Listes de contrôle d'accès de transit : Filtrage de la périphérie

Contenu

Introduction

Ce document présente des instructions et recommande des techniques de déploiement pour filtrer le transit et le trafic périphérique au niveau des points d'entrée de votre réseau. Des Listes de contrôle d'accès (ACL) du transit sont utilisées pour augmenter la sécurité des réseaux, ne permettant qu'au trafic requis de pénétrer dans votre ou vos réseau(x.)

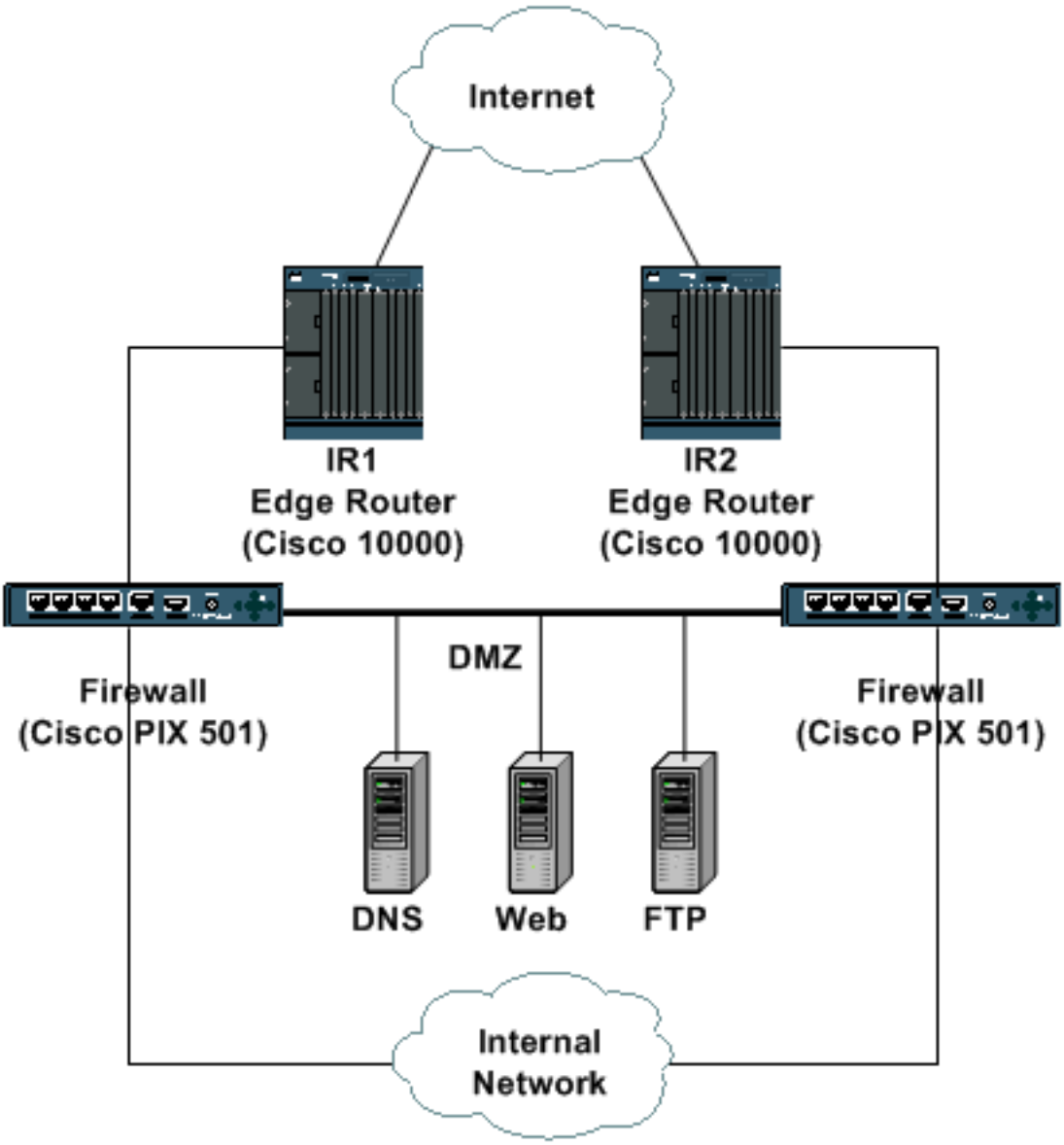
Filtres de transit

Installation typique

Dans la plupart des environnements de réseau de périphérie, tels qu'un point de présence typique d'Internet de réseau d'entreprise, le filtrage d'entrée devrait être utilisé pour relâcher le trafic non autorisé à la périphérie du réseau. Dans certains déploiements de fournisseur de services, cette forme du filtrage de périphérie ou de trafic de transit peut également être utilisée efficacement pour limiter l'écoulement du trafic de transit à et des clients aux protocoles permis par particularité seulement. Ce document se concentre sur un modèle de déploiement en entreprise.

Cet exemple dépeint une conception typique de connexion Internet d'entreprise. Deux Routeurs de périphérie, IR1 et IR2, fournissent la connexion en direct à l'Internet. Derrière ces deux

Routeurs, une paire de Pare-feu (Cisco PIXes dans cet exemple) permet d'accéder des capacités et d'inspection avec état au réseau interne et à la zone démilitarisée (DMZ). Le DMZ contient des services de public-revêtement tels que des DN et le Web ; c'est le seul réseau accessible directement de l'Internet public. Le réseau interne devrait ne jamais être accédé à directement par l'Internet, mais le trafic originaire du réseau interne doit pouvoir atteindre des sites Internet.



Les Routeurs de périphérie devraient être configurés pour fournir un premier niveau de sécurité par l'utilisation d'ACLs d'arrivée. L'ACLs permettent seulement le trafic spécifiquement permis au DMZ et permettent le trafic de retour pour des utilisateurs internes accédant à l'Internet. Tout le trafic nonauthorized devrait être abandonné sur les interfaces d'entrée.

Sections d'ACL de transit

Généralement un ACL de transit se compose de quatre sections.

- entrées d'adresse et d'anti-mystification d'Offre spéciale-utilisation qui refusent des sources illégitimes et des paquets avec les adresses sources qui appartiennent dans votre réseau d'écrire le réseau d'une source externe**Remarque:** Le RFC 1918 définit l'espace d'adressage réservé qui n'est pas une adresse source valide sur l'Internet. RFC 3330 définit les adresses d'offre spéciale-utilisation qui pourraient exiger le filtrage. RFC 2827 fournit des instructions

d'anti-mystification.
- Le trafic de retour explicitement permis pour les connexions à Internet internes
- Le trafic extérieurement originaire explicitement permis destiné aux adresses internes protégées
- **Instruction de refus** explicite**Remarque:** Bien que tout l'ACLs contiennent une **instruction de refus** implicite, Cisco recommande l'utilisation d'une **instruction de refus** explicite, par exemple, **refusez l'IP tout**. Sur la plupart des Plateformes, de telles déclarations mettent à jour un compte du nombre de paquets refusés qui peuvent être affichés utilisant la **commande access-list d'exposition**.

Comment développer un ACL de transit

La première étape dans le développement d'un ACL de transit est de déterminer les protocoles exigés dans vos réseaux. Bien que chaque site ait des conditions requises spécifiques, les certains protocoles et applications sont très utilisés et le plus souvent sont laissés. Par exemple, si le segment DMZ fournit la Connectivité pour un web server publiquement accessible, le TCP de l'Internet à l'adresse de serveur DMZ sur le port 80 est exigé. De même, les connexions à Internet internes exigent que le retour d'autorisation d'ACL a établi le trafic TCP – trafiquez qui a le bit de l'accusé de réception (ACK) réglé.

Identifiez les protocoles requis

Le développement de cette liste de protocoles exigés peut être une tâche effrayante, mais il y a plusieurs techniques qui peuvent être utilisées, comme nécessaire, afin d'aider à identifier le trafic exigé.

- **Passez en revue votre stratégie de sécurité locale/stratégie de service.**Votre stratégie de site local devrait aider à fournir une spécification de base des services permis et refusés.
- **Passez en revue/audit votre configuration de Pare-feu.**La configuration en cours de Pare-feu devrait contenir des déclarations explicites d'**autorisation** pour des services permis. Dans de nombreux cas, vous pouvez traduire cette configuration au format d'ACL et l'employer pour créer la partie des rubriques de liste ACL.**Remarque:** Les pare-feu dynamiques typiquement n'ont pas des règles explicites pour le trafic de retour aux connexions autorisées. Puisque le routeur ACLs ne sont pas avec état, on doit explicitement permettre le trafic de retour.
- **Passez en revue/audit vos applications.**Les applications hébergées sur le DMZ et ceux utilisés intérieurement peuvent aider à déterminer des conditions requises de filtrage. Passez en revue les conditions requises d'application afin de fournir les détails essentiels au sujet de la conception de filtrage.
- **Utilisez un ACL de classification.**Un ACL de classification se compose de déclarations d'**autorisation** pour les divers protocoles qui pourraient être destinés au réseau interne. (Voir l'annexe A pour une liste de protocoles et d'applications utilisés généralement.) Utilisez la **commande access-list d'exposition** d'afficher un compte de hit d'entrée de contrôle d'accès (ACE) pour identifier des protocoles requis. Étudiez et comprenez tous les résultats méfiants ou étonnants avant que vous créiez des déclarations explicites d'**autorisation** pour des protocoles inattendus.
- **Utilisez la caractéristique de Commutation Netflow.**Le NetFlow est une caractéristique de commutation qui, si activée, fournit des informations détaillées d'écoulement. Si le NetFlow est activé sur vos Routeurs de périphérie, la commande de **show ip cache flow** donne une

liste de protocoles connectés par NetFlow. Le NetFlow ne peut pas identifier tous les protocoles, ainsi cette technique doit être utilisée en même temps que d'autres.

Identifiez le trafic non valide

En plus de la protection directe, l'ACL de transit devrait également fournir une première ligne de défense contre certains types de trafic non valide sur l'Internet.

- Refusez l'espace RFC 1918.
- Refusez les paquets avec une adresse source qui tombe sous l'espace d'adressage d'offre spéciale-utilisation, comme défini dans RFC 3330.
- Apply anti-charrient des filtres, selon RFC 2827 ; votre espace d'adressage devrait ne jamais être la source des paquets de l'extérieur de votre système autonome (AS).

D'autres types de trafic à considérer incluent :

- **Protocoles externes et adresses IP qui doivent communiquer avec le routeur de périphérie**ICMP des adresses IP de fournisseur de servicesProtocoles de routageIPSec VPN, si un routeur de périphérie est utilisé comme arrêt
- **Le trafic de retour explicitement permis pour les connexions à Internet internes**Types spécifiques de Protocole ICMP (Internet Control Message Protocol)Réponses sortantes de requête de Système de noms de domaine (DNS)TCP établiLe trafic de retour de Protocole UDP (User Datagram Protocol)Connexions de données de FTPConnexions de données TFTPConnexions de multimédia
- **Le trafic extérieurement originaire explicitement permis destiné aux adresses internes protégées**Le trafic VPNProtocole ISAKMP (Internet Security Association and Key Management Protocol)Traversée de Traduction d'adresses de réseau (NAT)Encapsulation de propriété industrielleProtocole ESP (Encapsulating Security Payload)En-tête d'authentification (AH)HTTP aux web serverProtocole SSL (Secure Socket Layer) aux web serverFTP aux serveurs de FTPConnexions de données d'arrivée de FTPConnexions de données d'arrivée de passif de FTP (**pasv**)Protocole SMTP (Simple Mail Transfer Protocol)D'autres applications et serveursRequêtes DNS d'arrivéeTransferts d'arrivée de zone DNS

Appliquez l'ACL

L'ACL nouvellement construit devrait être d'arrivée appliqué sur des interfaces d'Internet-revêtement des Routeurs de périphérie. Dans l'exemple illustré dans la section typique d'installation, l'ACL isapplied dedans sur les interfaces d'Internet-revêtement sur IR1 et IR2.

Voir les sections sur des instructions de déploiement et l'exemple de déploiement pour plus de détails.

Exemple d'ACL

Cette liste d'accès fournit un exemple simple pourtant réaliste des entrées typiques exigées dans un ACL de transit. Cet ACL de base doit être personnalisé avec les détails locaux de configuration de site-particularité.

```
!--- Add anti-spoofing entries. !--- Deny special-use address sources. !--- Refer to RFC 3330
for additional special use addresses.

access-list 110 deny ip 127.0.0.0 0.255.255.255 any
access-list 110 deny ip 192.0.2.0 0.0.0.255 any
access-list 110 deny ip 224.0.0.0 31.255.255.255 any
access-list 110 deny ip host 255.255.255.255 any
!--- The deny statement should not be configured !--- on Dynamic Host Configuration Protocol
(DHCP) relays.

access-list 110 deny ip host 0.0.0.0 any
!--- Filter RFC 1918 space. access-list 110 deny ip 10.0.0.0 0.255.255.255 any access-list 110
deny ip 172.16.0.0 0.15.255.255 any access-list 110 deny ip 192.168.0.0 0.0.255.255 any !---
Permit Border Gateway Protocol (BGP) to the edge router. access-list 110 permit tcp host
bgp_peer gt 1023 host router_ip eq bgp access-list 110 permit tcp host bgp_peer eq bgp host
router_ip gt 1023 !--- Deny your space as source (as noted in RFC 2827). access-list 110 deny ip
your Internet-routable subnet any !--- Explicitly permit return traffic. !--- Allow specific
ICMP types.

access-list 110 permit icmp any any echo-reply
access-list 110 permit icmp any any unreachable
access-list 110 permit icmp any any time-exceeded
access-list 110 deny   icmp any any
!--- These are outgoing DNS queries. access-list 110 permit udp any eq 53 host primary DNS
server gt 1023 !--- Permit older DNS queries and replies to primary DNS server. access-list 110
permit udp any eq 53 host primary DNS server eq 53 !--- Permit legitimate business traffic.
access-list 110 permit tcp any Internet-routable subnet established access-list 110 permit udp
any range 1 1023 Internet-routable subnet gt 1023 !--- Allow ftp data connections. access-list
110 permit tcp any eq 20 Internet-routable subnet gt 1023 !--- Allow tftp data and multimedia
connections. access-list 110 permit udp any gt 1023 Internet-routable subnet gt 1023 !---
Explicitly permit externally sourced traffic. !--- These are incoming DNS queries.

access-list 110 permit udp any gt 1023 host <primary DNS server> eq 53
 !-- These are zone transfer DNS queries to primary DNS server. access-list 110 permit tcp host
secondary DNS server gt 1023 host primary DNS server eq 53 !--- Permit older DNS zone transfers.
access-list 110 permit tcp host secondary DNS server eq 53 host primary DNS server eq 53 !---
Deny all other DNS traffic. access-list 110 deny udp any any eq 53 access-list 110 deny tcp any
any eq 53 !--- Allow IPSec VPN traffic. access-list 110 permit udp any host IPSec headend device
eq 500 access-list 110 permit udp any host IPSec headend device eq 4500 access-list 110 permit
50 any host IPSec headend device access-list 110 permit 51 any host IPSec headend device access-
list 110 deny ip any host IPSec headend device !--- These are Internet-sourced connections to !-
-- publicly accessible servers. access-list 110 permit tcp any host public web server eq 80
access-list 110 permit tcp any host public web server eq 443 access-list 110 permit tcp any host
public FTP server eq 21 !--- Data connections to the FTP server are allowed !--- by the permit
established ACE. !--- Allow PASV data connections to the FTP server.

access-list 110 permit tcp any gt 1023 host public FTP server gt 1023 access-list 110 permit tcp
any host public SMTP server eq 25 !--- Explicitly deny all other traffic.

access-list 101 deny ip any any
```

Remarque: Veuillez maintenir ces suggestions dans l'esprit quand vous appliquez l'ACL de transit.

- **Le mot clé de journal** peut être utilisé afin de fournir le détail supplémentaire au sujet de la source et les destinations pour un protocole donné. Bien que ce mot clé fournisse l'importante vue dans les détails des hit d'ACL, des hit excessifs à un rubrique de liste ACL qui utilise l'utilisation du processeur d'augmentation de **mot clé de journal**. L'impact sur les performances lié à la journalisation varie en fonction de la plate-forme.
- Des messages ICMP inaccessibles sont générés pour les paquets qui sont administrativement refusés par un ACL. Ceci a pu affecter le routeur et joindre la

représentation. Considérez l'utilisation de l'**aucune** commande d'**ip unreachables** afin de désactiver l'ip unreachables sur l'interface où l'ACL de transit (périphérie) est déployé.
- Cet ACL peut être au commencement déployé avec toutes les déclarations d'**autorisation** afin de s'assurer que le trafic légitime d'affaires n'est pas refusé. Une fois que le trafic légitime d'affaires a été identifié et expliqué, la particularité **refusent des** éléments peut être configurée.

ACL et paquets fragmentés

Les ACL ont un mot clé de **fragments** qui active le comportement de gestion des paquets fragmentés spécialisés. Généralement des fragments noninitial qui apparient les déclarations de la couche 3 (protocole, adresse source, et adresse de destination) — indépendamment des informations de la couche 4 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 les fragments noninitial avec plus de finesse.

Le filtrage des fragments ajoute une couche supplémentaire de protection contre une attaque du déni de service (DOS) qui utilise seulement les fragments noninitial (comme FO > 0). L'utilisation d'une **instruction de refus** pour les fragments noninitial au début de l'ACL refuse tous les fragments noninitial 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 l'ACL. Les conditions qui pourraient mener à la fragmentation incluent l'utilisation des Certificats numériques pour l'authentification d'ISAKMP et l'utilisation du NAT Traversal d'IPSec.

Par exemple, considérez l'ACL partiel affiché ici.

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

Ajouter ces entrées au début d'un ACL refuse n'importe quel accès noninitial de fragment au réseau, alors que les paquets ou les fragments initiaux nonfragmented passent aux prochaines lignes de l'ACL inchangé par les déclarations de **fragment de refuser**. L'extrait précédent d'ACL facilite également la classification de l'attaque depuis chaque protocole — UDP, TCP, et ICMP — des incréments séparent des compteurs dans l'ACL.

Puisque beaucoup d'attaques se fondent sur l'inondation avec les paquets fragmentés, le filtrage des fragments entrants au réseau interne fournit une mesure ajoutée de protection et les aides s'assurent qu'une attaque ne peut pas injecter des fragments en appariant simplement des règles de la couche 3 dans l'ACL de transit.

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

Évaluation des risques

Quand vous déployez la protection ACLs du trafic de transit, considérez deux zones clé de risque.

- Assurez-vous que les instructions appropriées de **permis/refus** sont en place. Pour que l'ACL soit efficace, vous devez permettre tous les protocoles priés.

- Les performances de l'ACL varient entre une plate-forme et l'autre. Avant que vous déployiez ACLs, passez en revue les caractéristiques du fonctionnement de votre matériel.

Cisco recommande que vous testiez cette conception dans le laboratoire avant le déploiement.

Annexes

Protocoles et applications utilisés généralement

Noms de port TCP

Cette liste de noms de port TCP peut être utilisée au lieu des numéros de port quand vous configurez l'ACL en logiciel de Cisco IOS®. Référez-vous au RFC de l'assigned number en cours afin de trouver une référence à ces protocoles. Des numéros de port qui correspondent à ces protocoles peuvent également être trouvés par tandis que vous configurez l'ACL en écrivant a **?** au lieu d'un numéro de port.

BGP	kshell
chargen	procédure de connexion
cmd	lpd
en journée	NNTP
jetez	pim
domaine	pop2
écho	pop3
exécutif	SMTP
Finger	sunrpc
FTP	Syslog
FTP-données	tacacstalk
Gopher	telnet
adresse Internet	temps
ident	UUCP
IRC	WHOIS
klogin	WWW

Noms de port UDP

Cette liste de noms de port UDP peut être utilisée au lieu des numéros de port quand vous configurez l'ACL en logiciel de Cisco IOS. Référez-vous au RFC de l'assigned number en cours afin de trouver une référence à ces protocoles. Des numéros de port qui correspondent à ces protocoles peuvent également être trouvés par tandis que vous configurez l'ACL en écrivant a **?** au lieu d'un numéro de port.

coup de poing	ntp
bootpc	pim-automatique-RP
bootps	déchirure
jetez	SNMP

dnsix	snmptrap
domaine	sunrpc
écho	Syslog
ISAKMP	tacacs
IP mobile	entretien
nameserver	tftp
Netbios-dgm	temps
Netbios-NS	qui
Netbios-solides solubles	xdmcp

Directives de déploiement

Cisco recommande des pratiques de déploiement conservatrices. Vous devez avoir une compréhension claire des protocoles priés afin de déployer avec succès le transit ACLs. Ces instructions décrivent une méthode très conservatrice pour le déploiement de la protection ACLs qui utilisent l'approche itérative.

1. **Identifiez les protocoles de routage utilisés dans le réseau avec une ACL de classification.**Déployez un ACL qui permet tous les protocoles connus qui sont utilisés dans le réseau. Cette détection, ou classification, ACL en devrait avoir une adresse source de et une destination d'une adresse IP ou de l'IP de sous-réseau entier d'Internet-routable. Configurez une dernière entrée qui permet à **IP n'importe quelle n'importe quelle** commande de **procédure de connexion** pour aider à identifier les protocoles additionnels que vous devez permettre.L'objectif est de déterminer tous les protocoles exigés qui sont en service sur le réseau. Utilisez se connecter pour l'analyse afin de déterminer 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 les périodes de **mot clé de journal** pour faire court et seulement si nécessaire afin d'aider à classifier le trafic.Veuillez noter que le réseau est en danger d'attaque tandis qu'un ACL qui se compose de toutes les déclarations d'**autorisation** est en place. Exécutez le procédé de classification aussi rapidement que possible de sorte que des contrôles d'accès appropriés puissent être mis en place.
2. **Passez en revue les paquets identifiés et commencez à filtrer l'accès au réseau interne.**Une fois que vous avez identifié et avez passé en revue les paquets filtrés par l'ACL dans l'étape 1, mettez à jour l'ACL de classification pour expliquer des protocoles et des adresses IP nouvellement identifiés. Ajoutez les rubriques de liste ACL pour l'anti-mystification. Au besoin, la particularité de remplacement **refusent des** entrées pour des déclarations d'**autorisation** dans l'ACL de classification. Vous pouvez utiliser la **commande access-list d'exposition** de surveiller la particularité **refusez des** entrées pouvez être surveillé pour le nombre de hits. Ceci fournit des informations sur des tentatives interdites d'accès au réseau sans devoir activer les rubriques de liste ACL logging on. La dernière ligne de l'ACL devrait être un **IP de refuser tout**. De nouveau, le nombre de hits contre cette dernière entrée peut fournir des informations sur des tentatives interdites d'accès.
3. **Le moniteur et mettent à jour l'ACL.**Surveillez l'ACL terminé afin de s'assurer que des

protocoles exigés nouvellement introduits sont ajoutés d'une façon contrôlée. Si vous surveillez l'ACL, il fournit également des informations sur les tentatives interdites d'accès au réseau qui pourraient fournir des informations au sujet des attaques imminentes.

Exemple de déploiement

Cet exemple affiche un ACL de transit qui protège un réseau basé sur cet adressage.

- L'adresse IP de routeur de l'ISP est 10.1.1.1.L'adresse IP d'Internet-revêtement de routeur de périphérie est 10.1.1.2.Le sous-réseau d'Internet-routable est 192.168.201.0 255.255.255.0.Le headend VPN est 192.168.201.100.Le web server est 192.168.201.101.Le ftp server est 192.168.201.102.Le serveur SMTP est 192.168.201.103.Le serveur de DNS principal est 192.168.201.104.Le serveur de DNS secondaire est 172.16.201.50.

L'ACL de protection de transit a été développé a basé sur ces informations. L'ACL permet l'eBGP scrutant au routeur de l'ISP, fournit anti-charrient des filtres, permettent le trafic de retour de particularité, permettent le trafic d'arrivée spécifique, et refusent explicitement tout autre trafic.

```
no access-list 110
!--- Phase 1 – Add anti-spoofing entries. !--- Deny special-use address sources. !--- See RFC
3330 for additional special-use addresses.

access-list 110 deny   ip 127.0.0.0 0.255.255.255 any
access-list 110 deny   ip 192.0.2.0 0.0.0.255 any
access-list 110 deny   ip 224.0.0.0 31.255.255.255 any
access-list 110 deny   ip host 255.255.255.255 any
!--- This deny statement should not be configured !--- on Dynamic Host Configuration Protocol
(DHCP) relays.

access-list 110 deny   ip host 0.0.0.0 any
!--- Filter RFC 1918 space. access-list 110 deny ip 10.0.0.0 0.255.255.255 any access-list 110
deny ip 172.16.0.0 0.15.255.255 any access-list 110 deny ip 192.168.0.0 0.0.255.255 any !---
Permit BGP to the edge router. access-list 110 permit tcp host 10.1.1.1 gt 1023 host 10.1.1.2 eq
bgp access-list 110 permit tcp host 10.1.1.1 eq bgp host 10.1.1.2 gt 1023 !--- Deny your space
as source (as noted in RFC 2827). access-list 110 deny ip 192.168.201.0 0.0.0.255 any !--- Phase
2 – Explicitly permit return traffic. !--- Allow specific ICMP types.

access-list 110 permit icmp any any echo-reply
access-list 110 permit icmp any any unreachable
access-list 110 permit icmp any any time-exceeded
access-list 110 deny   icmp any any
!--- These are outgoing DNS queries. access-list 110 permit udp any eq domain host
192.168.201.104 gt 1023 !--- Permit older DNS queries and replies to primary DNS server. access-
list 110 permit udp any eq domain host 192.168.201.104 eq domain !--- Permit legitimate business
traffic. access-list 110 permit tcp any 192.168.201.0 0.0.0.255 established access-list 110
permit udp any range 1 1023 192.168.201.0 0.0.0.255 gt 1023 !--- Allow FTP data connections.
access-list 110 permit tcp any eq ftp-data 192.168.201.0 0.0.0.255 gt 1023 !--- Allow TFTP data
and multimedia connections. access-list 110 permit udp any gt 1023 192.168.201.0 0.0.0.255 gt
1023 !--- Phase 3 – Explicitly permit externally sourced traffic. !--- These are incoming DNS
queries.

access-list 110 permit udp any gt 1023 host 192.168.201.104 eq domain
!--- Zone transfer DNS queries to primary DNS server. access-list 110 permit tcp host
172.16.201.50 gt 1023 host 192.168.201.104 eq domain !--- Permit older DNS zone transfers.
access-list 110 permit tcp host 172.16.201.50 eq domain host 192.168.201.104 eq domain !--- Deny
all other DNS traffic. access-list 110 deny udp any any eq domain access-list 110 deny tcp any
any eq domain !--- Allow IPSec VPN traffic. access-list 110 permit udp any host 192.168.201.100
eq isakmp access-list 110 permit udp any host 192.168.201.100 eq non500-isakmp access-list 110
```

```
permit esp any host 192.168.201.100 access-list 110 permit ahp any host 192.168.201.100 access-
list 110 deny ip any host 192.168.201.100 !--- These are Internet-sourced connections to !---
publicly accessible servers. access-list 110 permit tcp any host 192.168.201.101 eq www access-
list 110 permit tcp any host 192.168.201.101 eq 443 access-list 110 permit tcp any host
192.168.201.102 eq ftp !--- Data connections to the FTP server are allowed !--- by the permit
established ACE in Phase 3. !--- Allow PASV data connections to the FTP server.

access-list 110 permit tcp any gt 1023 host 192.168.201.102 gt 1023
access-list 110 permit tcp any host 192.168.201.103 eq smtp

!--- Phase 4 – Add explicit deny statement.

access-list 110 deny   ip any any

Edge-router(config)#interface serial 2/0
Edge-router(config-if)#ip access-group 110 in
```

Informations connexes

- Access Lists Support Page
- Services de commutation Cisco IOS référence de commandes, version 12.2 - Commandes : access-list rate-limit par l'ip cef
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems