GSR : Réception des listes de contrôle d'accès

Contenu

Introduction

Ce document décrit une nouvelle fonctionnalité de sécurité appelée reçoivent des listes de contrôle d'accès (rACLs) [1] et présentent des recommandations et des instructions pour des déploiements de rACL. Recevez ACLs sont utilisés pour augmenter la Sécurité sur des Routeurs de Cisco 12000 en protégeant le processeur de la route Gigabit du routeur (GRP) contre le trafic inutile et potentiellement célérat. Recevez ACLs ont été ajoutés comme levée spéciale à la commande de puissance de maintenance pour la version de logiciel 12.0.21S2 de Cisco IOS® et intégrés dans le Logiciel Cisco IOS version 12.0(22)S.

Protection GRP

Des données reçues par un routeur de commutateur de gigabit (GSR) peuvent être divisées en deux larges catégories :

- Trafiquez qui traverse le routeur par l'intermédiaire du chemin de transfert.
- Trafiquez qui doit être envoyé par l'intermédiaire du chemin de réception au GRP pour l'analyse approfondie.

En fonctionnement les fonctionnement normal, l'immense majorité du trafic traverse simplement un GSR en route à d'autres destinations. Cependant, le GRP doit traiter de certains types de données, spécialement protocoles de routage, accès de routeur distant, et trafic de gestion du réseau (tel que protocole SNMP [SNMP]). En plus de ce trafic, d'autres paquets de la couche 3 pourraient exiger la flexibilité de traitement du GRP. Ceux-ci incluraient certaines options IP et certaines formes des paquets de Protocole ICMP (Internet Control Message Protocol). Référez-vous à l'annexe en fonction reçoivent des contiguïtés et des paquets donnés un coup de volée

pour des détails supplémentaires concernant des rACLs et reçoivent le trafic de chemin sur le GSR.

Un GSR a plusieurs chemins de données, chaque différentes formes de service du trafic. Le trafic de transit est expédié de la carte de ligne d'entrée (LC) à la matrice et puis à la carte de sortie pour la prochaine livraison de saut. En plus du chemin de données du trafic de transit, un GSR a deux autres chemins pour le trafic exigeant le traitement local : LC à la CPU LC et LC à la CPU LC à la matrice à GRP. Le tableau suivant affiche les chemins pour plusieurs caractéristiques et protocoles utilisés généralement.

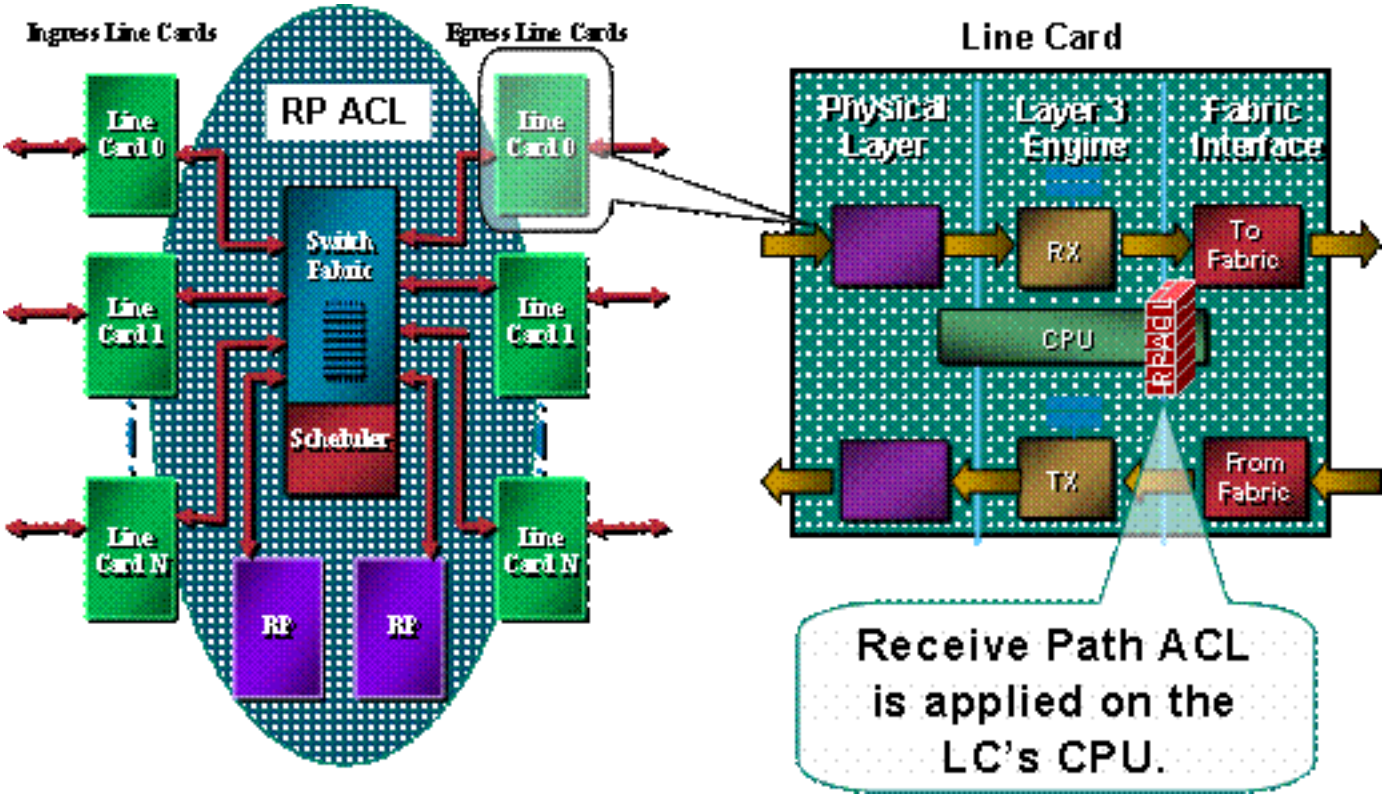
Type de trafic	Chemin de données
Le trafic normal (de transit)	LC à la matrice au LC
Acheminement de Protocols/SSH/SNMP	LC à la CPU LC à la matrice à GRP
Écho d'ICMP (ping)	LC à la CPU LC
Se connecter	

Le processeur d'artère pour le GSR a une capacité limitée de traiter le trafic fourni du LCS destiné pour le GRP lui-même. Si un grand volume de données exige donner un coup de volée au GRP, ce trafic peut accabler le GRP. Ceci a comme conséquence une attaque efficace du déni de service (DOS). La CPU du GRP lutte pour suivre l'examen de paquet et commence à relâcher des paquets, inondant l'entrée-attente et les files d'attente de Rejet sélectif de paquet (SPD). [2] GSR devraient être protégés contre trois scénarios, qui peuvent résulter des attaques DoS dirigées à un GRP du routeur.

- Perte de paquets de protocole de routage d'une inondation de normal-priorité
- Perte de paquets de session de Gestion (telnet, shell sécurisé [SSH], SNMP) d'une inondation de normal-priorité
- Perte de paquets d'une inondation prioritaire charriée

La perte potentielle de données de protocole de routage pendant une inondation de normal-priorité est actuellement allégée par classification statique et la limitation de débit du trafic destinée au GRP du LCS. Malheureusement, cette approche a des limites. La limitation de débit pour le trafic de normal-priorité destiné au GRP est insuffisante pour garantir la protection aux données prioritaires de protocole de routage si une attaque est fournie par l'intermédiaire de plusieurs LCS. Diminuant le seuil auquel des données de normal-priorité sont abandonnées pour assurer une telle protection aggrave seulement la perte du trafic d'administration d'une inondation de normal-priorité.

Pendant que cette image affiche, le rACL est exécuté sur chaque LC avant que le paquet soit transmis au GRP.



Un mécanisme de protection pour le GRP est exigé. le trafic d'affect de rACLs en raison dont est envoyé au GRP reçoivent des contiguïtés. Recevez les contiguïtés sont des contiguïtés de Cisco Express Forwarding pour le trafic destiné aux adresses IP du routeur, telles que l'adresse d'émission ou les adresses configurées sur les interfaces du routeur. [3] voyez l'annexe section pour plus de détails en fonction recevoir des contiguïtés et des paquets donnés un coup de volée.

Trafiquez qui écrit un LC est d'abord envoyé à la CPU de gens du pays du LC, et des paquets qui exigent le traitement par le GRP sont alignés pour expédier au processeur d'artère. L'ACL de réception est créé sur le GRP et puis abaissé aux CPU du divers LCS. Avant que le trafic soit envoyé de la CPU LC au GRP, le trafic est comparé au rACL. Si permis, le trafic passe au GRP, alors que tout autre trafic est refusé. Le rACL est examiné avant le LC à la fonction de limitation de débit GRP. Puisque le rACL est utilisé pour tous recevez les contiguïtés, quelques paquets qui sont manipulés par la CPU LC (telle que des requêtes d'écho) sont sujets au rACL filtrant aussi bien. Ceci doit être pris en considération en concevant des entrées de rACL.

Recevez ACLs sont la partie une d'une plage de liasse multiple de programme des mécanismes pour protéger les ressources dans un routeur. Les travaux futurs incluront un composant de limitation de débit au rACL.

Impact sur les performances

Aucune mémoire n'est consommée autre que celle nécessaire pour tenir l'entrée simple de configuration et la liste d'accès définie elle-même. Le rACL est copié sur chaque LC, ainsi une légère zone mémoire est prise sur chaque LC. De façon générale, les ressources utilisées sont minuscules, particulièrement en comparaison avec les avantages du déploiement.

Un ACL de réception n'affecte pas la représentation du trafic expédié. Le rACL s'applique seulement pour recevoir le trafic de contiguïté. Le trafic expédié n'est jamais sujet au rACL. Le trafic de transit est filtré utilisant l'interface ACLs. Ces le « militaire de carrière » ACLs sont appliqués aux interfaces dans une direction spécifiée. Le trafic est sujet à l'ACL traitant avant le rACL traitant, ainsi le trafic refusé par l'ACL d'interface ne sera pas reçu par le rACL. [4]

Le LC exécutant l'effectif filtrant (en d'autres termes, le LC recevant le trafic filtré par le rACL) aura augmenté l'utilisation du processeur en raison du traitement du rACL. Cette utilisation du processeur accrue, cependant, est provoqué par par un grand volume du trafic destiné au GRP ; l'avantage du GRP de la protection de rACL est supérieur loin à l'utilisation du processeur accrue sur un LC. L'utilisation du processeur sur un LC variera basé sur le type de moteur LC. Par exemple, donné la même attaque, une engine 3 LC aura l'utilisation du processeur inférieure qu'une engine 0 LC.

L'activation de turbo ACLs (à l'aide de la commande d'**access-list compiled**) convertit ACLs en gamme très efficace d'entrées de table de consultation. Quand turbo ACLs sont activés, la profondeur de rACL n'affecte pas la représentation. En d'autres termes, la vitesse de traitement est indépendant du nombre d'entrées dans l'ACL. Si le rACL est court, turbo ACLs n'augmentera pas de manière significative la représentation mais consommera la mémoire ; avec les rACLs courts, ACLs compilé sont non nécessaire probable.

En protégeant le GRP, les aides de rACL assurent le routeur et, finalement, la stabilité du réseau pendant une attaque. Comme décrit ci-dessus, le rACL est traité sur la CPU LC, ainsi l'utilisation du processeur sur chaque LC augmentera quand un de large volume des données est dirigé au routeur. Sur les paquets E0/E1 et un certain E2, l'utilisation du processeur de 100+% pourrait mener aux baisses de protocole de routage et de couche de liaison. Ces baisses sont localisées à la carte, et les processus de routage GRP sont protégés, de ce fait stabilité de mise à jour. Les cartes E2 avec le microcode étrangler-activé [5] lancent le mode d'étranglement quand sous la charge lourde et seulement la priorité en avant 6 et le trafic 7 au protocole de routage. D'autres types de moteur ont des architectures de multi-file d'attente ; par exemple, les cartes d'E3 ont trois files d'attente à la CPU, avec des paquets de protocole de routage (priorité 6/7) dans un distinct, file d'attente prioritaire. La CPU de la haute LC, à moins que les paquets de haute-priorité l'entraînent, n'aura pas comme conséquence des baisses de protocole de routage. Des paquets aux files d'attente de faible priorité queue-seront relâchés. En conclusion, les cartes E4-based ont huit files d'attente à la CPU, avec une dédiée aux paquets de protocole de routage.

Syntaxe

Un ACL de réception est appliqué avec la commande de configuration globale suivante de distribuer le rACL à chaque LC dans le routeur.

[no] ip receive access-list *<num>*
En cette syntaxe, le ***<num>*** est défini comme suit.

[no] ip receive access-list *<num>*

Modèle et exemples de base d'ACL

Pour pouvoir utiliser cette commande, vous devez définir une liste d'accès qui identifie le trafic qui devrait être permis pour parler au routeur. La liste d'accès doit inclure les protocoles de routage aussi bien que le trafic d'administration (protocole BGP [BGP], protocole OSPF [OSPF], SNMP, SSH, telnet). Référez-vous à la section sur des instructions de déploiement pour plus de détails.

L'ACL suivant d'échantillon fournit un contour simple et présente quelques exemples de configuration qui peuvent être adaptés pour des usages spécifiques. L'ACL illustre les configurations exigées pour plusieurs services généralement exigés/protocoles. Pour le SSH, le

telnet, et le SNMP, une adresse de bouclage est utilisée comme destination. Pour les protocoles de routage, l'adresse réelle d'interface est utilisée. Le choix des interfaces de routeur aux utiliser dans le rACL est déterminé par des stratégies et des exécutions de site local. Par exemple, si des bouclages sont utilisés pour toutes les sessions scrutantes BGP, puis seulement ces bouclages doivent être permis dans les déclarations d'**autorisation** pour le BGP.

```
[no] ip receive access-list <num>
```

Comme avec tout le Cisco ACLs, il y a une **instruction de refus** implicite à la fin de la liste d'accès, ainsi n'importe quel trafic qui n'apparie pas une entrée dans l'ACL sera refusé.

Remarque: Le mot clé de journal peut être utilisé pour aider à classifier le trafic destiné au GRP qui n'est pas permis. Bien que le **mot clé de journal** fournisse l'importante vue dans les détails des hit d'ACL, les hit excessifs à un rubrique de liste ACL qui utilise ce mot clé augmenteront l'utilisation du processeur LC. L'incidence des performances associée avec se connecter variera avec le type de moteur LC. Se connecter généralement devrait être utilisé seulement si nécessaire sur les engines 0/1/2. Pour les engines 3/4/4+, se connecter résulte dedans loin moins d'incidence en raison de la performance du CPU accrue et de l'architecture de multi-file d'attente.

Le niveau de la finesse de cette liste d'accès est déterminé par stratégie de sécurité locale (par exemple, le niveau du filtrage exigé pour des voisins OSPF).

rACLS et paquets fragmentés

Les ACL ont un mot clé de **fragments** qui active le comportement de gestion des paquets fragmentés spécialisés. Généralement des fragments non initiaux qui apparient les déclarations L3 (indépendamment des informations L4) dans un ACL sont affectés par l'**autorisation** ou l'**instruction de refus de l'**entrée appariée. Notez que l'utilisation du mot clé de **fragments** peut forcer ACLs à refusent ou permettent des fragments non initiaux avec plus de finesse.

Dans le contexte de rACL, le filtrage des fragments ajoute une couche supplémentaire de protection contre une attaque DoS qui utilise seulement des fragments non initiaux (comme FO > 0). Utilisant une **instruction de refus** pour des fragments non initiaux au début du rACL refuse tous les fragments non initiaux d'accéder au routeur. Sous des rares circonstances, une session valide pourrait exiger de la fragmentation et donc d'être filtrée si une déclaration de **fragment de refuser** existe dans le rACL.

Par exemple, considérez l'ACL partiel affiché 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>
```

Ajouter ces entrées au début d'un rACL refuse n'importe quel accès de fragment non initial au GRP, alors que les paquets ou les fragments initiaux nonfragmented passent aux prochaines lignes du rACL inchangé par les déclarations de **fragment de refuser**. L'extrait ci-dessus de rACL facilite également la classification de l'attaque depuis chaque protocole – Protocole universel de datagramme (UDP), TCP, et ICMP – des incréments séparent des compteurs dans l'ACL.

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

Évaluation des risques

Assurez-vous que le rACL ne filtre pas le trafic critique tel que des protocoles de routage ou l'accès interactif aux Routeurs. Le trafic nécessaire de filtrage a pu avoir comme conséquence une incapacité d'accéder à distance le routeur, de ce fait exigeant une connexion de console. Pour cette raison, les configurations de laboratoire devraient imiter le déploiement réel aussi près que possible.

En tant que toujours, Cisco recommande que vous testiez cette caractéristique dans le laboratoire avant le déploiement.

Annexes et notes

Recevez les contiguïtés et les paquets donnés un coup de volée

Comme décrit plus tôt dans ce document, quelques paquets exigent le traitement GRP. Les paquets sont donnés un coup de volée de l'avion de donnée-expédition au GRP. C'est une liste des formes communes des données de la couche 3 qui exigent l'accès GRP.

- Protocoles de routage
- Le trafic de contrôle de Multidiffusion (OSPF, routeur de secours immédiat Protocol [HSRP], protocole de distribution de balise [Protocole TDP], Protocol Independent Multicast [PIM], et tels)
- Paquets de Commutation multiprotocole par étiquette (MPLS) ayant besoin de fragmentation
- Paquets avec certaines options IP telles que l'alerte de routeur
- Premier paquet des flots de Multidiffusion
- Paquets fragmentés d'ICMP qui exigent le réassemblage
- Tous trafiquent destiné au routeur lui-même (excepté le trafic traité sur le LC)

Puisque les rACLs s'appliquent pour recevoir des contiguïtés, le rACL filtre du trafic qui n'est pas donné un coup de volée au GRP mais est une contiguïté de réception. La plupart d'exemple classique de ceci est une requête d'écho d'ICMP (ping). Des requêtes d'écho d'ICMP dirigées vers le routeur sont traitées par la CPU LC ; puisque les demandes sont recevez les contiguïtés, elles sont également filtrés par le rACL. Par conséquent, pour permettre des pings aux interfaces (ou aux bouclages) du routeur, le rACL doit explicitement permettre aux requêtes d'écho.

Recevez les contiguïtés peut être visualisé utilisant la commande de **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 rACLs, les conditions requises existantes d'accès d'avion de contrôle et de Gestion doivent être bien comprises. Dans quelques réseaux, la détermination du profil précis du trafic requis pour établir les listes de filtrage pourrait être difficile. Les instructions suivantes décrivent très une

approche prudente pour déployer des rACLs utilisant des configurations itératives de rACL pour aider à identifier et filtrer par la suite le trafic.

1. **Identifiez les protocoles de routage utilisés dans le réseau avec une ACL de classification.**Déployez un rACL qui permet tous les protocoles connus qui accèdent au GRP. Ce rACL de « détection » en devrait avoir la source et les adresses de destination réglées à. La journalisation peut être utilisée pour élaborer une liste d'adresses sources correspondant aux **instructions d'autorisation** du protocole. En plus de la déclaration d'**autorisation de** protocole, une **autorisation n'importe quelle n'importe quelle** ligne de **log à l'**extrémité du rACL peut être utilisée pour identifier d'autres protocoles qui seraient filtrés par le rACL et qui pourraient exiger l'accès au GRP.L'objectif est de déterminer quels protocoles utilise le réseau spécifique. Se connecter devrait être utilisé pour que l'analyse détermine « quoi d'autre » pourrait communiquer avec le routeur.**Remarque:** Bien que le **mot-clé de journal** fournisse des informations précieuses sur les détails des occurrences d'ACL, si les occurrences à une entrée de la liste ACL utilisant ce mot clé sont excessives, cela pourrait avoir comme conséquence un nombre écrasant d'entrées de journal et éventuellement une utilisation élevée de la 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. **Passez en revue les paquets identifiés et commencez à filtrer l'accès au GRP.**Une fois que les paquets filtrés par le rACL dans l'étape 1 ont été identifiés et passés en revue, déployez un rACL avec une **autorisation n'importe quelle n'importe quelle** déclaration pour les protocoles permis. Comme à l'étape 1, le **mot-clé de journal** peut fournir plus d'informations au sujet des paquets qui correspondent aux entrées **permit**. Utilisant **refusez n'importe quel n'importe quel log à l'**extrémité peut aider à identifier tous les paquets inattendus destinés au GRP. Ce rACL assurera la protection de base et permettra à des ingénieurs réseau pour s'assurer qu'on permet tout le trafic exigé.L'objectif est de tester la plage des protocoles qui doivent communiquer avec le routeur sans avoir la plage explicite des adresses d'origine et destination IP.
3. **Limitez une macro plage des adresses sources.**Permettez seulement la gamme complète de votre bloc alloué de Routage interdomaine sans classe (CIDR) à autoriser comme adresse source. Par exemple, si vous avez été alloué 171.68.0.0/16 pour votre réseau, puis permettez les adresses sources juste de 171.68.0.0/16.Cette étape rétrécit le risque sans ne casser aucun services. Il fournit également des points d'informations de périphériques/de personnes de l'extérieur de votre bloc CIDR qui pourrait accéder à votre matériel. Toute l'adresse d'extérieur sera abandonnée.Les pairs de BGP externe auront besoin d'une exception, puisque les adresses sources permises pour la session se trouveront en dehors du bloc CIDR.Cette phase peut être laissée en fonction pendant quelques jours pour collecter des données pour la phase suivante de rétrécir le rACL.
4. **Rétrécissez les déclarations d'autorisation de rACL pour permettre seulement les adresses sources autorisées connues.**Limitez de plus en plus l'adresse source pour permettre seulement les sources qui communiquent avec le GRP.
5. **Limitez les adresses de destination sur le rACL. (*facultatif*)**Quelques fournisseurs d'accès Internet (ISP) peuvent choisir de permettre seulement à des protocoles spécifiques pour utiliser les adresses de destination spécifiques sur le routeur. Cette phase finale est censée pour limiter la plage des adresses de destination qui recevront le trafic pour un protocole. [6]

Exemple de déploiement

L'exemple ci-dessous affiche un ACL de réception protégeant un routeur basé sur l'adressage suivant.

- Le bloc d'adresses de l'ISP est 169.223.0.0/16.
- Le bloc d'infrastructure de l'ISP est 169.223.252.0/22.
- Le bouclage pour le routeur est 169.223.253.1/32.
- Le routeur est un routeur de circuit principal, ainsi seulement les sessions BGP internes sont en activité.

Fourni ces informations, l'initiale reçoivent l'ACL pourrait être quelque chose comme l'exemple ci-dessous. Puisque nous connaissons le bloc d'adresses d'infrastructure, nous d'abord permettrons le bloc de totalité. Plus tard, des entrées de contrôle d'accès plus détaillées (as) seront ajoutées comme adresses spécifiques sont obtenues pour tous les périphériques ayant besoin de l'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 compréhension derrière le Rejet sélectif de paquet (SPD) SPD et des instructions de file d'attente d'attente pour augmenter la résistance DOS.
2. Pour plus d'informations sur Cisco Express Forwarding et les contiguïtés, référez-vous à l'aperçu de Cisco Express Forwarding.
3. Pour une analyse détaillée des instructions de déploiement d'ACL et des commandes relatives, se rapportent à mettre en application ACLs sur des Routeur Internet de la série Cisco 12000.
4. Ceci se rapporte à la vanille, la comptabilité de stratégie de protocole BGP (BGPPA), par paquets du contrôle (PIRC), et du Fonction Frame Relay Traffic Policing (FRTP) de débit d'interface.
5. La phase II de la protection de chemin de réception tiendra compte de la création d'une interface de gestion, limitant automatiquement quelle adresse IP écoutera des paquets entrant.

Informations connexes

- Access Lists Support Page
- Support technique - Cisco Systems