コンテキストベースアクセスコントロール (CBAC)の設定

内容

概要

Cisco IOS® ファイアウォール機能セットのコンテキストベースのアクセス コントロール（CBAC）機能は、ファイアウォールの背後のアクティビティをアクティブに検査します。CBAC は、アクセス リストを（Cisco IOS がアクセス リストを使用するのと同じ方法で）使用して入力するトラフィックと出力す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、プロトコルがファイアウォールの背後にあるシステムに移動する前に改ざんされていないことを確認するための、プロトコルの検査を許可する ip inspect ステートメントが含まれています。

前提条件

要件

このドキュメントに特有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内容は、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、ネットワーク アドレス変換（NAT）と併用することもできますが、このマニュアルの設定では、主に純粋な検査を扱います。NAT を実行する場合、アクセス リストは、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。

設定する前に、次の質問を検討してください。

どのようなトラフィックを送信しますか。

送信するトラフィックの種類は、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、すべてがアウトバウンドで許可されています。アクセス リストがすべてを拒否すると、トラフィックは送信できません。この拡張アクセス リストを使用して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
```

どのようなトラフィックを受信しますか。

受信するトラフィックの種類は、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、論理的な答えは、ネットワークに損害を与えないということです。

この例には、受信するのが理にかなっているように見える一連のトラフィックが含まれています。Internet Control Message Protocol（ICMP）のトラフィックは一般に許容できますが、DOS 攻撃の可能性を排除できない場合があります。次は、着信トラフィックのアクセス リストの例です。

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）、および指定された ICMP 着信トラフィックのみが許可されます。

この例では、ルータのイーサネット側のサーバは、インターネットからアクセスできません。アクセス リストによって、セッションの確立がブロックされます。アクセスできるようにするには、カンバセーションの発生を許可するようにアクセス リストを変更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：編集および再適用の前にアクセスリスト102を削除する理由は、アクセスリストの最後にある「deny ip any any」によるものです。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、新しいエントリはその拒否の後に表示されます。そのため、そのエントリはチェックされません。

この例では、10.10.10.1 に対し Simple Mail Transfer Protocol（SMTP）を追加しているだけです。

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.
```

どのようなトラフィックを検査しますか。

Cisco IOS 内の CBAC は、次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（ファイル転送プロトコル）の略。
h323	H.323 プロトコル（たとえば Microsoft NetMeeting または Intel Video Phone）
http	HTTPプロトコル
rcmd	R コマンド (r-exec、r-login、r-sh)
realaudio	リアル オーディオ 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（シンプル メール転送プロトコル）の略。
sqlnet	SQL Net プロトコル
streamworks	StreamWorks プロトコル
tcp	TCP
TFTP	TFTP プロトコル
udp	ユーザ データグラム プロトコル
vdolive	VDOLive プロトコル

各プロトコルはキーワード名に関連付けられています。検査対象のインターフェイスにキーワード名を適用します。たとえば、次の設定では、FTP、SMTP、および Telnet を検査します。

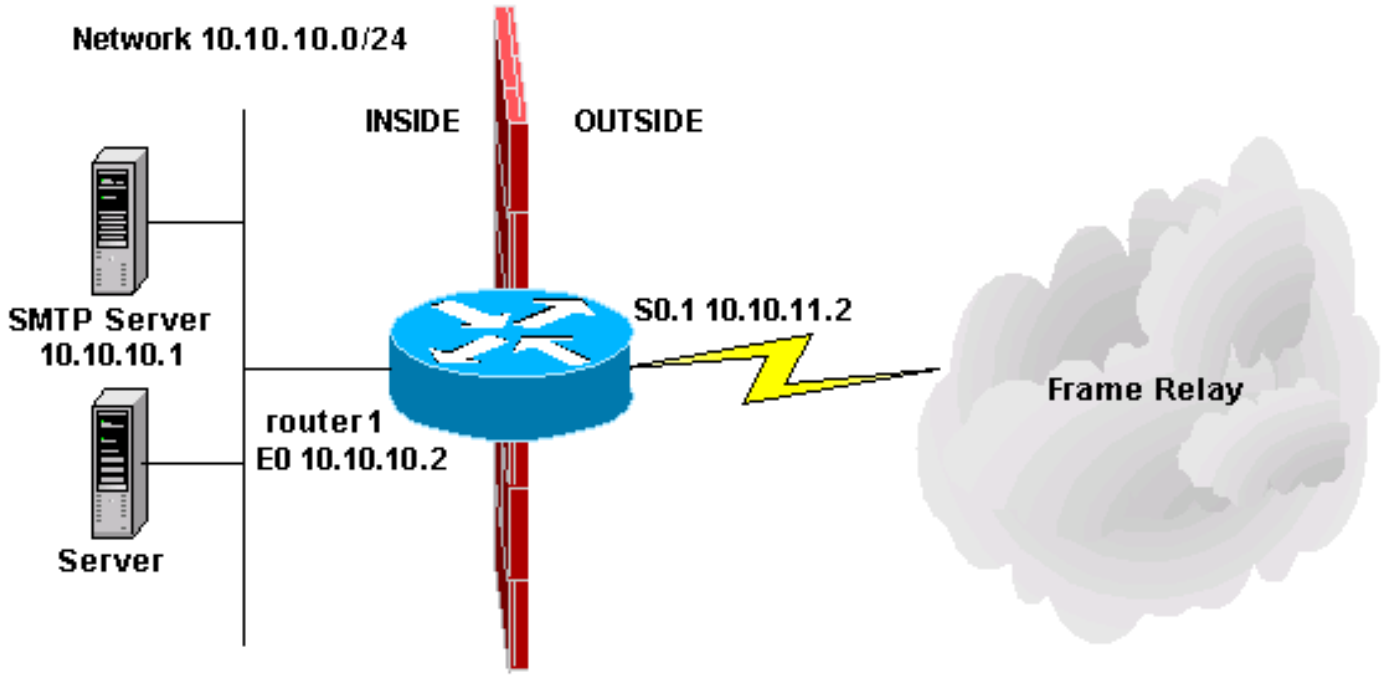
```
router1#configure
Configuring from terminal, memory, or network [terminal]? Enter configuration
commands, one per line. End with CNTL/Z.
router1(config)#ip inspect name mysite ftp
router1(config)#ip inspect name mysite smtp
router1(config)#ip inspect name mysite tcp
router1#show ip inspect config
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、どのトラフィックを送信するか、どのトラフィックを受信するか、およびどのトラフィックを検査するかについて説明します。CBAC を設定する準備ができたので、次の手順を実行します。

1. 設定を適用します。
2. 上記で設定されているアクセス リストを入力します。
3. インスペクション ステートメントを設定します。
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、設定が次の図と設定に示すように表示されます。



コンテキストベースのアクセス コントロールの設定

```
!
version 11.2
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname router1
!
!
no ip domain-lookup
ip inspect name mysite ftp
ip inspect name mysite smtp
ip inspect name mysite tcp
!
interface Ethernet0
ip address 10.10.10.2 255.255.255.0
ip access-group 101 in
ip inspect mysite in


no keepalive
!
interface Serial0
no ip address
encapsulation frame-relay
no fair-queue
!
interface Serial0.1 point-to-point
ip address 10.10.11.2 255.255.255.252
ip access-group 102 in
frame-relay interface-dlci 200 IETF
!
router eigrp 69
network 10.0.0.0
no auto-summary
!
ip default-gateway 10.10.11.1
no ip classless
ip route 0.0.0.0 0.0.0.0 10.10.11.1
```

```
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 permit tcp any host 10.10.10.1 eq smtp
access-list 102 deny ip any any
!
line con 0
line vty 0 4
login
!
end
```

関連情報

- Cisco IOS ファイアウォールのサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems