GSR : Réception des listes de contrôle d'accès

Contenu

Introduction

Ce document décrit une nouvelle fonctionnalité de sécurité appelée listes de contrôle d'accès de réception (rACLs) [1] et présente des recommandations et des directives pour les déploiements de rACL. Les listes de contrôle d’accès de réception sont utilisées pour accroître la sécurité sur les routeurs Cisco 12000 en protégeant le processeur de routage gigabit (GRP) du routeur contre le trafic inutile et potentiellement dangereux. Des listes de contrôle d'accès de réception ont été ajoutées en tant que dispense spéciale au mécanisme de maintenance pour le logiciel Cisco IOS ® Version 12.0.21S2 et intégrées dans le logiciel Cisco IOS Version 12.0(22)S.

Protection GRP

Les données reçues par un routeur de commutation gigabit (GSR) peuvent être divisées en deux grandes catégories :

- Trafic qui passe par le routeur via le chemin de transfert.
- Trafic qui doit être envoyé via le chemin de réception vers le protocole GRP pour une analyse plus approfondie.

Dans les opérations normales, la grande majorité du trafic passe simplement par un GSR en route vers d'autres destinations. Cependant, le protocole GRP doit gérer certains types de données, notamment les protocoles de routage, l’accès à distance au routeur et le trafic de gestion du réseau (tels que SNMP [Simple Network Management Protocol]). Outre ce trafic, d'autres paquets de couche 3 peuvent nécessiter la flexibilité de traitement du protocole GRP. Il s’agit notamment de certaines options IP et de certaines formes de paquets ICMP (Internet Control Message Protocol). Reportez-vous à l'annexe sur les contiguïtés de réception et les paquets pointus pour

plus de détails concernant les rACL et le trafic de chemin de réception sur le GSR.

Un GSR comporte plusieurs chemins de données, chacun assurant la maintenance de différentes formes de trafic. Le trafic de transit est transféré de la carte de ligne d'entrée (LC) au fabric, puis à la carte de sortie pour la livraison du tronçon suivant. Outre le chemin de données du trafic de transit, un GSR dispose de deux autres chemins pour le trafic nécessitant un traitement local : LC à LC CPU et LC à LC CPU à fabric à GRP. Le tableau suivant présente les chemins de plusieurs fonctions et protocoles couramment utilisés.

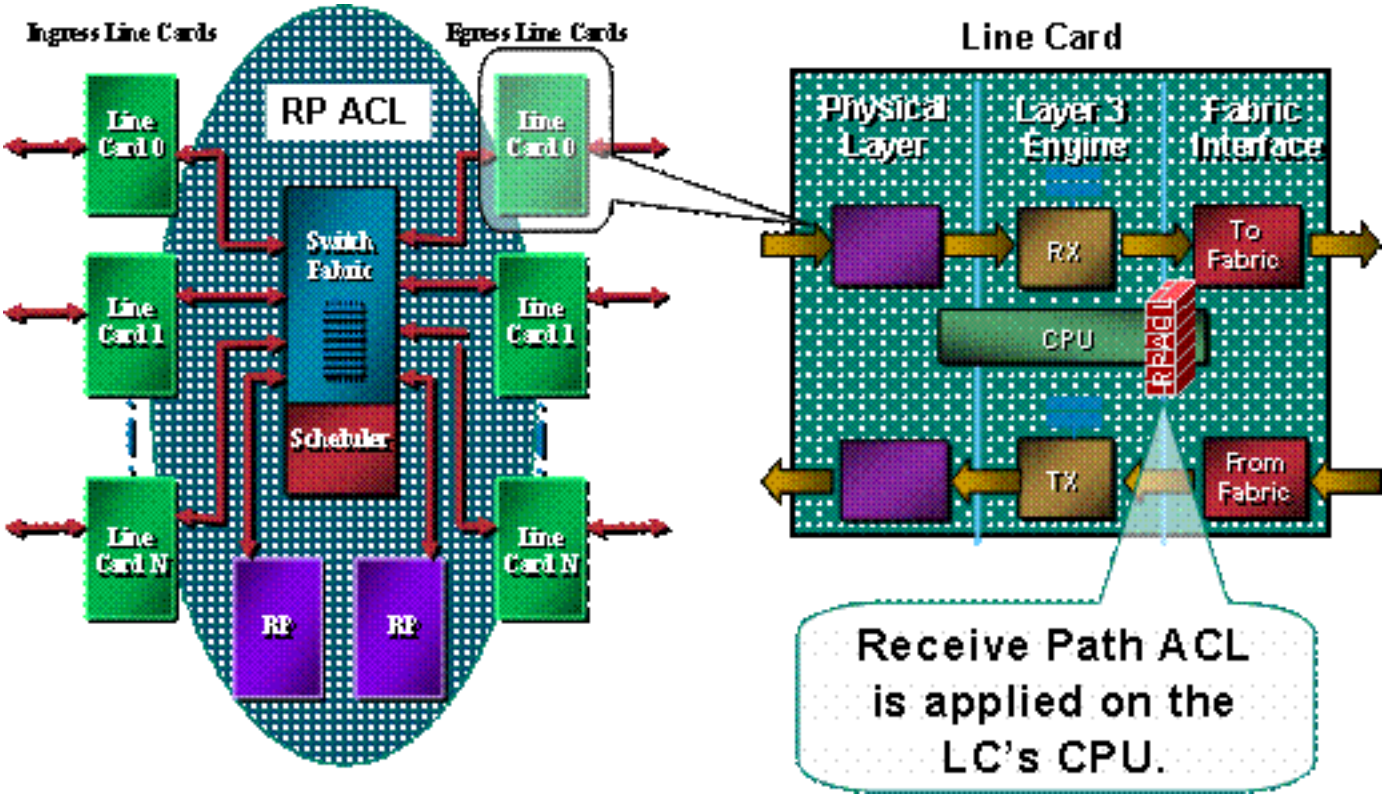
Type de trafic	Chemin des données
Trafic normal (de transit)	LC vers fabric vers LC
Protocoles de routage/SSH/SNMP	LC à LC CPU vers fabric vers GRP
Écho ICMP (ping)	LC à LC CPU
Journalisation	

Le processeur de routage du GSR a une capacité limitée pour traiter le trafic livré à partir des LC destinées au GRP lui-même. Si un volume élevé de données nécessite un pontage au protocole GRP, ce trafic peut submerger le protocole GRP. Cela entraîne une attaque par déni de service (DoS) efficace. Le processeur du protocole GRP a du mal à suivre l'examen des paquets et commence à abandonner les paquets, inondant les files d'attente d'entrée-attente et de rejet sélectif de paquets (SPD). [2] Les GSR doivent être protégés contre trois scénarios, qui peuvent résulter d'attaques DoS dirigées contre un GRP du routeur.

- Perte de paquets de protocole de routage suite à une inondation de priorité normale
- Perte de paquets de session de gestion (Telnet, Secure Shell [SSH], SNMP) due à une inondation de priorité normale
- Perte de paquets suite à une inondation de haute priorité usurpée

La perte potentielle de données de protocole de routage lors d'une inondation de priorité normale est actuellement atténuée par la classification statique et la limitation de débit du trafic destiné au protocole GRP en provenance des LC. Malheureusement, cette approche a des limites. La limitation de débit pour le trafic de priorité normale destiné au protocole GRP est insuffisante pour garantir la protection des données de protocole de routage de priorité élevée si une attaque est livrée via plusieurs LC. La réduction du seuil à partir duquel les données de priorité normale sont abandonnées pour fournir une telle protection ne fait qu'aggraver la perte de trafic de gestion d'une inondation de priorité normale.

Comme le montre cette image, la rACL est exécutée sur chaque LC avant que le paquet ne soit transmis au GRP.



Un mécanisme de protection du protocole GRP est nécessaire. Les rACL affectent le trafic envoyé au protocole GRP en raison de contiguïtés de réception. Les contiguïtés de réception sont des contiguïtés Cisco Express Forwarding pour le trafic destiné aux adresses IP du routeur, telles que l'adresse de diffusion ou les adresses configurées sur les interfaces du routeur. [3] Reportez-vous à la section annexe pour plus de détails sur les contiguïtés de réception et les paquets punis.

Le trafic qui entre dans une LC est d'abord envoyé au processeur local de la LC, et les paquets qui nécessitent un traitement par le GRP sont mis en file d'attente pour être transférés au processeur de routage. La liste de contrôle d'accès de réception est créée sur le protocole GRP, puis repoussée vers les processeurs des différents LC. Avant que le trafic ne soit envoyé du CPU LC au GRP, le trafic est comparé à la rACL. Si cela est autorisé, le trafic passe au protocole GRP, tandis que tout autre trafic est refusé. La rACL est inspectée avant la fonction de limitation de débit LC à GRP. Puisque la rACL est utilisée pour toutes les contiguïtés de réception, certains paquets qui sont gérés par le CPU LC (comme les requêtes d'écho) sont également soumis au filtrage de la rACL. Il faut en tenir compte lors de la conception des entrées rACL.

Les listes de contrôle d'accès de réception font partie d'une plage de mécanismes de programme en plusieurs parties pour protéger les ressources d'un routeur. Les travaux futurs comprendront un composant de limitation de débit à la liste de contrôle d'accès.

Impact sur les performances

Aucune mémoire n'est consommée autre que celle nécessaire pour contenir l'entrée de configuration unique et la liste d'accès définie elle-même. La rACL est copiée sur chaque LC, de sorte qu'une légère zone de mémoire est prise sur chaque LC. Dans l'ensemble, les ressources utilisées sont minuscules, surtout si on les compare aux avantages du déploiement.

Une liste de contrôle d'accès de réception n'affecte pas les performances du trafic transféré. La rACL s'applique uniquement au trafic de contiguïté de réception. Le trafic transféré n'est jamais soumis à la rACL. Le trafic de transit est filtré à l'aide de listes de contrôle d'accès d'interface. Ces listes de contrôle d'accès " régulières " sont appliquées aux interfaces dans une direction

spécifiée. Le trafic est soumis au traitement des listes de contrôle d'accès avant le traitement des listes de contrôle d'accès rACL, de sorte que le trafic refusé par la liste de contrôle d'accès de l'interface ne sera pas reçu par la liste de contrôle d'accès rACL. [4]

Le LC effectuant le filtrage réel (en d'autres termes, le LC recevant le trafic filtré par la rACL) aura une utilisation accrue du CPU en raison du traitement de la rACL. Cette augmentation de l'utilisation du CPU est toutefois due à un volume élevé de trafic destiné au GRP ; l'avantage du protocole GRP de la protection rACL l'emporte de loin sur l'utilisation accrue du CPU sur un LC. L'utilisation du CPU sur un LC varie en fonction du type de moteur LC. Par exemple, compte tenu de la même attaque, une LC de moteur 3 aura une utilisation CPU plus faible qu'une LC de moteur 0.

L'activation des listes de contrôle d'accès turbo (à l'aide de la commande **access-list compilée**) convertit les listes de contrôle d'accès en une série d'entrées de table de recherche extrêmement efficaces. Lorsque les listes de contrôle d'accès turbo sont activées, la profondeur de la liste de contrôle d'accès n'affecte pas les performances. En d'autres termes, la vitesse de traitement est indépendante du nombre d'entrées dans la liste de contrôle d'accès. Si la rACL est courte, les ACL turbo n'augmenteront pas significativement les performances mais consommeront de la mémoire ; avec les rACL courtes, les ACL compilées ne sont probablement pas nécessaires.

En protégeant le protocole GRP, la rACL permet d'assurer la stabilité du routeur et, en fin de compte, du réseau lors d'une attaque. Comme décrit ci-dessus, la rACL est traitée sur le CPU LC, de sorte que l'utilisation du CPU sur chaque LC augmentera lorsqu'un volume important de données est dirigé vers le routeur. Sur E0/E1 et certains bundles E2, l'utilisation du CPU de plus de 100 % peut conduire à des abandons de protocole de routage et de couche liaison. Ces pertes sont localisées sur la carte et les processus de routage GRP sont protégés, assurant ainsi la stabilité. Les cartes E2 avec microcode de régulation [5] activé activent le mode de régulation lorsqu'elles sont sous charge lourde et transmettent uniquement le trafic de priorité 6 et 7 au protocole de routage. D'autres types de moteurs ont des architectures multifile d'attente ; par exemple, les cartes E3 ont trois files d'attente au processeur, avec des paquets de protocole de routage (priorité 6/7) dans une file d'attente séparée à haute priorité. Le CPU LC élevé, à moins que des paquets de priorité élevée ne le provoquent, n'entraînera pas de pertes de protocole de routage. Les paquets destinés aux files d'attente de priorité inférieure seront abandonnés à la queue. Enfin, les cartes basées sur E4 comportent huit files d'attente au processeur, dont une dédiée aux paquets de protocole de routage.

Syntaxe

Une liste de contrôle d'accès de réception est appliquée à l'aide de la commande de configuration globale suivante pour distribuer la liste de contrôle d'accès de rACL à chaque liste de contrôle d'accès du routeur.

```
[no] ip receive access-list
```

Dans cette syntaxe, *<num>* est défini comme suit.

```
<1-199> IP access list (standard or extended)
<1300-2699> IP expanded access list (standard or extended)
```

Exemples de modèles de base et de listes de contrôle d'accès

Pour pouvoir utiliser cette commande, vous devez définir une liste d'accès qui identifie le trafic qui doit être autorisé à parler au routeur. La liste d'accès doit inclure à la fois les protocoles de routage et le trafic de gestion (Border Gateway Protocol [BGP], Open Shortest Path First [OSPF], SNMP, SSH, Telnet). Reportez-vous à la section relative aux directives de déploiement pour plus de détails.

L'exemple suivant de liste de contrôle d'accès fournit un aperçu simple et présente quelques exemples de configuration qui peuvent être adaptés à des utilisations spécifiques. La liste de contrôle d'accès illustre les configurations requises pour plusieurs services/protocoles couramment requis. Pour SSH, Telnet et SNMP, une adresse de bouclage est utilisée comme destination. Pour les protocoles de routage, l'adresse d'interface réelle est utilisée. Le choix des interfaces de routeur à utiliser dans la liste de contrôle d'accès rACL est déterminé par les politiques et les opérations du site local. Par exemple, si les bouclages sont utilisés pour toutes les sessions d'appairage BGP, seuls ces bouclages doivent être autorisés dans les instructions **permit** pour BGP.

```
!--- Permit BGP. access-list 110 permit tcp host bgp_peer host loopback eq bgp !--- Permit OSPF.
access-list 110 permit ospf host ospf_neighbor host 224.0.0.5 !--- Permit designated router
multicast address, if needed. access-list 110 permit ospf host ospf_neighbor host 224.0.0.6
access-list 110 permit ospf host ospf_neighbor host local_ip !--- Permit Enhanced Interior
Gateway Routing Protocol (EIGRP). access-list 110 permit eigrp host eigrp_neighbor host
224.0.0.10 access-list 110 permit eigrp host eigrp_neighbor host local_ip !--- Permit remote
access by Telnet and SSH. access-list 110 permit tcp management_addresses host loopback eq 22
access-list 110 permit tcp management_addresses host loopback eq telnet !--- Permit SNMP.
access-list 110 permit udp host NMS_stations host loopback eq snmp !--- Permit Network Time
Protocol (NTP). access-list 110 permit udp host ntp_server host loopback eq ntp !--- Router-
originated traceroute: !--- Each hop returns a message that time to live (ttl) !--- has been
exceeded (type 11, code 3); !--- the final destination returns a message that !--- the ICMP port
is unreachable (type 3, code 0). access-list 110 permit icmp any any ttl-exceeded access-list
110 permit icmp any any port-unreachable !--- Permit TACACS for router authentication. access-
list 110 permit tcp host tacacs_server router_src established !--- Permit RADIUS. access-list
110 permit udp host radius_server router_src log !--- Permit FTP for IOS upgrades. access-list
110 permit tcp host image_server eq ftp host router_ip_address access-list 110 permit tcp host
image_sever eq ftp-data host router_ip_address
```

Comme pour toutes les listes de contrôle d'accès Cisco, il existe une instruction **deny** implicite à la fin de la liste d'accès, de sorte que tout trafic qui ne correspond pas à une entrée de la liste de contrôle d'accès sera refusé.

Remarque : Le mot clé **log** peut être utilisé pour aider à classer le trafic destiné au protocole GRP qui n'est pas autorisé. Bien que le mot clé **log** fournisse des informations précieuses sur les détails des accès ACL, les accès excessifs à une entrée ACL qui utilise ce mot clé augmenteront l'utilisation du CPU LC. L'impact sur les performances associé à la journalisation varie selon le type de moteur LC. En général, l'enregistrement ne doit être utilisé que lorsque cela est nécessaire sur les moteurs 0/1/2. Pour les moteurs 3/4/4+, la journalisation a un impact beaucoup moins important en raison de l'augmentation des performances du processeur et de l'architecture multifile d'attente.

Le niveau de granularité de cette liste d'accès est déterminé par la stratégie de sécurité locale (par exemple, le niveau de filtrage requis pour les voisins OSPF).

Listes de contrôle d'accès et paquets fragmentés

Les ACL ont un mot clé de **fragments qui active le comportement de gestion des paquets**

fragmentés spécialisés. En général, les fragments non initiaux qui correspondent aux instructions L3 (indépendamment des informations L4) dans une liste de contrôle d'accès sont affectés par l'instruction **permit** ou **deny** de l'entrée correspondante. Notez que l'utilisation du mot clé **fragments** peut forcer les ACL à refuser ou autoriser les fragments non initiaux avec plus de granularité.

Dans le contexte rACL, le filtrage des fragments ajoute une couche supplémentaire de protection contre une attaque DoS qui utilise uniquement des fragments non initiaux (tels que FO > 0). L'utilisation d'une instruction **deny** pour les fragments non initiaux au début de la liste de contrôle d'accès rACL empêche tous les fragments non initiaux d'accéder au routeur. Dans de rares circonstances, une session valide peut nécessiter une fragmentation et donc être filtrée si une instruction **deny fragment** existe dans la liste de contrôle d'accès rACL.

Par exemple, prenez en compte la liste de contrôle d'accès partielle ci-dessous.

```
access-list 110 deny tcp any any fragments
access-list 110 deny udp any any fragments
access-list 110 deny icmp any any fragments
<rest of ACL>
```

L'ajout de ces entrées au début d'une rACL refuse tout accès de fragment non initial au GRP, tandis que les paquets non fragmentés ou les fragments initiaux passent aux lignes suivantes de la rACL non affectées par les instructions **de fragment de refus**. L'extrait de liste de contrôle d'accès rACL ci-dessus facilite également la classification de l'attaque puisque chaque protocole - UDP (Universal Datagram Protocol), TCP et ICMP - incrémente des compteurs distincts dans la liste de contrôle d'accès.

Consultez les listes de contrôle d'accès et les fragments d'IP pour une analyse détaillée des options.

Évaluation des risques

Assurez-vous que la rACL ne filtre pas le trafic critique tel que les protocoles de routage ou l'accès interactif aux routeurs. Le filtrage du trafic nécessaire peut entraîner une incapacité à accéder à distance au routeur, ce qui nécessite une connexion console. Pour cette raison, les configurations des travaux pratiques doivent imiter le déploiement réel le plus possible.

Comme toujours, Cisco vous recommande de tester cette fonctionnalité dans les travaux pratiques avant le déploiement.

Annexes et notes

Réception de contiguïtés et de paquets pointus

Comme décrit précédemment dans ce document, certains paquets nécessitent un traitement GRP. Les paquets sont acheminés du plan de transfert de données au protocole GRP. Il s'agit d'une liste des formes courantes de données de couche 3 qui nécessitent un accès GRP.

- Protocoles de routage
- Trafic de contrôle de multidiffusion (OSPF, HSRP [Hot Standby Router Protocol], TDP [Tag Distribution Protocol], PIM [Protocol Independent Multicast], etc.)

- Paquets MPLS (Multiprotocol Label Switching) nécessitant une fragmentation
- Paquets avec certaines options IP, telles que les alertes de routeur
- Premier paquet de flux de multidiffusion
- Paquets ICMP fragmentés nécessitant un réassemblage
- Tout le trafic destiné au routeur lui-même (à l'exception du trafic traité sur le LC)

Puisque les rACL s'appliquent aux contiguïtés de réception, la rACL filtre le trafic qui n'est pas pointé vers le GRP mais qui est une contiguïté de réception. L'exemple le plus courant est une requête d'écho ICMP (ping). Les requêtes d'écho ICMP dirigées vers le routeur sont traitées par le processeur LC ; étant donné que les requêtes sont des contiguïtés de réception, elles sont également filtrées par la rACL. Par conséquent, pour autoriser les requêtes ping aux interfaces (ou bouclages) du routeur, la liste de contrôle d'accès r doit explicitement autoriser les requêtes d'écho.

Les contiguïtés de réception peuvent être affichées à l'aide de la commande **show ip cef**.

```
12000-1#show ip cef
Prefix              Next Hop            Interface
0.0.0.0/0           drop                Null0 (default route handler entry)
1.1.1.1/32          attached            Null0
2.2.2.2/32          receive
64.0.0.0/30         attached            ATM4/3.300
...
```

Directives de déploiement

Cisco recommande des pratiques de déploiement conservatrices. Pour déployer avec succès des listes de contrôle d'accès rACL, les exigences d'accès au plan de contrôle et de gestion existantes doivent être bien comprises. Dans certains réseaux, il peut être difficile de déterminer le profil de trafic exact nécessaire pour créer les listes de filtrage. Les directives suivantes décrivent une approche très prudente pour le déploiement de listes de contrôle d'accès réactives à l'aide de configurations de listes de contrôle d'accès réitératives afin d'identifier et éventuellement de filtrer le trafic.

1. **Identifiez les protocoles de routage utilisés dans le réseau avec une ACL de classification.**Déployez une rACL qui autorise tous les protocoles connus qui accèdent au protocole GRP. Cette " détection " rACL doit avoir des adresses source et de destination définies sur **n'importe quelle**. La journalisation peut être utilisée pour élaborer une liste d'adresses sources correspondant aux **instructions d'autorisation du protocole.** En plus de l'instruction **permit** de protocole, une **permit any any log** line à la fin de la rACL peut être utilisée pour identifier d'autres protocoles qui seraient filtrés par la rACL et qui pourraient nécessiter un accès au GRP.L'objectif est de déterminer quels protocoles utilise le réseau spécifique. La journalisation doit être utilisée pour l'analyse " déterminer ce que " communiquer avec le routeur.**Remarque :** bien que le mot clé **log** fournisse des informations précieuses sur les détails des accès ACL, les accès excessifs à une entrée ACL qui utilise ce mot clé peuvent entraîner un nombre écrasant d'entrées de journal et éventuellement une utilisation élevée du CPU du routeur. Employez le **mot-clé de journal pour de courtes périodes de temps et seulement si nécessaire pour aider à classifier le trafic.**
2. **Examiner les paquets identifiés et commencer à filtrer l'accès au protocole GRP.**Une fois que les paquets filtrés par la rACL à l'étape 1 ont été identifiés et examinés, déployez une rACL avec une instruction **permit any any any** pour les protocoles autorisés. Comme à l'étape 1, le **mot-clé de journal peut fournir plus d'informations au sujet des paquets qui correspondent**

aux entrées permit. L'utilisation de **deny any any log** à la fin peut aider à identifier les paquets inattendus destinés au protocole GRP. Cette rACL fournit une protection de base et permet aux ingénieurs réseau de s'assurer que tout le trafic requis est autorisé.L'objectif est de tester la plage de protocoles qui doivent communiquer avec le routeur sans avoir la plage explicite d'adresses IP source et de destination.

3. **Restreindre une plage macro d'adresses source.**Autorisez uniquement la plage complète de votre bloc CIDR (Classless Interdomain Routing) alloué comme adresse source. Par exemple, si 171.68.0.0/16 vous a été attribué pour votre réseau, autorisez les adresses source de seulement 171.68.0.0/16.Cette étape réduit les risques sans interrompre les services. Il fournit également des points de données de périphériques/personnes externes à votre bloc CIDR qui peuvent accéder à votre équipement. Toute adresse externe sera supprimée.Les homologues BGP externes nécessitent une exception, car les adresses source autorisées pour la session se trouvent en dehors du bloc CIDR.Cette phase peut être prolongée de quelques jours pour collecter des données pendant la prochaine phase de réduction de la liste de contrôle d'accès.
4. **Affinez les instructions permit rACL pour autoriser uniquement les adresses source autorisées connues.**Limitez de plus en plus l'adresse source pour autoriser uniquement les sources qui communiquent avec le protocole GRP.
5. **Limitez les adresses de destination sur la liste de contrôle d'accès. (facultatif)**Certains fournisseurs de services Internet (FAI) peuvent choisir d'autoriser uniquement des protocoles spécifiques à utiliser des adresses de destination spécifiques sur le routeur. Cette dernière phase vise à limiter la plage d'adresses de destination qui accepteront le trafic pour un protocole. [6]

Exemple de déploiement

L'exemple ci-dessous montre une liste de contrôle d'accès de réception protégeant un routeur en fonction de l'adressage suivant.

- Le bloc d'adresses du FAI est 169.223.0.0/16.
- Le bloc d'infrastructure du FAI est 169.223.252.0/22.
- Le bouclage pour le routeur est 169.223.253.1/32.
- Le routeur est un routeur fédérateur principal, de sorte que seules les sessions BGP internes sont actives.

Compte tenu de ces informations, la liste de contrôle d'accès de réception initiale peut être similaire à l'exemple ci-dessous. Puisque nous connaissons le bloc d'adresses d'infrastructure, nous allons d'abord autoriser l'ensemble du bloc. Plus tard, des entrées de contrôle d'accès (ACE) plus détaillées seront ajoutées lorsque les adresses spécifiques seront obtenues pour tous les périphériques ayant besoin d'un accès au routeur.

```
!
no access-list 110
!
!--- This ACL is an explicit permit ACL. !--- The only traffic permitted will be packets that !-
-- match an explicit permit ACE.

!
! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 1 - Explicit Permit !--- Permit only applications whose destination address !--- is
the loopback and whose source addresses !--- come from an valid host.
```

```
!
!--- Note: This template must be tuned to the network's !--- specific source address
environment. Variables in !--- the template need to be changed.

!
!--- Permit BGP. ! access-list 110 permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq bgp
! !--- Permit OSPF. ! access-list 110 permit ospf 169.223.252.0 0.0.3.255 host 224.0.0.5 ! !---
Permit designated router multicast address, if needed. ! access-list 110 permit ospf
169.223.252.0 0.0.3.255 host 224.0.0.6 access-list 110 permit ospf 169.223.252.0 0.0.3.255 host
169.223.253.1 ! !--- Permit EIGRP. ! access-list 110 permit eigrp 169.223.252.0 0.0.3.255 host
224.0.0.10 access-list 110 permit eigrp 169.223.252.0 0.0.3.255 host 169.223.253.1 ! !--- Permit
remote access by Telnet and SSH. ! access-list 110 permit tcp 169.223.252.0 0.0.3.255 host
169.223.253.1 eq 22 access-list 110 permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq
telnet ! !--- Permit SNMP. ! access-list 110 permit udp 169.223.252.0 0.0.3.255 host
169.223.253.1 eq snmp ! !--- Permit NTP. ! access-list 110 permit udp 169.223.252.0 0.0.3.255
host 169.223.253.1 eq ntp ! !--- Router-originated traceroute: !--- Each hop returns a message
that ttl !--- has been exceeded (type 11, code 3); !--- the final destination returns a message
that !--- the ICMP port is unreachable (type 3, code 0). ! access-list 110 permit icmp any
169.223.253.1 ttl-exceeded access-list 110 permit icmp any 169.223.253.1 port-unreachable ! !---
Permit TACACS for router authentication. ! access-list 110 permit tcp 169.223.252.0 0.0.3.255
host 169.223.253.1 established ! !--- Permit RADIUS. ! ! access-list 110 permit udp
169.223.252.0 0.0.3.255 169.223.253.1 log ! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !---
Phase 2 – Explicit Deny and Reaction !--- Add ACEs to stop and track specific packet types !---
that are destined for the router. This is the phase !--- where you use ACEs with counters to
track and classify attacks.

!
!--- SQL WORM Example – Watch the rate of this worm. !--- Deny traffic destined to UDP ports
1434 and 1433. !--- from being sent to the GRP. This is the SQL worm. ! access-list 110 deny udp
any any eq 1433 access-list 110 deny udp any any eq 1434 !
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 3 – Explicit Denies for
Tracking !--- Deny all other traffic, but count it for tracking.

!
access-list 110 deny udp any any
access-list 110 deny tcp any any range 0 65535
access-list 110 deny ip any any
```

Notes

1. Référez-vous à Comprendre le SPD (Selective Packet Discard) SPD et les consignes de file d'attente pour augmenter la résistance DoS.
2. Pour plus d'informations sur Cisco Express Forwarding et les contiguïtés, reportez-vous à Présentation de Cisco Express Forwarding.
3. Pour une discussion détaillée des directives de déploiement des listes de contrôle d'accès et des commandes associées, référez-vous à Mise en oeuvre des listes de contrôle d'accès sur les routeurs Internet de la gamme Cisco 12000.
4. Il s'agit des offres Vanilla, BGPPA (Border Gateway Protocol Policy Accounting), PIRC (Per Interface Rate Control) et FRTP (Frame Relay Traffic Policing).
5. La phase II de la protection Receive Path permet la création d'une interface de gestion, limitant automatiquement l'adresse IP qui écoute les paquets entrants.

Informations connexes

- Access Lists Support Page
- Support technique - Cisco Systems