Protection de votre noyau : Listes de contrôle d'accès de protection d'infrastructure

Contenu

Introduction

Ce document présente des directives et les techniques recommandées de déploiement pour les listes de contrôle d'accès (ACL) de protection de l'infrastructure. Les listes de contrôle d'accès d'infrastructure sont employées afin de réduire au minimum le risque et l'efficacité d'une attaque directe de l'infrastructure par l'autorisation explicite du trafic autorisé seulement au matériel d'infrastructure tout en permettant tout autre trafic de transit.

Protection de l'infrastructure

Fond

Pour protéger les routeurs contre différents risques - accidentels et malveillants - les ACL de protection de l'infrastructure doivent être déployées aux points d'entrée du réseau. Ces listes de contrôle d'accès IPv4 et IPv6 refusent l'accès depuis des sources extérieures vers toutes les adresses d'infrastructure, telles que des interfaces du routeur. En même temps, les ACL permettent au trafic de transit de routine de circuler sans interruption et fournit des RFC 1918 , RFC 3330 de base, ainsi que le filtrage anti-mystification.

Les données reçues par un routeur peuvent être divisées en deux vastes catégories :

- trafic qui passe par le routeur via le chemin de transfert
- trafic destiné au routeur via le chemin de routage de réception pour la gestion du processeur

de routage

En fonctionnement normal, l'immense majorité du trafic de routage traverse simplement un routeur en allant vers sa destination finale.

Cependant, le processeur de routage (RP) doit prendre en charge certains types de données directement, spécialement des protocoles de routage, l'accès de routeur distant (tel que Secure Shell [SSH]) et le trafic de gestion du réseau tel que le Protocole de gestion de réseau simple (SNMP). En outre, les protocoles tels qu'Internet Control Message Protocol (ICMP) et les options d'IP peuvent requérir un traitement direct par le RP. Le plus souvent, l'accès au routeur direct d'infrastructure est requis seulement depuis les sources internes. Quelques exceptions notables incluent le protocole Border Gateway Protocol (BGP) d'appairage externe, les protocoles qui se terminent sur le routeur réel (tel que l'encapsulation de routage générique [GRE] ou les tunnels IPv6 sur IPv4), et les paquets ICMP potentiellement limités pour le test de connectivité tel que la requête d'écho ou les ICMP inatteignables et les messages Time to Live (TTL) expirés pour la commande traceroute.

Remarque: Souvenez-vous que l'ICMP est souvent employé pour des attaques simples de déni de service (DoS) et ne devrait être autorisé que depuis les sources extérieures s'il y a lieu.

Toutes les RP ont une enveloppe de performances dans laquelle elles fonctionnent. Le trafic excessif destiné au RP peut accabler le routeur. Ceci entraîne une utilisation élevée de la CPU et a finalement comme conséquence les abandons de paquet et de protocole de routage qui entraînent un déni de service. En filtrant l'accès aux routeurs d'infrastructure des sources extérieures, plusieurs risques externes liés à une attaque directe du routeur sont atténués. Les attaques originaires de l'extérieur ne peuvent plus accéder au matériel d'infrastructure. L'attaque est déposée sur des interfaces d'entrée dans le système autonome (AS).

Les techniques de filtrage décrites dans ce document sont destinées à filtrer des données destinées au matériel d'infrastructure réseau. Ne confondez pas le filtrage d'infrastructure avec le filtrage générique. La fonction singulière de l'ACL de protection de l'infrastructure est de restreindre à un niveau granulaire les protocoles et les sources pouvant accéder au matériel critique d'infrastructure.

Le matériel d'infrastructure réseau comprend ces zones :

- Toutes les adresses de gestion du routeur et de la commutation, y compris les interfaces de bouclage
- Toutes les adresses de liaison internes : liens routeur vers routeur (accès point à point et multiple)
- Serveurs internes ou services auxquels il ne faut pas accéder depuis des sources extérieures

Dans ce document, tout le trafic non destiné à l'infrastructure est souvent appelé trafic de transit.

Techniques

La protection de l'infrastructure peut être réalisée à l'aide de différentes techniques :

- **ACL de réception (rACL)**Les plates-formes Cisco 12000 et 7500 prennent en charge les rACL qui filtrent tout le trafic destiné au RP et n'affectent pas le trafic de transit. Le trafic doit être explicitement autorisé et la rACL doit être déployée sur chaque routeur. Reportez-vous à GSR : Recevez les listes de contrôle d'accès pour plus d'informations.
- **Listes de contrôle d'accès saut-par-saut**Les routeurs peuvent également être protégés en

définissant les listes de contrôle d'accès qui permettent seulement le trafic autorisé aux interfaces du routeur, refusant toutes les autres sauf le trafic de transit, qui doit être explicitement permis. Cette ACL est logiquement semblable à une rACL mais affecte le trafic de transit, et peut donc avoir un impact négatif sur les performances au niveau du débit de transfert d'un routeur.

- **Filtrage de périphérie par l'intermédiaire des ACL d'infrastructure**Les ACL peuvent être appliquées à la périphérie du réseau. Dans le cas d'un prestataire de service (SP), il s'agit de la périphérie du AS. Cette ACL filtre explicitement le trafic destiné à l'espace d'adresses d'infrastructure. Le déploiement des ACL d'infrastructure de périphérie requiert que vous définissiez clairement votre espace d'infrastructure et les protocoles requis/autorisés qui accèdent à cet espace. L'ACL est appliquée à l'entrée de votre réseau sur toutes les connexions qui font face à l'extérieur, telles que les connexions d'appairage, les connexions de client, etc.Ce document se concentre sur le développement et de déploiement des ACL de protection de l'infrastructure de périphérie.

Exemples d'ACL

Ces listes d'accès IPv4 et IPv6 fournissent des exemples simples mais réalistes des entrées typiques requises dans une ACL de protection. Ces ACL de base doivent être personnalisées avec les détails de configuration spécifiques au site local. Dans de doubles environnements IPv4 et IPv6, les deux listes d'accès sont déployées.

Exemple d'IPv4

```
!--- Anti-spoofing entries are shown here. !--- Deny special-use address sources. !--- Refer to RFC 3330 for additional special use addresses. access-list 110 deny ip host 0.0.0.0 any 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 !--- 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 !--- Deny your space as source from entering your AS. !--- Deploy only at the AS edge. access-list 110 deny ip YOUR_CIDR_BLOCK any !--- Permit BGP. access-list 110 permit tcp host bgp_peer host router_ip eq bgp access-list 110 permit tcp host bgp_peer eq bgp host router_ip !--- Deny access to internal infrastructure addresses. access-list 110 deny ip any INTERNAL_INFRASTRUCTURE_ADDRESSES !--- Permit transit traffic. access-list 110 permit ip any any
```

Exemple d'IPv6

La liste d'accès IPv6 doit être appliquée en tant que liste d'accès nommée étendue.

```
!--- Configure the access-list. ipv6 access-list iacl !--- Deny your space as source from entering your AS. !--- Deploy only at the AS edge. deny ipv6 YOUR_CIDR_BLOCK_IPV6 any !--- Permit multiprotocol BGP. permit tcp host bgp_peer_ipv6 host router_ipv6 eq bgp permit tcp host bgp_peer_ipv6 eq bgp host router_ipv6 !--- Deny access to internal infrastructure addresses. deny ipv6 any INTERNAL_INFRASTRUCTURE_ADDRESSES_IPV6 !--- Permit transit traffic. permit ipv6 any any
```

Remarque: Le **log keyword** peut être utilisé pour fournir des détails supplémentaires au sujet de la source et des destinations pour un protocole donné. Bien que ce mot clé permette d'avoir des informations précieuses sur les détails des occurrences de l'ACL, les occurrences excessives à une entrée de l'ACL qui utilise le **log keyword** augmente l'utilisation de la CPU. L'impact sur les performances lié à la journalisation varie en fonction de la plate-forme. En outre, l'utilisation du mot clé log désactive la commutation Cisco Express Forwarding (CEF) pour les paquets qui

correspondent à l'instruction de la liste d'accès. Ces paquets sont commutés rapidement à la place.

Développement d'une ACL de protection

Généralement, une ACL d'infrastructure se compose de quatre sections :

- entrées d'adresse et d'anti-mystification d'utilisation spéciale qui refusent des sources et des paquets illégitimes avec les adresses sources appartenant à votre AS d'entrer l'AS d'une source extérieure**Remarque:** RFC 3330 définit les adresses IPv4 d'utilisation spéciale qui pourraient requérir le filtrage. L'adresse RFC 1918 définit l'espace d'adresses réservé pour IPv4 qui n'est pas une adresse source valide sur Internet. RFC 3513 définit l'architecture d'adressage d'IPv6. RFC 2827 fournit des directives sur le filtrage d'entrée.
- Le trafic explicitement permis originaire de l'extérieur destiné aux adresses d'infrastructure
- les instructions de **refus** pour tout autre trafic originaire de l'extérieur vers les adresses d'infrastructure
- **les instructions d'autorisation** pour tout autre trafic du fédérateur normal en route vers les destinations de non-infrastructure

La ligne finale dans l'ACL d'infrastructure permet explicitement le trafic de transit : **permit ip any any** pour IPv4 et **permit ipv6 any any** pour IPv6. Cette entrée assure que tous les protocoles IP sont permis par le noyau et que les clients peuvent continuer à exécuter des applications sans problèmes.

La première étape quand vous développez une ACL de protection de l'infrastructure est de comprendre les protocoles de routage requis. Bien que chaque site ait des conditions requises spécifiques, certains protocoles sont généralement déployés et doivent être compris. Par exemple, le BGP vers les homologues externes doit être explicitement permis. Tous les autres protocoles qui requièrent l'accès direct au routeur d'infrastructure doit aussi être permis explicitement. Par exemple, si vous terminez un tunnel GRE sur un routeur d'infrastructure principale, le protocole de routage 47 (GRE) doit aussi être explicitement permis. De même, si vous terminez un tunnel IPv6 sur IPv4 sur un routeur d'infrastructure principale, le protocole 41 (IPv6 sur IPv4) doit aussi être explicitement permis.

Une ACL de classification peut être utilisée pour aider à identifier les protocoles requis. L'ACL de classification se compose d'**instructions d'autorisation** pour les divers protocoles de routage qui peuvent être destinés à un routeur d'infrastructure. Consultez l'annexe sur les protocoles IP pris en charge par le logiciel Cisco IOS® pour obtenir une liste complète. L'utilisation de la commande **show access-list** pour afficher un comptage des occurrences d'entrée de contrôle d'accès (ACE) identifie les protocoles requis. Les résultats suspects ou étonnants doivent être étudiés et compris avant que vous créiez des **instructions d'autorisation** pour des protocoles inattendus.

Par exemple, cette ACL IPv4 aide à déterminer si GRE, IPsec (ESP) et la transmission tunnel IPv6 (protocole IP 41) doivent être permis.

```
access-list 101 permit GRE any infrastructure_ips
access-list 101 permit ESP any infrastructure_ips
access-list 101 permit 41 any infrastructure_ips
access-list 101 permit ip any infrastructure_ips log
!--- The log keyword provides more details !--- about other protocols that are not explicitly
permitted. access-list 101 permit ip any any interface <int> ip access-group 101 in
```

Cette ACL IPv6 peut être utilisée pour déterminer si GRE et IPsec (ESP) doivent être permis.

```
ipv6 access-list determine_protocols
 permit GRE any infrastructure_ips_ipv6
 permit ESP any infrastructure_ips_ipv6
 permit ipv6 any infrastructure_ips_ipv6 log
!--- The log keyword provides more details !--- about other protocols that are not explicitly
permitted. permit ipv6 any any interface <int> ipv6 traffic-filter determine_protocols in
```

En plus des protocoles de routage requis, l'espace d'adresses d'infrastructure doit être identifié puisque c'est l'espace que l'ACL protège. L'espace d'adresses d'infrastructure inclut toutes les adresses qui sont utilisées pour le réseau interne et sont rarement accédées par des sources extérieures telles que des interfaces du routeur, l'adressage de liaison point à point et des services critiques d'infrastructure. Puisque ces adresses sont utilisées pour la partie de destination de l'ACL d'infrastructure, le résumé est critique. Dans la mesure du possible, ces adresses doivent être groupées dans des blocs de routage interdomaine sans classe (CIDR).

Avec l'utilisation des protocoles et des adresses identifiés, l'ACL d'infrastructure peut être construit de manière à permettre les protocoles et à protéger les adresses. En plus de la protection directe, l'ACL fournit également une première ligne de défense contre certains types de trafic incorrect sur Internet.

- L'espace RFC 1918 doit être refusé.
- Les paquets avec une adresse source classées sous l'espace d'adresses d'utilisation spéciale, comme défini dans RFC 3330, doivent être refusés.
- Des filtres anti-mystification doivent être appliqués. (Votre espace d'adresses ne doit jamais être la source des paquets provenant de l'extérieur de votre AS.)

Cette ACL nouvellement construite doit être appliquée en entrée sur toutes les interfaces d'entrée. Consultez les sections sur les directives de déploiement et les exemples de déploiement pour plus de détails.

ACL et paquets fragmentés

Les ACL ont un mot clé de **fragments** qui active le comportement de gestion des paquets fragmentés spécialisés. Sans ce mot clé de **fragments**, les fragments non initiaux correspondant aux instructions de la couche 3 (indépendamment des informations de couche 4) dans une ACL sont affectés par l'instruction de permis ou de refus de l'entrée correspondante. Cependant, en ajoutant le mot clé de **fragments** , vous pouvez obliger l'ACL à refuser ou à permettre les fragments non initiaux avec plus de finesse. Ce comportement est identique pour des listes d'accès IPv4 et IPv6, excepté que, alors que les ACL IPv4 permettent l'utilisation du mot clé de fragments dans les instructions de la couche 3 et de la couche 4, les ACL IPv6 permettent seulement l'utilisation du mot clé de fragments dans les instructions de la couche 3.

Filtrant des fragments ajoute une couche supplémentaire de protection contre une attaque du Déni de service (DOS) qui utilise les fragments non initiaux (c'est-à-dire, FO > 0). Si une instruction de **refus** est utilisée pour les fragments non initiaux au début de l'ACL, l'accès au routeur est refusé à tous les fragments non initiaux. Dans des circonstances rares, une session valide pourrait requérir la fragmentation, et donc être filtrée si une instruction de **fragment de refus** existe dans l'ACL.

Par exemple, considérez cette ACL IPv4 partielle :

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

L'ajout de ces entrées de routage au début d'une ACL refuse n'importe quel accès de fragment noninitial aux routeurs principaux, alors que les paquets ou les fragments initiaux non fragmentés passent aux prochaines lignes de l'ACL sans être changés par les instructions de **fragment de refus**. La commande précédente d'ACL facilite également la classification de l'attaque depuis chaque protocole de routage - Protocole universel de datagramme (UDP), TCP et ICMP - des incréments séparent des compteurs dans l'ACL.

Voici un exemple comparable pour IPv6 :

```
ipv6 access-list iacl deny ipv6 any infrastructure_IP fragments
```

L'ajout de cette entrée au début d'une ACL d'IPv6 refuse n'importe quel accès de fragment non initial aux routeurs principaux. Comme nous l'avons indiqué précédemment, les listes d'accès IPv6 permettent seulement l'utilisation du mot clé de fragments dans des instructions de la couche 3.

Puisque beaucoup d'attaques se fondent sur des routeurs principaux d'inondation avec les paquets fragmentés, le fait de filtrer les fragments entrants à l'infrastructure principale fournit une mesure de protection de plus et aide à assurer qu'une attaque ne peut pas injecter de fragments en correspondant simplement à des règles de la couche 3 dans l'ACL d'infrastructure.

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

Évaluation des risques

Considérez ces deux zones de risque principales quand vous déployez les ACL de protection de l'infrastructure :

- Assurez-vous que les instructions appropriées de **permis**/**refus** sont en place. Pour que l'ACL soit efficace, tous les protocoles requis doivent être permis et l'espace d'adresse exacte doit être protégé par les instructions de **refus**.
- Les performances de l'ACL varient entre une plate-forme et l'autre. Passez en revue les caractéristiques de fonctionnement de votre matériel avant de déployer les ACL.

Comme toujours, il est recommandé de tester cette conception dans un laboratoire avant le déploiement.

Annexes

Protocoles IP pris en charge par le logiciel Cisco IOS

Ces protocoles de routage d'IP sont pris en charge par le Logiciel Cisco IOS :

- 1 – ICMP
- 2 - IGMP
- 3 - GGP
- 4 – Encapsulation IP-in-IP
- 6 – TCP
- 8 - EGP
- 9 – IGRP

- 17 – UDP
- 20 - HMP
- 27 – RDP
- 41 - Transmission tunnel IPv6 en IPv4
- 46 – RSVP
- 47 – GRE
- 50 – ESP
- 51 – AH
- 53 – SWIPE
- 54 - NARP
- 55 - Mobilité d'IP
- 63 - tout réseau local
- 77 – Sun ND
- 80 – ISO IP
- 88 – EIGRP
- 89 – OSPF
- 90 – Sprite RPC
- 91 – LARP
- 94 - IP sur IP compatible KA9Q/NOS
- 103 - PIM
- 108 - Compression IP
- 112 - VRRP
- 113 – PGM
- 115 - L2TP
- 120 - UTI
- 132 - SCTP

Directives de déploiement

Cisco recommande des pratiques de déploiement conservatrices. Afin de déployer avec succès les ACL d'infrastructure, les protocoles requis doivent être bien compris, et l'espace d'adresses doit être clairement identifié et défini. Ces directives décrivent une méthode très conservatrice pour déployer les ACL de protection en utilisant une approche itérative.

1. **Identifiez les protocoles de routage utilisés dans le réseau avec une ACL de classification.**Déployez une ACL qui autorise tous les protocoles de routage connus qui accèdent à des équipements d'infrastructure. Cette ACL de détection a une adresse source **any** et une destination qui entoure l'espace IP d'infrastructure. La journalisation peut être utilisée pour élaborer une liste d'adresses sources correspondant aux **instructions d'autorisation** du protocole. Une dernière ligne permettant l'**ip any any** (ipv4) ou l'**ipv6 any any** (IPv6) est requise pour permettre le flux de trafic.L'objectif est de déterminer quels protocoles utilise le réseau spécifique. La journalisation est utilisée 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. En outre, l'utilisation du **mot clé log** désactive la commutation Cisco Express Forwarding (CEF) pour les paquets qui correspondent à

l'instruction de la liste d'accès. Ces paquets sont commutés rapidement à la place. 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 processeur de routage RP.**Une fois que les paquets filtrés par l'ACL à l'étape 1 ont été identifiés et passés en revue, déployez une ACL avec une autorisation **permit any source** vers des adresses d'infrastructure pour les protocoles de routage 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**. Le fait d'utiliser **deny any** à la fin peut aider à identifier tous les paquets inattendus destinés aux routeurs. La dernière ligne de cette ACL doit être une instruction **permit ip any any** (IPv4) ou **permit ipv6 any any** (IPv6) pour permettre l'écoulement du trafic de transit. Cette ACL assure une protection de base et permet à des ingénieurs réseau de s'assurer que tout le trafic requis est autorisé.
3. **Restreignez les adresses sources.**Une fois que vous avez une bonne compréhension des protocoles qui doivent être permis, vous pouvez effectuer plus de filtrage pour ne permettre que des sources autorisées pour ces protocoles. Par exemple, vous pouvez explicitement autoriser des voisins BGP externes ou des adresses d'homologue GRE spécifiques.Cette étape réduit le risque sans rompre aucun service et vous permet d'appliquer le contrôle précis aux sources qui accèdent à votre matériel d'infrastructure.
4. **Limitez les adresses de destination sur l'ACL. (*facultatif*)**Certains fournisseurs de services Internet (ISP) pourraient choisir de permettre seulement à des protocoles de routage spécifiques d'utiliser certaines adresses de destination sur le routeur. Cette phase finale est conçue pour limiter la portée des adresses de destination qui peuvent accepter le trafic pour un protocole.

Exemples de déploiement

Exemple d'IPv4

Cet exemple d'IPv4 montre une ACL d'infrastructure protégeant un routeur basé sur cet adressage :

- Le bloc d'adresses ISP est 169.223.0.0/16.
- Le bloc d'infrastructure ISP est 169.223.252.0/22.
- Le bouclage pour le routeur est 169.223.253.1/32.
- Le routeur est de type d'appairage et homologue avec 169.254.254.1 (pour s'adresser à 169.223.252.1).

L'ACL de protection de l'infrastructure affichée est développée en fonction des informations précédentes. L'ACL permet l'appairage de BGP externe vers l'homologue externe, fournit des filtres anti-mystification et protège l'infrastructure de tout accès externe.

```
!
no access-list 110
!
! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 1 – Anti-spoofing Denies !--- These ACEs deny fragments, RFC 1918 space, !--- invalid source addresses, and spoofs of !--- internal space (space as an external source). ! !--- Deny fragments to the infrastructure block. access-list 110 deny tcp any 169.223.252.0 0.0.3.255 fragments access-list 110 deny udp any 169.223.252.0 0.0.3.255 fragments access-list 110 deny icmp any 169.223.252.0 0.0.3.255 fragments !--- Deny special-use address sources. !--- See RFC 3330 for additional special-use addresses. access-list 110 deny ip host 0.0.0.0 any 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 !--- 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 !--- Deny our internal space as an external source. !---
This is only deployed at the AS edge access-list 110 deny ip 169.223.0.0 0.0.255.255 any
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 2 – Explicit Permit !--- Permit only
applications/protocols whose destination !--- address is part of the infrastructure IP block. !-
-- The source of the traffic should be known and authorized. ! !--- Note: This template must be
tuned to the network's !--- specific source address environment. Variables in !--- the template
need to be changed. !--- Permit external BGP. access-list 110 permit tcp host 169.254.254.1 host
169.223.252.1 eq bgp access-list 110 permit tcp host 169.254.254.1 eq bgp host 169.223.252.1 !
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 3 – Explicit Deny to
Protect Infrastructure access-list 110 deny ip any 169.223.252.0 0.0.3.255 !
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 4 – Explicit Permit for
Transit Traffic access-list 110 permit ip any any
```

Exemple d'IPv6

Cet exemple d'IPv6 montre une ACL d'infrastructure protégeant un routeur basé sur cet adressage :

- Le bloc global de préfixe alloué à l'ISP est 2001:0DB8::/32.
- Le bloc de préfixe IPv6 utilisé par l'ISP pour des adresses d'infrastructure réseau est 2001:0DB8:C18::/48.
- Il y a un routeur d'appairage BGP avec une adresse IPv6 source de 2001:0DB8:C18:2:1::1 qui homologue vers l'adresse IPv6 de destination 2001:0DB8:C19:2:1::F.

L'ACL de protection de l'infrastructure affichée est développée en fonction des informations précédentes. L'ACL permet l'appairage de BGP multi-protocole externe vers l'homologue externe, fournit des filtres anti-mystification et protège l'infrastructure de tout accès externe.

```
no ipv6 access-list iacl
ipv6 access-list iacl
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 1 – Anti-spoofing and Fragmentation Denies !--- These ACEs deny fragments and spoofs
of !--- internal space as an external source. !--- Deny fragments to the infrastructure block.
deny ipv6 any 2001:0DB8:C18::/48 fragments !--- Deny our internal space as an external source.
!--- This is only deployed at the AS edge. deny ipv6 2001:0DB8::/32 any
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 2 – Explicit Permit !--- Permit only
applications/protocols whose destination !--- address is part of the infrastructure IP block. !-
-- The source of the traffic should be known and authorized. !--- Note: This template must be
tuned to the !--- specific source address environment of the network. Variables in !--- the
template need to be changed. !--- Permit multiprotocol BGP. permit tcp host 2001:0DB8:C19:2:1::F
host 2001:0DB8:C18:2:1::1 eq bgp permit tcp host 2001:0DB8:C19:2:1::F eq bgp host
2001:0DB8:C18:2:1::1 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 3 –
Explicit Deny to Protect Infrastructure deny ipv6 any 2001:0DB8:C18::/48
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 4 – Explicit Permit for
Transit Traffic permit ipv6 any any
```

Informations connexes

- Access Lists Support Page
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems