Bescherm uw kern: Toegangscontrolelijsten voor bescherming van infrastructuur

Inhoud

Inleiding

Dit document bevat richtsnoeren en aanbevolen inzettechnieken voor toegangscontrolelijsten voor infrastructuurbeveiliging (ACL's). InfrastructuurACL's worden gebruikt om het risico en de doeltreffendheid van directe infrastructuuraanvallen te minimaliseren door uitsluitend toegestaan verkeer naar de infrastructuurapparatuur toe te staan en tegelijkertijd al het andere transitoverkeer toe te staan.

Infrastructuurbeveiliging

Achtergrond

In een poging om routers te beschermen tegen verschillende risico's — zowel accidenteel als kwaadaardig — dient de bescherming van de infrastructuur ACL's te worden uitgevoerd op netwerkingspunten. Deze IPv4 en IPv6 ACLs ontkennen toegang van externe bronnen tot alle infrastructuuradressen, zoals routerinterfaces. Tegelijkertijd staan de ACL's routinevervoerverkeer toe om ononderbroken te stromen en basislijn RFC 1918 , RFC 3330 en antiparing-filtering te bieden.

De gegevens die door een router worden ontvangen kunnen in twee grote categorieën worden verdeeld:

- verkeer dat door de router via het verzendende pad gaat

- verkeer bestemd voor de router via het ontvangstpad voor de verwerking van de route

In normale operaties stroomt het overgrote deel van het verkeer eenvoudigweg door een router en route naar zijn uiteindelijke bestemming.

Echter, de routeprocessor (RP) moet bepaalde soorten gegevens direct verwerken, vooral routeprotocollen, externe routertoegang (zoals Secure Shell [SSH]) en netwerkbeheerverkeer zoals Simple Network Management Protocol (SNMP). Bovendien kunnen protocollen zoals Internet Control Message Protocol (ICMP) en IP-opties rechtstreeks door de RP-toets worden verwerkt. Meestal is de directe toegang tot de infrastructuurrouter alleen nodig uit interne bronnen. Een paar opmerkelijke uitzonderingen omvatten het uitgeven van het Protocol van de Grensgateway (BGP), protocollen die op de eigenlijke router eindigen (zoals generieke Routing Encapsulation [GRE] of IPv6 via IPv4-tunnels) en potentieel beperkte ICMP-pakketten voor connectiviteit-tests zoals echo-request of ICMP onbereikbaar en de tijd om te leven (TTL) is verlopen voor traceroute.

Opmerking: Onthoud dat ICMP vaak wordt gebruikt voor eenvoudige 'denial-of-service'-aanvallen (DoS) en indien nodig alleen uit externe bronnen mag worden gebruikt.

Alle RP's hebben een prestatiekloof waarin ze werken. Het buitensporige verkeer dat voor de RP is bestemd kan de router overweldigen. Dit veroorzaakt een hoog CPU-gebruik en leidt uiteindelijk tot pakje- en routingprotocollen die een serviceontkenning veroorzaken. Door de toegang tot infrastructuurrouters van externe bronnen te filteren, worden veel van de externe risico's verbonden aan een directe routeraanval verminderd. Aanvallen van buitenaf kunnen geen toegang meer krijgen tot infrastructurele apparatuur. De aanval wordt op toegangsinterfaces in het autonome systeem (AS) gevallen.

De in dit document beschreven filtertechnieken zijn bedoeld om gegevens te filteren die bestemd zijn voor netwerkinfrastructuren. Verwar het filteren van de infrastructuur niet met algemeen filteren. Het enige doel van de ACL van de infrastructuurbescherming is om op granulair niveau te beperken tot welke protocollen en bronnen toegang hebben tot kritieke infrastructurele apparatuur.

Netwerkinfrastructuur omvat deze gebieden:

- Alle router- en switch-beheeradressen, inclusief loopback-interfaces
- Alle interne link adressen: router-naar-router links (point-to-point en meervoudige toegang)
- Interne servers of diensten die niet toegankelijk zouden moeten zijn vanuit externe bronnen

In dit document wordt al het verkeer dat niet bestemd is voor de infrastructuur vaak het transitoverkeer genoemd.

Technieken

De bescherming van de infrastructuur kan worden bereikt door middel van verschillende technieken:

- **Ontvang ACL's (rACL's)**Cisco 12000- en 7500-platforms ondersteunen rs die al het verkeer dat bestemd is voor de RP filteren en geen effect hebben op het transitoverkeer. Het geautoriseerde verkeer moet expliciet worden toegestaan en de rACL moet op elke router worden gebruikt. Zie GSR: Ontvang toegangscontrolelijsten voor meer informatie.
- **Hop-by-hoprouter ACL's**De routers kunnen ook worden beschermd door ACL's te definiëren die alleen toegestaan verkeer naar de interfaces van de router toestaan, en alle anderen behalve doorvoerverkeer ontkennen, wat expliciet moet worden toegestaan. Deze ACL is

logisch vergelijkbaar met een rACL maar heeft invloed op doorvoerverkeer en kan daarom een negatieve impact hebben op de snelheid van een router.
- **Edge-filtering via infrastructuur ACL's**ACL's kunnen worden toegepast op de rand van het netwerk. In het geval van een dienstverlener (SP) is dit de rand van het AS. Dit ACL filtert expliciet verkeer voor de ruimte van het infrastructuuradres. De plaatsing van rand infrastructuur ACLs vereist dat u uw infrastructuurruimte en de vereiste/geautoriseerde protocollen die deze ruimte toegang hebben duidelijk definieert. ACL wordt toegepast bij toegang tot uw netwerk op alle extern gerichte verbindingen, zoals peerverbindingen, klantenverbindingen, enz.Dit document is gericht op de ontwikkeling en invoering van grensinfrastructurele beveiligingsACL's.

ACL-voorbeelden

Deze toegangslijsten van IPv4 en IPv6 bieden eenvoudige maar realistische voorbeelden van typische ingangen die in een beschermde ACL worden vereist. Deze basis-ACL's moeten worden aangepast met plaatselijke site-specifieke configuratiegegevens. In dubbele IPv4- en IPv6-omgevingen worden beide toegangslijsten uitgevoerd.

IPv4-voorbeeld

```
!--- 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
```

IPv6-voorbeeld

De IPv6-toegangslijst moet worden toegepast als een uitgebreide, genoemde toegangslijst.

```
!--- 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
```

Opmerking: Het **logsleutelwoord** kan worden gebruikt om extra detail over bron en bestemmingen voor een bepaald protocol te verstrekken. Hoewel dit sleutelwoord waardevolle inzichten in de details van ACL hits biedt, kunnen buitensporige hits naar een ACL-ingang die het gebruik van de CPU-toepassing gebruikt. De prestatiekimpact verbonden aan houtkap varieert per platform. Gebruik van het logsleutelwoord schakelt ook de omschakeling van Cisco Express Forwarding (CEF) in voor pakketten die de toegangs-lijst verklaring overeenkomen. Die pakketten zijn snel geschakeld.

ACL-bescherming ontwikkelen

In het algemeen bestaat een ACL-infrastructuur uit vier delen:

- Special-use adres en anti-spoofing items die onwettige bronnen en pakketten met bronadressen ontzeggen die binnen uw AS behoren van het invoeren van AS van een externe bron**Opmerking:** RFC 3330 definieert IPv4 speciale gebruikersadressen die mogelijk filtering vereisen. RFC 1918 definieert IPv4 gereserveerde adresruimte die geen geldig bronadres op het internet is. RFC 3513 definieert de IPv6-adresseringsarchitectuur. RFC 2827 biedt ingangsfilterrichtlijnen.
- Expliciet toegestaan extern verkeer bestemd voor infrastructuuradressen
- verklaringen **ontkennen** voor alle andere extern gebronsde verkeer naar infrastructuuradressen
- verklaringen **mogelijk** voor al het andere verkeer voor het normale backbone-verkeer op de weg naar niet-infrastructuurbestemmingen

De laatste regel in de infrastructuur ACL maakt transitovervoer expliciet mogelijk: **sta IP toe elke** voor IPv4 en **laat ipv6 elk** voor IPv6 **toe**. Deze ingang waarborgt dat alle IP protocollen door de kern zijn toegestaan en dat klanten toepassingen zonder problemen kunnen blijven uitvoeren.

De eerste stap wanneer u een infrastructuur bescherming ACL ontwikkelt is de vereiste protocollen te begrijpen. Hoewel elke site specifieke vereisten heeft, worden bepaalde protocollen algemeen gebruikt en moeten deze worden begrepen. Externe BGP naar externe peers moet bijvoorbeeld expliciet worden toegestaan. Alle andere protocollen die directe toegang tot de infrastructuurrouter vereisen moeten ook expliciet worden toegestaan. Bijvoorbeeld, als u een GRE-tunnel op een router van de kerninfrastructuur eindigt, moet protocol 47 (GRE) ook expliciet worden toegestaan. Op dezelfde manier moet, als u een IPv6-over-IPv4-tunnel op een core infrastructuur router beëindigt, protocol 41 (IPv6-over-IPv4) ook expliciet worden toegestaan.

Een classificatie ACL kan worden gebruikt om de vereiste protocollen te identificeren. De classificatie ACL bestaat uit vergunningen verklaringen voor de verschillende protocollen die voor een infrastructuurrouter kunnen worden bestemd. Raadpleeg de bijlage over ondersteunde IP-protocollen in Cisco IOS® Software voor een volledige lijst. Het gebruik van de **opdracht** van de **show access-list** om een telling van de hits van de toegangscontrole (ACE) te tonen identificeert de vereiste protocollen. Verdachte of verrassende resultaten moeten worden onderzocht en begrepen voordat u een **vergunning** voor onverwachte protocollen maakt.

Bijvoorbeeld, deze IPv4 ACL helpt bepalen of GRE, IPsec (ESP) en IPv6 tunneling (IP Protocol 41) moeten worden toegestaan.

```
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
```

Deze IPv6 ACL kan worden gebruikt om te bepalen of GRE en IPsec (ESP) moeten worden

toegestaan.

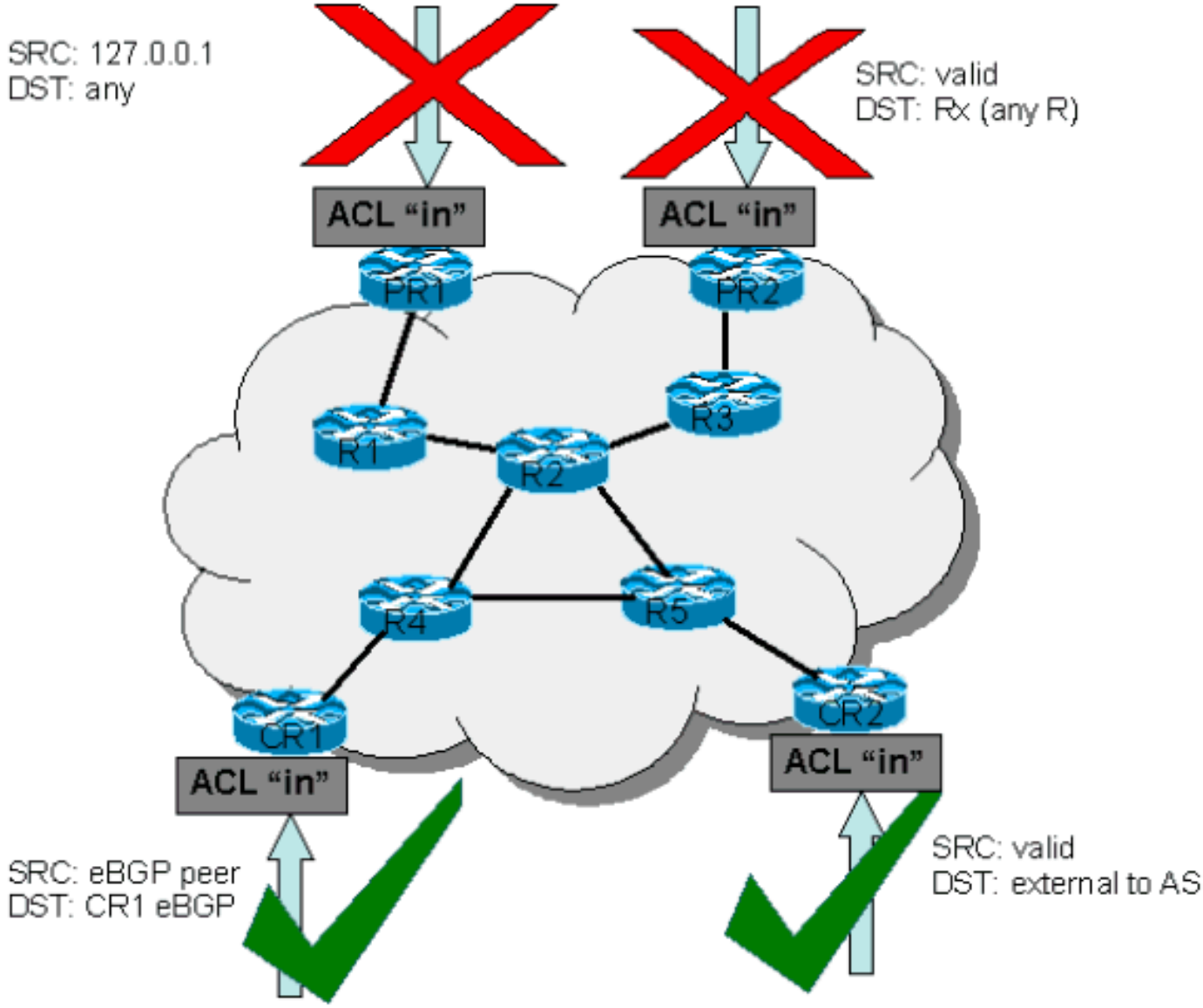
```
ipv6 access-list determine_protocols
 permit GRE any infrastructure_ips_ipv6
 permit ESP any infrastructure_ips_ipv6
 permit ipv6 any infrastructure_ips_ipv6 log
!--- The log keyword provides more details !--- about other protocols that are not explicitly
permitted. permit ipv6 any any interface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

Naast de vereiste protocollen moet de ruimte voor infrastructurele adresgebieden worden geïdentificeerd, aangezien dit de ruimte is die de ACL beschermt. De adresruimte van de infrastructuur omvat om het even welke adressen die voor het interne netwerk worden gebruikt en zelden door externe bronnen zoals routerinterfaces, point-to-point link adressering, en kritieke infrastructuurservices worden benaderd. Aangezien deze adressen voor het doelgedeelte van de infrastructuur ACL worden gebruikt, is de samenvatting kritiek. Waar mogelijk moeten deze adressen worden gegroepeerd in klasse interdomain Routing (CIDR) blokken.

Met het gebruik van de geïdentificeerde protocollen en adressen, kan de infrastructuur ACL worden gebouwd om de protocollen toe te staan en de adressen te beschermen. Naast directe bescherming biedt ACL ook een eerste verdedigingslinie tegen bepaalde soorten ongeldig verkeer op het internet.

- RFC 1918-ruimte moet worden ontkend.
- Packets met een bronadres dat valt onder een speciale adresruimte, zoals gedefinieerd in RFC 3330, moeten worden geweigerd.
- Er moeten antispooffilters worden toegepast. (Uw adresruimte mag nooit de bron van pakketten zijn van buiten uw netwerk.)

Deze nieuw geconstrueerde ACL moet inkomende op alle ingangsinterfaces worden toegepast. Zie de paragrafen over inzetrichtsnoeren en inzetvoorbeelden voor meer informatie.



ACL's en gefragmenteerde pakketten

ACLs heeft een sleutelwoord van fragmenten dat gespecialiseerd gefragmenteerd pakket-behandelend gedrag toelaat. Zonder dit **fragmenten** sleutelwoord, worden niet-initiële fragmenten die de Layer 3 verklaringen (ongeacht Layer 4 informatie) in een ACL aanpassen door de vergunning of ontkennen verklaring van de gematchte ingang beïnvloed. Maar door het sleutelwoord van het **fragmenten** toe te voegen, kunt u ACLs dwingen om niet-initiële fragmenten met meer granulariteit te ontkennen of toe te staan. Dit gedrag is het zelfde voor zowel IPv4 als IPv6 toegangslijsten, met uitzondering dat, terwijl IPv4 ACLs het gebruik van het sleutelwoord van fragmenten binnen Layer 3 en Layer 4 verklaringen toestaat, IPv6 ACLs slechts het gebruik van het sleutelwoord van fragmenten in Layer 3 verklaringen toestaat.

Filtering fragmenten voegt een extra laag bescherming toe tegen een DoS-aanval (Denial of Service) die niet-initiële fragmenten (dwz, FO > 0) gebruikt. Gebruik een **ontken** verklaring voor niet-initiële fragmenten in het begin van ACL om alle niet-initiële fragmenten toegang tot de router te ontzeggen. Onder zeldzame omstandigheden kan een geldige sessie fragmentatie vereisen en daarom gefilterd worden als een **ontkenningsfragment** verklaring in ACL bestaat.

Denk bijvoorbeeld aan dit gedeeltelijke IPv4ACL:

```
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>
```

De toevoeging van deze ingangen aan het begin van ACL ontkent elke niet-aanvankelijke gefragmenteerde toegang tot de kernrouters, terwijl niet-gefragmenteerde pakketten of aanvankelijke fragmenten naar de volgende lijnen van ACL overgaan zonder het **ontkende fragment** verklaringen. Het bovenstaande ACL-opdracht vergemakkelijkt ook de classificatie van de aanval sinds elk protocol-Universal Datagram Protocol (UDP), TCP- en ICMP-stappen in afzonderlijke tellers in de ACL.

Dit is een vergelijkbaar voorbeeld voor IPv6:

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

De toevoeging van deze ingang aan het begin van IPv6 ACL ontkent elke niet-aanvankelijke fragmentatie toegang tot de kernrouters. Zoals eerder opgemerkt, staan IPv6 toegangslijsten slechts het gebruik van het fragmenten sleutelwoord in Layer 3 verklaringen toe.

Omdat veel aanvallen afhankelijk zijn van het overspoelen van kernrouters met gefragmenteerde pakketten, biedt het filteren van inkomende fragmenten aan de kerninfrastructuur een extra bescherming en helpt u ervoor te zorgen dat een aanval geen fragmenten kan injecteren door Layer 3-regels in de infrastructuur ACL eenvoudig te koppelen.

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

Risicobeoordeling

Neem deze twee gebieden van zeer groot risico in overweging wanneer u infrastructuuropslag ACLs implementeert:

- Zorg ervoor dat de juiste **vergunning/ontkennende** verklaringen zijn afgegeven. Om ACL effectief te kunnen zijn, moeten alle vereiste protocollen worden toegestaan en moet de juiste adresruimte door de **ontkennende** verklaringen worden beschermd.
- De prestaties van ACL variëren van platform tot platform. Bekijk de prestatiekenmerken van uw hardware voordat u ACL's implementeert.

Zoals altijd wordt aanbevolen om dit ontwerp in het lab te testen voordat het wordt ingezet.

Aanhangsels

Ondersteunde IP-protocollen in Cisco IOS-software

Deze IP-protocollen worden ondersteund door Cisco IOS-software:

- 1 - ICMP

- 2 - IGMP
- 3 GGP
- 4 - IP-insluiting
- 6 - TCP
- 8 EGP
- 9 - IGRP
- 17 - UDP
- 20 - HMP
- 27 - RDP
- 41 - IPv6-tunneling in IPv4
- 46 - RSVP
- 47 - GRE
- 50 ESP
- 51 - AH
- 53 - SWIPE
- 54 - NARP
- 55 - IP-mobiliteit
- 63 - elk lokaal netwerk
- 77 - Sun ND
- 80 - ISO IP
- 88 - EW
- 89 - OSPF-beperking
- 90 - Sprite RPC
- 91 - LARP
- 94 - KA9Q/NOS compatibele IP over IP
- 103 - PIM
- 108 - IP-compressie
- 112 - VRRP
- 113 - PGM
- 115 - L2TP
- 120 - UTI
- 132 - SCTP

Uitvoeringsrichtsnoeren

Cisco beveelt conservatieve implementatiepraktijken aan. Om met succes infrastructuur ACLs te kunnen implementeren moeten de vereiste protocollen goed begrepen worden, en adresruimte moet duidelijk geïdentificeerd en gedefinieerd worden. Deze richtlijnen beschrijven een zeer conservatieve methode om bescherming ACL's te gebruiken met een iteratieve benadering.

1. **Identificeer protocollen die in het netwerk met een classificatie ACL worden gebruikt.**Hiermee implementeert u een ACL die alle bekende protocollen toestaat die toegang hebben tot infrastructurele apparaten. Deze ontdekking ACL heeft een bronadres van **om het** even welke en een bestemming die infrastructuur IP ruimte omvat. Vastlegging kan worden gebruikt om een lijst met bronadressen te ontwikkelen die overeenkomen met de verklaringen van de **protocolvergunning**. Een laatste regel die **elke** IP (IPv4) of **ipv6 om het even welke** (IPv6) toestaat is vereist om verkeersstroom toe te staan.Het doel is te bepalen welke protocollen het specifieke netwerk gebruikt. Vastlegging wordt gebruikt voor analyse

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. Tevens schakelt het **logsleutelwoord** in de omschakeling van Cisco Express Forwarding (CEF) voor pakketten die de toegangs-lijst verklaring overeenkomen. Die pakketten zijn snel geschakeld. Gebruik het sleutelwoord van het **logboek** voor korte periodes en slechts wanneer nodig om verkeer te classificeren.

2. **Bekijk de geïdentificeerde pakketten en begin om toegang tot de routeprocessor RP te filteren.**Nadat de pakketten die in stap 1 door ACL werden gefilterd zijn geïdentificeerd en geëvalueerd, stelt u een ACL in met een **vergunning om het even welke bron** aan de infrastructuuradressen voor de toegestane protocollen. Net zoals in stap 1, kan het **logsleutelwoord** meer informatie over de pakketten verstrekken die de **vergunning** ingangen aanpassen. Met **ontkennen** kan **elke** computer aan het einde helpen om onverwachte pakketten te identificeren die bestemd zijn voor de routers. De laatste regel van deze ACL moet een **vergunninghouder zijn IP elke** (IPv4) of **elke** (IPv6) verklaring **ipv6 toestaan** om de doorvoerstroom mogelijk te maken. Deze ACL biedt wel basisbescherming en laat netwerkingenieurs toe om er zeker van te zijn dat al het vereiste verkeer is toegestaan.
3. **Bron adressen beperken.**Zodra u een duidelijk inzicht hebt in de protocollen die moeten worden toegestaan, kan er verder filteren worden uitgevoerd om alleen geautoriseerde bronnen voor deze protocollen mogelijk te maken. U kunt bijvoorbeeld expliciet externe BGP-buren of specifieke GRE-peer-adressen toestaan.Deze stap versmalt het risico zonder de services te breken en stelt u in staat om granulaire controle uit te oefenen op bronnen die toegang hebben tot uw infrastructuur.
4. **Beperk de doeladressen op ACL. (*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 kan accepteren.

Installatievoorbeelden

IPv4-voorbeeld

Dit IPv4 voorbeeld toont een infrastructuur ACL die een router beschermt die op deze het richten gebaseerd is:

- Het ISP-adresblok is 169.223.0.0/16.
- Het infrastructuurblok van ISP is 169.223.252.0/22.
- De loopback voor de router is 169.223.253.1/32.
- De router is een peer router en peers met 169.254.254.1 (om 169.223.252.1 aan te pakken).

De weergegeven ACL-toegangsbeveiliging van de infrastructuur wordt ontwikkeld op basis van de bovenstaande informatie. ACL toestaat extern BGP peering aan de externe peer, verstrekt anti-spoof filters en beschermt de infrastructuur tegen alle externe toegang.

```
!
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
```

IPv6-voorbeeld

Dit IPv6-voorbeeld toont een infrastructuur ACL die een router beschermt die op deze het volgende is gebaseerd:

- Het totale aan de ISP toegewezen prefix blok is 2001:0DB8::/32.
- Het IPv6-prefix blok dat door de ISP wordt gebruikt voor netwerkinfrastructuuradressen is 2001:0DB8:C18::/48.
- Er is een BGP peerrouter met een IPv6-adres van de bron van 2001:0DB8:C18:2:1:1:1 dat neigt naar IPv6-adres van de bestemming van 2001:0DB8:C19:2:1:F.

De weergegeven ACL-toegangsbeveiliging van de infrastructuur wordt ontwikkeld op basis van de bovenstaande informatie. ACL maakt externe multiprotocol BGP mogelijk door te gaan naar de externe peer, biedt anti-spoof filters en beschermt de infrastructuur tegen alle externe toegang.

```
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
```

Gerelateerde informatie

- Ondersteuningspagina voor ACL's
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems