SR: Ontvang toegangscontrolelijsten

Inhoud

Inleiding

Dit document beschrijft een nieuwe beveiligingsfunctie die toegangscontrolelijsten (rACL's)[1] wordt genoemd [en] bevat aanbevelingen en richtlijnen voor ACL-implementaties. Ontvang ACL's (ACL's) worden gebruikt om de beveiliging van Cisco 12000 routers te verhogen door de Gigabit-routeprocessor (GRP) van de router te beschermen tegen onnodig en mogelijk schadelijk verkeer. Ontvang ACL's (ACL's) als speciale ontheffing aan de onderhoudsbehandeling voor Cisco IOS ® softwarerelease 12.0.21S2 en geïntegreerd in Cisco IOS-softwarerelease 12.0(22)S.

GRP-bescherming

De gegevens die door een Gigabit switch router (GSR) worden ontvangen kunnen in twee brede categorieën worden verdeeld:

- Verkeer dat door de router via het verzendingspad gaat.
- Verkeer dat via het ontvangstpad naar de GRP wordt verzonden voor verdere analyse.

Bij normale exploitatie stroomt het overgrote deel van het verkeer gewoon door een SR op de route naar andere bestemmingen. Niettemin moet het GRP bepaalde typen gegevens verwerken, met name routingprotocollen, toegang tot externe router en netwerkbeheerverkeer (zoals Simple Network Management Protocol [SNMP]). Naast dit verkeer kunnen andere Layer 3-pakketten ook de verwerkingsflexibiliteit van de GRP vereisen. Hieronder vallen bepaalde IP-opties en bepaalde vormen van ICMP-pakketten (Internet Control Message Protocol). Raadpleeg het appendix bij ontvang nabijheid en gepunte pakketten voor extra details betreffende rACL's en ontvang padverkeer op de GSR.

Een GSR heeft meerdere gegevenspaden, die elk verschillende vormen van verkeer onderhouden. Het transitoverkeer gaat van de ingangslijnkaart (LC) naar de stof en daarna naar de perskaart voor de volgende hoplevering. Naast het transitovervoer datapad heeft een GSR twee andere paden voor verkeer die lokale verwerking vereisen: LC naar LC CPU en LC naar LC CPU naar fabric naar GRP. De volgende tabel toont de paden voor meerdere veelgebruikte functies en protocollen.

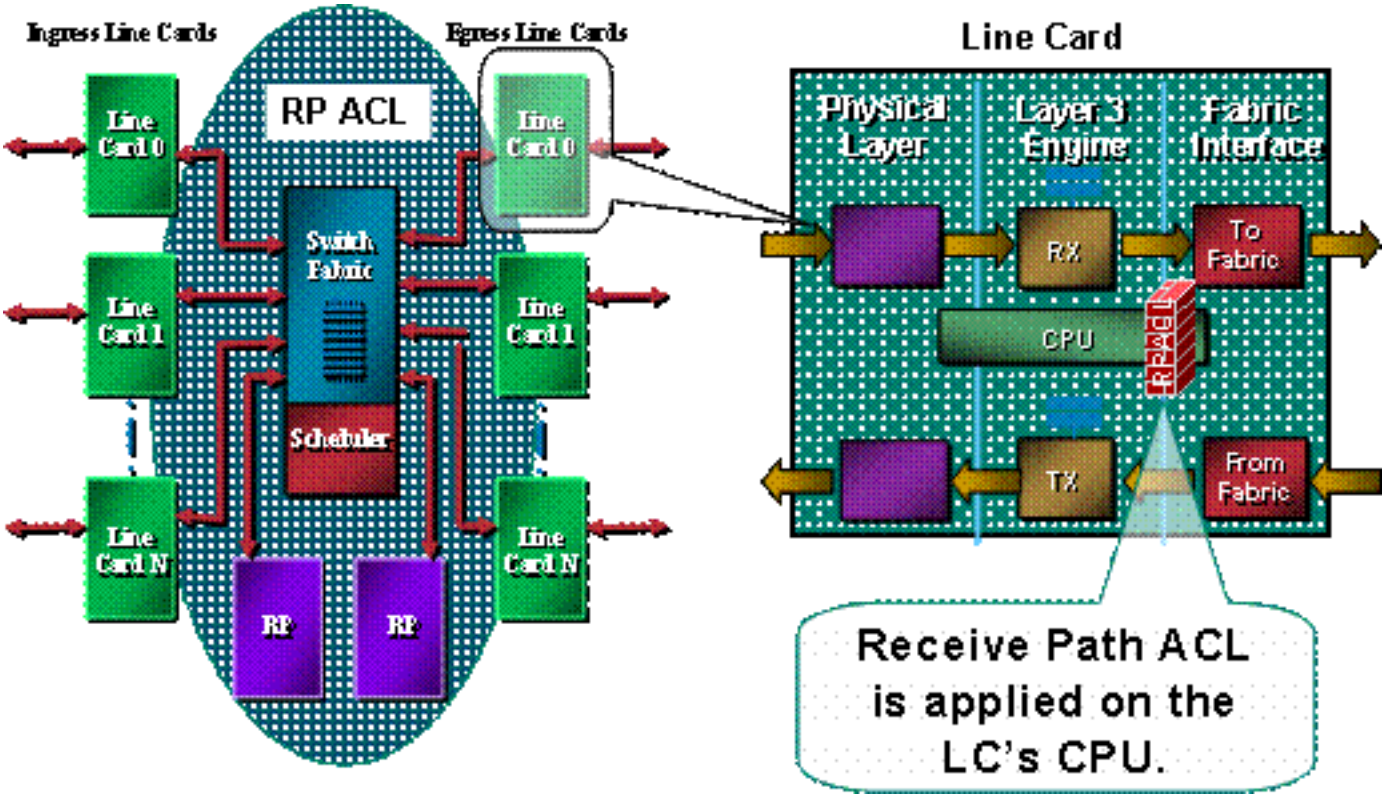
Type verkeer	Gegevenspad
Normaal (transitoverkeer) verkeer	LC aan stof op LC
Routing Protocols/SSH/SNMP	LC naar LC CPU naar fabric naar GRP
ICMP Echo (ping)	LC naar LC CPU
Vastlegging	

De routeprocessor voor de GSR heeft een beperkte capaciteit om het door de LC's geleverde verkeer dat bestemd is voor de GRP zelf te verwerken. Als er een hoog gegevensvolume nodig is om aan het GRP te worden gestraft, kan dat verkeer de GRP-functie overslaan. Dit resulteert in een effectieve denial-of-service (DoS)-aanval. CPU van de GRP-oplossing worstelt met het pakketonderzoek en begint pakketten te drogen, waardoor de wachtrijen (Input-hold en Selective Packet Discard (SPD) worden overspoeld. [2] GSR's moeten worden beschermd tegen drie scenario's die kunnen voortvloeien uit DoS-aanvallen die op een GRP van de router zijn gericht.

- Routing protocol-pakketverlies uit een vloedgolf van normale prioriteit
- Management-sessie (telnet, Secure Shell [SSH], SNMP), pakketverlies door een vloed met normale prioriteit
- Packet-verlies van een gespuugde overstroming met hoge prioriteit

Potentieel verlies van routingprotocolgegevens tijdens een vloedgolf van normale prioriteit wordt momenteel verminderd door statische classificatie en de snelheidsbeperking van verkeer dat bestemd is voor de GRP van de LC's. Helaas kent deze aanpak beperkingen. De snelheidsbeperking voor verkeer met een normale prioriteit dat bestemd is voor de GRP is onvoldoende om bescherming te bieden aan routeringsprotocolgegevens met hoge prioriteit indien een aanval via meerdere LC's wordt uitgevoerd. Het verlagen van de drempel waarboven gegevens met een normale prioriteit worden teruggebracht om een dergelijke bescherming te bieden, vergroot het verlies van beheersverkeer als gevolg van een overstroming met een normale prioriteit.

Zoals dit beeld toont, wordt rACL op elke LC uitgevoerd alvorens het pakket wordt verzonden naar GRP.



Er is een beschermingsmechanisme nodig voor de GRP. rACL's beïnvloeden verkeer dat naar GRP wordt verzonden vanwege ontvangen nabijheid. Ontvang nabijheid is het Doorsturen van nabijheid van Cisco Express voor verkeer bestemd voor de IP adressen van de router, zoals het uitzending adres of de adressen gevormd op de interfaces van de router. [3] Zie het Bijlage gedeelte voor meer details over het ontvangen van nabijheid en gepunte pakketten.

Het verkeer dat een LC ingaat wordt eerst naar lokale CPU van de LC verzonden, en pakketten die verwerking door GRP vereisen worden in de wachtrij geplaatst voor verzending naar de routeprocessor. Ontvang ACL wordt gecreëerd op de GRP en dan naar beneden geduwd tot de CPUs van de verschillende LCs. Voordat er verkeer wordt verzonden van de LC CPU naar GRP, wordt het verkeer vergeleken met de ACL. Indien toegestaan, passeert het verkeer naar de Filippijnse regering, terwijl alle andere verkeer wordt ontkend. De rACL wordt vóór de LC geïnspecteerd op GRP-functie voor snelheidsbeperking. Aangezien rACL voor al die nabijheid wordt gebruikt, zijn sommige pakketten die door de LC CPU (zoals echo-verzoeken) worden behandeld ook onderworpen aan rACL-filtering. Dit moet in aanmerking worden genomen bij het ontwerpen van rACL-items.

Ontvang ACLs (ACLs) is deel van een veeldelig programma gebied van mechanismen om de middelen in een router te beschermen. Toekomstige werkzaamheden zullen een snelheidsbeperkende component aan de rACL omvatten.

Prestatieimpact

Er wordt geen ander geheugen geconsumeerd dan dat nodig is om het één-configuratie-item en de gedefinieerde toegangslijst zelf te houden. De rACL wordt gekopieerd naar elke LC zodat er een klein geheugengebied op elke LC wordt weergegeven. Over het geheel genomen zijn de gebruikte hulpbronnen zeer gering, vooral in vergelijking met de voordelen van de inzet.

Een ontvangt ACL heeft geen invloed op de prestaties van doorgestuurd verkeer. De rACL is alleen van toepassing op nabijheidsverkeer. Doorsturen is nooit onderworpen aan de rACL. Het transitoverkeer wordt gefilterd met behulp van interface-ACL's. Deze "regelmatige" ACL's worden

toegepast op interfaces in een bepaalde richting. Het verkeer is onderworpen aan ACL-verwerking voorafgaand aan rACL-verwerking, zodat verkeer dat door de interface wordt ontkend niet door rACL ontvangen zal worden.[4]

Het LC dat het eigenlijke filteren uitvoert (met andere woorden, de LC die het verkeer ontvangt dat door de rACL wordt gefilterd) zal het gebruik van de CPU vanwege de verwerking van de rACL verhoogd hebben. Dit toegenomen gebruik van CPU's wordt echter veroorzaakt door een groot verkeersvolume dat bestemd is voor de GRP; het voordeel van de bescherming van de rACL door de Filippijnse regering weegt veel zwaarder dan het toegenomen gebruik van de CPU op een LC. Het CPU-gebruik op een LC-systeem zal verschillen afhankelijk van het type LC-motor. Gezien dezelfde aanval zal bijvoorbeeld een motor 3 LC een lager CPU-gebruik hebben dan een motor 0 LC.

Toestellen van turbo ACL's (door het **toegang-lijst gecompileerde** bevel te gebruiken) converteert ACL's in een zeer efficiënte reeks lookup-items. Wanneer turbo ACL's zijn ingeschakeld heeft de rACL-diepte geen invloed op de prestaties. Met andere woorden, de verwerkingssnelheid is onafhankelijk van het aantal ingangen in de ACL. Als de rACL klein is, zullen turbo ACL's de prestaties niet significant verhogen maar geheugen consumeren; Bij korte rACL's zijn compileerde ACL's waarschijnlijk niet nodig.

Door de GRP te beschermen, helpt de ACL de router en uiteindelijk de netwerkstabiliteit tijdens een aanval te verzekeren. Zoals hierboven beschreven wordt rACL verwerkt op de LC CPU, zodat het CPU-gebruik bij elke LC toeneemt wanneer een groot gegevensvolume op de router wordt gericht. Op E0/E1 en sommige E2 bundels, kan het gebruik van cpu van 100+% tot het routing protocol en link-laag dalingen leiden. Deze vallen zijn gelokaliseerd aan de kaart, en de GRP-routingprocessen worden beschermd, zodat stabiliteit behouden blijft. E2-kaarten met throttling-enabled microcode[5] activeert de draaiingsmodus bij zware lading en alleen voorwaartse voorrang 6 en 7 verkeer naar het routingprotocol. Andere motortypen hebben meerdere rijtuigenarchitecturen; E3-kaarten hebben bijvoorbeeld drie wachtrijen voor de CPU's, waarbij het routeren van protocolpakketten (voorrang 6/7) in een afzonderlijke wachtrij met hoge prioriteit plaatsvindt. Hoge LC CPU, tenzij pakketten met een hoge prioriteit deze veroorzaken, zal niet resulteren in het routeren van protocoldruppels. Pakketten aan de lagere prioriteitswachtrijen zullen worden achtergelaten. Tot slot hebben E4-gebaseerde kaarten acht rijen aan de CPU, met één die aan het verzenden van protocol-pakketten is gewijd.

Syntax

Een ontvangen ACL wordt toegepast met het volgende mondiale configuratiebevel om rACL aan elke LC in de router te verdelen.

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

In deze syntaxis **is *<um>*** als volgt gedefinieerd.

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

Basisjabloon en ACL-voorbeelden

Om deze opdracht te kunnen gebruiken, moet u een toegangslijst definiëren die verkeer identificeert dat toegestaan zou moeten zijn om met de router te praten. De toegangslijst moet zowel routeringsprotocollen als beheerverkeer omvatten (Border Gateway Protocol [BGP], Open Snelste pad eerst [OSPF], SNMP, SSH, telnet). Raadpleeg het gedeelte over inzetrichtsnoeren voor meer informatie.

De volgende steekproef ACL biedt een eenvoudig overzicht en presenteert een paar configuratievoorbeelden die voor specifiek gebruik kunnen worden aangepast. De ACL illustreert de vereiste configuraties voor verschillende veelgebruikte vereiste services/protocollen. Voor SSH, telnet, en SNMP, wordt een loopback adres gebruikt als bestemming. Voor de routingprotocollen wordt het eigenlijke interfaceadres gebruikt. De keuze van routerinterfaces in de ACL wordt bepaald door lokaal beleid en lokale bewerkingen. Bijvoorbeeld, als de "loopbacks" voor alle BGP-sessies worden gebruikt, hoeven alleen die "loopbacks" in de vergunningen van BGP te worden toegestaan.

```
!--- 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
```

Zoals met alle ACL's van Cisco is er een impliciete **ontkenningsverklaring** aan het eind van de toegangslijst, zodat elk verkeer dat niet overeenkomt met een ingang in ACL zal worden ontkend.

Opmerking: Het **logsleutelwoord** kan worden gebruikt om verkeer te classificeren dat voorbestemd is om de GRP te gebruiken dat niet is toegestaan. Hoewel het **logsleutelwoord** waardevolle inzicht in de details van ACL hits biedt, zullen buitensporige hits naar een ACL-ingang die dit sleutelwoord gebruikt het gebruik van LC CPU verhogen. De prestatiekimpact die aan houtkap is verbonden, zal variëren met het motortype LC. In het algemeen mag houtkap alleen worden gebruikt wanneer dat nodig is bij motoren 0/1/2. Voor motoren 3/4/4+, levert de houtkap veel minder effect op vanwege de verhoogde CPU-prestaties en de architectuur met meerdere wachtrij.

Het niveau van granulariteit van deze toegangslijst wordt bepaald door lokaal veiligheidsbeleid (bijvoorbeeld, het niveau van het filteren vereist voor OSPF buren).

ACLS en gefragmenteerde pakketten

ACLs heeft een sleutelwoord van fragmenten dat gespecialiseerd gefragmenteerd pakket-behandelend gedrag toelaat. In het algemeen worden niet-initiële fragmenten die overeenkomen met de L3-verklaringen (ongeacht de L4-informatie) in een ACL, beïnvloed door de **vergunning** of

ontkennen van de afgedekte vermelding. Merk op dat het gebruik van het sleutelwoord van **fragmenten** ACLs kan dwingen om niet-initiële fragmenten met meer granulariteit te ontkennen of toe te staan.

In de rACL-context toevoegen filterfragmenten een extra beschermingslaag tegen een DoS-aanval die alleen gebruik maakt van niet-initiële fragmenten (zoals FO > 0). Gebruik van een **ontken** verklaring voor niet-initiële fragmenten aan het begin van de ACL om alle niet-initiële fragmenten de router niet te bereiken. Onder zeldzame omstandigheden kan een geldige sessie fragmentatie vereisen en daarom gefilterd worden als een **ontkenningsfragment** statement bestaat in de rACL.

Denk bijvoorbeeld aan de hieronder weergegeven gedeeltelijke ACL.

```
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>
```

Wanneer u deze items aan het begin van een rACL toevoegt, ontkent u geen toegang tot het niet-beginfragment tot het GRP, terwijl niet-gefragmenteerde pakketten of aanvankelijke fragmenten naar de volgende lijnen van het rACL worden doorgegeven, zonder dat dit door de verklaringen van **het** fragment **wordt** beïnvloed. Het bovenstaande fragment van ACL vergemakkelijkt ook de classificatie van de aanval sinds elk protocol - Universal Datagram Protocol (UDP), TCP- en ICMP-invoeging van afzonderlijke tellers in de ACL.

Raadpleeg Toegangscontrolelijsten en IP-fragmenten voor een gedetailleerde discussie over de opties.

Risicobeoordeling

Zorg ervoor dat rACL geen kritiek verkeer zoals het routeren van protocollen of interactieve toegang tot de routers filtert. Het filteren van noodzakelijk verkeer zou kunnen resulteren in een onvermogen om ver toegang tot de router te hebben, waardoor een console verbinding vereist is. Om deze reden zouden labconfiguraties de eigenlijke inzet zo nauwkeurig mogelijk moeten nadoen.

Zoals altijd, adviseert Cisco u deze optie in het laboratorium vóór plaatsing te testen.

Aanhangsels en opmerkingen

Ontvang nakomingen en puntspakketten

Zoals eerder in dit document beschreven, vereisen sommige pakketten een GRP-verwerking. De pakketten worden van het gegevens-door:sturen vliegtuig naar GRP gestraft. Dit is een lijst van de gemeenschappelijke vormen van Layer 3 gegevens die GRP-toegang vereisen.

- Routing protocollen
- Multicast voor controleverkeer (OSPF), Hot Standby Router Protocol [HSRP], tagdistributieprotocol [TDP], Protocol-onafhankelijke multicast [PIM], enzovoort
- Multiprotocol Label Switching (MPLS)-pakketten die fragmentatie nodig hebben
- Pakketten met bepaalde IP-opties, zoals meldingen op de router

- Eerste pakket van multicast stromen
- Fragmented ICMP-pakketten die opnieuw moeten worden geassembleerd
- Al verkeer dat voor de router zelf is bestemd (behalve het verkeer dat op de LC is verwerkt)

Aangezien rACLs op nabijheid van toepassing is, filtreert rACL sommige verkeer dat niet aan GRP wordt gestraft maar een ontvangstnabijheid is. Het meest voorkomende voorbeeld hiervan is een ICMP-echo-verzoek (ping). De ICMP-echo-verzoeken die op de router zijn gericht, worden door de LC CPU's verwerkt; Aangezien de verzoeken nabijheid ontvangen, worden zij ook door de rACL gefilterd. Om deze reden, om pings aan de interfaces (of loopbacks) van de router toe te staan, moet rACL de verzoeken van echo expliciet toestaan.

Ontvang nabijheid kan worden bekeken met de **show ip cef** opdracht.

```
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
...
```

Uitvoeringsrichtsnoeren

Cisco beveelt conservatieve implementatiepraktijken aan. Om rACL's met succes te kunnen implementeren moeten de bestaande eisen voor de toegang tot besturings- en beheersvliegtuigen goed worden begrepen. In sommige netwerken is het moeilijk om het exacte verkeersprofiel te bepalen dat nodig is om de filterlijsten te maken. De volgende richtlijnen beschrijven een zeer conservatieve benadering voor het inzetten van rACL's die iteratieve rACL-configuraties gebruiken om verkeer te identificeren en uiteindelijk te filteren.

1. **Identificeer protocollen die in het netwerk met een classificatie ACL worden gebruikt.**Stel een rACL in die alle bekende protocollen toestaat die tot de GRP toegang hebben. Deze "ontdekking" of ACL moet zowel bron- als doeladressen op **elk gewenst** bestand hebben ingesteld. Vastlegging kan worden gebruikt om een lijst met bronadressen te ontwikkelen die overeenkomen met de verklaringen van de **protocolvergunning**. Naast de verklaring **van de** protocolvergunning, **staat** een **vergunning elke** lange lijn aan het eind van de rACL toe om andere protocollen te identificeren die door rACL zouden worden gefilterd en die toegang tot de GRP zouden kunnen vereisen.Het doel is te bepalen welke protocollen het specifieke netwerk gebruikt. Vastlegging zou voor analyse moeten worden gebruikt om te bepalen "wat anders" met de router zou kunnen communiceren.**Opmerking:** Hoewel het **logsleutelwoord** waardevolle inzichten in de details van hits biedt, kunnen buitensporige hits naar een ACL-ingang die dit trefwoord gebruikt, leiden tot een overweldigend aantal logitems en mogelijk een hoog gebruik van CPU's. Gebruik het sleutelwoord van het **logboek** voor korte periodes en slechts wanneer nodig om verkeer te classificeren.
2. **Bekijk geïdentificeerde pakketten en begin om toegang tot het GRP te filteren.**Nadat de pakketten die in stap 1 door rACL werden gefilterd zijn geïdentificeerd en geëvalueerd, stelt u een rACL in met een **vergunning om het even welke** verklaring voor de toegestane protocollen. Net zoals in stap 1, kan het **logsleutelwoord** meer informatie over de pakketten verstrekken die de **vergunning** ingangen aanpassen. Door **elk logbestand** aan het eind te ontkennen kan men onverwachte pakketten identificeren die bestemd zijn voor de GRP. Deze rACL zal basisbescherming bieden en zal netwerkingenieurs toestaan om te verzekeren dat al vereist verkeer wordt toegestaan.Het doel is het bereik van protocollen te

testen die met de router moeten communiceren zonder het expliciete bereik van IP bron en bestemmingsadressen te hebben.

3. **Beperk een macro bereik van bronadressen.**Laat slechts het volledige bereik van uw toegewezen klasse interdomain routing (CIDR) toe om als bronadres te worden toegestaan. Bijvoorbeeld, als u 171.68.0.0/16 voor uw netwerk toegewezen bent geweest, dan zou van de bron adressen van de vergunning slechts 171.68.0.0/16 zijn.Deze stap verkleint het risico zonder de services te breken. Het levert ook datapunten van apparaten/mensen van buiten uw CIDR-blok die uw apparatuur zouden kunnen benaderen. Al het externe adres wordt verwijderd.Externe BGP-peers hebben een uitzondering nodig, aangezien de toegestane bronadressen voor de sessie buiten het CIDR-blok zullen liggen.Deze fase kan een paar dagen worden ingeschakeld om gegevens te verzamelen voor de volgende fase waarin de rACL wordt versmald.
4. **Sluit de rACL-vergunningen aan om alleen bekende geautoriseerde bronadressen toe te staan.**Beperk steeds meer het bronadres om alleen bronnen toe te staan die met de GRP communiceren.
5. **Beperk de doeladressen op de rACL. (*optioneel*)**Sommige internetserviceproviders (ISP) kunnen ervoor kiezen alleen bepaalde protocollen toe te staan om specifieke doeladressen op de router te gebruiken. Deze laatste fase is bedoeld om het bereik van de doeladressen te beperken dat verkeer voor een protocol accepteert. [6]

Installatievoorbeeld

Het voorbeeld hieronder toont een ontvangen ACL die een router op basis van het volgende richten beschermt.

- Het adresblok van de ISP is 169.223.0.0/16.
- Het infrastructuurblok van de ISP is 169.223.252.0/22.
- De loopback voor de router is 169.223.253.1/32.
- De router is een core backbone router, zodat alleen interne BGP-sessies actief zijn.

Gegeven deze informatie, ontvangt het eerste ACL zoals het voorbeeld hieronder. Aangezien we de infrastructuur adresblok kennen, zullen we eerst het hele blok toestaan. Later zullen meer gedetailleerde toegangscontrole-ingangen (ACE's) worden toegevoegd aangezien de specifieke adressen worden verkregen voor alle apparaten die toegang tot de router nodig hebben.

```
!
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
```

Opmerkingen

1. Raadpleeg Inzicht op SPD (Selective Packet Discard) (SPD) en werklastrichtlijnen voor het verhogen van DoS-resistentie.
2. Raadpleeg voor meer informatie over het doorsturen van Cisco Express en de nabijheid een overzicht van Cisco Express doorsturen.
3. Voor een gedetailleerde discussie van ACL-implementatierichtlijnen en verwante opdrachten raadpleegt u ACL's implementeren op Cisco 12000 Series Internet-routers.
4. Dit verwijst naar Vanilla, Border Gateway Protocol Policy Accounting (BGPPA), Per Interface Rate Control (PIRC) en Frame Relay Traffic Policing (FRTP)-bundels.
5. Fase II van de Bescherming van het Ontvangend Pad zal voor het creëren van een beheersinterface toestaan, automatisch beperkt welk IP adres naar inkomende pakketten zal luisteren.

Gerelateerde informatie

- Ondersteuningspagina voor ACL's
- Technische ondersteuning - Cisco-systemen