Contrôle d'accès basé sur contexte (CBAC) : Introduction et configuration

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.

Composants utilisés

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

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

CBAC peut également être utilisé avec le Traduction d'adresses de réseau (NAT), mais la configuration dans des affaires de ce document principalement avec l'inspection pure. Si vous exécutez NAT, vos Listes d'accès doivent refléter les adresses globales, pas les vraies adresses.

Avant la configuration, considérez ces questions.

- Quel trafic voulez-vous permettre ?
- Quel trafic voulez-vous permettre dedans ?
- Quel trafic voulez-vous examiner ?

Quel trafic voulez-vous permettre ?

Quel trafic vous voulez permettre dépend de votre stratégie de sécurité de site, mais dans cet exemple général tout est permis sortant. Si votre liste d'accès refuse tout, alors aucun trafic ne peut partir. 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 permettre dedans ?

Quel trafic vous voulez permettre dedans dépend de votre stratégie de sécurité de site. Cependant, la réponse logique est quelque chose qui n'endommage pas votre réseau.

Dans cet exemple, il y a une liste du trafic il semble logique permettre que dedans. Le trafic de Protocole ICMP (Internet Control Message Protocol) est généralement acceptable, mais il peut permettre quelques possibilités pour des attaques DoS. C'est une liste d'accès témoin pour le trafic entrant :

Extended IP Access List 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
```

Extended IP Access List 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 pour le trafic sortant. La liste d'accès 102 est pour le trafic d'arrivée. Les Listes d'accès permettent seulement un protocole de routage, un Protocole EIGPR (Enhanced Interior Gateway Routing Protocol), et un trafic d'arrivée spécifié d'ICMP.

Dans l'exemple, un serveur du côté Ethernet du routeur n'est pas accessible de l'Internet. La liste d'accès le bloque d'établir une session. Pour le rendre accessible, la liste d'accès doit être modifiée pour permettre à la conversation pour se produire. Pour changer une liste d'accès, retirez la liste d'accès, éditez-la, et réappliquez la liste d'accès mise à jour.

Remarque: La raison pour laquelle vous retirez la liste d'accès 102 avant qu'éditiez et réappliquiez, est due au « refusent l'IP tout » à la fin de la liste d'accès. Dans ce cas, si vous deviez ajouter une nouvelle entrée avant que vous retiriez la liste d'accès, la nouvelle entrée apparaît après le refuser. Par conséquent, il n'est jamais vérifié.

Cet exemple ajoute le Protocole SMTP (Simple Mail Transfer Protocol) pour 10.10.10.1 seulement.

Extended IP Access List 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 examiner ?

Le CBAC dans des supports de Cisco IOS :

Nom de mot clé	Protocol
cuseeme	CUSeeMe Protocol
FTP	Protocole de transfert de fichiers
h323	H.323 Protocol (par exemple Microsoft NetMeeting ou téléphone visuel d'Intel)
HTTP	Protocole HTTP
rcmd	R commande (r-exécutif, r-procédure de connexion, r-SH)

RealAudio	Vrai Protocol sonore
RPC	Protocole d'appel de procédure à distance
SMTP	Simple Mail Transfer Protocol
sqlnet	Net Protocol SQL
streamworks	StreamWorks Protocol
TCP	Transmission Control Protocol
tftp	TFTP Protocol
UDP	User Datagram Protocol
vdolive	VDOLive Protocol

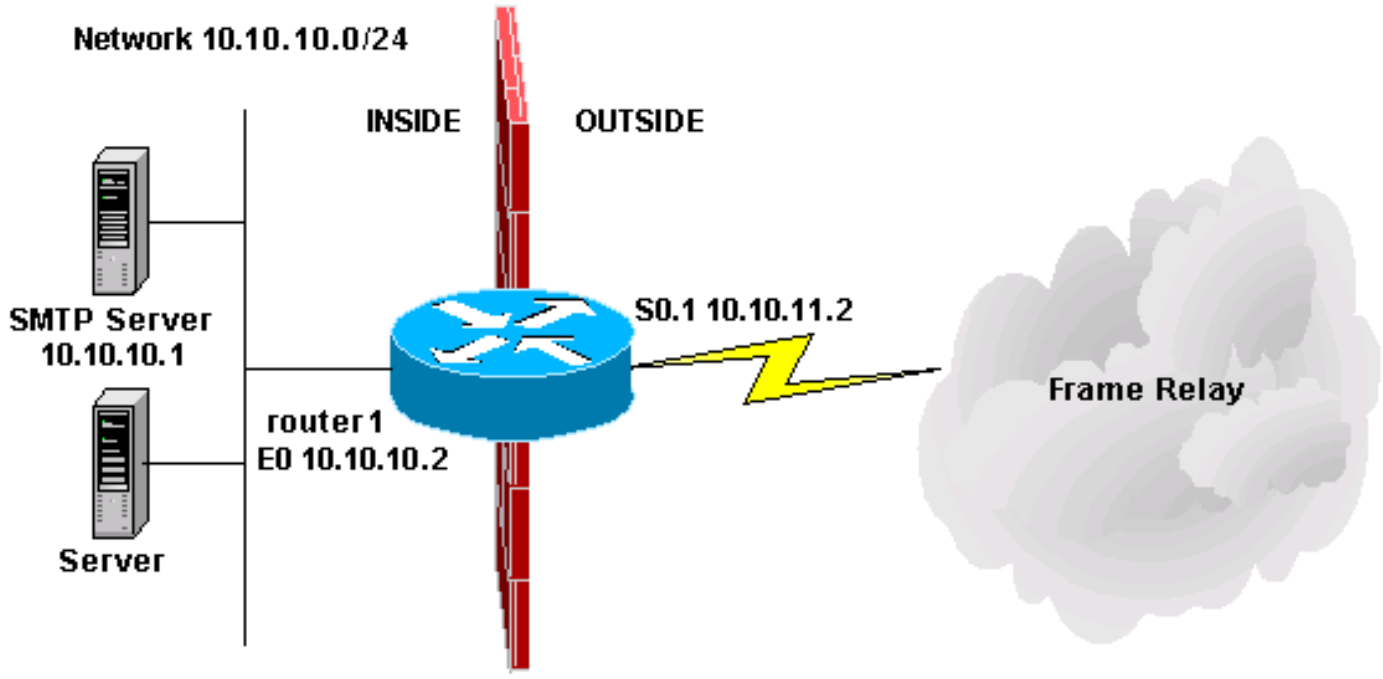
Chaque protocole est attaché à un nom de mot clé. Appliquez-vous le nom de mot clé à une interface que vous voulez examiner. Par exemple, cette configuration examine le FTP, le SMTP, et le telnet :

```
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 adresse quel trafic vous voulez permettre, quel trafic vous voulez permettre dedans, et quel trafic vous voulez examiner. Maintenant que vous êtes disposé à configurer CBAC, terminez-vous ces étapes :

1. Appliquez la configuration.
2. Écrivez les Listes d'accès comme configuré ci-dessus.
3. Configurez les déclarations d'inspection.
4. Appliquez les Listes d'accès aux interfaces.

Après cette procédure, votre configuration apparaît suivant les indications de ces diagramme et configuration.



Configuration de contrôle d'accès basé sur 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 de support de Pare-feu Cisco IOS
- Support et documentation techniques - Cisco Systems