Protezione del core: Access Control List di protezione dell'infrastruttura

Sommario

Introduzione

In questo documento vengono fornite linee guida e tecniche di distribuzione consigliate per gli Access Control List (ACL) di protezione dell'infrastruttura. Questi ACL di protezione vengono usati per ridurre al minimo i rischi e l'efficacia di attacchi diretti all'infrastruttura permettendo esplicitamente solo il traffico autorizzato ai dispositivi dell'infrastruttura e tutto il resto del traffico di transito.

Protezione dell'infrastruttura

Sfondo

Per proteggere i router da diversi rischi, sia accidentali che dannosi, è necessario implementare gli ACL di protezione dell'infrastruttura nei punti di ingresso della rete. Questi ACL IPv4 e IPv6 negano l'accesso da origini esterne a tutti gli indirizzi dell'infrastruttura, ad esempio le interfacce del router. Allo stesso tempo, gli ACL permettono al traffico di transito di routine di fluire senza interruzioni e forniscono la RFC 1918 , RFC 3330 e il filtro anti-spoof.

I dati ricevuti da un router possono essere suddivisi in due categorie:

- il traffico che attraversa il router tramite il percorso di inoltro
- traffico destinato al router tramite il percorso di ricezione per la gestione del processore di routing

In condizioni operative normali, la maggior parte del traffico passa semplicemente attraverso un router in viaggio verso la destinazione finale.

Tuttavia, il processore di routing (RP) deve gestire direttamente alcuni tipi di dati, in particolare i protocolli di routing, l'accesso remoto al router (ad esempio Secure Shell [SSH]) e il traffico di gestione della rete, ad esempio il protocollo SNMP (Simple Network Management Protocol). Inoltre, protocolli quali ICMP (Internet Control Message Protocol) e opzioni IP possono richiedere l'elaborazione diretta da parte dell'RP. Molto spesso, l'accesso diretto al router dell'infrastruttura è richiesto solo da fonti interne. Alcune eccezioni degne di nota includono il peering BGP (Border Gateway Protocol) esterno, i protocolli che terminano sul router effettivo (ad esempio, GRE (Generic Routing Encapsulation) o IPv6 sui tunnel IPv4) e i pacchetti ICMP potenzialmente limitati per i test di connettività, quali i messaggi echo-request o ICMP "unreachables" e "time to live" (TTL) scaduti per il traceroute.

Nota: tenere presente che l'ICMP è spesso utilizzato per semplici attacchi DoS (Denial-of-Service) e deve essere autorizzato solo da fonti esterne, se necessario.

Tutti gli RP hanno un massimo di prestazioni in cui operano. Il traffico eccessivo destinato all'RP può sovraccaricare il router. Ciò provoca un utilizzo elevato della CPU e in ultima analisi la perdita di pacchetti e protocolli di routing che causano una negazione del servizio. Filtrando l'accesso ai router dell'infrastruttura da fonti esterne, molti dei rischi esterni associati a un attacco diretto al router vengono ridotti. Gli attacchi provenienti dall'esterno non possono più accedere alle apparecchiature dell'infrastruttura. L'attacco viene fatto cadere sulle interfacce in entrata nel sistema autonomo (AS).

Le tecniche di filtraggio descritte in questo documento hanno lo scopo di filtrare i dati destinati alle apparecchiature dell'infrastruttura di rete. Non confondere il filtro dell'infrastruttura con il filtro generico. Lo scopo esclusivo dell'ACL di protezione dell'infrastruttura è quello di limitare a livello granulare i protocolli e le origini in grado di accedere alle apparecchiature dell'infrastruttura critica.

Le apparecchiature dell'infrastruttura di rete comprendono le seguenti aree:

- Tutti gli indirizzi di gestione di router e switch, incluse le interfacce di loopback
- Tutti gli indirizzi dei collegamenti interni: collegamenti router-to-router (accesso point-to-point e multiplo)
- Server o servizi interni a cui non è possibile accedere da origini esterne

In questo documento, tutto il traffico non destinato all'infrastruttura viene spesso definito traffico di transito.

Tecniche

La protezione dell'infrastruttura può essere ottenuta attraverso una varietà di tecniche:

- **Receive ACL (rACL)**Le piattaforme Cisco 12000 e 7500 supportano gli ACL che filtrano tutto il traffico destinato all'RP e non influiscono sul traffico di transito. Il traffico autorizzato deve essere autorizzato esplicitamente e l'rACL deve essere implementato su ogni router. Per ulteriori informazioni, fare riferimento al documento GSR: receive Access Control List.
- **ACL hop-by-hop sui router**Per proteggere i router, è possibile definire gli ACL che autorizzano solo il traffico autorizzato verso le interfacce del router, negando tutti gli altri accessi, ad eccezione del traffico di transito, che deve essere autorizzato esplicitamente. Questo ACL è simile da un punto di vista logico a un rACL, ma influisce sul traffico di transito e può quindi

avere un impatto negativo sulle prestazioni sulla velocità di inoltro di un router.

- **Filtraggio dei edge tramite ACL di infrastruttura**È possibile applicare gli ACL al bordo della rete. Nel caso di un provider di servizi (SP), questo è il margine del SA. Questo ACL filtra esplicitamente il traffico destinato allo spazio di indirizzi dell'infrastruttura. L'implementazione di ACL di infrastrutture perimetrali richiede una chiara definizione dello spazio dell'infrastruttura e dei protocolli richiesti/autorizzati che vi accedono. L'ACL viene applicato in ingresso alla rete su tutte le connessioni rivolte verso l'esterno, come le connessioni peer, le connessioni dei clienti e così via.In questo documento viene descritto lo sviluppo e l'implementazione di ACL di protezione delle infrastrutture perimetrali.

Esempi di ACL

Questi elenchi degli accessi IPv4 e IPv6 forniscono esempi semplici ma realistici delle voci tipiche richieste in un ACL di protezione. Questi ACL di base devono essere personalizzati con dettagli di configurazione specifici del sito locale. In ambienti IPv4 e IPv6 doppi, vengono implementati entrambi gli elenchi degli accessi.

Esempio di 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
```

Esempio di IPv6

L'elenco degli accessi IPv6 deve essere applicato come elenco degli accessi esteso con nome.

```
!--- 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
```

Nota: La parola chiave **log** può essere utilizzata per fornire ulteriori dettagli sull'origine e le destinazioni di un determinato protocollo. Sebbene questa parola chiave fornisca informazioni preziose sui dettagli degli accessi agli ACL, un numero eccessivo di accessi a una voce ACL che usa la parola chiave **log** aumenta l'utilizzo della CPU. L'impatto sulle prestazioni associato alla registrazione varia in base alla piattaforma. Inoltre, l'uso della parola chiave log disabilita la commutazione Cisco Express Forwarding (CEF) per i pacchetti che corrispondono all'istruzione access-list. Questi pacchetti sono invece commutati rapidamente.

Sviluppo di un ACL di protezione

In generale, un ACL di infrastruttura è composto da quattro sezioni:

- Immissione di indirizzi speciali e di voci anti-spoofing che impediscono a fonti e pacchetti non autorizzati con indirizzi di origine appartenenti al SA di immettere il SA da un'origine esterna**Nota: la** RFC 330 definisce gli indirizzi IPv4 per usi speciali che potrebbero richiedere l'applicazione di filtri. La RFC 1918 definisce lo spazio degli indirizzi riservato IPv4 che non è un indirizzo di origine valido su Internet. La RFC 3513 definisce l'architettura di indirizzamento IPv6. RFC 2827 fornisce le linee guida per il filtro degli ingressi.
- Traffico autorizzato esplicitamente da fonti esterne destinato a indirizzi di infrastruttura
- istruzioni **deny** per tutto il traffico di origine esterna diretto agli indirizzi dell'infrastruttura
- **autorizzare** le istruzioni per tutto il resto del traffico della backbone normale in viaggio verso destinazioni non legate all'infrastruttura

L'ultima riga dell'ACL dell'infrastruttura autorizza esplicitamente il traffico di transito: **consentire ip any any** per IPv4 e **permettere ipv6 any any** per IPv6. Questa voce garantisce che tutti i protocolli IP siano consentiti attraverso il core e che i clienti possano continuare a eseguire applicazioni senza problemi.

Il primo passo nello sviluppo di un ACL di protezione dell'infrastruttura è comprendere i protocolli richiesti. Sebbene ogni sito abbia requisiti specifici, alcuni protocolli vengono comunemente implementati e devono essere compresi. Ad esempio, i BGP esterni ai peer esterni devono essere esplicitamente autorizzati. Anche gli altri protocolli che richiedono un accesso diretto al router dell'infrastruttura devono essere autorizzati esplicitamente. Ad esempio, se si termina un tunnel GRE su un router dell'infrastruttura principale, anche il protocollo 47 (GRE) deve essere autorizzato esplicitamente. Analogamente, se si termina un tunnel IPv6 su IPv4 su un router dell'infrastruttura di base, anche il protocollo 41 (IPv6 su IPv4) deve essere esplicitamente autorizzato.

Èpossibile utilizzare un ACL di classificazione per identificare i protocolli richiesti. L'ACL di classificazione è composto dalle istruzioni di **autorizzazione** per i vari protocolli che possono essere destinati a un router di infrastruttura. Per un elenco completo, fare riferimento all'appendice sui protocolli IP supportati nel software Cisco IOS®. L'uso del comando **show access-list** per visualizzare il numero di accessi riusciti alla voce di controllo di accesso (ACE) identifica i protocolli obbligatori. Prima di creare dichiarazioni di **autorizzazione per** protocolli inattesi, è necessario indagare sui risultati sospetti o sorprendenti e comprenderli.

Ad esempio, questo ACL IPv4 aiuta a determinare se è necessario autorizzare il tunneling GRE, IPsec (ESP) e IPv6 (IP Protocol 41).

```
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
```

Questo ACL IPv6 può essere utilizzato per determinare se è necessario autorizzare GRE e IPsec (ESP).

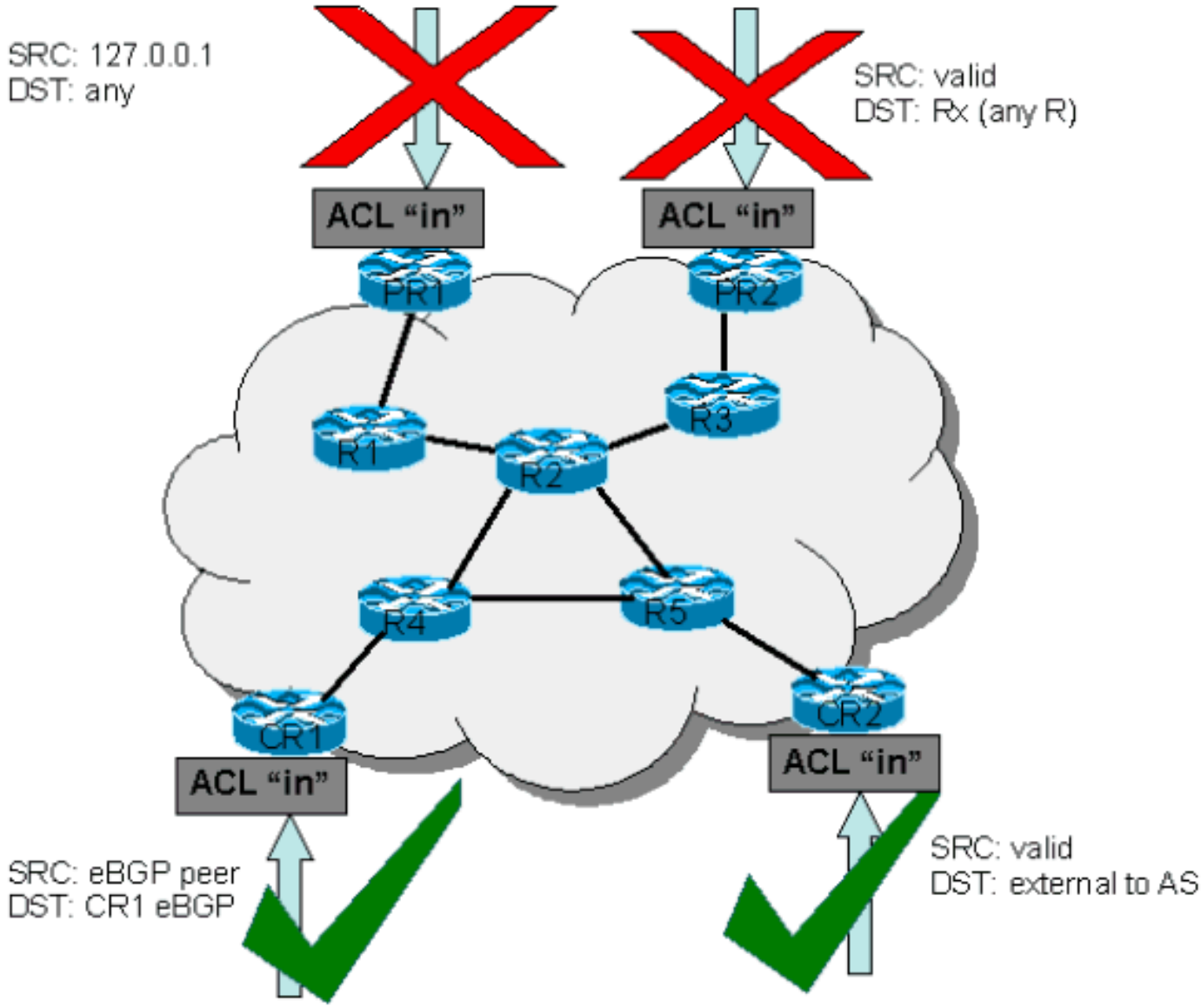
```
ipv6 access-list determine_protocols
 permit GRE any infrastructure_ips_ipv6
 permit ESP any infrastructure_ips_ipv6
 permit ipv6 any infrastructure_ips_ipv6 log
!--- The log keyword provides more details !--- about other protocols that are not explicitly
permitted. permit ipv6 any any interface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

Oltre ai protocolli richiesti, è necessario identificare lo spazio di indirizzamento dell'infrastruttura, poiché è lo spazio che l'ACL protegge. Lo spazio di indirizzi dell'infrastruttura include qualsiasi indirizzo utilizzato per la rete interna e a cui si accede raramente da origini esterne, ad esempio interfacce di router, indirizzamento di collegamenti point-to-point e servizi di infrastruttura critici. Poiché questi indirizzi vengono utilizzati per la parte di destinazione dell'ACL dell'infrastruttura, la generazione del riepilogo è un'operazione critica. Ove possibile, questi indirizzi devono essere raggruppati in blocchi CIDR (Classless Interdomain Routing).

Utilizzando i protocolli e gli indirizzi identificati, è possibile creare l'ACL dell'infrastruttura per autorizzare i protocolli e proteggere gli indirizzi. Oltre alla protezione diretta, l'ACL fornisce anche una prima linea di difesa contro alcuni tipi di traffico non valido su Internet.

- Lo spazio RFC 1918 deve essere rifiutato.
- I pacchetti con un indirizzo di origine che rientra nello spazio degli indirizzi per uso speciale, come definito nella RFC 3330, devono essere rifiutati.
- È necessario applicare filtri antispam. (il tuo spazio di indirizzi non deve mai essere l'origine dei pacchetti provenienti dall'esterno dell'appliance ASA).

Questo ACL appena costruito deve essere applicato in entrata su tutte le interfacce in entrata. Per ulteriori informazioni, vedere le sezioni relative alle linee guida e agli esempi di distribuzione.



ACL e pacchetti frammentati

Gli ACL usano la parola chiave **fragments** per attivare una gestione specializzata dei pacchetti frammentati. Senza questa parola chiave **fragments**, i frammenti non iniziali che corrispondono alle istruzioni di layer 3 (indipendentemente dalle informazioni di layer 4) in un ACL sono interessati dall'istruzione allow o deny della voce corrispondente. Tuttavia, aggiungendo la parola chiave **fragments**, è possibile forzare gli ACL a rifiutare o consentire i frammenti non iniziali con una maggiore granularità. Questo comportamento è lo stesso per gli elenchi di accesso IPv4 e IPv6, con l'eccezione che, mentre gli ACL IPv4 consentono l'uso della parola chiave fragments nelle istruzioni di livello 3 e 4, gli ACL IPv6 consentono l'uso della parola chiave fragments solo nelle istruzioni di livello 3.

Il filtro dei frammenti aggiunge un ulteriore livello di protezione contro un attacco Denial of Service (DoS) che utilizza frammenti non iniziali (ossia FO > 0). L'uso dell'istruzione **deny** sui frammenti non iniziali all'inizio dell'ACL impedisce a tutti i frammenti non iniziali di accedere al router. In rari casi, una sessione valida può richiedere la frammentazione e quindi essere filtrata se nell'ACL esiste un'istruzione **deny fragment**.

Ad esempio, considerare questo ACL IPv4sec parziale:

```
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'aggiunta di queste voci all'inizio di un ACL impedisce a qualsiasi frammento non iniziale di accedere ai router principali, mentre i pacchetti non frammentati o i frammenti iniziali passano alle righe successive dell'ACL senza essere influenzati dalle istruzioni **deny fragment**. Il precedente comando ACL semplifica anche la classificazione dell'attacco, in quanto ciascun protocollo (UDP, Universal Datagram Protocol), TCP e ICMP incrementa i contatori separati nell'ACL.

Questo è un esempio paragonabile per IPv6:

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

L'aggiunta di questa voce all'inizio di un ACL IPv6 impedisce a qualsiasi frammento non iniziale di accedere ai router principali. Come indicato in precedenza, gli elenchi degli accessi IPv6 consentono solo l'utilizzo della parola chiave fragments nelle istruzioni di layer 3.

Poiché molti attacchi si basano sull'invio di pacchetti frammentati ai router principali, filtrare i frammenti in arrivo nell'infrastruttura principale offre un'ulteriore misura di protezione e aiuta a garantire che un attacco non possa inviare frammenti semplicemente rispettando le regole di layer 3 nell'ACL dell'infrastruttura.

Per una descrizione dettagliata delle opzioni, consultare il documento Access Control Lists and IP Fragments.

Valutazione dei rischi

Quando si implementano gli ACL di protezione dell'infrastruttura, prendere in considerazione le due aree di rischio chiave seguenti:

- Accertarsi che siano presenti le opportune dichiarazioni di **autorizzazione/rifiuto**. Affinché l'ACL sia effettivo, tutti i protocolli richiesti devono essere autorizzati e lo spazio di indirizzi corretto deve essere protetto dalle istruzioni **deny**.
- Le prestazioni degli ACL variano a seconda della piattaforma in uso. Esaminare le caratteristiche delle prestazioni dell'hardware prima di distribuire gli ACL.

Come sempre, si consiglia di testare questo progetto in laboratorio prima della distribuzione.

Appendici

Protocolli IP supportati nel software Cisco IOS

Questi protocolli IP sono supportati dal software Cisco IOS:

- 1 - ICMP
- 2 - IGMP

- 3 - GGP
- 4 - Incapsulamento IP in IP
- 6 - TCP
- 8 - EGP
- 9 - IGRP
- 17 - UDP
- 20 - HMP
- 27 - RDP
- 41 - IPv6 nel tunneling IPv4
- 46 - RSVP
- 47 - GRE
- 50 - ESP
- 51 - AH
- 53 - SCORRIMENTO RAPIDO
- 54 - NARP
- 55 - Mobilità IP
- 63 - qualsiasi rete locale
- 77 - Sun ND
- 80 - IOS IP
- 88 - EIGRP
- 89 - OSPF
- 90 - RPC sprite
- 91 - LARP
- 94 - Compatibile con KA9Q/NOS IP over IP
- 103 - PIM
- 108 - Compressione IP
- 112 - VRRP
- 113 - PGM
- 115 - L2TP
- 120 - UTI
- 132 - SCTP

Linee guida per la distribuzione

Cisco consiglia pratiche di installazione conservative. Per implementare correttamente gli ACL dell'infrastruttura, i protocolli richiesti devono essere ben compresi e lo spazio di indirizzi deve essere chiaramente identificato e definito. Le seguenti linee guida descrivono un metodo molto conservativo per implementare gli ACL di protezione con un approccio iterativo.

1. **Identificare i protocolli usati nella rete con un ACL di classificazione.**Implementare un ACL che autorizzi tutti i protocolli noti che accedono ai dispositivi dell'infrastruttura. Questo ACL di rilevamento ha un indirizzo di origine **qualsiasi** e una destinazione che include lo spazio IP dell'infrastruttura. La registrazione può essere utilizzata per sviluppare un elenco di indirizzi di origine che corrispondono alle istruzioni **allow** del protocollo. Per autorizzare il flusso del traffico, è necessaria un'ultima riga che autorizzi **ip any** (IPv4) o **ipv6 any** (IPv6).L'obiettivo è determinare i protocolli utilizzati dalla rete specifica. La registrazione viene usata per l'analisi per determinare quali altri elementi potrebbero comunicare con il router.**Nota:** anche se la parola chiave **log** offre informazioni utili sui dettagli degli accessi ACL, un numero eccessivo

di accessi a una voce ACL che usa questa parola chiave potrebbe causare un numero eccessivo di voci log e un possibile elevato utilizzo della CPU del router. Inoltre, l'uso della parola chiave **log** disabilita la commutazione Cisco Express Forwarding (CEF) per i pacchetti che corrispondono all'istruzione access-list. Questi pacchetti sono invece commutati rapidamente. Usare la parola chiave **log** per brevi periodi di tempo e solo quando è necessario per classificare il traffico.

2. **Esaminare i pacchetti identificati e iniziare a filtrare l'accesso al processore di routing RP.**Dopo aver identificato e revisionato i pacchetti filtrati dall'ACL nel passaggio 1, implementare un ACL con il **permesso di** inviare **qualsiasi origine** agli indirizzi dell'infrastruttura per i protocolli consentiti. Come al passaggio 1, la parola chiave **log** può fornire ulteriori informazioni sui pacchetti che corrispondono alle voci dell'**autorizzazione**. L'uso del comando **deny any** alla fine può aiutare a identificare eventuali pacchetti imprevisti destinati ai router. L'ultima riga di questo ACL deve essere un'istruzione **allow ip any** (IPv4) o **allow ipv6 any** (IPv6) per consentire il flusso del traffico di transito. Questo ACL fornisce la protezione di base e consente ai tecnici di rete di verificare che tutto il traffico richiesto sia autorizzato.
3. **Limitare gli indirizzi di origine.**Dopo aver compreso chiaramente i protocolli che devono essere autorizzati, è possibile eseguire ulteriori operazioni di filtro per consentire solo le origini autorizzate per tali protocolli. Ad esempio, è possibile consentire in modo esplicito i vicini BGP esterni o indirizzi peer GRE specifici.Questa procedura riduce il rischio senza interrompere i servizi e consente di applicare un controllo granulare alle origini che accedono ai dispositivi dell'infrastruttura.
4. **Limitare gli indirizzi di destinazione nell'ACL (*facoltativo*).**Alcuni provider di servizi Internet (ISP) potrebbero scegliere di consentire solo a protocolli specifici di utilizzare indirizzi di destinazione specifici sul router. Questa fase finale consente di limitare l'intervallo di indirizzi di destinazione che possono accettare il traffico per un protocollo.

Esempi di distribuzione

Esempio di IPv4

Nell'esempio di IPv4, viene mostrato un ACL di infrastruttura che protegge un router in base a questo indirizzo:

- Il blocco di indirizzi dell'ISP è 169.223.0.0/16.
- Il blocco dell'infrastruttura dell'ISP è 169.223.252.0/22.
- Il loopback del router è 169.223.253.1/32.
- Il router è un router peer e un peer con 169.254.254.1 (indirizzo 169.223.252.1).

L'ACL di protezione dell'infrastruttura visualizzato viene sviluppato in base alle informazioni precedenti. L'ACL consente il peering BGP esterno sul peer esterno, fornisce filtri anti-spoof e protegge l'infrastruttura da tutti gli accessi esterni.

```
!
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
```

Esempio di IPv6

Nell'esempio di IPv6 viene mostrato un ACL di infrastruttura che protegge un router in base a questo indirizzo:

- Il blocco di prefissi complessivo allocato all'ISP è 2001:0DB8::/32.
- Il blocco di prefissi IPv6 utilizzato dall'ISP per gli indirizzi dell'infrastruttura di rete è 2001:0DB8:C18::/48.
- Esiste un router peer BGP con indirizzo IPv6 di origine 2001:0DB8:C18:2:1:1 che esegue il peer all'indirizzo IPv6 di destinazione 2001:0DB8:C19:2:1::F.

L'ACL di protezione dell'infrastruttura visualizzato viene sviluppato in base alle informazioni precedenti. L'ACL consente il peering BGP multiprotocollo esterno sul peer esterno, fornisce filtri anti-spoof e protegge l'infrastruttura da tutti gli accessi esterni.

```
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
```

Informazioni correlate

- Pagina di supporto sugli elenchi degli accessi
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems