Configuración del control de acceso basado en el contexto (CBAC)

Contenido

Introducción

La función Context-Based Access Control (CBAC) del conjunto de funciones del Cisco IOS® Firewall examina activamente la actividad que existe detrás de un firewall. La CBAC especifica qué tráfico se debe dejar entrar y dejar salir mediante listas de acceso (de la misma manera que Cisco IOS utiliza las listas de acceso). Sin embargo, las listas de acceso CBAC incluyen declaraciones de inspección de IP que permiten el examen del protocolo para asegurarse de que no es alterado antes de que el protocolo vaya a los sistemas que existen detrás del firewall.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Antecedentes

CBAC también se puede utilizar con la traducción de direcciones de red (NAT), pero la configuración de este documento se ocupa principalmente de la inspección pura. Si realiza NAT, sus listas de acceso deben reflejar las direcciones globales, no las direcciones reales.

Antes de la configuración, tenga en cuenta estas preguntas.

- ¿Qué tráfico quiere dejar salir?
- ¿Qué trafico desea permitir?
- ¿Qué tráfico quiere inspeccionar?

¿Qué tráfico quiere dejar salir?

El tráfico que desea liberar depende de la política de seguridad del sitio, pero en este ejemplo general, todo está permitido para salir. Si su lista de acceso lo niega todo, no puede salir ningún tráfico. Especifique el tráfico saliente con esta lista de acceso ampliada:

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

¿Qué trafico desea permitir?

El tráfico que desea permitir depende de la política de seguridad del sitio. Sin embargo, la respuesta lógica es cualquier cosa que no dañe su red.

En este ejemplo, hay una lista de tráfico que parece lógico permitir la entrada. Por lo general, el tráfico del Protocolo de mensajes de control de Internet (ICMP) es aceptable, pero puede permitir algunas posibilidades para ataques DOS. Esta es una lista de acceso de ejemplo para el tráfico entrante:

Lista 101 de acceso IP ampliado

```
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
```

Lista 102 de acceso IP ampliado

```
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
```

La lista de acceso 101 está dedicada al tráfico saliente. La lista de acceso 102 está dedicada al tráfico entrante. Las listas de acceso permiten sólo un protocolo de ruteo, el Protocolo de ruteo de gateway interior mejorado (EIGRP), y el tráfico entrante ICMP especificado.

En el ejemplo, un servidor en el lado Ethernet del router no es accesible desde la Internet. La lista de acceso le impide establecer una sesión. Para hacerla accesible, se debe modificar la lista de acceso para permitir que se produzca la conversación. Para cambiar una lista de acceso, quite la lista de acceso, edítela y vuelva a aplicar la lista de acceso actualizada.

Nota: El motivo por el que elimina la lista de acceso 102 antes de editarla y volver a aplicarla, se debe a la "denegación de ip any any" al final de la lista de acceso. En este caso, si desea agregar una nueva entrada antes de eliminar la lista de acceso, la nueva entrada aparece después de la denegación. Por lo tanto, nunca se verifica.

Este ejemplo agrega el Protocolo simple de transferencia de correo (SNTP) sólo para 10.10.10.1.

Lista 102 de acceso IP ampliado

```
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.
```

¿Qué tráfico quiere inspeccionar?

El CBAC dentro de Cisco IOS soporta:

Nombre de palabra clave	Protocolo
cuseeme	Protocolo CUSeeMe
FTP	File Transfer Protocol
h323	Protocolo H.323 (por ejemplo, Microsoft NetMeeting o Intel Video Phone)
http	Protocolo HTTP
rcmd	Comandos R (r-exec, r-login, r-sh)
realaudio	Protocolo de audio real
rpc	Protocolo de llamada de procedimiento remoto
smtp	Protocolo Simple Mail Transfer

sqlnet	Protocolo de red SQL
streamworks	Protocolo StreamWorks
tcp	Protocolo de control de transmisión
tftp	Protocolo TFTP
udp	Protocolo de datagrama de usuario
vdolive	Protocolo VDOLive

Cada protocolo está unido a un nombre de palabra clave. Aplique el nombre de la palabra clave a una interfaz que desee inspeccionar. Por ejemplo, esta configuración inspecciona FTP, SMTP y Telnet:

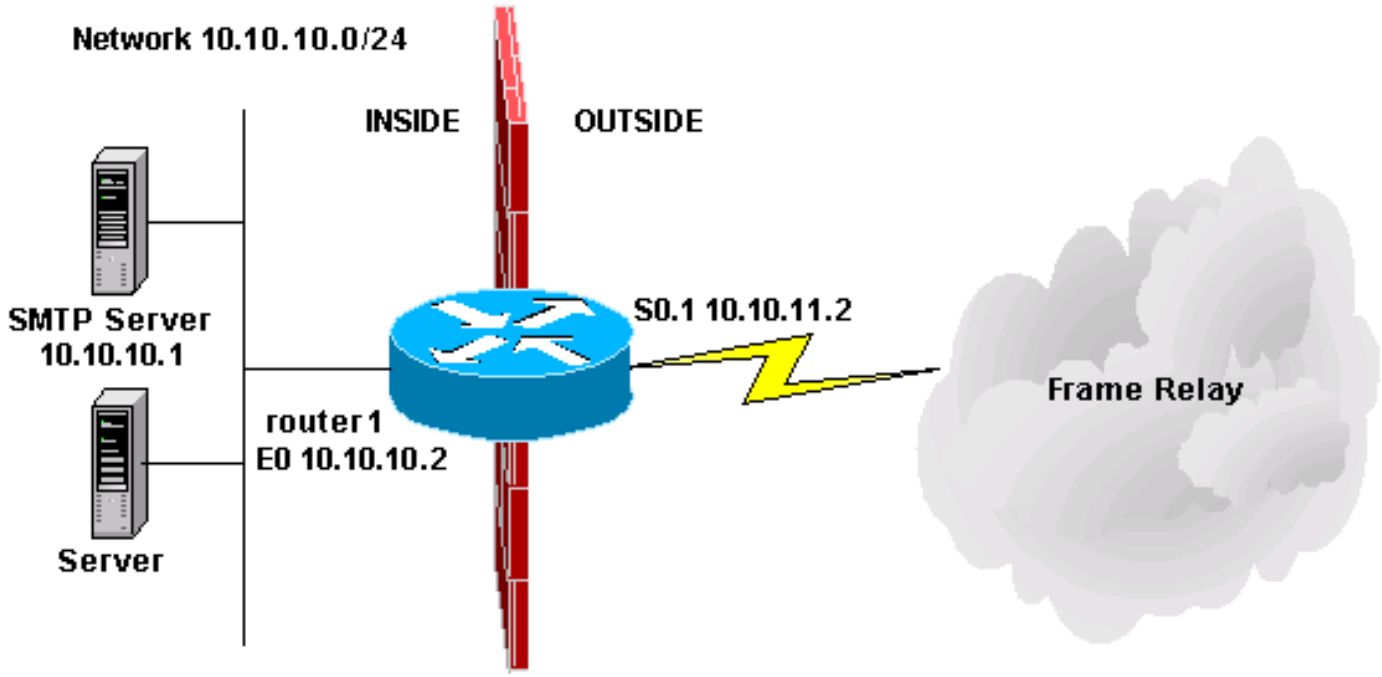
```
router1#configure
Configuring from terminal, memory, or network [terminal]? Enter configuration
commands, one per line. End with CNTL/Z.
router1(config)#ip inspect name mysite ftp
router1(config)#ip inspect name mysite smtp
router1(config)#ip inspect name mysite tcp
router1#show ip inspect config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

Este documento aborda el tráfico que desea dejar salir, el tráfico que desea permitir y el tráfico que desea inspeccionar. Ahora que está preparado para configurar CBAC, complete estos pasos:

1. Aplique la configuración.
2. Ingrese las listas de acceso según la configuración que figura más arriba.
3. Configure los enunciados de la inspección.
4. Aplique las listas de acceso a las interfaces.

Después de este procedimiento, su configuración aparece como se muestra en este diagrama y configuración.



Configuración del control de acceso basado en contexto

```
!
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
```

Información Relacionada

- Página de soporte de Cisco IOS Firewall
- Soporte Técnico y Documentación - Cisco Systems