Control de acceso basado en el contexto (CBAC): Introducción y configuración

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.

prerrequisitos

Requisitos

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

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

Antecedentes

El CBAC se puede también utilizar con el Network Address Translation (NAT), pero la configuración en los tratos de este documento sobre todo con la inspección pura. Si usted realiza el NAT, sus Listas de acceso necesitan reflejar a las direcciones globales, no las direcciones reales.

Antes de la configuración, considere estas preguntas.

- ¿Qué tráfico quiere dejar salir?
- ¿Qué tráfico usted quiere dejar adentro?
- ¿Qué tráfico quiere inspeccionar?

¿Qué tráfico quiere dejar salir?

Qué tráfico usted quiere dejar hacia fuera depende de su política de seguridad del sitio, pero en este ejemplo general todo es saliente permitido. Si su lista de acceso niega todo, después ningún tráfico puede irse. 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?

Qué tráfico usted quiere dejar adentro depende de su política de seguridad del sitio. Sin embargo, la respuesta lógica es cualquier cosa que no daña su red.

En este ejemplo, hay una lista de tráfico que parezca lógico de dejar adentro. Por lo general, el tráfico del Protocolo de mensajes de control de Internet (ICMP) es aceptable, pero puede permitir algunas posibilidades para ataques DOS. Esto es una lista de acceso de la muestra 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, editela, y reaplique la lista de acceso actualizada.

Note: La razón que usted quita la lista de acceso 102 antes de que edite y reaplique, es debido al “deny ip any any” en el extremo de la lista de acceso. En este caso, si usted agregara una nueva entrada antes de que usted quite la lista de acceso, la nueva entrada aparece después de la negación. Por lo tanto, nunca se marca.

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 los soportes del Cisco IOS:

Nombre de palabra clave	Protocolo
cuseeme	Protocolo del CUSeeMe
FTP	File Transfer Protocol
h323	Protocolo de H.323 (por ejemplo NetMeeting de Microsoft o teléfono con

	video de Intel)
http	Protocolo HTTP
rcmd	Comandos R (r-exec, r-login, r-sh)
realaudio	Protocolo de audio real
RPC	Remote Procedure Call Protocol
smtp	Protocolo Simple Mail Transfer
sqlnet	Protocolo de red SQL
streamworks	Protocolo StreamWorks
tcp	Protocolo Protocolo de control de transmisión (TCP)
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 palabra cleve a una interfaz que usted quiera examinar. Por ejemplo, esta configuración examina el FTP, el S TP, y Telnet:

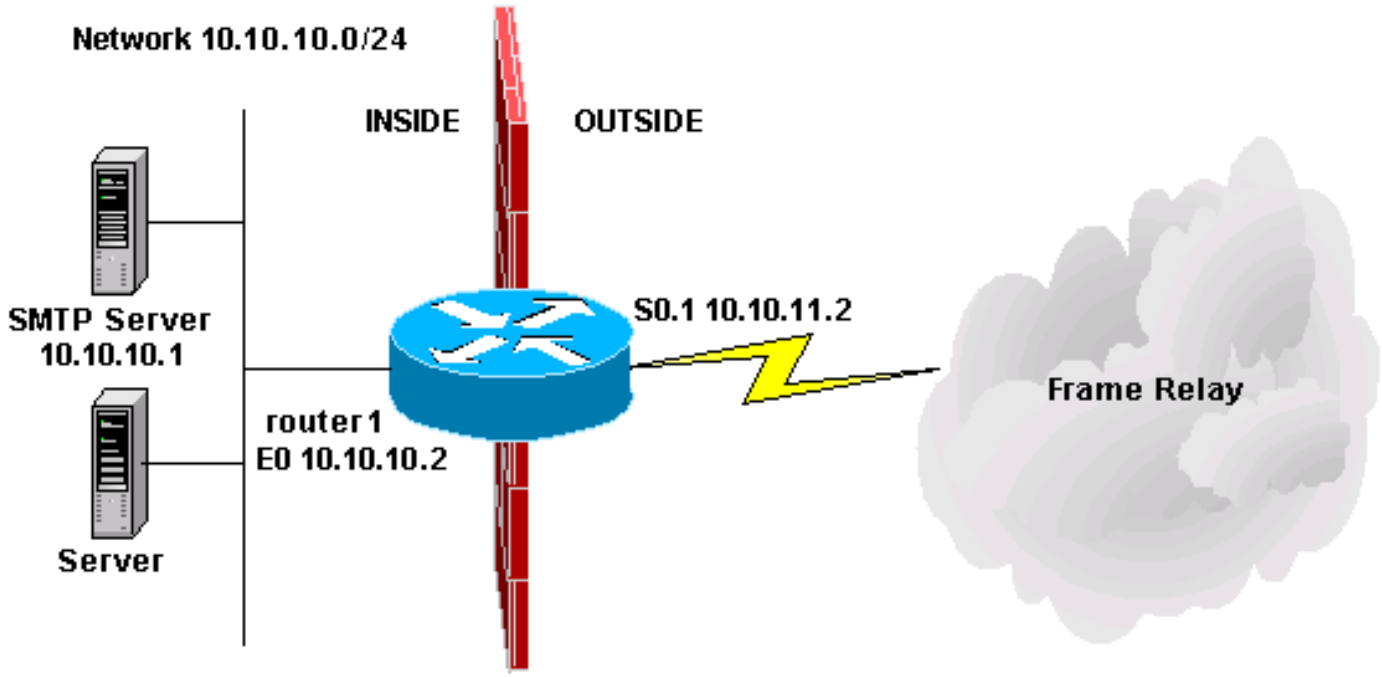
```
router1#configure
Configuring from terminal, memory, or network [terminal]? Enter configuration
commands, one per line. End with CNTL/Z.
router1(config)#ip inspect name mysite ftp
router1(config)#ip inspect name mysite smtp
router1(config)#ip inspect name mysite tcp
router1#show ip inspect config
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 dirige qué tráfico usted quiere dejar hacia fuera, qué tráfico usted quiere dejar adentro, y qué tráfico usted quiere examinar. Ahora que le preparan para configurar el 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 tal y como se muestra en de este diagrama y configuración.



Configuración del control de acceso basado en contexto

```
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
```

Información Relacionada

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