Configurer le contrôle d'accès basé sur le contexte (CBAC)

Contenu

Introduction

La caractéristique de contrôle d'accès basé sur contexte (CBAC) de la fonctionnalité d'ensemble de pare-feu de Cisco IOS® examine activement l'activité derrière un pare-feu. CBAC spécifie quel trafic doit être permis à l'intérieur et quel trafic doit être a permis à l'extérieur à l'aide des listes d'accès (de la même manière que Cisco IOS utilise les listes d'accès). Cependant, les listes d'accès CBAC incluent les déclarations d'inspection IP qui permettent à l'inspection du protocole de s'assurer qu'il n'est pas trafiqué avant que le protocole se dirige aux systèmes derrière le pare-feu.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

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

Informations générales

Le contrôle CBAC peut également être utilisé avec la traduction d'adresses de réseau (NAT), mais la configuration de ce document traite principalement de l'inspection pure. Si vous effectuez la NAT, vos listes d'accès doivent refléter les adresses globales, et non les adresses réelles.

Avant de procéder à la configuration, tenez compte de ces questions.

Quel trafic voulez-vous laisser sortir ?

Le trafic que vous souhaitez distribuer dépend de votre stratégie de sécurité de site, mais dans cet exemple général tout est autorisé en sortie. Si votre liste d'accès refuse tout, aucun trafic ne peut quitter. Spécifiez le trafic sortant avec cette liste d'accès étendue :

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

Quel trafic voulez-vous laisser entrer ?

Le trafic que vous souhaitez autoriser dépend de votre stratégie de sécurité de site. Cependant, la réponse logique est tout ce qui n'endommage pas votre réseau.

Dans cet exemple, il y a une liste de trafic qui semble logique à laisser entrer. Le trafic ICMP (Internet Control Message Protocol) est généralement acceptable, mais il peut permettre certaines attaques DOS. Voici un exemple de liste d'accès pour le trafic entrant :

Liste d'accès IP étendue 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
```

Liste d'accès IP étendue 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
```

La liste d'accès 101 est destinée au trafic sortant. La liste d'accès 102 est destinée au trafic entrant. Les listes d'accès autorisent uniquement un protocole de routage, le protocole EIGRP (Enhanced Interior Gateway Routing Protocol) et le trafic entrant ICMP spécifié.

Dans l'exemple, un serveur du côté Ethernet du routeur n'est pas accessible depuis Internet. La liste d'accès l'empêche d'établir une session. Pour le rendre accessible, la liste d'accès doit être modifiée pour permettre la conversation. Pour modifier une liste d'accès, supprimez-la, modifiez-la et réappliquez-la.

Remarque : La raison pour laquelle vous supprimez la liste d'accès 102 avant de la modifier et de la réappliquer est due à la mention « deny ip any any any » à la fin de la liste d'accès. Dans ce cas, si vous deviez ajouter une nouvelle entrée avant de supprimer la liste d'accès, la nouvelle entrée apparaît après le refus. Par conséquent, il n'est jamais vérifié.

Cet exemple montre comment ajouter le protocole SMTP (Simple Mail Transfer Protocol) pour 10.10.10.1 uniquement.

Liste d'accès IP étendue 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.
```

Quel trafic voulez-vous inspecter ?

Le CBAC de Cisco IOS prend en charge :

Nom du mot clé	Protocol
cuseeme	Protocole CUSeeMe
ftp	Protocole FTP (File Transfer Protocol)
h323	Protocole H.323 (par exemple Microsoft NetMeeting ou Intel Video Phone)
http	Protocole HTTP
rcmd	Commandes R (r-exec, r-login, r-sh)
Réel audio	Real Audio Protocol
rpc	Protocole d'appel de procédure distante
smtp	Simple Mail Transfer Protocol

sqlnet	Protocole SQL Net
flux	Protocole StreamWorks
tcp	Protocole de contrôle de transmission
tftp	Protocole TFTP
udp	Protocole de datagramme utilisateur
vaudou	Protocole VDOLive

Chaque protocole est lié à un nom de mot clé. Appliquez le nom de mot clé à une interface que vous voulez inspecter. Par exemple, cette configuration inspecte FTP, SMTP et Telnet :

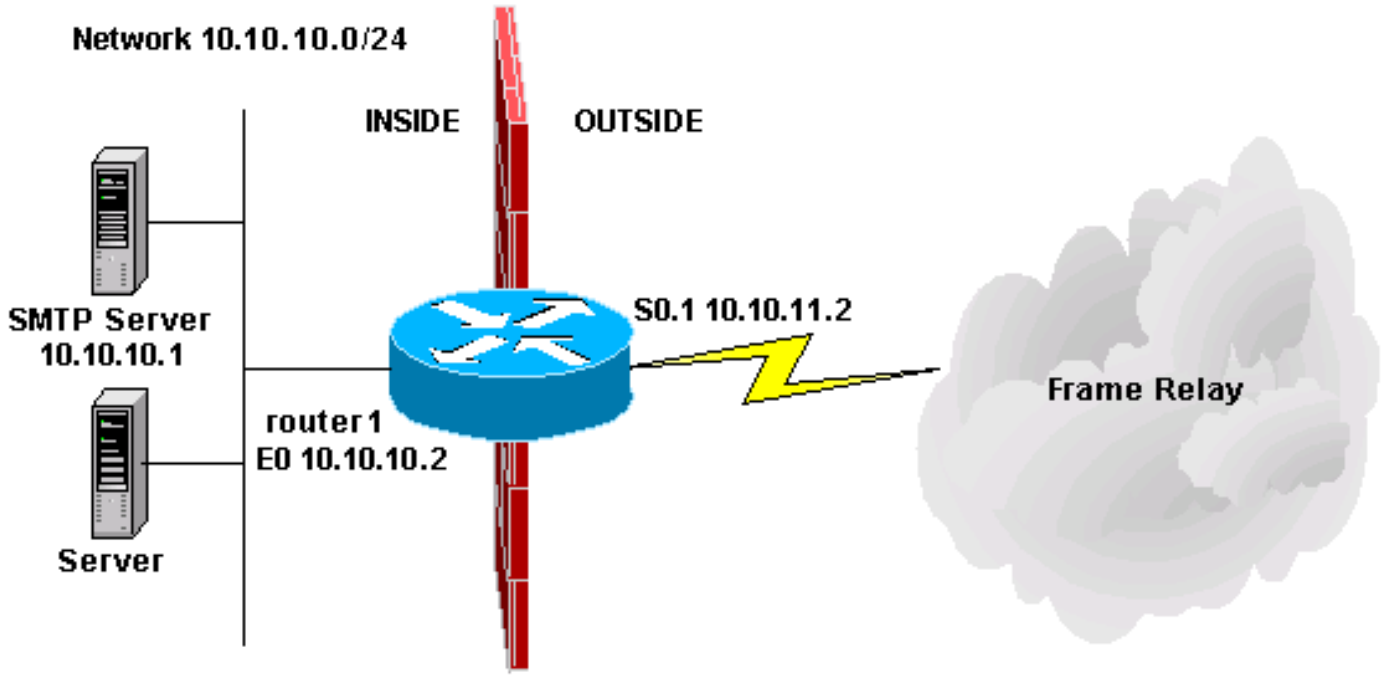
```
router1#configure
Configuring from terminal, memory, or network [terminal]? Enter configuration
commands, one per line. End with CNTL/Z.
router1(config)#ip inspect name mysite ftp
router1(config)#ip inspect name mysite smtp
router1(config)#ip inspect name mysite tcp
router1#show ip inspect config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

Ce document traite du trafic que vous voulez libérer, du trafic que vous voulez autoriser et du trafic que vous voulez inspecter. Maintenant que vous êtes prêt à configurer CBAC, procédez comme suit :

1. Appliquez la configuration.
2. Saisissez les listes d'accès configurées ci-dessus.
3. Configurez les instructions d'inspection.
4. Appliquez les listes d’accès aux interfaces.

Après cette procédure, votre configuration apparaît comme illustré dans ce schéma et cette configuration.



Configuration du contrôle d'accès basé sur le contexte

```
!
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
```

Informations connexes

- Page d'assistance Cisco IOS Firewall
- Support et documentation techniques - Cisco Systems