基于上下文的访问控制 (CBAC)：简介和配置

目录

简介

Cisco IOS.防火墙功能集的基于上下文的访问控制(CBAC)功能可主动检测防火墙后面的活动。
CBAC 通过使用访问列表指定需要允许什么数据流进入和需要允许什么数据流流出（以 Cisco IOS 使用访问列表的相同方式）。但是，CBAC 访问列表包括 IP 检查语句，这些语句允许检查协议以确保协议在进入防火墙保护的系统之前不会被篡改。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

CBAC 还可以与网络地址转换 (NAT) 一起使用，但本文档中的配置主要处理纯检查。如果执行 NAT，则访问列表需要反映全局地址而不是实际地址。

在进行配置之前，请考虑以下问题。

您希望允许什么数据流流出？

您希望允许什么数据流流出取决于您的站点安全策略，但在此常规示例中，允许所有数据流出站。如果您的访问列表拒绝所有数据流，则任何数据流都不能流出。请使用以下扩展访问列表指定出站数据流：

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

您希望允许什么数据流进入？

您希望允许什么数据流进入取决于您的站点安全策略。但是，合乎逻辑的答案是任何不会损害您的网络的数据流。

在本示例中，有一个数据流的列表，其中的数据流似乎在逻辑上都可以进入。Internet 控制消息协议 (ICMP) 数据流通常是可接受的，但使用它可能会受到 DOS 攻击。以下是传入数据流的示例访问列表：

扩展IP访问列表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
```

扩展 IP 访问列表 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
```

访问列表 101 针对出站数据流。访问列表 102 针对入站数据流。这些访问列表仅允许路由协议、增强型内部网关路由协议 (EIGRP) 和指定的 ICMP 入站数据流。

在示例中，路由器以太网端上的服务器不能访问互联网。访问列表阻止它建立会话。为了使它可以访问，需要修改访问控制列表，以允许会话发生。要更改访问列表，请删除访问列表，对其进行编辑，然后重新应用更新的访问列表。

注意： 在编辑并重新应用访问列表 102 之前将其删除是由于此访问列表末尾存在“deny ip any any”。在这种情况下，如果要在删除访问列表前添加新条目，新条目将在 deny 条目后出现。因此，它从不会受到检查。

本示例仅为 10.10.10.1 添加简单邮件传输协议 (SMTP)。

扩展 IP 访问列表 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.
```

您希望检查什么数据流？

Cisco IOS 中的 CBAC 支持：

关键字名称	协议
cuseeme	CUSeeMe 协议
ftp	文件传输协议
h323	H.323 协议（例如，Microsoft NetMeeting 或 Intel Video Phone）
http	HTTP 协议
rcmd	R 命令 (r-exec, r-login, r-sh)
realaudio	Real Audio协议
rpc	远程 过程 调用 协议
smtp	简单邮件传输协议
sqlnet	SQL Net协议
streamworks	StreamWorks协议
tcp	传输控制协议
tftp	TFTP 协议
udp	用户数据报协议

vdolive	VDOLive 协议

每个协议都绑定到一个关键字名称。对要检查的接口应用关键字名称。例如，以下配置将检查 FTP、SMTP 和 Telnet：

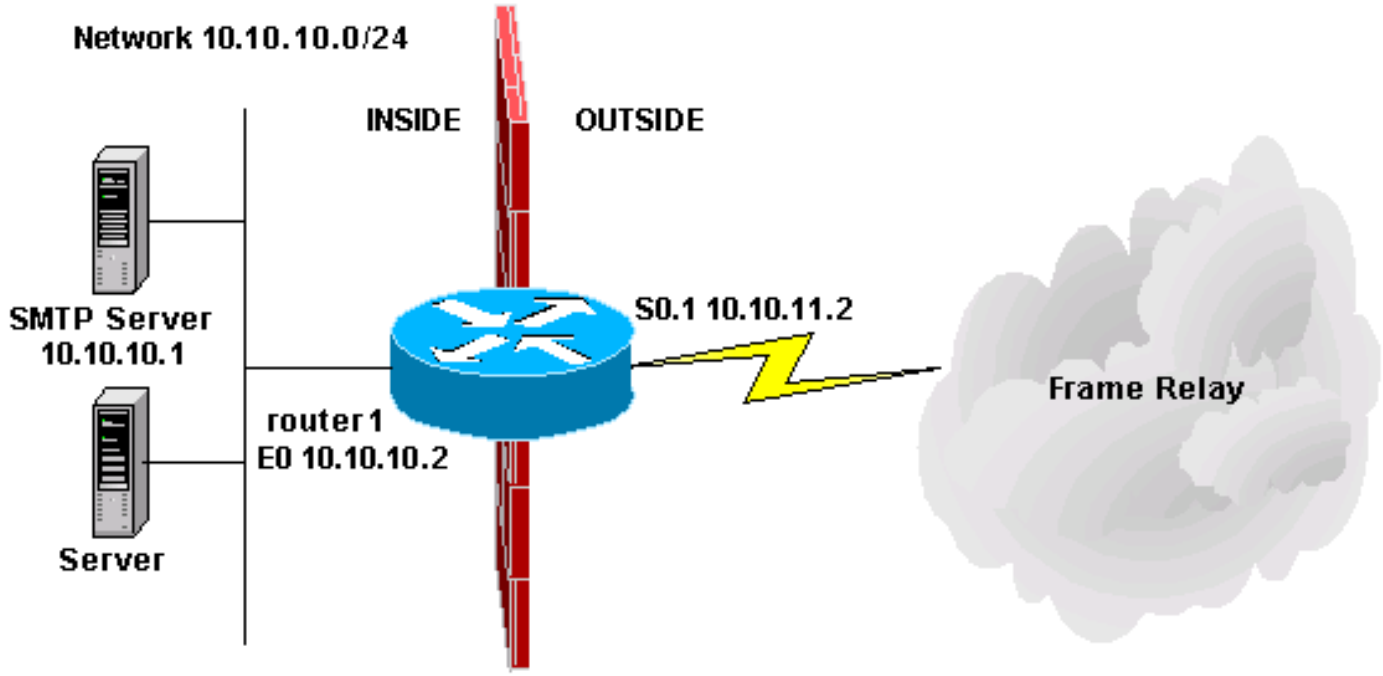
```
router1#configure
Configuring from terminal, memory, or network [terminal]? Enter configuration
commands, one per line. End with CNTL/Z.
router1(config)#ip inspect name mysite ftp
router1(config)#ip inspect name mysite smtp
router1(config)#ip inspect name mysite tcp
router1#show ip inspect config
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
```

本文档讨论您希望允许什么数据流进入、您希望允许什么数据流流出，以及您希望检查什么数据流。既然已准备好要配置 CBAC，请完成以下步骤：

1. 应用配置。
2. 输入上面配置的访问列表。
3. 配置检查语句。
4. 向接口应用访问列表。

此过程后，您的配置将如此图和配置中所示。



基于上下文的访问控制配置

```
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
```

相关信息

- Cisco IOS 防火墙支持页
- 技术支持和文档 - Cisco Systems