設定

```
router1#configure
Configuring from terminal, memory, or network
[terminal]? Enter configuration
commands, one per line. End with CNTL/Z.
router1(config)#ip inspect name mysite ftp
router1(config)#ip inspect name mysite smtp
router1(config)#ip inspect name mysite tcp
router1#show ip inspect config
Session audit trail is disabled
one-minute (sampling period) thresholds are
[400:500]connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50.
Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
Inspection name mysite

ftp timeout 3600
smtp timeout 3600
tcp timeout 3600
```

関連情報

- Cisco IOS Firewall に関するサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems