GSR: Receive Access Control List

Sommario

Introduzione

In questo documento viene descritta una nuova funzionalità di sicurezza denominata receive Access Control List (rACL) [1] e vengono forniti suggerimenti e linee guida per le distribuzioni degli ACL. I receive ACL vengono usati per aumentare la sicurezza sui router Cisco 12000 proteggendo il Gigabit Route Processor (GRP) del router dal traffico non necessario o potenzialmente dannoso. I receive ACL sono stati aggiunti come funzionalità speciale nel software Cisco IOS ® versione 12.0.21S2 e sono stati integrati nel software Cisco IOS versione 12.0(22)S.

Protezione GRP

I dati ricevuti da un router di switching Gigabit (GSR) possono essere suddivisi in due categorie principali:

- Il traffico che attraversa il router tramite il percorso di inoltro.
- Il traffico che deve essere inviato al GRP tramite il percorso di ricezione per ulteriori analisi.

In condizioni operative normali, la maggior parte del traffico passa semplicemente attraverso una GSR in rotta verso altre destinazioni. Tuttavia, il GRP deve gestire alcuni tipi di dati, in particolare i protocolli di routing, l'accesso remoto ai router e il traffico di gestione di rete (ad esempio SNMP (Simple Network Management Protocol)). Oltre a questo traffico, altri pacchetti di layer 3 potrebbero richiedere la flessibilità di elaborazione del GRP. Queste includono alcune opzioni IP e alcune forme di pacchetti ICMP (Internet Control Message Protocol). Fare riferimento all'appendice sui pacchetti adiacenti di ricezione e puntati per ulteriori informazioni sugli ACL e sul traffico di ricezione sul GSR.

Un GSR ha diversi percorsi di dati, ognuno dei quali serve diverse forme di traffico. Il traffico di transito viene inoltrato dalla scheda di linea in entrata (LC) alla struttura e quindi alla scheda in uscita per la consegna nell'hop successivo. Oltre al percorso dei dati sul traffico di transito, un GSR dispone di altri due percorsi per il traffico che richiede l'elaborazione locale: CPU da LC a LC e da LC a LC da CPU a fabric a GRP. Nella tabella seguente vengono illustrati i percorsi per diverse funzionalità e protocolli di uso comune.

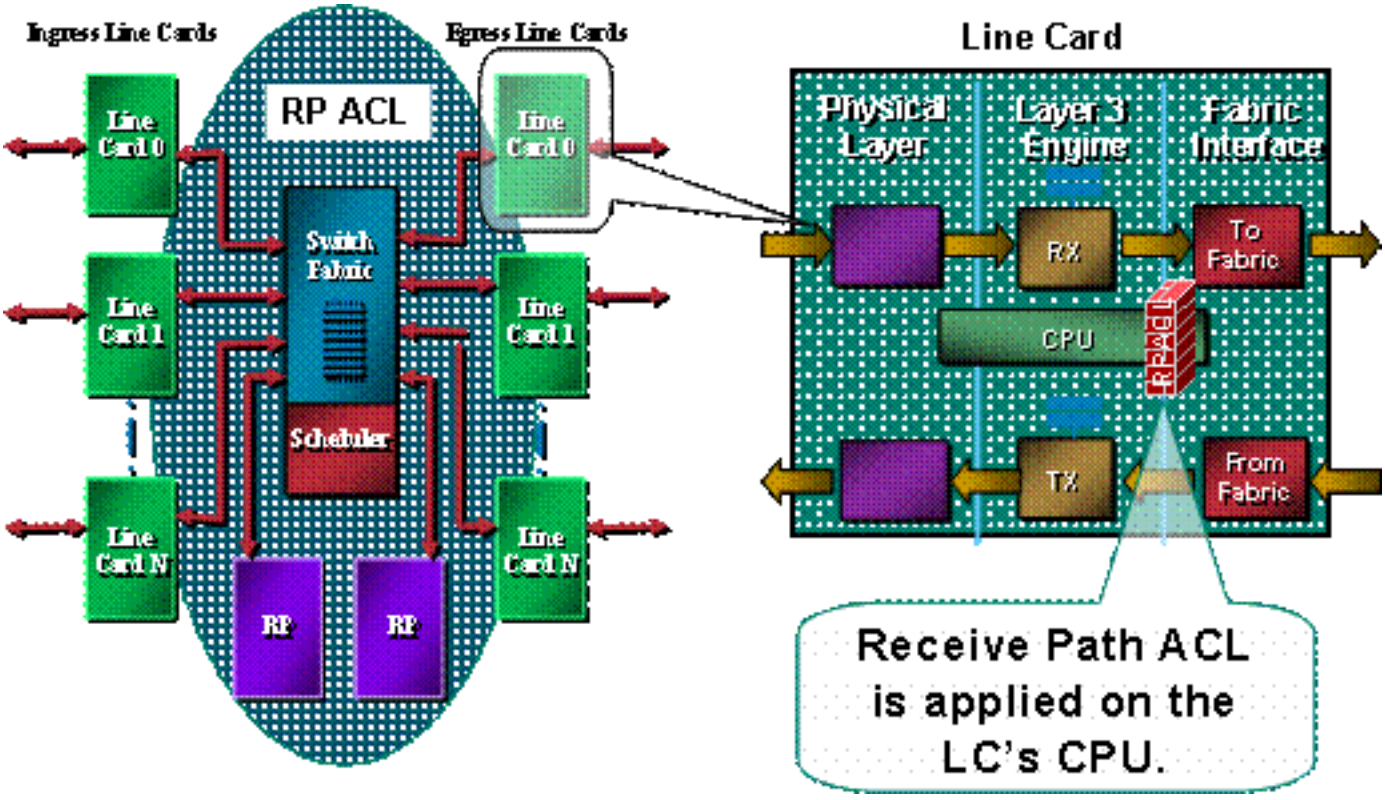
Tipo di traffico	Percorso dati
Traffico normale (in transito)	Da LC a fabric a LC
Protocolli di routing/SSH/SNMP	Da LC a LC da CPU a fabric a GRP
Eco ICMP (ping)	CPU da LC a LC
Registrazione	

Il processore di routing per il GSR ha una capacità limitata di elaborare il traffico proveniente dai LC destinati al GRP stesso. Se un volume elevato di dati richiede punzonatura al GRP, tale traffico può sovraccaricare il GRP. Ciò determina un attacco Denial-of-Service (DoS) efficace. La CPU del GRP fatica a stare al passo con l'esame dei pacchetti e inizia a scartare i pacchetti, inondando le code di attesa dell'input e di rifiuto selettivo del pacchetto (SPD). [2] È necessario proteggere i GSR da tre scenari, che possono derivare da attacchi DoS diretti a un GRP del router.

- Perdita di pacchetti del protocollo di routing da un flusso con priorità normale
- Perdita di pacchetti in una sessione di gestione (Telnet, Secure Shell [SSH], SNMP) da un flusso con priorità normale
- Perdita di pacchetti da un'inondazione ad alta priorità oggetto di spoofing

La potenziale perdita di dati del protocollo di routing durante un'inondazione a priorità normale è attualmente mitigata dalla classificazione statica e dalla limitazione della velocità del traffico destinato al GRP proveniente dai LC. Sfortunatamente, questo approccio ha dei limiti. La limitazione della velocità per il traffico a priorità normale destinato al GRP non è sufficiente a garantire la protezione dei dati del protocollo di routing ad alta priorità se un attacco viene consegnato tramite più LC. Abbassare la soglia alla quale i dati con priorità normale vengono eliminati per fornire tale protezione non fa che esacerbare la perdita di traffico di gestione da un'inondazione con priorità normale.

Come mostra questa immagine, l'rACL viene eseguito su ciascun LC prima che il pacchetto venga trasmesso al GRP.



Ènecessario un meccanismo di protezione per il GRP. Gli rACL influiscono sul traffico inviato al GRP a causa delle adiacenze di ricezione. Le adiacenze di ricezione sono adiacenze di inoltro Cisco Express per il traffico destinato agli indirizzi IP del router, ad esempio l'indirizzo o gli indirizzi di broadcast configurati sulle interfacce del router. [3] Vedere la sezione dell'appendice per ulteriori dettagli sulle adiacenze di ricezione e sui pacchetti perforati.

Il traffico che entra in una LC viene prima inviato alla CPU locale della LC, e i pacchetti che devono essere elaborati dal GRP vengono accodati per l'inoltro al processore di routing. L'ACL di ricezione viene creato sul GRP e quindi compresso sulle CPU dei vari LC. Prima di inviare il traffico dalla CPU LC al GRP, il traffico viene confrontato con l'rACL. Se autorizzato, il traffico passa al GRP, mentre tutto il resto del traffico viene rifiutato. L'rACL viene ispezionato prima della funzione di limitazione della velocità da LC a GRP. Poiché l'rACL viene usato per tutte le adiacenze di ricezione, alcuni pacchetti gestiti dalla CPU LC (come le richieste echo) sono soggetti anche al filtro rACL. Di questo bisogna tenere conto quando si progettano le voci degli elenchi degli accessi.

I receive ACL fanno parte di un intervallo di meccanismi a più parti che proteggono le risorse di un router. I lavori futuri includeranno una componente di limitazione della velocità nell'ACL.

Impatto sulle prestazioni

Non viene utilizzata memoria diversa da quella necessaria per contenere la singola voce di configurazione e lo stesso elenco degli accessi definito. L'rACL viene copiato su ciascun LC, quindi su ciascun LC viene acquisita una piccola area di memoria. Nel complesso, le risorse utilizzate sono minime, soprattutto se confrontate con i vantaggi dell'installazione.

Un ACL di ricezione non influisce sulle prestazioni del traffico inoltrato. L'rACL si applica solo al traffico adiacente alla ricezione. Il traffico inoltrato non è mai soggetto all'ACL. Il traffico di transito viene filtrato usando gli ACL di interfaccia. Questi ACL "normali" vengono applicati alle interfacce in una direzione specificata. Il traffico è soggetto all'elaborazione di ACL prima dell'elaborazione di rACL, quindi il traffico negato dall'ACL di interfaccia non verrà ricevuto dall'rACL. [4]

La scheda LC che esegue il filtro effettivo (in altre parole, la scheda LC che riceve il traffico filtrato dall'rACL) avrà un maggiore utilizzo della CPU a causa dell'elaborazione dell'rACL. Questo maggiore utilizzo della CPU, tuttavia, è causato da un elevato volume di traffico destinato al GRP; il vantaggio del GRP della protezione degli ACL supera di gran lunga l'aumento dell'utilizzo della CPU su un LC. L'utilizzo della CPU su un LC varia in base al tipo di motore LC. Ad esempio, dato lo stesso attacco, un LC del motore 3 avrà un utilizzo della CPU inferiore rispetto a un LC del motore 0.

L'abilitazione degli ACL turbo (con il comando **access-list compiled**) converte gli ACL in una serie di voci della tabella di ricerca molto efficiente. Quando gli ACL turbo sono abilitati, la profondità degli ACL turbo non influisce sulle prestazioni. In altre parole, la velocità di elaborazione è indipendente dal numero di voci nell'ACL. Se l'rACL è corto, gli ACL turbo non aumenteranno significativamente le prestazioni ma consumeranno memoria; con ACL brevi, è probabile che gli ACL compilati non siano necessari.

Proteggendo il GRP, l'rACL aiuta a garantire la stabilità del router e, in ultima analisi, della rete durante un attacco. Come descritto sopra, l'rACL viene elaborato sulla CPU del controller LC, in modo che l'utilizzo della CPU su ciascun controller LC aumenti quando un grande volume di dati viene indirizzato al router. Su E0/E1 e su alcuni bundle E2, un utilizzo della CPU pari a oltre il 100% potrebbe causare la perdita del protocollo di routing e del livello di collegamento. Queste gocce vengono localizzate nella scheda e i processi di routing GRP sono protetti, mantenendo così la stabilità. Le schede E2 con microcodice [5] abilitato alla limitazione attivano la modalità di limitazione quando sono sottoposte a un carico elevato e inoltrano solo il traffico con precedenza 6 e 7 al protocollo di routing. Altri tipi di motori hanno architetture a più code; ad esempio, le schede E3 hanno tre code alla CPU, con pacchetti del protocollo di routing (precedenza 6/7) in una coda separata ad alta priorità. Una CPU LC elevata, a meno che non sia causata da pacchetti con precedenza elevata, non causerà interruzioni del protocollo di routing. I pacchetti alle code con priorità inferiore verranno scartati. Infine, le schede basate su E4 hanno otto code alla CPU, una dedicata al routing dei pacchetti del protocollo.

Sintassi

Un ACL di ricezione viene applicato con il seguente comando di configurazione globale per distribuire l'ACL di ricezione a ciascun LC del router.

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

In questa sintassi, *<num>* viene definito come segue.

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

Esempi di modello e ACL di base

Per poter utilizzare questo comando, è necessario definire un elenco degli accessi che identifichi il traffico che deve essere autorizzato a comunicare con il router. L'elenco degli accessi deve includere sia i protocolli di routing che il traffico di gestione (Border Gateway Protocol [BGP], Open Shortest Path First [OSPF], SNMP, SSH, Telnet). Fare riferimento alla sezione sulle linee guida per la distribuzione per ulteriori dettagli.

L'ACL di esempio che segue fornisce una struttura semplice e presenta alcuni esempi di configurazione che possono essere adattati per utilizzi specifici. L'ACL mostra le configurazioni richieste per diversi servizi/protocolli comunemente richiesti. Per SSH, Telnet e SNMP, viene usato un indirizzo di loopback come destinazione. Per i protocolli di routing, viene utilizzato l'indirizzo di interfaccia effettivo. La scelta delle interfacce del router da usare nell'elenco di controllo di accesso è determinata dai criteri e dalle operazioni del sito locale. Ad esempio, se i loopback vengono utilizzati per tutte le sessioni di peering BGP, nelle istruzioni **allow** per BGP devono essere consentiti solo tali loopback.

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

Come per tutti gli ACL Cisco, alla fine dell'elenco degli accessi è presente un'istruzione implicita di **rifiuto**, quindi tutto il traffico che non corrisponde a una voce dell'elenco verrà rifiutato.

Nota: la parola chiave **log** può essere utilizzata per classificare il traffico destinato al GRP non autorizzato. Anche se la parola chiave **log** offre utili informazioni sui dettagli degli accessi agli ACL, un numero eccessivo di accessi a una voce ACL che usa questa parola chiave aumenterà l'utilizzo della CPU degli LC. L'impatto sulle prestazioni associato alla registrazione varia a seconda del tipo di motore LC. In generale, la registrazione deve essere utilizzata solo quando necessario sui motori 0/1/2. Per i motori 3/4/4+, la registrazione produce un impatto molto minore a causa delle prestazioni migliorate della CPU e dell'architettura a più code.

Il livello di granularità dell'elenco degli accessi è determinato dai criteri di sicurezza locali, ad esempio il livello di filtro richiesto per i router adiacenti OSPF.

ACL e pacchetti frammentati

Gli ACL usano la parola chiave **fragments** per attivare una gestione specializzata dei pacchetti frammentati. In generale, i frammenti non iniziali che corrispondono alle istruzioni L3 (indipendentemente dalle informazioni L4) in un ACL sono influenzati dall'istruzione **allow** o **deny** della voce corrispondente. L'uso della parola chiave **fragments** può forzare gli ACL a negare o consentire i frammenti non iniziali con una maggiore granularità.

Nel contesto rACL, filtrando i frammenti si aggiunge un ulteriore livello di protezione da un attacco DoS che usa solo frammenti non iniziali (ad esempio FO > 0). L'uso di un'istruzione **deny** per i frammenti non iniziali all'inizio dell'rACL impedisce a tutti i frammenti non iniziali di accedere al router. In rari casi, una sessione valida potrebbe richiedere la frammentazione e quindi essere

filtrata se nell'elenco dei contatti è presente un'istruzione **deny fragment**.

Ad esempio, considerare l'ACL parziale mostrato di seguito.

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

L'aggiunta di queste voci all'inizio di un ACL nega l'accesso al GRP ai frammenti non iniziali, mentre i pacchetti non frammentati o i frammenti iniziali passano alle righe successive dell'ACL senza essere influenzati dalle istruzioni **deny fragment**. Lo snippet di codice ACL sopra riportato semplifica anche la classificazione dell'attacco, in quanto ogni protocollo (UDP, Universal Datagram Protocol), TCP e ICMP incrementa i contatori separati nell'ACL.

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

Valutazione dei rischi

Verificare che l'elenco di controllo di accesso non filtri il traffico critico, ad esempio i protocolli di routing, o l'accesso interattivo ai router. Il filtraggio del traffico necessario potrebbe impedire l'accesso remoto al router e richiedere quindi una connessione alla console. Per questo motivo, le configurazioni lab devono simulare il più possibile l'installazione effettiva.

Come sempre, Cisco consiglia di testare questa funzione nel laboratorio prima dell'implementazione.

Appendici e note

Adiacenti di ricezione e pacchetti perforati

Come descritto in precedenza in questo documento, alcuni pacchetti richiedono l'elaborazione GRP. I pacchetti vengono trasmessi dal piano di inoltro dati al GRP. Elenco delle forme comuni di dati di livello 3 che richiedono l'accesso GRP.

- Protocolli di routing
- Traffico di controllo multicast (OSPF, Hot Standby Router Protocol [HSRP], Tag Distribution Protocol [TDP], Protocol Independent Multicast [PIM] e così via)
- Pacchetti Multiprotocol Label Switching (MPLS) da frammentare
- Pacchetti con determinate opzioni IP, ad esempio l'avviso del router
- Primo pacchetto di flussi multicast
- Pacchetti ICMP frammentati che devono essere riassemblati
- Tutto il traffico destinato al router stesso (ad eccezione del traffico gestito sul CLI)

Poiché gli rACL si applicano alle adiacenze di ricezione, l'rACL filtra parte del traffico che non è indirizzato al GRP ma è adiacente alla ricezione. L'esempio più comune è una richiesta echo ICMP (ping). Le richieste echo ICMP dirette al router vengono gestite dalla CPU LC; poiché le richieste sono adiacenti, vengono filtrate anche dall'rACL. Pertanto, per consentire i ping alle interfacce (o loopback) del router, l'rACL deve consentire esplicitamente le richieste echo.

Le adiacenze di ricezione possono essere visualizzate con il comando **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
...
```

Linee guida per la distribuzione

Cisco consiglia pratiche di installazione conservative. Per distribuire correttamente gli rACL, è necessario comprendere bene i requisiti di accesso al control plane e al management plane esistenti. In alcune reti potrebbe essere difficile determinare il profilo di traffico esatto necessario per creare gli elenchi di filtro. Le seguenti linee guida descrivono un approccio molto conservativo per la distribuzione degli rACL con configurazioni iterative degli rACL, al fine di identificare ed eventualmente filtrare il traffico.

1. **Identificare i protocolli usati nella rete con un ACL di classificazione.**Distribuire un rACL che consenta tutti i protocolli noti che accedono al GRP. Per questo ACL di "individuazione", gli indirizzi di origine e di destinazione devono essere entrambi impostati su **any (qualsiasi)**. La registrazione può essere utilizzata per sviluppare un elenco di indirizzi di origine che corrispondono alle istruzioni **allow** del protocollo. Oltre all'istruzione protocol **allow**, è **possibile autorizzare qualsiasi** riga di **registro** alla fine dell'elenco degli accessi, in modo da identificare altri protocolli che verrebbero filtrati dall'elenco degli accessi e che potrebbero richiedere l'accesso al GRP.L'obiettivo è determinare i protocolli utilizzati dalla rete specifica. La registrazione deve essere usata per l'analisi per determinare "cos'altro" potrebbe 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. 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 GRP.**Dopo aver identificato e esaminato i pacchetti filtrati dall'rACL nel passaggio 1, implementare un rACL con un'**autorizzazione o un'**istruzione 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 di **deny any log** al termine può aiutare a identificare eventuali pacchetti imprevisti destinati al GRP. Questo ACL fornisce una protezione di base e consente ai tecnici di rete di assicurare che tutto il traffico richiesto sia autorizzato.L'obiettivo è quello di testare l'intervallo di protocolli che devono comunicare con il router senza avere l'intervallo esplicito di indirizzi di origine e di destinazione IP.
3. **Limitare un intervallo macro di indirizzi di origine.**Consentire solo l'intero intervallo del blocco CIDR (Classless Interdomain Routing) allocato come indirizzo di origine. Ad esempio, se è stato allocato 171.68.0.0/16 per la rete, consentire gli indirizzi di origine solo da 171.68.0.0/16.Questa procedura consente di limitare i rischi senza interrompere i servizi. Fornisce inoltre punti dati di dispositivi/persone esterni al blocco CIDR che potrebbero accedere alle apparecchiature. Tutti gli indirizzi esterni verranno eliminati.I peer BGP esterni richiedono un'eccezione, poiché gli indirizzi di origine consentiti per la sessione si trovano all'esterno del blocco CIDR.Questa fase può essere lasciata attiva per alcuni giorni per

raccogliere i dati per la fase successiva di restringimento dell'elenco.

4. **Limitare le istruzioni allow dell'ACL in modo da consentire solo indirizzi di origine autorizzati noti.**Limitare sempre più l'indirizzo di origine per consentire solo le origini che comunicano con il GRP.
5. **Limitare gli indirizzi di destinazione nell'ACL (*facoltativo*).**Alcuni provider di servizi Internet (ISP) possono 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 accetteranno il traffico per un protocollo. [6]

Esempio di distribuzione

L'esempio seguente mostra un ACL di ricezione che protegge un router in base all'indirizzo seguente.

- Il blocco di indirizzi dell'ISP è 169.223.0.0/16.
- Il blocco infrastruttura dell'ISP è 169.223.252.0/22.
- Il loopback del router è 169.223.253.1/32.
- Il router è un router backbone principale, quindi sono attive solo le sessioni BGP interne.

Date queste informazioni, l'ACL di ricezione iniziale potrebbe essere simile all'esempio seguente. Poiché conosciamo il blocco degli indirizzi delle infrastrutture, in un primo momento lo permetteremo. Successivamente, verranno aggiunte voci di controllo di accesso (ACE) più dettagliate man mano che gli indirizzi specifici vengono ottenuti per tutti i dispositivi che devono accedere al router.

```
!
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
```

Note

1. Per aumentare la resistenza DoS, fare riferimento a Descrizione della SPD (Selective Packet Discard) e alle linee guida della coda di attesa.
2. Per ulteriori informazioni su Cisco Express Forwarding e le adiacenze, fare riferimento alla panoramica di Cisco Express Forwarding.
3. Per una descrizione dettagliata delle linee guida sulla distribuzione degli ACL e dei comandi correlati, consultare il documento sull'implementazione degli ACL sui router Internet Cisco serie 12000.
4. Questo si riferisce ai bundle Vanilla, Border Gateway Protocol Policy Accounting (BGPPA), Per Interface Rate Control (PIRC) e Frame Relay Traffic Policing (FRTP).
5. La fase II della protezione del percorso di ricezione consentirà la creazione di un'interfaccia di gestione, limitando automaticamente l'indirizzo IP che ascolterà i pacchetti in arrivo.

Informazioni correlate

- Pagina di supporto sugli elenchi degli accessi
- Supporto tecnico – Cisco Systems