Cisco Guide to Harden Cisco IOS-apparaten

Inhoud

Inleiding

Dit document beschrijft de informatie om u te helpen uw Cisco IOS® systeemapparaten te beveiligen, wat de algemene veiligheid van uw netwerk verhoogt. Gestructureerd rond de drie vlakken waarin de functies van een netwerkapparaat kunnen worden gecategoriseerd, biedt dit document een overzicht van elke opgenomen functie en verwijzingen naar gerelateerde documentatie.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

De drie functionele vlakken van een netwerk, het managementvlak, het bedieningspaneel en het dataplaat bieden verschillende functionaliteit die beschermd moet worden.

- **Management Plan** - het beheervliegtuig beheert verkeer dat naar het Cisco IOS-apparaat wordt verzonden en uit toepassingen en protocollen bestaat zoals Secure Shell (SSH) en Simple Network Management Protocol (SNMP).

- **Bedieningsplatform** - Het bedieningspaneel van een netwerkapparaat verwerkt het verkeer dat het allerbelangrijkst is om de functionaliteit van de netwerkinfrastructuur te behouden. Het controlevliegtuig bestaat uit toepassingen en protocollen tussen netwerkapparaten, die het Protocol van de Grenzen (BGP) omvatten, evenals de Protocollen van de Gateway van het Binnenhuis (IGPs) zoals het Uitgebreide Interior Gateway Routing Protocol (DHCP) en Open Snelste Pad First (OSPF) omvatten.

- **Datacentervlak** - Het gegevensvlak verstuurt gegevens door een netwerkapparaat. Het gegevensvliegtuig omvat geen verkeer dat naar het lokale Cisco IOS apparaat wordt verzonden.

De dekking van de veiligheidseigenschappen in dit document verstrekt vaak genoeg detail om de eigenschap te configureren. Indien dit niet het geval is, wordt de functie echter zodanig uitgelegd dat u kunt beoordelen of extra aandacht voor de functie nodig is. Waar mogelijk en passend bevat dit document aanbevelingen die, indien ze worden uitgevoerd, bijdragen tot de beveiliging van een netwerk.

Beveiligingsbewerkingen

Beveiligde netwerkbewerkingen zijn een substantieel onderwerp. Hoewel het meeste van dit document is gewijd aan de veilige configuratie van een Cisco IOS apparaat, beveiligen configuraties alleen niet volledig een netwerk. De op het netwerk toegepaste operationele procedures dragen evenveel bij tot de veiligheid als de configuratie van de onderliggende apparatuur.

Deze onderwerpen bevatten operationele aanbevelingen die u geadviseerd wordt te implementeren. Deze onderwerpen benadrukken specifieke kritieke gebieden van netwerkoperaties en zijn niet uitgebreid.

Cisco Security Advisories en antwoorden bewaken

Het Cisco Product Security Incident Response Team (PSIRT) maakt en onderhoudt publicaties, vaak PSIRT Advisories, voor security-gerelateerde problemen in Cisco-producten. De methode die wordt gebruikt voor communicatie van minder ernstige problemen is de Cisco Security Response. Security advisories en antwoorden zijn beschikbaar op http://www.cisco.com/go/psirt.

Aanvullende informatie over deze communicatievoertuigen is beschikbaar in het Cisco Security kwetsbaarheidsbeleid.

Om een veilig netwerk te onderhouden moet u op de hoogte zijn van de Cisco security adviseurs en de reacties die zijn vrijgegeven. U moet op de hoogte zijn van een kwetsbaarheid voordat de dreiging die het kan vormen voor een netwerk kan worden beoordeeld. Raadpleeg de risicoanalyse voor de kwetsbaarheid van de beveiliging en de aankondigingen voor ondersteuning van dit evaluatieproces.

Levering verificatie, autorisatie en accounting

Het kader voor verificatie, autorisatie en accounting (AAA) is essentieel om netwerkapparaten te beveiligen. Het AAA-kader biedt verificatie van beheersessies en kan gebruikers ook beperken tot specifieke, door een beheerder gedefinieerde opdrachten en alle opdrachten die door alle gebruikers zijn ingevoerd, registreren. Zie het gedeelte Verificatie, autorisatie en accounting van dit document voor meer informatie over hoe u AAA kunt gebruiken.

Gecentraliseerde bestandsverzameling en -bewaking

Om kennis te verwerven over bestaande, opkomende en historische gebeurtenissen die betrekking hebben op veiligheidsincidenten, moet uw organisatie een gezamenlijke strategie hebben voor het registreren van gebeurtenissen en het correleren daarvan. Deze strategie moet de houtkap van alle netwerkapparaten aanvullen en vooraf verpakte en aanpasbare correlatiemogelijkheden gebruiken.

Nadat gecentraliseerde houtkap is geïmplementeerd, moet u een gestructureerde benadering van loganalyse en het opsporen van incidenten ontwikkelen. Gebaseerd op de behoeften van uw organisatie, kan deze benadering variëren van een eenvoudig zorgvuldig onderzoek van loggegevens tot geavanceerde op regelgeving gebaseerde analyse.

Zie de sectie Best Practices van dit document voor meer informatie over hoe u houtkap op Cisco IOS-netwerkapparaten kunt implementeren.

Indien mogelijk beveiligde protocollen gebruiken

Veel protocollen worden gebruikt om gevoelige netwerkbeheergegevens over te dragen. U moet waar mogelijk veilige protocollen gebruiken. Een veilige protocolkeuze omvat het gebruik van SSH in plaats van telnet, zodat zowel de authenticatiegegevens als de beheerinformatie worden versleuteld. Daarnaast moet u veilige protocollen voor bestandsoverdracht gebruiken wanneer u configuratiegegevens kopieert. Een voorbeeld is het gebruik van het Secure Copy Protocol (SCP) in plaats van FTP of TFTP.

Zie het gedeelte Secure Interactive Management Sessies van dit document voor meer informatie over het beveiligde beheer van Cisco IOS-apparaten.

Gain Traffic Visibility and met NetFlow

Met NetFlow kunt u de verkeersstromen in het netwerk bewaken. Oorspronkelijk bedoeld om verkeersinformatie naar netwerkbeheertoepassingen uit te voeren, kan NetFlow ook worden gebruikt om stroominformatie op een router weer te geven. Deze mogelijkheid stelt u in staat om te zien wat verkeer het netwerk in real time overbrengt. Ongeacht of de stroominformatie naar een afstandsbediening wordt geëxporteerd, wordt u geadviseerd om netwerkapparaten voor NetFlow te configureren zodat deze indien nodig reactief gebruikt kan worden.

Meer informatie over deze optie is beschikbaar in het gedeelte Verkeersidentificatie en Traceback van dit document en op http://www.cisco.com/go/netflow (alleen geregistreerde klanten).

Configuratie-beheer

Configuratiebeheer is een proces waarmee configuratiewijzigingen worden voorgesteld, beoordeeld, goedgekeurd en ingezet. Binnen de context van een Cisco IOS apparatenconfiguratie, zijn twee extra aspecten van configuratiebeheer essentieel: archivering en beveiliging van de configuratie.

U kunt configuratiearchieven gebruiken om veranderingen terug te draaien die aan netwerkapparaten gemaakt worden. In een veiligheidscontext kunnen de configuratie archieven ook worden gebruikt om te bepalen welke beveiligingswijzigingen zijn aangebracht en wanneer deze wijzigingen zich hebben voorgedaan. Deze informatie kan, in combinatie met de gegevens van het AAA-logboek, helpen bij de veiligheidscontrole van netwerkapparaten.

De configuratie van een Cisco IOS apparaat bevat veel gevoelige details. Gebruikersnaam, wachtwoorden en de inhoud van toegangscontrolelijsten zijn voorbeelden van dit type informatie. De opslagplaats die u gebruikt om Cisco IOS-apparaatconfiguraties te archiveren moet beveiligd zijn. Onveilige toegang tot deze informatie kan de veiligheid van het gehele netwerk ondermijnen.

beheermaatschappij

Het beheersvlak bestaat uit functies die de beheersdoelstellingen van het netwerk bereiken. Dit omvat interactieve beheersessies die SSH gebruiken, evenals statistiek-verzamelen met SNMP of NetFlow. Wanneer u de beveiliging van een netwerkapparaat in overweging neemt, is het van cruciaal belang dat het beheervlak wordt beschermd. Als een veiligheidsincident de functies van het managementvliegtuig kan ondermijnen, kan het voor u onmogelijk zijn om het netwerk te herstellen of te stabiliseren.

Deze secties van dit document geven details over de beveiligingsfuncties en -configuraties die in Cisco IOS-software beschikbaar zijn die helpen het beheervliegtuig te versterken.

Hardnekkige algemene beheersplannen

Het beheersvliegtuig wordt gebruikt om toegang te krijgen tot, te vormen en een apparaat te beheren, evenals zijn operaties en het netwerk te controleren waarop het wordt ingezet. Het beheersvliegtuig is het vliegtuig dat verkeer ontvangt en verstuurt voor de exploitatie van deze functies. U moet zowel het managementvlak als het bedieningspaneel van een voorziening beveiligen, omdat de bediening van het bedieningspaneel rechtstreeks van invloed is op de werking van het managementvlak. Deze lijst van protocollen wordt gebruikt door het managementvlak:

- Eenvoudig netwerkbeheerprotocol
- Telnet
- Secure Shell-protocol
- File Transfer Protocol
- HyperText Transfer Protocol / Secure HyperText Transfer Protocol
- Trial File Transfer Protocol
- Secure-kopiëren
- TACACS+
- RADIUS
- NetFlow
- Netwerktijdprotocol
- Syslog

Er moeten maatregelen worden genomen om het voortbestaan van de beheers- en controlesystemen tijdens veiligheidsincidenten te waarborgen. Als een van deze vliegtuigen succesvol wordt geëxploiteerd, kunnen alle vliegtuigen in gevaar worden gebracht.

Wachtwoordbeheer

Wachtwoorden regelen de toegang tot hulpmiddelen en hulpmiddelen. Dit wordt bereikt door de definitie een wachtwoord of geheim dat wordt gebruikt om verzoeken voor authenticatie te verklaren. Wanneer een verzoek om toegang tot een bron of apparaat wordt ontvangen, wordt het verzoek ter verificatie van het wachtwoord en de identiteit betwist, en kan toegang worden verleend, geweigerd of beperkt op basis van het resultaat. Als best practice moeten wachtwoorden worden beheerd met een TACACS+ of RADIUS-verificatieserver. Merk op dat een lokaal ingesteld wachtwoord voor bevoorrechte toegang nog steeds nodig is in geval van een storing van de TACACS+ of RADIUS-diensten. Een apparaat kan ook andere wachtwoordinformatie hebben die binnen zijn configuratie aanwezig is, zoals een NTP-toets, SNMP-community-string of Routing Protocol-toets.

Laat geheime opdracht toe wordt gebruikt om het wachtwoord in te stellen dat bevoorrechte administratieve toegang tot het Cisco IOS systeem verleent. **Schakel de** opdracht **geheim** uit in plaats van de opdracht **Wachtwoord** inschakelen. **Schakel** de opdracht **Wachtwoord** in met een zwak coderingsalgoritme.

Als er geen geheimen worden ingesteld en er een wachtwoord wordt ingesteld voor de console-tty lijn, kan het console-wachtwoord worden gebruikt om geprivilegieerde toegang te ontvangen, zelfs vanaf een externe virtuele tty (vty) sessie. Deze actie is vrijwel zeker ongewenst en is een andere reden om de configuratie van een mogelijk geheim te verzekeren.

De opdracht **voor** het wereldwijd configureren **van** de **service wachtwoord-encryptie** leidt de Cisco IOS-software om de wachtwoorden, de Challenge Handshake Authentication Protocol (CHAP) en soortgelijke gegevens te versleutelen die in het configuratiebestand zijn opgeslagen. Een dergelijke codering is handig om te voorkomen dat waarnemers wachtwoorden lezen, zoals wanneer ze naar het scherm kijken bij het verzamelen van een beheerder. Echter, het algoritme dat door de **dienst wachtwoord-encryptie** opdracht wordt gebruikt is een eenvoudig het algoritme van Vigen. De algoritme is niet ontworpen om configuratiebestanden tegen serieuze analyse te beschermen door zelfs licht geavanceerde hackers en moet niet voor dit doel gebruikt worden. Ieder Cisco IOS-configuratiebestand dat versleutelde wachtwoorden bevat, moet met dezelfde zorg worden behandeld als een klare lijst met dezelfde wachtwoorden.

Terwijl dit zwakke encryptie-algoritme niet wordt gebruikt door de **optie geheime** opdracht **inschakelen**, wordt het gebruikt door de opdracht **om** het **wachtwoord** wereldwijd te configureren en door de opdracht voor het configureren van de **wachtwoord**. Wachtwoorden van dit type moeten worden verwijderd en de **optie** openen **dient** het **geheime** opdracht of de functie Verbeterde wachtwoordbeveiliging te worden gebruikt.

Schakel **geheime** opdrachten en de optie Verbeterde wachtwoordbeveiliging in met berichtversie 5 (MD5) voor het hashen van het wachtwoord. Dit algoritme heeft een aanzienlijke publieke recensie gehad en is waarvan bekend is dat het omkeerbaar is. De algoritme is echter onderworpen aan woordenboekaanvallen. Bij een woordenboekaanval probeert een aanvaller elk woord in een woordenboek of een andere lijst met kandidaat-wachtwoorden om een overeenkomst te vinden. Daarom moeten configuratiebestanden veilig worden opgeslagen en alleen worden gedeeld met vertrouwde individuen.

Verbeterde wachtwoordbeveiliging

Met de optie Verbeterde wachtwoordbeveiliging, geïntroduceerd in Cisco IOS-softwarerelease 12.2(8)T, kunt u een beheerder toestaan om MD5-hashing van wachtwoorden te configureren voor de opdracht **gebruikersnaam**. Voor deze optie waren er twee typen wachtwoorden: Type 0, dat een duidelijk tekstwachtwoord is, en Type 7, dat het algoritme van het algoritme van Vigen

gebruikt. De functie Verbeterde wachtwoordbeveiliging kan niet worden gebruikt met protocollen waarvoor het wachtwoord voor de klaring moet worden opgevraagd, zoals het wachtwoord voor de invoer met vaste schijf.

Om een gebruikerswachtwoord met een MD5-hashing te versleutelen, geeft u de **gebruikersnaam** voor de wereldwijde configuratie uit.

```
!

username <name> secret <password>

!
```

Raadpleeg Verbeterde wachtwoordbeveiliging voor meer informatie over deze functie.

Wachtwoord opnieuw instellen

Met de optie Wachtwoord voor opnieuw proberen van inloggen, toegevoegd in Cisco IOS-softwarerelease 12.3(14)T, kunt u na een ingesteld aantal mislukte inlogpogingen een lokale gebruikersaccount uitsluiten. Wanneer een gebruiker is vergrendeld, is hun account geblokkeerd totdat u de account ontgrendelt. Een geautoriseerde gebruiker die is ingesteld met voorkeursniveau 15 kan niet met deze functie worden uitgesloten. Het aantal gebruikers met voorkeursniveau 15 moet tot een minimum worden beperkt.

Als het aantal onsuccesvolle inlogpogingen is bereikt, kunnen geautoriseerde gebruikers zichzelf uit een apparaat vergrendelen. Bovendien kan een kwaadaardige gebruiker een 'denial of service'-conditie (DoS) maken bij herhaalde pogingen om authenticatie met een geldige gebruikersnaam te bewerkstelligen.

Dit voorbeeld toont hoe u de optie Wachtwoord opnieuw instellen kunt inschakelen:

```
!

aaa new-model
aaa local authentication attempts max-fail <max-attempts>
aaa authentication login default local

!

username <name> secret <password>

!
```

Deze optie is ook van toepassing op authenticatiemethoden zoals CHAP en Password Authentication Protocol (PAP).

Geen servicewachtwoord voor het herstellen van

In Cisco IOS-softwarerelease 12.3(14)T en later biedt de functie Geen Wachtwoord-herstel voor service niemand met console toegang tot onveilige toegang tot de apparaatconfiguratie en het wachtwoord. Het staat ook kwaadwillige gebruikers niet toe om de waarde van het configuratieregister en toegang NVRAM te veranderen.

```
!

no service password-recovery

!
```

Cisco IOS-software biedt een wachtwoordherstelprocedure die afhankelijk is van de toegang tot de ROM-monitor (ROMMON) met behulp van de Break-toets tijdens het opstarten van het systeem. In ROMMON kan de software van het apparaat worden opnieuw geladen om een nieuwe systeemconfiguratie te veroorzaken die een nieuw wachtwoord omvat.

De huidige procedure voor het terugwinnen van het wachtwoord stelt iedereen met toegang tot het apparaat en zijn netwerk in staat. De optie No Service Password-recovery voorkomt de voltooiing van de Break-toets en de invoer van ROMMON tijdens het opstarten van het systeem.

Als **geen dienstwachtwoord-herstel** op een apparaat is ingeschakeld, wordt aanbevolen een offline kopie van de apparaatconfiguratie op te slaan en een configuratie archiveringsoplossing te implementeren. Als het nodig is om het wachtwoord van een Cisco IOS apparaat terug te krijgen wanneer deze functie is ingeschakeld, wordt de gehele configuratie verwijderd.

Raadpleeg het voorbeeld Secure ROMMON Configuration voor meer informatie over deze functie.

Ongebruikte services uitschakelen

Als beste beveiligingsmiddel moet elke overbodige dienst worden uitgeschakeld. Deze niet-noodzakelijke services, vooral die welke gebruik maken van User Datagram Protocol (UDP), worden niet vaak voor legitieme doeleinden gebruikt, maar kunnen wel worden gebruikt om DoS en andere aanvallen te starten die anders zijn voorkomen door pakketfiltering.

De kleine TCP- en UDP-services moeten worden uitgeschakeld. Deze diensten omvatten:

- echo (poortnummer 7)
- teruggooi (havennummer 9)
- overdag (poortnummer 13)
- chargen (haven nummer 19)

Hoewel misbruik van kleine diensten kan worden voorkomen of minder gevaarlijk kan worden gemaakt door het opstellen van toegangslijsten tegen spoofing, moeten de diensten worden uitgeschakeld op elk apparaat dat binnen het netwerk toegankelijk is. De kleine services worden standaard uitgeschakeld in Cisco IOS-softwarereleases 12.0 en hoger. In eerdere software kunnen de **geen service-partp-small-servers** en **geen service-udp-small-servers** global configuratie opdrachten worden uitgegeven om ze uit te schakelen.

Dit is een lijst van extra diensten die moeten worden uitgeschakeld als ze niet worden gebruikt:

- Geef de opdracht **geen ip vinger** uit om Finger-service uit te schakelen. Cisco IOS-softwarerelease later dan 12.1(5) en 12.1(5)T schakelt deze service standaard uit.
- Geef de opdracht voor het configureren van de **geen IP bootstrap server** uit om Bootstrap Protocol (BOOTP) uit te schakelen.

- In Cisco IOS-softwarerelease 12.2(8)T en later **geeft** u de **ip** dhcp-functie **uit** om de opdracht in de mondiale configuratie uit te schakelen om BOTP uit te schakelen. Hierdoor worden Dynamic Host Configuration Protocol (DHCP) ingeschakeld.

- DHCP-services kunnen worden uitgeschakeld als DHCP-relais niet nodig is. Geef de **opdracht geen service dhcp** uit in de mondiale configuratie.

- Geef de opdracht **mop niet** meer **aan** in de interfaceconfiguratiemodus om de onderhoudsdienst van het Protocol (MOP) uit te schakelen.

- Geef de opdracht **voor** mondiale configuratie op **geen ip-domein-lookup** om de afwikkelingsservices van het Domain Name System (DNS) uit te schakelen.

- Geef de opdracht **geen service pad** uit in de mondiale configuratiemodus om Packet Assembler/Disassembler (PAD) dienst uit te schakelen, die voor X.25-netwerken wordt gebruikt.

- De HTTP-server kan worden uitgeschakeld met de opdracht **geen ip http server** in de mondiale configuratiemodus en de Secure HTTP (HTTPS)-server kan worden uitgeschakeld met de opdracht voor **de** wereldwijde configuratie **van de geen ip http Secure-server**.

- Tenzij Cisco IOS de apparaten configuraties van het netwerk tijdens opstarten terugkrijgen, moet het **geen dienst configuratie** mondiaal configuratiebevel worden gebruikt. Dit voorkomt het Cisco IOS apparaat van een poging om een configuratiebestand in het netwerk met TFTP te vinden.

- Cisco Discovery Protocol (CDP) is een netwerkprotocol dat wordt gebruikt om andere CDP-enabled-apparaten voor nabijheid en netwerktopologie te ontdekken. CDP kan worden gebruikt door Network Management Systems (NMS) of tijdens de probleemoplossing. CDP moet worden uitgeschakeld op alle interfaces die zijn aangesloten op onvertrouwde netwerken. Dit wordt bereikt zonder **cdp** interfaceopdracht. Als alternatief kan CDP mondiaal worden uitgeschakeld met de opdracht **geen cdp-**configuratie. Merk op dat CDP door een kwaadaardige gebruiker kan worden gebruikt voor verkenning en netwerkmapping.

- Link Layer Discovery Protocol (LLDP) is een IEEE-protocol dat in 802.1AB wordt gedefinieerd. LLDP lijkt op CDP. Dit protocol maakt echter interoperabiliteit mogelijk tussen andere apparaten die CDP niet ondersteunen. LLDP moet op dezelfde manier worden behandeld als CDP en op alle interfaces worden uitgeschakeld die verbinding maken met onvertrouwde netwerken. Om dit te bereiken, geeft u de **opdracht** voor de configuratie van de interface uit **dat er geen** opdrachten **voor de vloeibaarheid worden verzonden** en dat er **geen** opdrachten voor de **taakconfiguratie worden ontvangen**. Geef de **opdracht voor** mondiale configuratie **niet-run uit** om LLDP mondiaal uit te schakelen. LLDP kan ook door een kwaadaardige gebruiker worden gebruikt voor verkenning en netwerkmapping.

- Voor switches die flitser ondersteunen om te beginnen, kan de beveiliging worden verbeterd door vanaf flitser te starten en flitser uit te schakelen met de configuratieopdracht "no sdflash".

EXEC-timeout

Om het interval in te stellen dat de EXEC opdrachttolk wacht op de gebruikerstoets voordat deze een sessie beëindigt, geeft u de configuratieopdracht voor de **exec-timeout** lijn uit. De opdracht **exec-timeout** moet worden gebruikt om sessies op te loggen of op tty lijnen die leeg zijn. De standaardinstelling is dat de sessies worden losgekoppeld na tien minuten inactiviteit.

```
!

line con 0
exec-timeout <minutes> [seconds]
line vty 0 4
exec-timeout <minutes> [seconds]
!
```

Keepalives voor TCP-sessies

De opdrachten **voor** de wereldwijde configuratie **van de** service **tcp-keepalives-in** en **service** TCP-keepalives kunnen een apparaat TCP-keepalives voor TCP-sessies verzenden. Deze configuratie moet worden gebruikt om TCP-keepalives op inkomende verbindingen naar het apparaat en uitgaande verbindingen van het apparaat in te schakelen. Dit waarborgt dat het apparaat op het verafgelegen einde van de verbinding nog toegankelijk is en dat de half-open of weesverbindingen van het lokale Cisco IOS apparaat worden verwijderd.

```
!

service tcp-keepalives-in
service tcp-keepalives-out
!
```

Beheerinterfacegebruik

Het managementvlak van een apparaat is toegankelijk in-band of buiten-band op een fysieke of logische beheersinterface. Idealiter zowel in-band- als out-of-band beheertoegang voor elk netwerkapparaat bestaat zodat het managementvlak tijdens netwerkstoringen toegankelijk is.

Eén van de meest gebruikelijke interfaces die gebruikt worden voor toegang in-band tot een apparaat is de logische loopback interface. De interfaces zijn altijd omhoog, terwijl de fysieke interfaces de staat kunnen veranderen, en de interface kan potentieel niet toegankelijk zijn. Het wordt aanbevolen een loopback-interface aan elk apparaat toe te voegen als een beheersinterface en deze uitsluitend voor het managementvlak te gebruiken. Dit stelt de beheerder in staat om beleid op het gehele netwerk toe te passen voor het managementvlak. Zodra de loopback interface op een apparaat is geconfigureerd, kan deze door de protocollen van het beheersvliegtuig, zoals SSH, SNMP en syslog, worden gebruikt om verkeer te verzenden en ontvangen.

```
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.0
!
```

Geheugenmeldingen

Met de melding van de drempel voor het functiegeheugen, toegevoegd aan Cisco IOS-softwarerelease 12.3(4)T, kunt u de geheugenomstandigheden op een apparaat beperken. Voor deze functie worden twee methoden gebruikt: Geheugenmelding en geheugenreservering

De melding van de geheugendrempel genereert een logbericht om aan te geven dat het vrije geheugen op een apparaat lager is dan de ingestelde drempel. Dit configuratievoorbeeld toont hoe deze eigenschap met de **geheugenvrije laag-watermark** mondiale configuratieopdracht mogelijk te maken. Dit stelt een apparaat in staat om een waarschuwing te genereren wanneer beschikbaar vrij geheugen onder de gespecificeerde drempel valt, en opnieuw wanneer beschikbaar vrij geheugen stijgt tot vijf procent hoger dan de opgegeven drempel.

```
!

memory free low-watermark processor <threshold>
memory free low-watermark io <threshold>
!
```

Geheugenreservering wordt gebruikt zodat er voldoende geheugen beschikbaar is voor kritische meldingen. Dit configuratievoorbeeld laat zien hoe u deze functie kunt activeren. Dit waarborgt dat de beheerprocessen blijven functioneren wanneer het geheugen van het apparaat is uitgeput.

```
!
memory reserve critical <value> !
```

Raadpleeg Geheugendrempels voor meer informatie over deze functie.

Meldingen van CPU-drempels

Inleiding in Cisco IOS-softwarerelease 12.3(4)T, kunt u met de voorziening voor melding van CPU-drempels detecteren en hiervan op de hoogte worden gesteld wanneer de CPU-lading op een apparaat een ingestelde drempel overschrijdt. Wanneer de drempel wordt overschreden, genereert het apparaat een SNMP-trap en verstuurt het een bericht. Er worden twee opslagmethoden voor CPU's ondersteund op Cisco IOS-software: Stijgende drempel en dalende drempel.

Deze voorbeeldconfiguratie toont hoe de stijgende en dalende drempels die een waarschuwing van de cpu van de drempelwaardemelding veroorzaken kunnen worden ingeschakeld:

```
!

snmp-server enable traps cpu threshold
!

snmp-server host <host-address> <community-string> cpu
!

process cpu threshold type <type> rising <percentage> interval <seconds>
[falling <percentage> interval <seconds>]
process cpu statistics limit entry-percentage <number> [size <seconds>]
!
```

Raadpleeg de melding *van de* CPU-drempelwaarde voor meer informatie over deze functie.

Reserve-geheugen voor console-toegang

In Cisco IOS-softwarerelease 12.4(15)T en hoger kan de Reserve Geheugen voor Console Access Functie worden gebruikt om genoeg geheugen te reserveren om console-toegang tot een Cisco IOS-apparaat te verzekeren voor administratieve doeleinden en voor het oplossen van problemen. Deze optie is vooral nuttig wanneer het apparaat weinig geheugen heeft. U kunt de opdracht voor **de** configuratie van de **geheugenreserveconcern** uitgeven om deze functie in te schakelen. Dit voorbeeld vormt een Cisco IOS apparaat om 4096 kilobytes voor dit doel te reserveren.

```
!
memory reserve console 4096
!
```

Raadpleeg het gedeelte Reserve *Memory for* Console Access voor meer informatie over deze functie.

Geheugendetectie

De technologie die in Cisco IOS-softwarerelease 12.3(8)T1 is geïntroduceerd, stelt u in de functie Geheugendetectie van lekken op een apparaat in staat om geheugenlekken te detecteren. Memory Leak Detector kan lekkages vinden in alle geheugenpools, pakketbuffers en stukjes. Geheugenlekken zijn statische of dynamische toewijzingen van geheugen die geen bruikbaar doel dienen. Deze eigenschap concentreert zich op geheugentoewijzingen die dynamisch zijn. U kunt de opdracht **Show memory debug leaks** EXEC gebruiken om te detecteren of er een geheugenlek bestaat.

Bufferoverloop: Detectie en correctie van corruptie in de zone

In Cisco IOS-softwarerelease 12.3(7)T en later, de bufferoverloop: De detectie en correctie van de optie voor corruptie in de redundantie van de zone kan door op een apparaat worden ingeschakeld om een overloop van het geheugenblok te detecteren en te corrigeren en om de bewerking voort te zetten.

Deze mondiale configuratieopdrachten kunnen worden gebruikt om deze functie in te schakelen. Indien geconfigureerd kan de opdracht **Show memory overflow** worden gebruikt om de detectie- en correctiestatistieken van de buffer weer te geven.

```
!
exception memory ignore overflow io
exception memory ignore overflow processor
!
```

Uitgebreide verzameling van crashinformatie

De functie Uitgebreide crashinformatie File Collector verwijdert automatisch oude crashinformatie bestanden. Deze functie, toegevoegd in Cisco IOS-softwarerelease 12.3(11)T, maakt het mogelijk dat een apparaat ruimte terugwint om nieuwe crashinformatie-bestanden te maken wanneer het apparaat crasht. Met deze functie kan ook het aantal crashinformatie-bestanden worden opgeslagen.

```
!
exception crashinfo maximum files <number-of-files>
!
```

Netwerktijdprotocol

Het Network Time Protocol (NTP) is geen bijzonder gevaarlijke service, maar elke overbodige service kan een aanvalsvector vertegenwoordigen. Als NTP wordt gebruikt, is het belangrijk om expliciet een vertrouwde tijdbron te configureren en juiste authenticatie te gebruiken. Nauwkeurige en betrouwbare tijd is vereist voor syslig-doeleinden, zoals tijdens forensisch onderzoek van mogelijke aanvallen, en voor succesvolle VPN-connectiviteit wanneer dit afhankelijk is van certificaten voor Fase 1-verificatie.

- **NTP Time Zone** - Wanneer u NTP configureren moet de tijdzone worden ingesteld zodat tijdstempels accuraat gecorreleerd kunnen worden. Er zijn gewoonlijk twee benaderingen om de tijdzone voor apparaten in een netwerk met een mondiale aanwezigheid te vormen. Eén methode is om alle netwerkapparaten aan te passen met de gecoördineerde Universal Time (UTC) (voorheen Greenwich Mean Time (GMT)). De andere benadering is om netwerkapparaten met de lokale tijdzone te configureren. Meer informatie over deze optie is te vinden in "kloktijd" in de productdocumentatie van Cisco.

- **NTP-verificatie** - Als u de NTP-verificatie configureren biedt deze de garantie dat NTP-berichten worden uitgewisseld tussen vertrouwde NTP-peers.

Monsterconfiguratie met NTP-verificatie:

Cliënt:

```
(config)#ntp authenticate
(config)#ntp authentication-key 5 md5 ciscotime
(config)#ntp trusted-key 5
(config)#ntp server 172.16.1.5 key 5
```

Server:

```
(config)#ntp authenticate
(config)#ntp authentication-key 5 md5 ciscotime
(config)#ntp trusted-key 5
```

Smart Install

De best practices voor beveiliging rond de optie Cisco Smart Install (SMI) zijn afhankelijk van de manier waarop de functie in een specifieke klantomgeving wordt gebruikt. Cisco maakt een onderscheid tussen deze gebruiksgevallen:

- Klanten die de functie Smart Install niet gebruiken.
- Klanten die de functie Smart Install alleen gebruiken voor een nul-aanraking implementatie.
- Klanten die gebruik maken van de Smart Install-optie voor meer dan nul-aanraking implementatie (configuratie en beeldbeheer).

In deze delen wordt elk scenario uitvoerig beschreven:

- Klanten die de functie Smart Install niet gebruiken.
- Klanten die de functie Cisco Smart Install niet gebruiken en een release van Cisco IOS en Cisco IOS XE software uitvoeren waar de opdracht beschikbaar is, moeten de functie Smart Install zonder opdracht uitschakelen.

Opmerking: De opdracht **Vstack** is geïntroduceerd in Cisco IOS release 12.2(55)SE03.

Dit is voorbeelduitvoer van het bevel van **show** vstack op een Cisco Catalyst switch met de optie Smart Install client uitgeschakeld:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Klanten die gebruik maken van de Smart Install-optie alleen voor aanraakacties

Schakel de Smart Install client-functionaliteit uit nadat de installatie zonder aanraking is voltooid of gebruik de opdracht **No Vstack**.

Om het **geen vstack**-opdracht in het netwerk te propageren, gebruikt u een van deze methoden:

- Voer het **geen** vstack-opdracht in op alle clientswitches handmatig of met een script.
- Voeg de **geen** vstack-opdracht toe als onderdeel van de Cisco IOS-configuratie die in elke Smart Install client wordt geduwd als onderdeel van de installatie zonder aanraking.
- In de releases die de opdracht **niet** ondersteunen (Cisco IOS release 12.2(55)SE02 en eerdere releases) past u een toegangscontrolelijst (ACL) toe op clientswitches om het verkeer op TCP poort 4786 te blokkeren.

Om de Smart Install client-functionaliteit later in te schakelen, voert u de vstack-opdracht in op alle clientswitches handmatig of met een script.

Klanten die gebruik maken van de Smart Install-functie voor meer dan nulpunch implementaties

In het ontwerp van een Smart Install-architectuur moet ervoor worden gezorgd dat de IP-adresruimte van de infrastructuur niet toegankelijk is voor onbetrouwbare partijen. In releases die de opdracht niet ondersteunen, zorg er dan voor dat alleen de Smart Install-regisseur TCP-connectiviteit heeft op alle Smart Install-clients in poort 4786.

De beheerders kunnen deze veiligheidsbeste praktijken voor Cisco Smart Install implementaties op getroffen apparaten gebruiken:

- Interface ACL's
- Toezicht besturingsplane (CoPP). Deze optie is niet beschikbaar in alle Cisco IOS-softwarereleases.

Dit voorbeeld toont een interface ACL met het Smart Install regisseur IP-adres als 10.10.10.1 en het Smart Install client IP-adres als 10.10.10.200:

```
ip access-list extended SMI_HARDENING_LIST
Permit tcp host 10.10.10.1 host 10.10.10.200 eq 4786
deny tcp any any eq 4786
permit ip any any
```

Deze ACL moet op alle IP interfaces op alle cliënten worden uitgevoerd. Hij kan ook via de regisseur worden geduwd wanneer de schakelaars voor het eerst worden ingezet.

Om de toegang tot alle klanten binnen de infrastructuur verder te beperken, kunnen beheerders deze veiligheidsbeste praktijken op andere apparaten in het netwerk gebruiken:

- Toegangscontrolelijsten voor infrastructuur (iACL's)
- VLAN Access Control List (VACL's)

Beperkte toegang tot het netwerk met infrastructuur ACL's

Bewerkt om onbevoegde directe communicatie met netwerkapparaten te voorkomen, zijn infrastructuurtoegangscontrolelijsten (iACL's) een van de meest kritische beveiligingscontroles die in netwerken kunnen worden uitgevoerd. Infrastructuur ACL's maken gebruik van het idee dat bijna al het netwerkverkeer het netwerk overbrengt en niet bestemd is voor het netwerk zelf.

Een iACL wordt gebouwd en toegepast om verbindingen van hosts of netwerken te specificeren die aan netwerkapparaten moeten worden toegestaan. De meest voorkomende voorbeelden van deze soorten verbindingen zijn eBGP, SSH en SNMP. Nadat de vereiste verbindingen zijn toegestaan, wordt al het andere verkeer naar de infrastructuur expliciet geweigerd. Al het transitoverkeer dat het netwerk oversteekt en niet bestemd is voor infrastructurele voorzieningen is dan uitdrukkelijk toegestaan.

De door iACL's geboden bescherming is relevant voor zowel het beheer- als het controlegebied. De implementatie van iACL's kan worden vergemakkelijkt door het gebruik van een specifieke adressering voor netwerkinfrastructuurauts. *Raadpleeg* Een beveiligingsgerichte benadering van IP-adressering voor meer informatie over de beveiligingsimplicaties van IP-adressering.

Dit voorbeeld iACL-configuratie illustreert de structuur die als uitgangspunt moet worden gebruikt wanneer u het iACL-implementatieproces start:

```
!

ip access-list extended ACL-INFRASTRUCTURE-IN
!
!--- Permit required connections for routing protocols and
!--- network management
!

permit tcp host <trusted-ebgp-peer> host <local-ebgp-address> eq 179
permit tcp host <trusted-ebgp-peer> eq 179 host <local-ebgp-address>
permit tcp host <trusted-management-stations> any eq 22
permit udp host <trusted-netmgmt-servers> any eq 161
!
!--- Deny all other IP traffic to any network device
!

deny ip any <infrastructure-address-space> <mask>
!
!--- Permit transit traffic
!

permit ip any any
!
```

Eenmaal gemaakt moet iACL worden toegepast op alle interfaces die op niet-infrastructuren zijn gericht. Dit omvat interfaces die verbinding maken met andere organisaties, externe toegangssegmenten, gebruikerssegmenten en segmenten in datacenters.

Raadpleeg Protecting Your Core: Toegangscontrolelijsten voor bescherming van de infrastructuur voor meer informatie over ACL's van de infrastructuur.

ICMP-pakketfiltering

Het Internet Control Message Protocol (ICMP) is ontworpen als een IP-controleprotocol. Als dergelijk, kunnen de berichten die het transporteert vergaande implicaties hebben aan de TCP- en IP-protocollen in het algemeen. Terwijl de middelen van het netwerk het oplossen van problemen **pingelen** en **tracoute** ICMP gebruiken, is de externe ICMP connectiviteit zelden nodig voor het juiste beheer van een netwerk.

Cisco IOS-software biedt functionaliteit om ICMP-berichten door naam of type en code specifiek te filteren. Dit voorbeeld ACL, dat moet worden gebruikt met de Access Control Insights (ACE's) uit vorige voorbeelden, maakt gebruik van vertrouwde beheerstations en NMS-servers mogelijk en blokkeert alle andere ICMP-pakketten:

```
!

ip access-list extended ACL-INFRASTRUCTURE-IN
!
!--- Permit ICMP Echo (ping) from trusted management stations and servers
!

permit icmp host <trusted-management-stations> any echo
permit icmp host <trusted-netmgmt-servers> any echo
!
!--- Deny all other IP traffic to any network device
!

deny ip any <infrastructure-address-space> <mask>
!
!--- Permit transit traffic
!

permit ip any any
!
```

IP-fragmentaties filteren

Het filterproces voor gefragmenteerde IP-pakketten kan een uitdaging voor beveiligingsapparaten betekenen. Dit komt doordat de informatie van Layer 4 die wordt gebruikt om TCP- en UDP-pakketten te filteren alleen in het eerste fragment aanwezig is. Cisco IOS-software gebruikt een specifieke methode om niet-initiële fragmenten te controleren met geconfigureerde toegangslijsten. Cisco IOS-software evalueert deze niet-initiële fragmenten tegen de ACL en negeert alle Layer 4-filterinformatie. Dit veroorzaakt dat niet-initiële fragmenten alleen op Layer 3 van een geconfigureerde ACE worden beoordeeld.

In deze voorbeeldconfiguratie, als een TCP-pakket bestemd voor **192.168.1.1** op **poort 22** gefragmenteerd is in transit, wordt het aanvankelijke fragment gedaald zoals verwacht door de tweede ACE gebaseerd op Layer 4 informatie in het pakket. Alle resterende (niet-initiële) fragmenten zijn echter toegestaan door de eerste ACE-schijf die volledig is gebaseerd op Layer 3-informatie in het pakket en de ACE-schijf. Dit scenario wordt in deze configuratie getoond:

```
!

ip access-list extended ACL-FRAGMENT-EXAMPLE
permit tcp any host 192.168.1.1 eq 80
deny tcp any host 192.168.1.1 eq 22
```

```
!
```

Vanwege de niet-intuïtieve aard van fragmentatieverwerking worden IP-fragmenten door ACL's vaak per ongeluk toegestaan. Fragmentation wordt ook vaak gebruikt in pogingen om detectie door inbraakdetectiesystemen te ontwijken. Het is om deze redenen dat IP-fragmenten vaak in aanvallen worden gebruikt en waarom ze expliciet moeten worden gefilterd boven aan een geconfigureerde iACL's. Dit voorbeeld ACL omvat uitgebreid filteren van IP fragmenten. De functionaliteit van dit voorbeeld moet worden gebruikt in samenhang met de functionaliteit van de voorgaande voorbeelden.

```
!

ip access-list extended ACL-INFRASTRUCTURE-IN
!
!--- Deny IP fragments using protocol-specific ACEs to aid in
!--- classification of attack traffic
!

deny tcp any any fragments
deny udp any any fragments
deny icmp any any fragments
deny ip any any fragments
!
!--- Deny all other IP traffic to any network device
!

deny ip any <infrastructure-address-space> <mask>
!
!--- Permit transit traffic
!

permit ip any any
!
```

Raadpleeg Toegangscontrolelijsten en IP-fragmentaties voor meer informatie over de manier waarop ACL gefragmenteerde IP-pakketten verwerkt.

ACL-ondersteuning voor filtering van IP-opties

Ondersteuning van Cisco IOS-softwarerelease 12.3(4)T voor het gebruik van ACL's om IP-pakketten te filteren op basis van de IP-opties die in het pakket zitten. IP-opties bieden een beveiligingsprobleem voor netwerkapparaten aan, omdat deze opties als uitzondering-pakketten moeten worden verwerkt. Hiervoor is een niveau van CPU-inspanning nodig dat niet nodig is voor standaardpakketten die het netwerk oversteken. De aanwezigheid van IP-opties in een pakje kan ook duiden op een poging om de beveiligingsinstellingen in het netwerk te ondermijnen of op een andere manier de doorvoerkenmerken van een pakje te wijzigen. Om deze redenen moeten IP-pakketten met opties worden gefilterd aan de rand van het netwerk.

Dit voorbeeld moet met de ACE's van vorige voorbeelden worden gebruikt om het volledige filteren van IP pakketten op te nemen die IP opties bevatten:

```
!

ip access-list extended ACL-INFRASTRUCTURE-IN
!
!--- Deny IP packets containing IP options
!
```

```
deny ip any any option any-options
!
!--- Deny all other IP traffic to any network device
!

deny ip any <infrastructure-address-space> <mask>
!
!--- Permit transit traffic
!

permit ip any any
!
```

ACL-ondersteuning voor filter op TTL-waarde

Cisco IOS-softwarerelease 12.4(2)T heeft ACL-ondersteuning toegevoegd aan filter voor IP-pakketten op basis van de TXT-waarde (Time to Live). De TTL-waarde van een IP-datagram wordt door elk netwerkapparaat verlaagd als pakketstromen van bron naar bestemming. Hoewel de aanvankelijke waarden door het besturingssysteem verschillen, moet het pakketje bij TTL of a Packet op nul worden gebracht. Het apparaat dat de TTL tot nul vermindert, en daarom het pakje daalt, wordt vereist om een ICMP Tijd Overgedraaid bericht aan de bron van het pakket te genereren en te verzenden.

Het genereren en doorgeven van deze berichten is een uitzonderingsproces. Routers kunnen deze functie uitvoeren wanneer het aantal IP-pakketten dat moet worden verlopen laag is, maar als het aantal te verlopen pakketten hoog is, kunnen de generatie en transmissie van deze berichten alle beschikbare CPU-bronnen gebruiken. Dit is een DoS aanval-vector. Dit is de reden dat de apparaten tegen de aanvallen van Dos moeten worden geharde die een hoog tempo van IP pakketten gebruiken die zullen verlopen.

Aanbevolen wordt dat organisaties IP-pakketten met lage TTL-waarden filteren aan de rand van het netwerk. Volledig filteren van pakketten met TTL-waarden die niet genoeg zijn om het netwerk over te steken verzacht de dreiging van op TTL gebaseerde aanvallen.

Dit voorbeeld ACL-filters filtert met TTL-waarden van minder dan zes. Dit biedt bescherming tegen TTL-vervalaanvallen voor netwerken tot vijf hop in breedte.

```
!

ip access-list extended ACL-INFRASTRUCTURE-IN
!
!--- Deny IP packets with TTL values insufficient to traverse the network
!

deny ip any any ttl lt 6
!
!--- Deny all other IP traffic to any network device
!

deny ip any <infrastructure-address-space> <mask>
!
!--- Permit transit traffic
!

permit ip any any
!
```

Opmerking: Sommige protocollen maken legitiem gebruik van pakketten met lage TTL-waarden. eBGP is zo'n protocol. Raadpleeg de TTL-lijst met gegevens over identificatie en beperking van aanvallen bij beëindiging van het TTL-bestand voor meer informatie over het beperken van op TL gebaseerde aanvallen bij EXP.

Raadpleeg ACL-ondersteuning voor filtering op TTL-waarde voor meer informatie over deze functie.

Secure Interactive Management-sessies

Beheersessies naar apparaten waarmee u informatie over een apparaat en de bewerkingen kunt bekijken en verzamelen. Als deze informatie aan een kwaadwillige gebruiker wordt verstrekt, kan het apparaat het doel van een aanval worden, gecompromitteerd, en gebruikt om extra aanvallen uit te voeren. Iedereen die bevoorrechte toegang heeft tot een apparaat heeft de mogelijkheid om volledig administratief te controleren. Het is van het grootste belang dat beheersessies worden beveiligd om informatieverstrekking en ongeoorloofde toegang te voorkomen.

Bescherming van besturingsplane

In Cisco IOS-softwarerelease 12.4(6)T en hoger staat de Protection (MPP) van het functiebeheersplan een beheerder toe om te beperken op welke interfaces-beheerverkeer door een apparaat kan worden ontvangen. Dit geeft de beheerder extra controle over een apparaat en hoe het apparaat wordt benaderd.

Dit voorbeeld laat zien hoe u MPP in staat moet stellen om alleen SSH en HTTPS op de Gigabit Ethernet0/1-interface toe te staan:

```
!

control-plane host
management-interface GigabitEthernet 0/1 allow ssh https
!
```

Raadpleeg de Bescherming *van* Management Plane voor meer informatie over MPP.

Bescherming van besturingsplane

CPPr (Control Plane Protection) bouwt voort op de functionaliteit van de controle van vliegtuigen om het vliegtuigverkeer dat bestemd is voor de routeprocessor van het IOS-apparaat te beperken en te controleren. CPPr, toegevoegd in Cisco IOS-softwarerelease 12.4(4)T, verdeelt het bedieningspaneel in afzonderlijke categorieën die bekend staan als subinterfaces. Drie subinterfaces bestaan: Host, Transit en CEF-Exception. Daarnaast bevat CPPr deze aanvullende beschermingsinrichtingen:

- **Poortfilterfunctie** - Deze functie biedt toezicht op en het neerzetten van pakketten die naar gesloten of niet-luisterende TCP- en UDP-poorten gaan.

- **Wachtrij-drempelbeleidsfunctie** - Deze optie beperkt het aantal pakketten voor een bepaald protocol dat is toegestaan in de IP-invoerwachtrij van het besturingsplane.

CPPr staat een beheerder toe om verkeer te classificeren, te politiseren en te beperken dat naar een apparaat voor beheersdoeleinden met de gastheer subinterface wordt verzonden.

Voorbeelden van pakketten die voor de categorie van de gastheer subinterface worden geclassificeerd omvatten beheerverkeer zoals SSH of Telnet en routingprotocollen.

> Opmerking: CPPr ondersteunt IPv6 niet en is beperkt tot het IPv4-invoerpad.

Raadpleeg de Functiehandleiding voor bescherming van het besturingsplane - 12.4T en begrip van het besturingsplane voor meer informatie over de Cisco CPPr-functie.

Encrypt Management-sessies

Omdat informatie in een interactieve beheersessie kan worden openbaar gemaakt, moet dit verkeer worden versleuteld zodat een kwaadwillige gebruiker geen toegang kan krijgen tot de verzonden gegevens. Verkeersencryptie maakt een beveiligde externe toegangsverbinding naar het apparaat mogelijk. Als het verkeer voor een beheersessie via het netwerk in duidelijke tekst wordt verzonden, kan een aanvaller gevoelige informatie over het apparaat en het netwerk verkrijgen.

Een beheerder kan een gecodeerde en veilige verbinding van het afstandstoegangsbeheer met een apparaat maken met de eigenschappen SSH of HTTPS (Secure Hypertext Transfer Protocol). Cisco IOS-software ondersteunt SSH versie 1.0 (SSHv1), SSH versie 2.0 (SSHv2) en HTTPS die Secure Socket Layer (SSL) en Transport Layer Security (TLS) voor verificatie en gegevensencryptie gebruikt. SSHv1 en SSHv2 zijn niet compatibel. SSHv1 is onveilig en niet gestandaardiseerd, dus wordt het niet aanbevolen als SSHv2 een optie is.

Cisco IOS-software ondersteunt ook het Secure Kopie Protocol (SCP), dat een versleutelde en beveiligde verbinding toestaat om apparaatconfiguraties of softwareafbeeldingen te kopiëren. SCP is afhankelijk van SSH. Deze voorbeeldconfiguratie maakt SSH op een Cisco IOS-apparaat mogelijk:

```
!

ip domain-name example.com
!

crypto key generate rsa modulus 2048
!

ip ssh time-out 60
ip ssh authentication-retries 3
ip ssh source-interface GigabitEthernet 0/1
!

line vty 0 4
transport input ssh
!
```

Dit configuratievoorbeeld maakt de diensten van SCP mogelijk:

```
!

ip scp server enable
!
```

Dit is een configuratievoorbeeld voor HTTPS-services:

```
!

crypto key generate rsa modulus 2048
!

ip http secure-server
!
```

Raadpleeg Secure Shell *op routers en switches* die Cisco IOS en Secure Shell (SSH) FAQ *uitvoeren* voor meer informatie over de Cisco IOS-software SSH-functie.

SSHv2

Met de SSHv2-ondersteuningsfunctie die in Cisco IOS-softwarerelease 12.3(4)T is geïntroduceerd, kan een gebruiker SSHv2 configureren. (Ondersteuning van SSHv1 werd geïmplementeerd in een eerdere release van Cisco IOS-software.) SSH loopt bovenop een betrouwbare transportlaag en biedt sterke authenticatie- en encryptiemogelijkheden. Het enige betrouwbare transport dat voor SSH wordt gedefinieerd is TCP. SSH biedt een middel om veilig toegang te krijgen tot en opdrachten op een andere computer of apparaat via een netwerk veilig uit te voeren. Met de optie Secure Kopie Protocol (SCP) die via SSH wordt getunneld, kunnen bestanden veilig worden overgedragen.

Als de opdracht IP **versie 2** niet expliciet wordt geconfigureerd, maakt Cisco IOS SSH versie 1.9 mogelijk. SSH versie 1.9 maakt zowel SSHv1- als SSHv2-verbindingen mogelijk. SSHv1 wordt als onveilig beschouwd en kan nadelige effecten op het systeem hebben. Als SSH is ingeschakeld, wordt aanbevolen SSHv1 uit te schakelen door de opdracht **ip ssh versie 2** te gebruiken.

Deze voorbeeldconfiguratie maakt SSHv2 (met SSHv1 uitgeschakeld) mogelijk op een Cisco IOS-apparaat:

```
!

hostname router

!

ip domain-name example.com

!

crypto key generate rsa modulus 2048

!

ip ssh time-out 60
ip ssh authentication-retries 3
ip ssh source-interface GigabitEthernet 0/1

!

ip ssh version 2

!

line vty 0 4
transport input ssh
```

```
!
```

Raadpleeg Ondersteuning van Secure Shell, versie 2, voor meer informatie over het gebruik van SSHv2.

Verbeteringen in SSHv2 voor RSA-toetsen

Cisco IOS SHv2 ondersteunt toetsenbord-interactieve en op wachtwoord gebaseerde verificatiemethoden. Verbeteringen in SSHv2 voor RSA-toetsen ondersteunen ook op RSA gebaseerde openbare basisverificatie voor de client en server.

Voor gebruikersverificatie gebruikt RSA-gebaseerde gebruikersverificatie een privaat/openbaar sleutelpaar dat bij elke gebruiker is gekoppeld voor verificatie. De gebruiker moet een privaat/publiek zeer belangrijk paar op de client genereren en een openbare sleutel op de Cisco IOS SSH server configureren om de verificatie te voltooien.

Een SSH-gebruiker die probeert de aanmeldingsgegevens in te voeren, geeft een versleutelde handtekening met de particuliere sleutel. De handtekening en de openbare sleutel van de gebruiker worden naar de SSH-server gestuurd voor authenticatie. De SSH server compileert een hash over de openbare sleutel die door de gebruiker wordt geleverd. De hash wordt gebruikt om te bepalen of de server een melding heeft die aansluit. Als er een match is gevonden, wordt de op RSA gebaseerde berichtverificatie uitgevoerd met de openbare sleutel. Vandaar dat de gebruiker op basis van de versleutelde handtekening voor authentiek verklaard of toegang geweigerd is.

Voor serververificatie moet de Cisco IOS SSH-client een host-toets voor elke server toewijzen. Wanneer de client probeert een SSH-sessie met een server op te zetten, ontvangt de client de handtekening van de server als onderdeel van het belangrijke uitwisselingsbericht. Als de strikte host key check flag op de client is ingeschakeld, controleert de client of deze de host key entry heeft die overeenkomt met de vooraf ingestelde server. Als een match gevonden wordt, probeert de client de signatuur te valideren met de server host-toets. Indien de server beveiligd is, gaat de sessieinstelling verder; anders wordt het beëindigd en wordt een **mislukt** bericht door **serververificatie** weergegeven.

Deze voorbeeldconfiguratie maakt het gebruik van RSA-toetsen met SSHv2 op een Cisco IOS-apparaat mogelijk:

```
!
! Configure a hostname for the device
!

hostname router
!
! Configure a domain name
!

ip domain-name cisco.com
!
! Specify the name of the RSA key pair (in this case, "sshkeys") to use for SSH
!

ip ssh rsa keypair-name sshkeys
!
! Enable the SSH server for local and remote authentication on the router using
! the "crypto key generate" command
! For SSH version 2, the modulus size must be at least 768 bits
```

```
!

crypto key generate rsa usage-keys label sshkeys modulus 2048
!
! Configure an ssh timeout (in seconds)
!
! The following enables a timeout of 120 seconds for SSH connections
!

ip ssh time-out 120
!
! Configure a limit of five (5) authentication retries
!

ip ssh authentication-retries 5
!
! Configure SSH version 2
!

ip ssh version 2
!
```

Raadpleeg Verbeteringen in Secure Shell versie 2 voor RSA-toetsen voor meer informatie over het gebruik van RSA-toetsen met SSHv2.

Deze voorbeeldconfiguratie stelt de Cisco IOS SSH-server in staat om op RSA gebaseerde gebruikersverificatie uit te voeren. De gebruikersverificatie is succesvol als de openbare RSA-toets die op de server is opgeslagen, wordt geverifieerd met het publiek of de privé-sleutelpaar dat op de client is opgeslagen.

```
!
! Configure a hostname for the device
!

hostname router
!
! Configure a domain name
!

ip domain-name cisco.com
!
! Generate RSA key pairs using a modulus of 2048 bits
!

crypto key generate rsa modulus 2048
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Configure the SSH username
!

username ssh-user
!
! Specify the RSA public key of the remote peer
!
! You must then configure either the key-string command
```

```
! (followed by the RSA public key of the remote peer) or the
! key-hash command (followed by the SSH key type and version.)
!
```

Raadpleeg De Cisco IOS SSH Server configureren om op RSA gebaseerde gebruikersverificatie uit te voeren voor meer informatie over het gebruik van RSA-toetsen met SSHv2.

Deze voorbeeldconfiguratie stelt de Cisco IOS SSH client in staat om op RSA gebaseerde serververificatie uit te voeren.

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

Raadpleeg De Cisco IOS SSH-client configureren om RSA-gebaseerde serververificatie uit te voeren voor meer informatie over het gebruik van RSA-toetsen met SSHv2.

Console- en AUX-poorten

In Cisco IOS apparaten, zijn de console en de hulphavens (AUX) asynchrone lijnen die voor lokale en verre toegang tot een apparaat kunnen worden gebruikt. U moet weten dat de troostpoorten op Cisco IOS apparaten speciale voorrechten hebben. Met name kunnen deze rechten een beheerder toestaan de wachtwoordherstelprocedure uit te voeren. Om het herstel van het wachtwoord uit te voeren, zou een niet-geauthentiseerde aanvaller toegang tot de troostpoort en de mogelijkheid moeten hebben om de macht aan het apparaat te onderbreken of om het apparaat te veroorzaken om te crashen.

Elke methode die wordt gebruikt om toegang te krijgen tot de troostpoort van een apparaat moet

op een manier worden beveiligd die gelijk is aan de veiligheid die wordt afgedwongen voor bevoorrechte toegang tot een apparaat. Methoden die worden gebruikt om toegang te beveiligen moeten het gebruik van wachtwoorden van AAA, exec-timeout en modemwachtwoorden omvatten als een modem aan de console is bevestigd.

Als er geen herstel van het wachtwoord nodig is, kan een beheerder de mogelijkheid verwijderen om de wachtwoordherstelprocedure uit te voeren met behulp van de opdracht **geen herstel van het** wachtwoord tijdens de **service**; echter, zodra de opdracht **voor het** terugwinnen van **een serviceswachtwoord** is ingeschakeld, kan een beheerder niet langer het herstel van een wachtwoord op een apparaat uitvoeren.

In de meeste gevallen moet de AUX poort van een apparaat worden uitgeschakeld om ongeoorloofde toegang te voorkomen. Een AUX-poort kan met deze opdrachten worden uitgeschakeld:

```
!

line aux 0
transport input none
transport output none
no exec
exec-timeout 0 1
no password
!
```

Ventig- en twijglijnen controleren

Interactieve beheersessies in Cisco IOS-software maken gebruik van een ty of virtuele tty (vty). Een Tty is een lokale asynchrone lijn waaraan een terminal kan worden bevestigd voor lokale toegang tot het apparaat of tot een modem voor dialup toegang tot een apparaat. Merk op dat de tys voor verbindingen kunnen worden gebruikt om poorten van andere apparaten te troosten. Deze functie stelt een apparaat met tty lijnen in staat om als een consoleserver te handelen waar verbindingen over het netwerk kunnen worden gelegd met de console poorten van apparaten aangesloten op de tty lijnen. De tty lijnen voor deze omgekeerde verbindingen over het netwerk moeten ook worden gecontroleerd.

Een vty lijn wordt gebruikt voor alle andere externe netwerkverbindingen die door het apparaat worden ondersteund, ongeacht het protocol (SSH, SCP of telnet zijn voorbeelden). Om ervoor te zorgen dat een apparaat via een lokale of externe beheersessie toegankelijk is, moeten de juiste controles op zowel vty- als tty-lijnen worden uitgevoerd. Cisco IOS-apparaten hebben een beperkt aantal vty lijnen; het aantal beschikbare lijnen kan worden bepaald met de opdracht van de tonen lijn EXEC. Wanneer alle vty lijnen in gebruik zijn, kunnen er geen nieuwe beheersessies worden ingesteld die een DoS-voorwaarde voor toegang tot het apparaat creëren.

De eenvoudigste vorm van toegangscontrole tot een Vty of tty van een apparaat is door het gebruik van authenticatie op alle lijnen ongeacht de apparaatlocatie binnen het netwerk. Dit is van cruciaal belang voor vele lijnen omdat ze toegankelijk zijn via het netwerk. Een tty line die is aangesloten op een modem die gebruikt wordt voor toegang op afstand tot het apparaat, of een tty line die aangesloten is op de console poort van andere apparaten zijn ook toegankelijk via het netwerk. Andere vormen van vty en tty toegangscontroles kunnen worden uitgevoerd met de configuratieopdrachten van de **transportingang** of **toegangsklasse**, met gebruik van de CoPP- en CPPr-functies, of als u toegangslijsten op interfaces op het apparaat toepast.

Verificatie kan worden afgedwongen door het gebruik van AAA, de aanbevolen methode voor

geauthenticeerde toegang tot een apparaat, met het gebruik van de lokale gebruikersdatabase, of door eenvoudige wachtwoordverificatie direct ingesteld op de vty- of tty-lijn.

De opdracht **exec-timeout** moet worden gebruikt om sessies op te loggen of op tty lijnen die leeg zijn. De **service tcp-keepalives-in** opdracht moet ook worden gebruikt om TCP-overzichten op inkomende verbindingen naar het apparaat in te schakelen. Dit waarborgt dat het apparaat op het verafgelegen einde van de verbinding nog toegankelijk is en dat half open of weeshuizen van het lokale IOS apparaat worden verwijderd.

Controle op transport voor Vty- en tty-lijnen

Een Vty en tty moeten worden geconfigureerd om alleen versleutelde en beveiligde externe toegangsbeheerverbindingen naar het apparaat te aanvaarden, of via het apparaat als het als een console server wordt gebruikt. Deze sectie richt zich op manieren omdat dergelijke lijnen kunnen worden aangesloten om poorten op andere apparaten te troosten, die de tty toegang over het netwerk toestaan. Om informatieverstrekking of ongeoorloofde toegang tot de gegevens te voorkomen die tussen de beheerder en het apparaat worden verzonden, moet de **input voor transport** worden gebruikt in plaats van duidelijke tekstprotocollen, zoals telnet en rlogin. De **transport invoer** kan **geen** configuratie op een tty worden geactiveerd, die in feite het gebruik van de tty lijn voor omgekeerde console verbindingen blokkeert.

Zowel de vty- als de tty lijnen staan een beheerder toe om aan andere apparaten te verbinden. Om het type transport te beperken dat een beheerder kan gebruiken voor uitgaande verbindingen, gebruikt u de opdracht voor het configureren van de transportuitvoerlijn. Als er geen uitgaande verbindingen nodig zijn, **mag** de **vervoersoutput** niet worden gebruikt. Als uitgaande verbindingen echter worden toegestaan, moet een versleutelde en beveiligde methode van de toegang op afstand voor de verbinding worden gehandhaafd met behulp van de **transportoutput ssh**.

> Opmerking: IPSec kan worden gebruikt voor versleutelde en beveiligde externe toegangsverbindingen naar een apparaat, indien ondersteund. Als u IPSec gebruikt, voegt het ook extra CPU-overhead aan het apparaat toe. SSH's moeten echter nog steeds als transport worden gehandhaafd, zelfs wanneer IPSec wordt gebruikt.

Waarschuwingsbanners

In sommige rechtsgebieden kan het onmogelijk zijn om kwaadwillige gebruikers te vervolgen en illegaal te controleren, tenzij ze ervan op de hoogte zijn gebracht dat ze het systeem niet mogen gebruiken. Eén methode om dit te melden is om deze informatie in een banner bericht te plaatsen dat met de Cisco IOS-softwarerelease opdracht om te inloggen wordt geconfigureerd.

Juridische kennisgevingsvereisten zijn complex, verschillen per rechtsgebied en per situatie, en moeten met juridische bijstand worden besproken. Zelfs binnen jurisdicties kunnen juridische meningen verschillen. In samenwerking met een advocaat kan een spandoek al deze informatie verstrekken:

- Merk op dat het systeem alleen door specifiek geautoriseerd personeel moet worden ingelogd of gebruikt en dat er ook informatie moet zijn over wie het gebruik kan toestaan.

- Merk op dat elk ongeoorloofd gebruik van de regeling onrechtmatig is en onderworpen kan worden aan civiel- en strafrechtelijke sancties.

- Merk op dat elk gebruik van het systeem zonder verdere kennisgeving kan worden vastgelegd of gecontroleerd en dat de resulterende stammen als bewijs in de rechtbank kunnen worden gebruikt.

- Specifieke mededelingen vereist door de plaatselijke wetgeving.

Uit veiligheidsoogpunt, in plaats van juridisch, zou een logbanner geen specifieke informatie over de routernaam, model, software of eigendom moeten bevatten. Deze informatie kan door kwaadaardige gebruikers worden misbruikt.

Verificatie, autorisatie en accounting

Het kader voor verificatie, autorisatie en accounting (AAA) is cruciaal om interactieve toegang tot netwerkapparaten te garanderen. Het AAA-kader biedt een zeer aanpasbare omgeving die op basis van de behoeften van het netwerk kan worden aangepast.

TACACS+ verificatie

TACACS+ is een authenticatieprotocol dat Cisco IOS apparaten voor authenticatie van beheergebruikers tegen een verre AAA server kunnen gebruiken. Deze beheergebruikers kunnen het IOS-apparaat benaderen via SSH, HTTPS, telnet of HTTP.

TACACS+-verificatie, of meer in het algemeen AAA-verificatie, biedt de mogelijkheid om voor elke netwerkbeheerder individuele gebruikersrekeningen te gebruiken. Als u niet afhankelijk bent van één gedeeld wachtwoord, wordt de beveiliging van het netwerk verbeterd en wordt uw verantwoordingsplicht versterkt.

RADIUS is een protocol dat vergelijkbaar is met TACACS+; het versleutelt echter alleen het wachtwoord dat over het netwerk wordt verzonden. In contrast hiermee versleutelt TACACS+ de gehele TCP-lading, die zowel de gebruikersnaam als het wachtwoord bevat. Om deze reden zou TACACS+ in plaats van RADIUS moeten worden gebruikt wanneer TACACS+ door de AAA server wordt ondersteund. Raadpleeg TACACS+ en RADIUS-vergelijking voor een gedetailleerdere vergelijking van deze twee protocollen.

De verificatie van TACACS+ kan worden ingeschakeld op een Cisco IOS apparaat met een configuratie gelijkend op dit voorbeeld:

```
!

aaa new-model
aaa authentication login default group tacacs+
!

tacacs-server host <ip-address-of-tacacs-server>
tacacs-server key <key>
!
```

De vorige configuratie kan worden gebruikt als startpunt voor een organisatiespecifiek AAA-verificatiemechanisme. Raadpleeg Verificatie, autorisatie en accounting voor meer informatie over de configuratie van AAA.

Een methodelijst is een sequentiële lijst waarin de authenticatiemethoden worden beschreven die

moeten worden gevraagd om een gebruiker te authentiseren. Methodelijsten stellen u in staat één of meer veiligheidsprotocollen aan te wijzen die gebruikt moeten worden voor echtheidscontrole en verzekeren zo een reservesysteem voor authenticatie in het geval de initiële methode faalt. Cisco IOS-software gebruikt de eerste genoemde methode die een gebruiker met succes accepteert of afwijst. De volgende methoden worden alleen geprobeerd in gevallen waar eerdere methoden falen vanwege onbeschikbaarheid van de server of onjuiste configuratie.

Raadpleeg de Benoemde methodelijsten voor verificatie voor meer informatie over de configuratie van Benoemde methodelijsten.

Verificatieback-up

Als alle geconfigureerde TACACS+-servers niet beschikbaar worden, kan een Cisco IOS-apparaat op secundaire verificatieprotocollen vertrouwen. De typische configuraties omvatten het gebruik van lokale of maken verificatie mogelijk als alle geconfigureerde TACACS+-servers niet beschikbaar zijn.

De volledige lijst van opties voor on-device authenticatie omvat toelaten, lokaal, en lijn. Elk van deze opties heeft voordelen. Het gebruik van het machtigingsgeheim wordt geprefereerd omdat het geheim met een eenrichtingsalgoritme wordt gehakt dat inherent veiliger is dan het encryptiealgoritme dat met de wachtwoorden van Type 7 voor lijn of lokale authenticatie wordt gebruikt.

Op Cisco IOS-softwarereleases die het gebruik van geheime wachtwoorden voor lokaal gedefinieerde gebruikers ondersteunen, kan echter back-up naar lokale verificatie wenselijk zijn. Hierdoor kan een lokaal gedefinieerde gebruiker voor een of meer netwerkbeheerders worden gemaakt. Als TACACS+ volledig niet beschikbaar zou worden, kan elke beheerder hun lokale gebruikersnaam en wachtwoord gebruiken. Hoewel deze actie de verantwoordingsplicht van netwerkbeheerders bij TACACS+-uitval versterkt, verhoogt zij de administratieve last aanzienlijk omdat de lokale gebruikersrekeningen op alle netwerkapparaten moeten worden gehandhaafd.

Dit configuratievoorbeeld bouwt op het vorige TACACS+ authenticatievoorbeeld om back-back authenticatie aan het wachtwoord op te nemen dat lokaal wordt ingesteld met de **mogelijkheid tot geheime** opdracht:

```
!

enable secret <password>
!

aaa new-model
aaa authentication login default group tacacs+ enable
!

tacacs-server host <ip-address-of-tacacs-server>
tacacs-server key <key>
!
```

Raadpleeg Verificatie configureren voor meer informatie over het gebruik van back-upverificatie met AAA.

Gebruik van wachtwoorden van type 7

Oorspronkelijk ontworpen om snelle decryptie van opgeslagen wachtwoorden mogelijk te maken,

zijn de wachtwoorden van het type 7 geen veilige vorm van het bewaren van wachtwoord. Er zijn veel tools beschikbaar die deze wachtwoorden gemakkelijk kunnen decrypteren. Het gebruik van wachtwoorden van type 7 moet worden vermeden, tenzij dit vereist is door een functie die in gebruik is op het Cisco IOS-apparaat.

Type 9 (crypt) dient waar mogelijk te worden gebruikt:

```
username <username> privilege 15 algorithm-type scrypt secret <secret>
```

Het verwijderen van wachtwoorden van dit type kan worden vergemakkelijkt door AAA-verificatie en het gebruik van de optie Verbeterde wachtwoordbeveiliging waardoor u geheime wachtwoorden kunt gebruiken bij gebruikers die lokaal worden gedefinieerd via de opdracht **Gebruikersnaam voor** wereldwijde configuratie. Als u het gebruik van wachtwoorden van type 7 niet volledig kunt verhinderen, kunt u deze wachtwoorden overwegen, niet versleuteld.

Zie het gedeelte General Management Plane Hardening van dit document voor meer informatie over het verwijderen van wachtwoorden van type 7.

Verificatie voor TACACS+ opdracht

De opdracht voor opdracht met TACACS+ en AAA biedt een mechanisme dat elke opdracht toestaat of ontkent die door een administratieve gebruiker wordt ingevoerd. Wanneer de gebruiker EXEC-opdrachten invoert, stuurt Cisco IOS elke opdracht naar de geconfigureerde AAA-server. De AAA-server gebruikt vervolgens de ingestelde beleidslijnen om de opdracht voor die specifieke gebruiker toe te staan of te ontkennen.

Deze configuratie kan worden toegevoegd aan het vorige AAA-verificatievoorbeeld om een opdrachtvergunning in te voeren:

```
!

aaa authorization exec default group tacacs none
aaa authorization commands 0 default group tacacs none
aaa authorization commands 1 default group tacacs none
aaa authorization commands 15 default group tacacs none
!
```

Raadpleeg de autorisatie configureren voor meer informatie over een opdrachtautorisatie.

Accounting van TACACS+ opdracht

Indien geconfigureerd stuurt AAA-opdrachtaccounting informatie over elke EXEC-opdracht die in de geconfigureerde TACACS+-servers is ingevoerd. De informatie die naar de TACACS+ server wordt verzonden omvat de uitgevoerde opdracht, de datum waarop deze werd uitgevoerd en de gebruikersnaam van de gebruiker die de opdracht invoert. Opdrachtaccounting wordt niet ondersteund door RADIUS.

Deze voorbeeldconfiguratie maakt het mogelijk om AAA-commando-accounting voor EXEC-opdrachten ingevoerd op voorkeursniveau's 0, 1 en 15. Deze configuratie bouwt voort op eerdere voorbeelden die configuratie van de TACACS-servers omvatten.

```
!
```

```
aaa accounting exec default start-stop group tacacs
aaa accounting commands 0 default start-stop group tacacs
aaa accounting commands 1 default start-stop group tacacs
aaa accounting commands 15 default start-stop group tacacs
!
```

Raadpleeg Accounting voor meer informatie over de configuratie van AAA-accounting.

Redundant AAA-servers

De AAA-servers die in een omgeving actief zijn, moeten overbodig zijn en op een fouttolerante manier worden ingezet. Dit helpt ervoor te zorgen dat interactieve beheertoegang, zoals SSH, mogelijk is als een AAA-server niet beschikbaar is.

Wanneer u een overbodige AAA server-oplossing ontwerpt of implementeert, onthoud deze overwegingen:

- Beschikbaarheid van AAA-servers tijdens potentiële netwerkstoringen
- Geografische spreiding van AAA-servers
- Laad op afzonderlijke AAA-servers in steady-state- en storingsomstandigheden
- Netwerkverbinding tussen netwerktoegangsservers en AAA-servers
- AAA-serverdatabases synchroniseren

Raadpleeg De toegangscontroleservers implementeren voor meer informatie.

Eenvoudig netwerkbeheerprotocol versterken

Deze sectie benadrukt verscheidene methodes die kunnen worden gebruikt om de plaatsing van SNMP binnen IOS apparaten te verzekeren. Het is van cruciaal belang dat SNMP correct wordt beveiligd om de vertrouwelijkheid, integriteit en beschikbaarheid van zowel de netwerkgegevens als de netwerkapparaten te beschermen waardoor deze gegevens worden doorgegeven. SNMP biedt u een schat aan informatie over de gezondheid van netwerkapparaten. Deze informatie moet worden beschermd tegen kwaadwillige gebruikers die deze gegevens willen gebruiken om aanvallen tegen het netwerk uit te voeren.

SNMP-community-Streng

Community-strings zijn wachtwoorden die zijn toegepast op een IOS-apparaat om de toegang tot de SNMP-gegevens op het apparaat te beperken, zowel read-only als read-Writing. Deze community strings moeten, net als alle wachtwoorden, zorgvuldig worden gekozen om er zeker van te zijn dat ze niet triviaal zijn. De communautaire koorden moeten op gezette tijden en in overeenstemming met het beveiligingsbeleid van het netwerk worden gewijzigd. Bijvoorbeeld, zouden de koorden moeten worden veranderd wanneer een netwerkbeheerder rollen verandert of het bedrijf verlaat.

Deze configuratielijnen vormen een alleen-lezen string van READONLY en een read-writer community string van READSCHRIFT:

```
!

snmp-server community READONLY RO
snmp-server community READWRITE RW
!
```

> Opmerking: De vorige voorbeelden van een string van de gemeenschap zijn gekozen om het gebruik van deze strings duidelijk uit te leggen. Voor productieomgevingen moeten de communautaire koorden met voorzichtigheid worden gekozen en bestaan uit een reeks alfabetische, numerieke en niet-alfanumerieke symbolen. Raadpleeg Aanbevelingen voor het maken van sterke wachtwoorden voor meer informatie over het selecteren van niet-onbelangrijke wachtwoorden.

Raadpleeg de IOS SNMP-opdracht Referentie voor meer informatie over deze functie.

SNMP Community-Strings met ACL's

Naast de community string, moet ACL worden toegepast dat SNMP toegang verder beperkt tot een selecte groep bron IP adressen. Deze configuratie beperkt SNMP-alleen-toegang tot eindhost-apparaten die in de 192.168.100.0/24-adresruimte verblijven en beperkt SNMP-lezen-schrijftoegang tot alleen het eindhost-apparaat op 192.168.100.1.

> Opmerking: De apparaten die door deze ACLs worden toegestaan vereisen de juiste gemeenschapsreeks om tot de gevraagde SNMP informatie te toegang te hebben.

```
!

access-list 98 permit 192.168.100.0 0.0.0.255
access-list 99 permit 192.168.100.1
!

snmp-server community READONLY RO 98
snmp-server community READWRITE RW 99
!
```

Raadpleeg de SNMP-servergemeenschap in de Cisco IOS Network Management Opdracht Referentie voor meer informatie over deze optie.

Infrastructuur ACL's

Infrastructuur ACL's (iACL's) kan worden uitgevoerd om er zeker van te zijn dat alleen eindhosts met vertrouwde IP-adressen SNMP-verkeer naar een IOS-apparaat kunnen verzenden. Een iACL moet een beleid bevatten dat onbevoegde SNMP-pakketten op UDP poort 161 ontkent.

Zie het gedeelte Toegang tot het netwerk beperken met infrastructuur ACL's van dit document voor meer informatie over het gebruik van iACL's.

SNMP-standpunten

SNMP-standpunten zijn een beveiligingsfunctie die toegang tot bepaalde SNMP-MIB's kan toestaan of weigeren. Zodra een weergave gecreëerd is en van toepassing is op een string van de **snmp-server community** community-string configuratie opdrachten, als je toegang krijgt tot MIB

gegevens, ben je beperkt tot de permissie die door de weergave gedefinieerd wordt. Indien nodig is het raadzaam om weergave te gebruiken om gebruikers van SNMP te beperken tot de gegevens die ze nodig hebben.

Dit configuratievoorbeeld beperkt SNMP toegang met de community string LIMITED tot de MIB gegevens die in de systeemgroep geplaatst zijn:

```
!

snmp-server view VIEW-SYSTEM-ONLY system include
!

snmp-server community LIMITED view VIEW-SYSTEM-ONLY RO
!
```

Raadpleeg de SNMP-ondersteuning configureren voor meer informatie.

SNMP versie 3

SNMP versie 3 (SNMPv3) wordt gedefinieerd door RFC3410, RFC3411, RFC3412, RFC3413, RFC3414 en RFC3415 en is een interoperabel op standaarden gebaseerd protocol voor netwerkbeheer. SNMPv3 biedt veilige toegang tot apparaten omdat het pakketten over het netwerk authentiek verklaard en optioneel versleutelt. Waar ondersteund, kan SNMPv3 worden gebruikt om een andere laag van veiligheid toe te voegen wanneer u SNMP opstelt. SNMPv3 bestaat uit drie primaire configuratieopties:

- **geen auth** - Deze modus vereist geen verificatie of encryptie van SNMP-pakketten
- **Auth** - Deze modus vereist verificatie van het SNMP-pakket zonder encryptie
- **priv** - Deze modus vereist zowel verificatie als encryptie (privacy) van elk SNMP-pakket

Een gezaghebbende motor-ID moet bestaan om de SNMPv3-beveiligingsmechanismen - verificatie of verificatie en encryptie - te kunnen gebruiken om SNMP-pakketten te verwerken; de motor-ID wordt standaard lokaal gegenereerd. De motor-ID kan worden weergegeven met de **show-snmp-motorID**-opdracht zoals in dit voorbeeld wordt getoond:

```
router#show snmp engineID
Local SNMP engineID: 80000009030000152BD35496
Remote Engine ID IP-addr Port
```

> Opmerking: Als de engineID is gewijzigd, moeten alle SNMP-gebruikersaccounts worden aangepast.

De volgende stap is het configureren van een SNMPv3 groep. Deze opdracht vormt een Cisco IOS apparaat voor SNMPv3 met een SNMP server group AUTHGROUP en maakt alleen verificatie voor deze groep mogelijk met het **auth** sleutelwoord:

```
!
snmp-server group AUTHGROUP v3 auth
!
```

Deze opdracht vormt een Cisco IOS apparaat voor SNMPv3 met een SNMP servergroep

PRIVGROUP en maakt zowel verificatie als encryptie voor deze groep mogelijk met het **primaire** sleutelwoord:

```
!
snmp-server group PRIVGROUP v3 priv
!
```

Deze opdracht stelt een SNMPv3-gebruiker SNMPv3-gebruiker in met een MD5 verificatiewachtwoord van **autorpassword** en een 3DES-encryptiewachtwoord van **een** privé-**wachtwoord**:

```
!

snmp-server user snmpv3user PRIVGROUP v3 auth md5 authpassword priv 3des
privpassword
!
```

Merk op dat **de** configuratieopdrachten van de **snmp-server** niet in de configuratie-uitvoer van het apparaat worden weergegeven, zoals vereist door RFC 3414; daarom is het gebruikerswachtwoord niet zichtbaar vanuit de configuratie. Om de geconfigureerde gebruikers te bekijken, voert u de opdracht **show snmp user** in zoals in dit voorbeeld wordt getoond:

```
router#show snmp user
User name: snmpv3user
Engine ID: 80000009030000152BD35496
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: 3DES
Group-name: PRIVGROUP
```

Raadpleeg SNMP-ondersteuning configureren voor meer informatie over deze functie.

Bescherming van besturingsplane

De optie Management Plane Protection (MPP) in Cisco IOS-software kan worden gebruikt om SNMP te beveiligen omdat dit de interfaces beperkt waardoor SNMP-verkeer op het apparaat kan eindigen. Met de MPP-functie kan een beheerder een of meer interfaces als beheerinterfaces aanwijzen. Het verkeer van het beheer is toegestaan om een apparaat slechts door deze beheerinterfaces in te voeren. Nadat MPP is ingeschakeld, aanvaarden geen interfaces behalve de aangewezen beheerinterfaces netwerkbeheerverkeer dat bestemd is voor het apparaat.

Merk op dat MPP een subset van de CPPr optie is en een versie van IOS vereist die CPPr ondersteunt. Raadpleeg Inzicht op bescherming van besturingsplane voor meer informatie over CPPr.

In dit voorbeeld wordt MPP gebruikt om SNMP en SSH toegang tot slechts de FastEthernet 0/0 interface te beperken:

```
!
control-plane host
management-interface FastEthernet0/0 allow ssh snmp
!
```

Raadpleeg de Functiehandleiding voor landbescherming voor meer informatie.

Aanmelden van beste praktijken

Event logging biedt u zichtbaarheid in de werking van een Cisco IOS apparaat en het netwerk waarin het wordt ingezet. Cisco IOS-software biedt verschillende flexibele logopties die kunnen helpen de netwerkbeheer- en zichtbaarheidsdoelstellingen van een organisatie te bereiken.

Deze secties bieden een aantal basisloggbeste praktijken die een beheerder met succes kunnen helpen om houtkap te registreren terwijl het impact van houtkap op een Cisco IOS apparaat minimaliseert.

Logs naar een centrale locatie verzenden

U wordt geadviseerd om loginformatie naar een externe systeemserver te verzenden. Dit maakt het mogelijk om netwerk- en beveiligingsgebeurtenissen over netwerkapparaten effectiever te correleren en te controleren. Merk op dat syslogberichten onbetrouwbaar worden verzonden door UDP en in cleartext. Om deze reden moet elke bescherming die een netwerk biedt aan beheerverkeer (bijvoorbeeld encryptie of toegang buiten de band) worden uitgebreid, zodat het ook systeemverkeer omvat.

Dit configuratievoorbeeld vormt een Cisco IOS apparaat om houtloginformatie naar een afstandsbediening te sturen:

```
!
logging host <ip-address>
!
```

Raadpleeg het gedeelte Incidenten identificeren met Firewall- en IOS-routergebeurtenissen voor meer informatie over bestandscorrelatie.

Geïntegreerd in 12.4(15)T en oorspronkelijk geïntroduceerd in 12.0(26)S, maakt de optie Vastlegging aan Local Non-vlule Storage (ATA Disk) het mogelijk om berichten van systeemvastlegging op een ATA-flitsschijf (geavanceerde technologie-bijlage) op te slaan. Berichten die op een ATA-station zijn opgeslagen, blijven bestaan nadat een router is herstart.

Deze configuratielijnen vormen 134.217.728 bytes (128 MB) van houtlogberichten naar de syslogmap van de ATA-flitser (disk0), wat een bestandsgrootte van 16.384 bytes gespecificeerd heeft:

```
logging buffered
logging persistent url disk0:/syslog size 134217728 filesize 16384
```

Voordat logberichten op een bestand op de ATA-schijf worden geschreven, controleert Cisco IOS-software of er voldoende schijfruimte is. Als dit niet het geval is, wordt het oudste bestand van houtkapberichten (door tijdstempel) verwijderd en wordt het huidige bestand opgeslagen. De bestandsindeling is **log_maand:dag:jaar:tijd**.

> Opmerking: Een ATA-flash-station heeft een beperkte schijfruimte en moet dus worden gehandhaafd om te voorkomen dat opgeslagen gegevens worden overschreven.

Dit voorbeeld toont hoe te om houtkapberichten van de router ATA flitsschijf naar een externe schijf op FTP server 192.168.1.129 te kopiëren als deel van onderhoudsprocedures:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Raadpleeg Vastlegging aan lokale niet-vluchtige opslag (ATA-schijf) voor meer informatie over deze optie.

Logniveau

Elk logbericht dat door een Cisco IOS apparaat wordt gegenereerd wordt toegewezen aan één van de acht eigenschappen die van niveau 0, Noodsituaties, door niveau 7, Debug variëren. Tenzij specifiek vereist, wordt u geadviseerd om houtkap op niveau 7 te vermijden. Vastlegging op niveau 7 veroorzaakt een verhoogde lading CPU op het apparaat die tot apparaat en netwerkinstabiliteit kan leiden.

Het niveau van de mondiale configuratieopdracht **logingval** wordt gebruikt om te specificeren welke houtkapberichten naar verafgelegen snelservers worden verzonden. Het opgegeven niveau geeft het laagste ernst-bericht aan dat wordt verstuurd. Voor gebufferde houtkap wordt de opdracht **gebufferde** niveaus gebruikt.

Dit configuratievoorbeeld beperkt logberichten die naar op afstand aangesloten syslogservers worden verzonden en de lokale logbuffer naar versie 6 (informatie) door 0 (noodgevallen):

```
!

logging trap 6
logging buffered 6
!
```

Raadpleeg Problemen oplossen, foutenbeheer en vastlegging voor meer informatie.

Log niet in op console of monitor sessies

Met Cisco IOS-software is het mogelijk om logberichten naar monitor-sessies te verzenden - bewakingssessies zijn interactieve beheersessies waarin de EXEC **opdrachtterminalmonitor** is uitgegeven - en naar de console. Dit kan echter de CPU-lading van een IOS-apparaat verhogen en wordt daarom niet aanbevolen. In plaats daarvan, wordt u geadviseerd om houtkapinformatie naar de lokale logbuffer te verzenden, die met de opdracht **show logging logging logging** kan worden bekeken.

Gebruik de mondiale configuratieopdrachten **geen houtkapconsole** en **geen houtkapmonitor** om houtkap aan de console en de controlesessies uit te schakelen. Dit configuratievoorbeeld toont het gebruik van deze opdrachten:

```
!

no logging console
no logging monitor
!
```

Raadpleeg de handleiding voor Cisco IOS Network Management voor meer informatie over wereldwijde configuratieopdrachten.

Gebuffervastlegging gebruiken

Cisco IOS-software ondersteunt het gebruik van een lokale logbuffer, zodat een beheerder lokaal gegenereerde logberichten kan bekijken. Het gebruik van gebufferde houtkap wordt sterk aanbevolen in vergelijking met houtkap op de console of de controlesessies.

Er zijn twee configuratieopties die relevant zijn bij het configureren van gebufferde vastlegging: de grootte van de houtkapbuffer en de berichteigenschappen die in de buffer zijn opgeslagen. De grootte van de **houtkapbuffer** wordt ingesteld met de **gebufferde** grootte van de **gebufferde** configuratieopdracht. De laagste ernst in de buffer wordt ingesteld met de opdracht voor de gebufferde houternst. Een beheerder kan de inhoud van de houtkapbuffer bekijken door het bevel **van** de **show logging** EXEC.

Dit configuratievoorbeeld omvat de configuratie van een houtkapbuffer van 16384 bytes, evenals een ernst van 6, informatie, die aangeeft dat berichten op niveau 0 (noodgevallen) tot en met 6 (informatie) zijn opgeslagen:

```
!

logging buffered 16384 6
!
```

Raadpleeg de handleiding voor Cisco IOS Network Management voor meer informatie over gebufferde vastlegging.

Logsource-interface configureren

Om een hoger niveau van consistentie te bieden wanneer u logberichten verzamelt en controleert, wordt u geadviseerd om een logbroninterface statistisch te configureren. Klaar met de opdracht **logbron-interface**, vormt het statistisch configureren van een logbroninterface een garandeert dat hetzelfde IP-adres verschijnt in alle logberichten die worden verzonden van een individueel Cisco IOS-apparaat. Voor extra stabiliteit, wordt u geadviseerd om een loopback interface als houtkap te gebruiken.

Dit configuratievoorbeeld illustreert het gebruik van de **van de houtkap bron-interface** interface mondiale configuratieopdracht om te specificeren dat het IP adres van de loopback 0 interface voor alle logberichten gebruikt wordt:

```
!
logging source-interface Loopback 0
!
```

Raadpleeg de Cisco IOS-opdracht voor meer informatie.

Tijdlijnen voor vastlegging configureren

De configuratie van loggtimestamps helpt u gebeurtenissen over netwerkapparaten te correleren. Het is belangrijk om een correcte en consistente configuratie van de logtijd uit te voeren om ervoor te zorgen dat u de loggegevens kunt correleren. Logging timestamps moet worden geconfigureerd om de datum en de tijd met milliseconde precisie te bevatten en om de tijdzone in gebruik op het apparaat op te nemen.

Dit voorbeeld omvat de configuratie van houtkaptijden met milliseconde-precisie binnen de gecoördineerde Universal Time (UTC)-zone:

```
!
service timestamps log datetime msec show-timezone
!
```

Als u liever geen logtijden hebt vergeleken met UTC, kunt u een specifieke lokale tijdzone configureren en deze informatie configureren om in gegenereerde logberichten te verschijnen. Dit voorbeeld toont een apparaatconfiguratie voor de Pacific Standard Time (PST)-zone:

```
!

clock timezone PST -8
service timestamps log datetime msec localtime show-timezone
!
```

Cisco IOS-softwareconfiguratie

Cisco IOS-software bevat verschillende functies die een vorm van configuratiebeheer op een Cisco IOS-apparaat kunnen inschakelen. Zulke functies omvatten functionaliteit om configuraties te archiveren en de configuratie om te draaien naar een vorige versie evenals een gedetailleerd logbestand voor configuratie om te zetten.

Configuratie-vervanging en -configuratie

In Cisco IOS-softwarerelease 12.3(7)T en hoger kunt u met de functies Configuration Replace en Configuration Rollback de Cisco IOS-apparaatconfiguratie op het apparaat archiveren. Bewaar handmatig of automatisch, kunnen de configuraties in dit archief worden gebruikt om de huidige actieve configuratie te vervangen door de **configuratie** filename opdracht **vervangen**. Dit is in tegenstelling tot de opdracht bestandsnaam **in werking stellen-configuratie**. De opdracht filename **vervangen** de actieve configuratie in plaats van de fusie die wordt uitgevoerd door de opdracht **kopiëren**.

U wordt geadviseerd deze optie op alle Cisco IOS apparaten in het netwerk in te schakelen. Als deze optie is ingeschakeld, kan een beheerder de huidige actieve configuratie aanzetten om aan het archief toe te voegen met het opdracht **archiefbestand** bevoorrechte EXEC-toegang. De gearchiveerde configuraties kunnen worden bekeken met de opdracht **archief** EXEC.

Dit voorbeeld illustreert de configuratie van automatische configuratie archivering. Dit voorbeeld vertelt het Cisco IOS apparaat om gearchiveerde configuraties op te slaan als bestanden die gearchiveerd-configuratie-N op de disk0 worden genoemd: bestandssysteem, om maximaal 14 back-ups te behouden en één keer per dag te archiveren (1440 minuten) en wanneer een beheerder de opdracht **schrijfgeheugen** EXEC uitlevert.

```
!

archive
path disk0:archived-config
maximum 14
time-period 1440
write-memory
!
```

Hoewel de configuratie archieffunctie maximaal 14 back-upconfiguraties kan opslaan, is het raadzaam de ruimtevereisten in overweging te nemen voordat u de **maximale** opdracht gebruikt.

Toegang tot exclusieve configuratie

Toegevoegd aan Cisco IOS-softwarerelease 12.3(14)T, garandeert de functie exclusieve configuratie Change Access dat slechts één beheerder configuratie wijzigingen aanbrengt in een Cisco IOS-apparaat op een bepaald tijdstip. Deze optie helpt de ongewenste impact van gelijktijdige wijzigingen in gerelateerde configuratieonderdelen te elimineren. Deze optie is ingesteld in de **exclusieve** modus voor de configuratie van de configuratie van het **geheel** en werkt in een van de twee modi: auto en handleiding. In de automatische modus wordt de configuratie automatisch vergrendeld wanneer een beheerder de **configuratie** van de terminal EXEC uitvoert. In handmodus gebruikt de beheerder de opdracht **voor** de **configuratie** van de **eindvergrendeling** om de configuratie te vergrendelen wanneer deze in de configuratie-modus komt.

Dit voorbeeld illustreert de configuratie van deze optie voor automatische configuratie-blokkering:

```
!
configuration mode exclusive auto
!
```

Cisco IOS-softwarebestendige configuratie

Opgeleverd in Cisco IOS-softwarerelease 12.3(8)T maakt de functie voor veerkrachtige configuratie het mogelijk om een kopie van de Cisco IOS-softwareafbeelding en -apparaatconfiguratie veilig op te slaan die momenteel door een Cisco IOS-apparaat wordt gebruikt. Als deze optie is ingeschakeld, kunnen deze reservekopieën niet worden gewijzigd of verwijderd. U wordt geadviseerd deze optie in te schakelen om zowel onbedoelde als kwaadaardige pogingen te voorkomen om deze bestanden te verwijderen.

```
!
secure boot-image
secure boot-config!
```

Als deze functie is ingeschakeld, kan een verwijderde configuratie of Cisco IOS-softwarefobeeldgegevens worden hersteld. De huidige actieve status van deze optie kan met de opdracht **beveiligde start** EXEC-opdracht worden weergegeven.

Digitale ondertekende Cisco-software

Toegevoegd in Cisco IOS-softwarerelease 15.0(1)M voor de Cisco 1900, 2900 en 3900 Series routers, vergemakkelijkt de digitaal ondertekende Cisco-softwarefunctie het gebruik van Cisco IOS-software die digitaal ondertekend en dus vertrouwd is, met het gebruik van beveiligde asymmetrische (openbare) cryptografie.

Een digitaal ondertekend beeld heeft een gecodeerd (met een privé sleutel) handvat van zichzelf. Na controle decrypteert het apparaat de hash met de overeenkomstige openbare sleutel van de sleutels die het in zijn belangrijkste opslag heeft en berekent ook zijn eigen hash van de afbeelding. Als de gedecrypteerde hash overeenkomt met de berekende afbeelding hash, is de afbeelding niet geknoeid met de afbeelding en kan deze worden vertrouwd.

De digitaal ondertekende Cisco-softwaretoetsen worden geïdentificeerd door het type en de versie van de toets. Een sleutel kan een speciaal type, een productie of een rolomversleutel zijn. De productie en speciale sleuteltypes hebben een geassocieerde sleutelversie die alfabetisch stijgt wanneer de key wordt ingetrokken en vervangen. ROMMON en reguliere Cisco IOS-afbeeldingen

worden beide ondertekend met een speciale of productiesleutel wanneer u de Digitaal ondertekende Cisco-softwarefunctie gebruikt. Het ROMMON-beeld is upgradeerbaar en moet met de zelfde sleutel worden ondertekend als het speciale of productiebeeld dat wordt geladen.

Deze opdracht verifieert de integriteit van afbeelding c3900-universalk9-mz.SSA in flitser met de toetsen in de device key store:

```
show software authenticity file flash0:c3900-universalk9-mz.SSA
```

De digitaal ondertekende Cisco-softwarefunctie is ook geïntegreerd in Cisco IOS XE release 3.1.0.SG voor Cisco Catalyst 4500 E-Series switches.

Raadpleeg de Digitaal *ondertekende* Cisco-software voor meer informatie over deze functie.

In Cisco IOS-softwarerelease 15.1(1)T en later is toetsuitbreiding voor digitaal ondertekende Cisco-software geïntroduceerd. Belangrijke vervanging en herroeping vervangen en verwijderen een sleutel die wordt gebruikt voor een Digitaal Ondertekende controle van de Software van Cisco van de belangrijkste opslag van een platform. In geval van een belangrijk compromis kunnen alleen speciale en productiesleutels worden ingetrokken.

Een nieuwe (speciale of productie) sleutel voor een (speciaal of productieklek) beeld wordt geleverd in een (productie- of revocatie) beeld dat wordt gebruikt om de vorige speciale of productieklek in te trekken. De integriteit van het herroeping-beeld wordt geverifieerd met een rolomvergootsleutel die op het platform vooraf is opgeslagen. Een overlooptoets verandert niet. Wanneer u een productiesleutel intrekt, nadat het herroepingsbeeld is geladen, wordt de nieuwe toets die het vervoert aan de belangrijkste winkel toegevoegd en kan de corresponderende oude toets worden herroepen zolang het ROMMON-beeld is bijgewerkt en het nieuwe productiebeeld wordt opgestart. Wanneer u een speciale toets intrekt, wordt een productiebeeld geladen. Dit beeld voegt de nieuwe speciale toets toe en kan de oude speciale toets intrekken. Nadat u een upgrade van ROMMON hebt uitgevoerd, kan de nieuwe speciale afbeelding worden gestart.

In dit voorbeeld wordt het intrekken van een speciale sleutel beschreven. Deze opdrachten voegen de nieuwe speciale sleutel toe aan de belangrijkste winkel van het huidige productiebeeld, kopiëren een nieuw ROMMON-beeld (C3900_rom-monitor.srec.SSB) naar het opslaggebied (USB-flitser0:), verbeteren het ROMMON-bestand en trekken de oude speciale toets in:

```
software authenticity key add special
copy tftp://192.168.1.129/C3900_rom-monitor.srec.SSB usbflash0:
upgrade rom-monitor file usbflash0:C3900_PRIV_RM2.srec.SSB
software authenticity key revoke special
```

Een nieuwe speciale afbeelding (c3900-universalk9-mz.SSB) kan vervolgens naar de te laden flitser worden gekopieerd en de handtekening van de afbeelding wordt geverifieerd met de nieuwe speciale sleutel (.SSB):

```
copy /verify tftp://192.168.1.129/c3900-universalk9-mz.SSB flash:
```

Belangrijkste herroeping en vervanging wordt niet ondersteund op Catalyst 4500 E-Series switches die Cisco IOS XE-software uitvoeren, hoewel deze switches de Digitaal ondertekende Cisco-softwarefunctie ondersteunen.

Raadpleeg de Digitaal ondertekende sectie van de Software van Cisco Key Revocatie en Vervanging van de Digitaal Ondertekende Software van Cisco voor meer informatie over deze functie.

Kennisgeving van wijziging van configuratie en -vastlegging

Met de functie Wijzigen en vastlegging van de configuratie, toegevoegd in Cisco IOS-softwarerelease 12.3(4)T, kan de configuratie worden gewijzigd in een Cisco IOS-apparaat. Het logbestand wordt op het Cisco IOS-apparaat onderhouden en bevat de gebruikersinformatie van het individu dat de wijziging heeft aangebracht, het ingevoerde configuratieopdracht en het tijdstip waarop de wijziging is aangebracht. Deze functionaliteit wordt ingeschakeld met de opdracht **logger** configuratie configuratie configuratie configuratie configuratie modus. De optionele opdrachten **hidekeys** en **logging size** items worden gebruikt om de standaardconfiguratie te verbeteren, omdat ze de vastlegging van wachtwoordgegevens voorkomen en de lengte van het veranderingslogbestand vergroten.

U wordt geadviseerd om deze functionaliteit toe te laten, zodat de configuratieveranderingsgeschiedenis van een Cisco IOS apparaat beter begrepen kan worden. Daarnaast is het raadzaam de configuratie van de **configuratie** van de **syslogan** te gebruiken om het genereren van syslogberichten mogelijk te maken wanneer de configuratie verandert.

```
!

archive
log config
logging enable
logging size 200
hidekeys
notify syslog
!
```

Nadat de van de Verandering van de Configuratie en de Logging optie van de Logging van de Configuratie is toegelaten, **kan** de bevoorrechte EXEC opdracht **archieflogboek** worden gebruikt om het configuratielogbestand te bekijken.

besturingsplane

De functies van het bedieningspaneel bestaan uit de protocollen en processen die tussen netwerkapparaten communiceren om gegevens van bron naar bestemming te verplaatsen. Dit omvat routeringsprotocollen zoals het Border Gateway Protocol, evenals protocollen zoals ICMP en het Resource Reservation Protocol (RSVP).

Het is van belang dat gebeurtenissen in het beheers- en dataplatform geen negatieve invloed hebben op het bedieningspaneel. Als een gegevensgebeurtenis zoals een DoS-aanval het bedieningspaneel beïnvloedt, kan het gehele netwerk instabiel worden. Deze informatie over Cisco IOS-softwarefuncties en -configuraties kan helpen de veerkracht van het bedieningspaneel te verzekeren.

Hardnekkig besturingsplane

De bescherming van het bedieningspaneel van een netwerkvoorziening is van cruciaal belang omdat het bedieningspaneel en de dataplannen op peil houden en operationeel zijn. Als het bedieningspaneel tijdens een beveiligingsincident instabiel zou worden, kan het onmogelijk zijn voor u om de stabiliteit van het netwerk te herstellen.

In veel gevallen kunt u de ontvangst en transmissie van bepaalde typen berichten op een interface

uitschakelen om de hoeveelheid CPU-lading te minimaliseren die nodig is om niet-benodigde pakketten te verwerken.

IP ICMP-omleidingen

Een ICMP-bericht kan worden gegenereerd door een router wanneer een pakket op dezelfde interface wordt ontvangen en verzonden. In deze situatie, door de router het pakket door en stuurt een ICMP opnieuw bericht naar de afzender van het oorspronkelijke pakket. Dit gedrag laat de zender toe om de router te omzeilen en toekomstige pakketten direct naar de bestemming (of naar een router dichter naar de bestemming) door te sturen. In een goed functionerend IP netwerk, verstuurt een router redirecties slechts naar hosts op zijn eigen lokale subnetten. Met andere woorden: ICMP-omleidingen zouden nooit verder moeten gaan dan Layer 3 grenzen.

Er zijn twee typen ICMP-omleidingen: herleiden voor een adres van de gastheer en opnieuw richten voor een volledig netto. Een kwaadaardige gebruiker kan de mogelijkheid van de router gebruiken om ICMP-omleidingen te verzenden door voortdurend pakketten naar de router te verzenden, waardoor de router wordt gedwongen om te reageren met ICMP-omleidingen en resultaten in een schadelijk effect op de CPU en de prestaties van de router. Om de router te voorkomen ICMP-omleidingen te verzenden, gebruikt u de opdracht **Geen IP-omleidingen voor** interfacemodules.

ICMP onbereikbaar

Het filteren met een interface toegangslijst veroorzaakt de overdracht van ICMP onbereikbare berichten terug naar de bron van het gefilterde verkeer. De generatie van deze berichten kan het gebruik van CPU op het apparaat vergroten. In Cisco IOS-software is de onbereikbare generatie van ICMP beperkt tot één pakket per 500 milliseconden standaard. ICMP onbereikbare berichtgeneratie kan worden uitgeschakeld met de opdracht voor de interfaceconconfiguratie **zonder ip onbereikbaar**. ICMP onbereikbare snelheidsbeperking kan van de standaard gewijzigd worden met de **IP-snelheidsbeperking onbereikbaar** interval-in-ms **van de** globale configuratieopdracht.

Proxy ARP

Proxy ARP is de techniek waarin een apparaat, meestal een router, ARP-verzoeken beantwoordt die voor een ander apparaat zijn bedoeld. Door zijn identiteit te "faking", accepteert de router verantwoordelijkheid voor het verzenden van pakketten naar de echte bestemming. Proxy ARP kan machines op een subnetwerk helpen om externe subnetten te bereiken zonder routing of een standaardgateway te configureren. Proxy ARP is gedefinieerd in RFC 1027.

Er zijn verschillende nadelen voor proxy-ARP-gebruik. Het kan resulteren in een toename in de hoeveelheid ARP verkeer op het netwerksegment en uitputting van middelen en de man-in-het-midden aanvallen. Proxy ARP presenteert een resource uitputting aanval vector omdat elk uitgesproken ARP verzoek een kleine hoeveelheid geheugen verbruikt. Een aanvaller kan al beschikbaar geheugen uitputten als het een groot aantal ARP verzoeken verstuurt.

Man-in-the-middle aanvallen maken een host op het netwerk mogelijk om het MAC-adres van de router te bezetten, wat resulteert in nietsvermoedende hosts die verkeer naar de aanvaller stuurt. Proxy ARP kan worden uitgeschakeld met de opdracht voor de interfaceconconfiguratie **zonder ip proxy-arp**.

Raadpleeg Proxy ARP inschakelen voor meer informatie over deze functie.

Limiet CPU-effect van verkeer op besturingsplane

De bescherming van het bedieningspaneel is van cruciaal belang. Omdat de prestaties van de toepassing en de ervaring van de eindgebruiker kunnen lijden zonder de aanwezigheid van gegevens en beheersverkeer, zorgt de overlevingsvermogen van het bedieningspaneel ervoor dat de andere twee vliegtuigen behouden blijven en operationeel zijn.

Verkeer van besturingsplane begrijpen

Om het besturingsplane van het Cisco IOS-apparaat goed te beveiligen, is het van essentieel belang om de typen verkeer te begrijpen die door de CPU worden geschakeld. Procesgeschakeld verkeer bestaat normaal uit twee verschillende soorten verkeer. Het eerste type verkeer wordt naar het Cisco IOS apparaat gericht en moet direct door het Cisco IOS apparaat CPU worden verwerkt. Dit verkeer bestaat uit de categorie *Ontvang nabijheidsverkeer*. Dit verkeer bevat een ingang in de Cisco Express Forwarding (CEF)-tabel, waarbij de volgende routerhop het apparaat zelf is, die wordt aangegeven door het begrip ontvangt in de **show ip cef** CLI-uitgang. Deze indicatie is het geval voor een IP-adres dat direct handig gemaakt moet worden door het Cisco IOS-apparaat CPU, dat interface-IP-adressen, multicast-adresruimte en broadcast-adrestoewijzing bevat.

Het tweede type verkeer dat door de CPU wordt verwerkt is gegevensverkeer - verkeer met een bestemming buiten het Cisco IOS-apparaat zelf - waarvoor een speciale verwerking door de CPU nodig is. Hoewel geen uitputtende lijst van CPU-beïnvloedende gegevensverkeer is, worden deze typen verkeer op een proces overgeschakeld en kunnen zij derhalve de werking van het bedieningspaneel beïnvloeden:

- **Vastlegging toegangscontrolelijst** - ACL-logverkeer bestaat uit elke pakketten die gegenereerd worden door een overeenkomst (licentie of ontkennen) van een ACE waarop het logtrefwoord wordt gebruikt.
- **Unicast omgekeerd pad doorsturen (Unicast RPF)** - Unicast RPF, gebruikt in combinatie met ACL, kan in processwitching van bepaalde pakketten resulteren.
- **IP-opties** - Alle IP-pakketten met opties moeten door de CPU worden verwerkt.
- **Fragmentation** - Elk IP-pakket dat fragmentatie vereist, moet aan de CPU worden doorgegeven voor verwerking.
- **Time-to-live (TTL)** Vervaldatum - Packets met een TTL-waarde minder of gelijk aan één waarvoor Internet Control Message Protocol Time Overered (ICMP Type 11, Code 0) moeten worden verzonden, wat leidt tot verwerking in CPU.
- **ICMP Onbereikbaar** - Packets die in ICMP onbereikbare berichten resulteren door routing, MTU of filtering wordt door de CPU verwerkt.
- **Verkeer dat een ARP-aanvraag wordt ingediend** - Bestanden waarvoor een ARP-vermelding niet bestaat, moeten worden verwerkt door de CPU.

- **Niet-IP verkeer** - al het niet-IP verkeer wordt door de CPU verwerkt.

Deze lijst details verscheidene methodes om te bepalen welke types van verkeer door het Cisco IOS apparaat CPU worden verwerkt:

- De opdracht **ip cef** geeft de volgende informatie voor elk IP prefix dat in de CEF-tabel zit. Zoals eerder aangegeven, worden items die bevatten ontvangen als "Volgende hop" beschouwd als nabijheid en geven aan dat verkeer direct naar de CPU moet worden verzonden.

- De opdracht **interface-switching** geeft informatie over het aantal pakketten dat verwerkt wordt door een apparaat.

- De opdracht **tonen IP-verkeer** bevat informatie over het aantal IP-pakketten:

  met een lokale bestemming (dat wil zeggen, ontvang nabijheidsverkeer)met optiesdie fragmentatie vereisendie naar adresruimte worden verzondendie naar multicast adresruimte worden verzonden

- Ontvang nabijheidsverkeer kan door het gebruik van de **show ip cache flow** opdracht worden geïdentificeerd. Alle stromen die bestemd zijn voor het Cisco IOS-apparaat hebben een Destination Interface (DSTIf) van lokaal.

- **Toezicht op besturingsplane** kan worden gebruikt om het type en de snelheid van het verkeer te identificeren dat het besturingsplane van het Cisco IOS-apparaat bereikt. Toezicht op het bedieningspaneel kan worden uitgevoerd door middel van korrelclassificatie ACL's, houtkap en het gebruik van de opdracht **besturing-vlak met** een **toonbeleidslijn**.

Infrastructuur ACL's

Infrastructuur ACL's (iACL's) beperken de externe communicatie tot de apparatuur van het netwerk. ACL's (infrastructuur) vallen uitgebreid onder de sectie Limit Access to the Network met Infrastructuur en ACL's van dit document.

U wordt geadviseerd om iACLs uit te voeren om het controlevliegtuig van alle netwerkapparaten te beschermen.

Ontvangst-ACL's

Voor gedistribueerde platforms kan ontvangerACL's (rACL's) een optie zijn voor Cisco IOS-softwarereleases 12.0(21)S2 voor de 12000 (GSR), 12.0(24)S voor de 7500 en 12.0(31)S voor de 10720. rACL beschermt het apparaat tegen schadelijk verkeer voordat het verkeer de routeprocessor beïnvloedt. Ontvang ACL's (ACL's) zijn ontworpen om alleen het apparaat te beschermen waarop het is ingesteld en transitoverkeer wordt niet door een rACL-toegangsapparaat beïnvloed. Als resultaat hiervan verwijst het IP-adres van de bestemming dat in de onderstaande voorbeelden-items wordt gebruikt, alleen naar de fysieke of virtuele IP-adressen van de router. Ontvang ACL's worden ook beschouwd als de beste praktijk op het gebied van netwerkbeveiliging en moeten worden beschouwd als een aanvulling op de goede netwerkbeveiliging op lange termijn.

Dit is het ontvangen pad ACL dat wordt geschreven om SSH (TCP poort 22) verkeer van vertrouwde hosts op het 192.168.100.0/24 netwerk toe te staan:

```
!
!--- Permit SSH from trusted hosts allowed to the device.
!

access-list 151 permit tcp 192.168.100.0 0.0.0.255 any eq 22
!
!--- Deny SSH from all other sources to the RP.
!

access-list 151 deny tcp any any eq 22
!
!--- Permit all other traffic to the device.
!--- according to security policy and configurations.
!

access-list 151 permit ip any any
!
!--- Apply this access list to the receive path.
!

ip receive access-list 151
!
```

Zie GSR: Ontvang Toegangscontrolelijsten om te helpen om legaal verkeer naar een apparaat te identificeren en toe te staan en ontken alle ongewenste pakketten.

CoPP

De CoPP optie kan ook worden gebruikt om IP-pakketten te beperken die bestemd zijn voor het infrastructuurapparaat. In dit voorbeeld, wordt slechts het verkeer SSH van vertrouwde hosts toegestaan om het Cisco IOS apparaat CPU te bereiken.

> Opmerking: Het laten vallen van verkeer van onbekende of onvertrouwde IP adressen kan hosts met dynamisch toegewezen IP-adressen verhinderen aan het Cisco IOS apparaat te verbinden.

```
!

access-list 152 deny tcp <trusted-addresses> <mask> any eq 22
access-list 152 permit tcp any any eq 22
access-list 152 deny ip any any
!

class-map match-all COPP-KNOWN-UNDESIRABLE
match access-group 152
!

policy-map COPP-INPUT-POLICY
class COPP-KNOWN-UNDESIRABLE
drop
!

control-plane
service-policy input COPP-INPUT-POLICY
```

!
In het vorige CoP voorbeeld, resulteren de ACL ingangen die de onbevoegde pakketten met de de de vergunnings actie aanpassen in een teruggooi van deze pakketten door de beleid-kaart druppelfunctie, terwijl pakketten die de ontkennende actie aanpassen niet door de beleid-kaart valfunctie worden beïnvloed.

CoPP is beschikbaar in Cisco IOS-softwarerelease 12.0S, 12.2SX, 12.2S, 12.3T, 12.4 en 12.4T.

Raadpleeg Toezicht besturingsplane implementeren voor meer informatie over de configuratie en het gebruik van de CoPP-functie.

Bescherming van besturingsplane

CPPr (Control Plane Protection), geïntroduceerd in Cisco IOS-softwarerelease 12.4(4)T, kan worden gebruikt om vliegtuigverkeer dat bestemd is voor de CPU van het Cisco IOS-apparaat te beperken of te controleren. Hoewel vergelijkbaar met CoPP, is CPPr in staat om verkeer met fijnere granulariteit te beperken. CPPr verdeelt het geaggregeerde bedieningspaneel in drie afzonderlijke controlevlakcategorieën die als subinterfaces bekend staan. Subinterfaces bestaan voor verkeerscategorieën Host, Transit en CEF-Exception. Daarnaast bevat CPPr deze bedieningsvlakkigenschappen:

- **Poortfilterfunctie** - Deze functie biedt toezicht op en het neerzetten van pakketten die worden verzonden naar afgesloten of niet-luisterende TCP- of UDP-poorten.

- **Wachtrij-voden** - Deze optie beperkt het aantal pakketten voor een gespecificeerd protocol dat is toegestaan in de IP-invoerwachtrij van het besturingsplane.

Raadpleeg CPPr en Understanding Control Plane Protection (CPPr) voor meer informatie over de configuratie en het gebruik van de CPPr-functie.

Hardware snelheidsbeperkingen

Cisco Catalyst 6500 Series Supervisor Engine 32 en Supervisor Engine 720 voor ondersteuning van platform-specifieke, op hardware gebaseerde snelheidsbeperkingen (HWRL's) voor speciale netwerkscenario's. Deze hardware rate limiters worden aangeduid als 'special case rate limiters' omdat ze een specifieke vooraf gedefinieerde reeks IPv4, IPv6, unicast en multicast DoS-scenario's bestrijken. HWRLs kunnen het Cisco IOS apparaat tegen een verscheidenheid van aanvallen beschermen die pakketten vereisen om door de CPU worden verwerkt.

Er zijn verschillende HWRL's die standaard ingeschakeld zijn. Raadpleeg de op PFC3 hardware gebaseerde Rate Limiter-standaardinstellingen voor meer informatie.

Raadpleeg de op hardware gebaseerde snelheidsbegrenzers in de PFC3 voor meer informatie over HWRL's.

Secure BGP

Het Border Gateway Protocol (BGP) is de routingstichting van het internet. Als zodanig gebruikt elke organisatie met meer dan bescheiden aansluitingsvereisten vaak BGP. BGP wordt vaak het doelwit van aanvallers vanwege de alomtegenwoordigheid en de *set en vergeet* de aard van BGP-configuraties in kleinere organisaties. Er zijn echter veel BGP-specifieke beveiligingsfuncties die u kunt inzetten om de beveiliging van een BGP-configuratie te verbeteren.

Dit geeft een overzicht van de belangrijkste BGP-beveiligingsfuncties. Indien van toepassing, worden er configuratieaanbevelingen gedaan.

Op TTL gebaseerde security Protection

Elk IP-pakket bevat een veld van 1 bytes dat bekend staat als de tijd om te leven (TTL). Elk apparaat dat een IP-pakket koopt, verhoogt deze waarde met één. De startwaarde varieert per besturingssysteem en varieert doorgaans van 64 tot 255. Een pakje wordt verbroken wanneer de TTL-waarde nul bereikt.

Bij een TTL-gebaseerde security Protection Protection wordt de TTL-waarde van IP-pakketten die worden ontvangen van een direct verbonden peer gebruikt, ook bekend als het GTSM-gebaseerde Security Mechanism (GTSM) en BGP TTL Security Hack (BTSH). Deze functie vereist vaak coördinatie van het uitvoeren van routers; als deze echter eenmaal is ingeschakeld, kan zij veel TCP-gebaseerde aanvallen op BGP volledig verslaan.

GTSM voor BGP is ingeschakeld met de optie **TXT-beveiliging** voor de opdracht **voor** de routerconfiguratie van **de** buur BGP. Dit voorbeeld illustreert de configuratie van deze functie:

```
!

router bgp <asn>
neighbor <ip-address> remote-as <remote-asn>
neighbor <ip-address> ttl-security hops <hop-count>
!
```

Aangezien BGP-pakketten worden ontvangen, wordt de TTL-waarde gecontroleerd en moet deze groter zijn dan of gelijk aan 255 minus de opgegeven hoptelling.

BGP Peer-verificatie met MD5

Verificatie door peer met MD5 leidt tot een MD5-overzicht van elk pakket dat als onderdeel van een BGP-sessie wordt verzonden. In het bijzonder worden delen van de IP- en TCP-headers, TCP-payload en een geheime sleutel gebruikt om de samenvatting te genereren.

De gemaakte samenvatting wordt dan opgeslagen in TCP optie Kind 19, dat speciaal voor dit doel door RFC 2385 werd gecreëerd. De ontvangende BGP-luidspreker gebruikt hetzelfde algoritme en dezelfde geheime sleutel om de berichtsamenvatting te regenereren. Als de ontvangen en berekende gesten niet identiek zijn, wordt het pakket weggegooid.

Peer authenticatie met MD5 wordt ingesteld met de **wachtwoordoptie** voor de **buurnaam** BGP-routerconfiguratie. Het gebruik van deze opdracht wordt als volgt geïllustreerd:

```
!

router bgp <asn>
neighbor <ip-address> remote-as <remote-asn>
neighbor <ip-address> password <secret>
!
```

Raadpleeg de buurrouterverificatie voor meer informatie over BGP-peer-verificatie met MD5.

Maximum aantal voorvoegsels instellen

BGP-prefixes worden opgeslagen door een router in het geheugen. Hoe meer prefixes een router moet vasthouden, des te meer geheugen BGP moet consumeren. In sommige configuraties kan een subset van alle Internet prefixes worden opgeslagen, zoals in configuraties die slechts een standaardroute of routes voor de klantennetwerken van een provider hefboomeffect hebben.

Om uitputting van het geheugen te voorkomen, is het belangrijk om het maximum aantal prefixes te configureren dat op een per-peer basis wordt geaccepteerd. Aanbevolen wordt om voor elke BGP-peer een grenswaarde in te stellen.

Wanneer u deze optie aanpast met de opdracht **voor het** maximum**-prefix van de buurrouter** BGP, is er één argument nodig: het maximale aantal prefixes dat wordt geaccepteerd voordat een peer wordt afgesloten. Optioneel kan er ook een getal van 1 tot 100 worden ingevoerd. Dit getal vertegenwoordigt het percentage van de maximum prefixes waarde op welk punt een logbericht wordt verzonden.

```
!

router bgp <asn>
neighbor <ip-address> remote-as <remote-asn>
neighbor <ip-address> maximum-prefix <shutdown-threshold> <log-percent>
!
```

Raadpleeg de BGP-functie voor maximale prefixes voor meer informatie over de maximale prefixes per peer.

BGP-voorvoegsels filteren met prefixlijsten

Met prefixlijsten kan een netwerkbeheerder specifieke prefixes toestaan of ontkennen die via BGP worden verzonden of ontvangen. Voorfixlijsten dienen waar mogelijk te worden gebruikt om er zeker van te zijn dat het netwerkverkeer over de geplande paden wordt verzonden. Prefixlijsten dienen op elke eBGP-peer te worden toegepast in zowel de inkomende als de uitgaande richtingen.

Configureerde voorvoegsellijsten beperken de voorvoegsels die worden verzonden of ontvangen tot de voorvoegsels die specifiek zijn toegestaan door het routeringsbeleid van een netwerk. Als dit niet mogelijk is vanwege het grote aantal ontvangen prefixes, moet een prefix lijst worden geconfigureerd om bekende slechte prefixes specifiek te blokkeren. Deze bekende slechte prefixes omvatten niet toegewezen IP adresruimte en netwerken die voor interne of testdoeleinden door RFC 3330 zijn gereserveerd. Uitgaande prefix lijsten moeten worden geconfigureerd om alleen de prefixes toe te staan die een organisatie wil adverteren.

Dit configuratievoorbeeld gebruikt prefix lijsten om de routes te beperken die worden geleerd en geadverteerd. Met name is alleen een standaardroute toegestaan binnenkomend door voorvoegsellijst BGP-PL-INBOUND, en het voorvoegsel 192.168.2.0/24 is de enige route die mag worden geadverteerd door BGP-PL-OUTBOUND.

```
!

ip prefix-list BGP-PL-INBOUND seq 5 permit 0.0.0.0/0
ip prefix-list BGP-PL-OUTBOUND seq 5 permit 192.168.2.0/24
!

router bgp <asn>
neighbor <ip-address> prefix-list BGP-PL-INBOUND in
```

```
neighbor <ip-address> prefix-list BGP-PL-OUTBOUND out
!
```

Raadpleeg Een serviceprovider aansluiten door Externe BGP te gebruiken voor volledige dekking van BGP-filtering.

BGP-voorvoegsels filteren met autonome toegangslijsten voor het systeem

Met de toegangslijsten van het autonome BGP-systeem (AS) kan de gebruiker ontvangen en geadverteerde prefixes filteren op basis van het AS-pad-kenmerk van een voorvoegsel. Dit kan in combinatie met prefixlijsten worden gebruikt om een robuuste set filters op te zetten.

Dit configuratievoorbeeld gebruikt de lijsten van de toegang tot pad van AS om inkomende prefixes te beperken tot die die voortkomen uit het afgelegen AS en uitgaande prefixes tot die veroorzaakt door het lokale autonome systeem. Prefixes die uit alle andere autonome systemen komen worden gefilterd en niet in de routingtabel geïnstalleerd.

```
!

ip as-path access-list 1 permit ^65501$
ip as-path access-list 2 permit ^$
!

router bgp <asn>
neighbor <ip-address> remote-as 65501
neighbor <ip-address> filter-list 1 in
neighbor <ip-address> filter-list 2 out
!
```

Secure Interior Gateway-protocollen

Het vermogen van een netwerk om goed door te sturen verkeer en van topologie veranderingen of fouten terug te krijgen is afhankelijk van een nauwkeurige weergave van de topologie. U kunt vaak een Interior Gateway Protocol (IGP) gebruiken om deze weergave te geven. Standaard zijn IGP's dynamisch en ontdekken ze extra routers die communiceren met de gebruikte IGP. IGP's ontdekken ook routes die tijdens een storing van de netwerklink kunnen worden gebruikt.

Deze subsecties geven een overzicht van de belangrijkste IGP security kenmerken. Aanbevelingen en voorbeelden die Routing Information Protocol, versie 2 (RIPv2), Enhanced Interior Gateway Routing Protocol (DHCP) en Open Shortest Path First (OSPF) omvatten, worden indien nodig geleverd.

Routing Protocol-verificatie en -verificatie met berichtversie 5

Als u de uitwisseling van routeinformatie niet wilt beveiligen, kan een aanvaller valse routinginformatie in het netwerk introduceren. Door wachtwoordverificatie te gebruiken met protocollen tussen routers, kunt u de beveiliging van het netwerk verbeteren. Maar omdat deze authenticatie verzonden wordt als cleartext, kan het voor een aanvaller eenvoudig zijn om deze veiligheidscontrole te ondermijnen.

Door MD5 knoeikfuncties aan het authentificatieproces toe te voegen, bevat het routing updates niet langer kletswachtwoorden, en de gehele inhoud van de routingupdate is resistenter voor het knoeien. MD5-verificatie is echter nog steeds vatbaar voor bruut geweld en woordenboekaanvallen wanneer een zwakke wachtwoorden zijn geselecteerd. U wordt

aangeraden wachtwoorden te gebruiken met voldoende randomisatie. Aangezien MD5-verificatie veel veiliger is in vergelijking met wachtwoordverificatie, zijn deze voorbeelden specifiek voor MD5-verificatie. IPSec kan ook worden gebruikt om routingprotocollen te valideren en te beveiligen, maar deze voorbeelden gedetailleerd het gebruik ervan niet.

DHCP en RIPv2 gebruiken Belangrijkste Ketens als deel van de configuratie. *Raadpleeg de* sleutel voor meer informatie over de configuratie en het gebruik van Key Chains.

Dit is een voorbeeldconfiguratie voor Ecu routerverificatie met MD5:

```
!

key chain <key-name>
key <key-identifier>
key-string <password>
!

interface <interface>
ip authentication mode eigrp <as-number> md5
ip authentication key-chain eigrp <as-number> <key-name>
!
```

Dit is een voorbeeld MD5 router-verificatieconformatie voor RIPv2. RIPv1 ondersteunt geen verificatie.

```
!

key chain <key-name>
key <key-identifier>
key-string <password>
!

interface <interface>
ip rip authentication mode md5
ip rip authentication key-chain <key-name>
!
```

Dit is een voorbeeldconfiguratie voor OSPF-routerverificatie met behulp van MD5. OSPF maakt geen gebruik van Key Chains.

```
!

interface <interface>
ip ospf message-digest-key <key-id> md5 <password>
!

router ospf <process-id>
network 10.0.0.0 0.255.255.255 area 0
area 0 authentication message-digest
!
```

Raadpleeg OSPF-configuratie voor meer informatie.

Opdrachten met passieve interface

Informatie-lekken, of de introductie van valse informatie in een IGP, kunnen worden beperkt door gebruik te maken van de **passief-interface** opdracht die helpt bij het controleren van de advertentie

van routinginformatie. U wordt geadviseerd geen informatie aan netwerken bekend te maken die buiten uw administratieve controle vallen.

Dit voorbeeld laat het gebruik van deze functie zien:

```
!

router eigrp <as-number>
passive-interface default
no passive-interface <interface>
!
```

Routefiltering

Om de mogelijkheid te verminderen dat u valse routinginformatie in het netwerk introduceert, moet u Routefiltering gebruiken. In tegenstelling tot de opdracht van de **passieve-interface** routerconfiguratie, treedt de routing op op interfaces zodra routingfiltering is ingeschakeld, maar de informatie die wordt geadverteerd of verwerkt is beperkt.

Voor wanneer wanneer u een **signaal** wilt gebruiken, of wanneer u een opdracht **verdeelt** met het **uitrolsleutelwoord**, beperkt het gebruik van de **in** sleutelwoorden wordt gebruikt welke updates worden verwerkt. Het bevel **van de** distributie-lijst is beschikbaar voor OSPF, maar het voorkomt geen router van het propageren van gefilterde routes. In plaats daarvan kan de opdracht **Gebiedsfilter-lijsten** worden gebruikt.

Dit voorbeeld EHRM filtert uitgaande advertenties met de opdracht **verdelingslijst** en een voorvoegsellijst:

```
!

ip prefix-list <list-name> seq 10 permit <prefix>
!

router eigrp <as-number>
passive-interface default
no passive-interface <interface>
distribute-list prefix <list-name> out <interface>
!
```

Dit voorbeeld EHW vult inkomende updates met een voorvoegsellijst in:

```
!

ip prefix-list <list-name> seq 10 permit <prefix>
!

router eigrp <as-number>
passive-interface default
no passive-interface <interface>
distribute-list prefix <list-name> in <interface>
!
```

Raadpleeg het configureren van IP-routingprotocol-onafhankelijke functies voor meer informatie over hoe u de reclame en verwerking van routingupdates kunt controleren.

Dit voorbeeld OSPF gebruikt een prefixlijst met de OSPF-specifieke **gebiedsfilter-lijst** opdracht:

```
!

ip prefix-list <list-name> seq 10 permit <prefix>
!

router ospf <process-id>
area <area-id> filter-list prefix <list-name> in
!
```

Verbruik van routingbronnen

Routing Protocol prefixes worden opgeslagen door een router in het geheugen, en resource consumptie stijgt met extra prefixes die een router moet vasthouden. Om uitputting van middelen te voorkomen, is het belangrijk om het routeringsprotocol te configureren om verbruik van hulpbronnen te beperken. Dit is mogelijk met OSPF als u de optie Verticale database overload gebruikt.

Dit voorbeeld toont configuratie van de OSPF Link State Database Overload Protection optie:

```
!

router ospf <process-id>
max-lsa <maximum-number>
!
```

Raadpleeg het aantal zelfgenererende LSA's voor een OSPF-proces voor meer informatie over OSPF Link State Database Overload Protection.

Secure First hop-redundantieprotocollen

First Hopredundantie Protocols (FHRP's) bieden veerkracht en redundantie voor apparaten die als standaardgateways fungeren. Deze situatie en deze protocollen zijn gebruikelijk in omgevingen waar een paar apparaten van Layer 3 de standaardgatewayfunctionaliteit biedt voor een netwerksegment of een reeks VLAN's die servers of werkstations bevatten.

Het Gateway taakverdeling Protocol (GLBP), Hot Standby Router Protocol (HSRP) en Virtual Router Redundancy Protocol (VRRP) zijn alle FHRP's. Standaard communiceren deze protocollen met niet-geauthentiseerde communicatie. Dit soort communicatie kan een aanvaller in staat stellen om als FHRP-sprekend apparaat de standaard gateway rol op het netwerk op zich te nemen. Deze overname zou een aanvaller in staat stellen om een man-in-het-midden aanval uit te voeren en al gebruikersverkeer dat het netwerk afsluit te onderscheppen.

Om dit type aanval te voorkomen, omvatten alle FHRP's die door Cisco IOS-software worden ondersteund, een authenticatiecapaciteit met MD5 of tekstkoorden. Vanwege de dreiging die uitgaat van niet-geauthentiseerde FHRP's wordt aanbevolen dat instanties van deze protocollen MD5-verificatie gebruiken. Dit configuratievoorbeeld toont het gebruik van GLBP, HSRP, en VRRP MD5 authenticatie aan:

```
!

interface FastEthernet 1
description *** GLBP Authentication ***
glbp 1 authentication md5 key-string <glbp-secret>
glbp 1 ip 10.1.1.1
```

```
!

interface FastEthernet 2
description *** HSRP Authentication ***
standby 1 authentication md5 key-string <hsrp-secret>
standby 1 ip 10.2.2.1
!

interface FastEthernet 3
description *** VRRP Authentication ***
vrrp 1 authentication md5 key-string <vrrp-secret>
vrrp 1 ip 10.3.3.1
!
```

datacentrum

Hoewel het gegevensvliegtuig verantwoordelijk is voor het verplaatsen van gegevens van bron naar bestemming, is het gegevensvliegtuig binnen de context van beveiliging het minst belangrijke van de drie vlakken. Om deze reden is het belangrijk om de beheers- en besturingsplane in plaats van het gegevensvlak te beschermen wanneer u een netwerkapparaat vastlegt.

Maar binnen het gegevensvliegtuig zelf zijn er veel functies en configuratieopties die een veilig verkeer kunnen helpen. Deze secties gedetailleerd deze eigenschappen en opties zodat u uw netwerk makkelijker kunt beveiligen.

Algemene gegevensstructuur hardnekkig

Het overgrote deel van gegevensverkeer stroomt over het netwerk zoals bepaald door de routeconfiguratie van het netwerk. IP-netwerkfunctionaliteit bestaat echter om het pad van pakketten in het netwerk te wijzigen. Kenmerken zoals IP-opties, specifiek de bron-routingoptie, vormen een beveiligingsprobleem in de huidige netwerken.

Het gebruik van transito-ACL's is ook relevant voor de verharding van het gegevensvliegtuig.

Zie het gedeelte Transitoverkeer met transito-ACL's van dit document voor meer informatie.

IP-opties - selectieve drop

Er zijn twee veiligheidsoverwegingen die door IP-opties worden voorgesteld. Het verkeer dat IP-opties bevat moet door Cisco IOS-apparaten worden verwerkt, wat kan leiden tot een hogere CPU-lading. IP-opties omvatten ook de functionaliteit om het pad te wijzigen dat door het netwerk wordt gevolgd, waardoor beveiligingscontroles mogelijk kunnen worden omgedraaid.

Als gevolg van deze zorgen **vallen** de **ip-opties** van de configuratie **van het** mondiale **IP | Negeer** is toegevoegd aan Cisco IOS-softwarereleases 12.3(4)T, 12.0(22)S en 12.2(25)S. In de eerste vorm van deze opdracht, **vallen** de **ip-opties**, alle IP-pakketten die IP-opties bevatten die door het Cisco IOS-apparaat worden ontvangen, worden ingetrokken. Dit voorkomt zowel de verhoogde lading van CPU als mogelijke subversie van veiligheidscontroles die IP-opties kunnen inschakelen.

De tweede vorm van deze opdracht, **ip opties negeren**, vormt het Cisco IOS apparaat om IP opties te negeren die in ontvangen pakketten vervat zijn. Hoewel dit de bedreigingen met betrekking tot IP-opties voor het lokale apparaat verzacht, is het mogelijk dat downstreamapparaten kunnen worden beïnvloed door de aanwezigheid van IP-opties. Dit is de reden dat de valvorm van deze opdracht sterk wordt aanbevolen. Dit wordt aangetoond in het configuratievoorbeeld:

```
!
ip options drop
!
```

Let op dat sommige protocollen, bijvoorbeeld RSVP, bij rechtmatig gebruik van IP-opties maken. De functionaliteit van deze protocollen wordt beïnvloed door deze opdracht.

Nadat IP Opties Selectieve Drop is ingeschakeld, kan de opdracht **show ip traffic** EXEC worden gebruikt om het aantal pakketten te bepalen dat wordt ingetrokken vanwege de aanwezigheid van IP-opties. Deze informatie is aanwezig in de afdruppelteller.

Raadpleeg de selectieve *vervolgkeuzelijst* ACL-opties voor meer informatie over deze functie.

IP-brontrouting uitschakelen

IP-bronrouting maakt gebruik van de opties Lose Source Route Route en Record Route in dem of de strikte Source Route samen met de optie Record Route om de bron van het IP-datagram aan te passen om het netwerkpad te specificeren dat een pakje neemt. Deze functionaliteit kan worden gebruikt in pogingen om verkeer rond veiligheidscontroles in het netwerk te leiden.

Als IP-opties niet volledig uitgeschakeld zijn via de functie Opties Selectieve drop, is het belangrijk dat IP-bronrouting wordt uitgeschakeld. IP bron routing, die standaard ingeschakeld is in alle Cisco IOS-softwarereleases, wordt uitgeschakeld via het commando **van** wereldwijde configuratie **van** de **IP-bron**. Dit configuratievoorbeeld illustreert het gebruik van deze opdracht:

```
!
no ip source-route
!
```

ICMP-omleidingen uitschakelen

ICMP-omleidingen worden gebruikt om een netwerkapparaat te informeren over een beter pad naar een IP-bestemming. Standaard verstuurt de Cisco IOS-software een OCR-verbinding als deze een pakket ontvangt dat door de interface moet worden verzonden.

In sommige situaties, zou het voor een aanvaller mogelijk kunnen zijn om het Cisco IOS apparaat te veroorzaken om veel ICMP om berichten te verzenden opnieuw richten, wat in een verhoogde lading van CPU resulteert. Om deze reden wordt aanbevolen de overdracht van ICMP-omleidingen uit te schakelen. ICMP-omleidingen zijn uitgeschakeld met de **opdracht** voor **omleidingen van** de interface**, zoals in de voorbeeldconfiguratie wordt** getoond:

```
!

interface FastEthernet 0
no ip redirects
!
```

IP-gerichte omroepen uitschakelen of beperken

IP Directed Broadcasts maken het mogelijk om een IP-uitzendingspakket naar een externe IP-telefoon te verzenden. Zodra het het externe netwerk bereikt, verstuurt IP het apparaat het pakket als Layer 2-uitzending naar alle stations op het netwerk. Deze gerichte omroepfunctie is als versterker en reflectiehulpmiddel ingezet bij verschillende aanvallen, waaronder de aanslag op het

smurf.

Huidige versies van Cisco IOS-software hebben deze functionaliteit standaard uitgeschakeld; het kan echter worden ingeschakeld via de opdracht voor het configureren van **ip-radio-**interface. releases van Cisco IOS-software voorafgaand aan 12.0 hebben deze functionaliteit standaard ingeschakeld.

Als een netwerk absoluut behoefte heeft aan gerichte uitzending, moet het gebruik ervan worden gecontroleerd. Dit is mogelijk met het gebruik van een toegangscontrolelijst als optie voor de **ip gericht-uitzending** opdracht. Dit configuratievoorbeeld beperkt geregisseerde uitzendingen naar die UDP pakketten die bij een vertrouwd netwerk, 192.168.1.0/24 van oorsprong zijn:

```
!

access-list 100 permit udp 192.168.1.0 0.0.0.255 any
!

interface FastEthernet 0
ip directed-broadcast 100
!
```

Filterverkeer met transito-ACL's

Het is mogelijk om te controleren wat het verkeer het netwerk overbrengt met het gebruik van transito ACL's (tACL's). Dit is in tegenstelling tot infrastructuur ACL's die verkeer proberen te filteren dat voor het netwerk zelf bestemd is. Het filtreren dat door tACLs wordt verstrekt is voordelig wanneer het wenselijk is om verkeer naar een bepaalde groep apparaten of verkeer te filtreren die het netwerk overbrengt.

Dit type filtering wordt traditioneel door firewalls uitgevoerd. Er zijn echter gevallen waarin het goed kan zijn om dit filteren op een Cisco IOS-apparaat in het netwerk uit te voeren, bijvoorbeeld, waar filtering moet worden uitgevoerd maar er geen firewall is aanwezig.

Transit ACL's zijn ook een geschikte plaats om statische bescherming tegen spoofing toe te passen.

Raadpleeg het gedeelte Anti-Spoofing Protection van dit document voor meer informatie.

Raadpleeg Transit Access Control Lists: Filtering aan Uw Rand voor meer informatie over tACLs.

ICMP-pakketfiltering

Het Internet Control Message Protocol (ICMP) is ontworpen als een controleprotocol voor IP. Als dergelijk, kunnen de berichten die het transporteert vergaande implicaties hebben op de TCP- en IP-protocollen in het algemeen. ICMP wordt gebruikt door de gereedschappen voor netwerkprobleemoplossing **ping** en **traceroute**, alsmede door de detectie van padMTU's; externe ICMP-connectiviteit is echter zelden nodig voor de juiste werking van een netwerk.

Cisco IOS-software biedt functionaliteit om ICMP-berichten door naam of type en code specifiek te filteren. Dit voorbeeld ACL staat ICMP van vertrouwde netwerken toe terwijl het alle pakketten ICMP van andere bronnen blokkeert:

```
!

ip access-list extended ACL-TRANSIT-IN
!
!--- Permit ICMP packets from trusted networks only
!

permit icmp host <trusted-networks> any
!
!--- Deny all other IP traffic to any network device
!

deny icmp any any
!
```

IP-fragmentaties filteren

Zoals eerder in het gedeelte Limit Access to the Network met Infrastructuur ACL's van dit document gedetailleerd is, kan het filteren van gefragmenteerde IP-pakketten security apparaten uitdagen.

Vanwege de niet-intuïtieve aard van fragmentatieverwerking worden IP-fragmenten door ACL's vaak per ongeluk toegestaan. Fragmentation wordt ook vaak gebruikt in pogingen om detectie door inbraakdetectiesystemen te ontwijken. Het is om deze redenen dat IP-fragmenten vaak in aanvallen worden gebruikt en expliciet in de top van geconfigureerde ACL's moeten worden gefilterd. Het ACL-bestand hieronder bevat uitgebreide filtering van IP-fragmenten. De in dit voorbeeld geïllustreerde functionaliteit moet worden gebruikt in samenhang met de functionaliteit van de voorgaande voorbeelden:

```
!

ip access-list extended ACL-TRANSIT-IN
!
!--- Deny IP fragments using protocol-specific ACEs to aid in
!--- classification of attack traffic
!

deny tcp any any fragments
deny udp any any fragments
deny icmp any any fragments
deny ip any any fragments
!
```

Raadpleeg Toegangscontrolelijsten en IP-fragmentaties voor meer informatie over ACL-verwerking van gefragmenteerde IP-pakketten.

ACL-ondersteuning voor filtering van IP-opties

In Cisco IOS-softwarerelease 12.3(4)T en hoger ondersteunt Cisco IOS-software het gebruik van ACL's om IP-pakketten te filteren op basis van de IP-opties die in het pakket zitten. De aanwezigheid van IP-opties in een pakje kan duiden op een poging om de beveiligingsinstellingen in het netwerk te ondermijnen of op een andere manier de doorvoerkenmerken van een pakje te wijzigen. Om deze redenen moeten IP-pakketten met opties worden gefilterd aan de rand van het netwerk.

Dit voorbeeld moet met de inhoud uit vorige voorbeelden worden gebruikt om het volledige filteren van IP pakketten op te nemen die IP opties bevatten:

```
!

ip access-list extended ACL-TRANSIT-IN
!
!--- Deny IP packets containing IP options
!

deny ip any any option any-options
!
```

Beschermingen tegen schuimvorming

Vele aanvallen gebruiken bron IP adres spoofing om effectief te zijn of om de ware bron van een aanval te verbergen en nauwkeurige traceerbaarheid te belemmeren. Cisco IOS-software biedt Unicast RPF en IP Source Guard (IPSG) om aanvallen af te schrikken die afhankelijk zijn van bron IP-adresspoofing. Daarnaast worden ACL's en ongeldige routing vaak gebruikt als een handmatige manier om te voorkomen.

IP Source Guard werkt om spoofing voor netwerken te minimaliseren die onder directe administratieve controle zijn door switchpoort, het adres van MAC, en de controle van het bronadres uit te voeren. Unicast RPF verstrekt de controle van het bronnetwerk en kan spoofed aanvallen van netwerken verminderen die niet onder directe administratieve controle zijn. Poortbeveiliging kan worden gebruikt om MAC-adressen op de toegangslaag te valideren. Dynamic Address Resolutie Protocol (ARP) Inspection (DAI) minimaliseert aanval vectoren die ARP-vergiftiging op lokale segmenten gebruiken.

Unicast RPF

Unicast RPF laat een apparaat toe om te verifiëren dat het bronadres van een doorgestuurd pakket door de interface kan worden bereikt die het pakket ontving. U mag niet vertrouwen op Unicast RPF als de enige bescherming tegen spoofing. Gespoelde pakketten kunnen het netwerk door een Unicast RPF-enabled interface binnendringen als een aangewezen terugkeerroute naar het bron IP adres bestaat. Unicast RPF is afhankelijk van u om het doorsturen van Cisco Express op elk apparaat toe te laten en wordt gevormd op een per-interface basis.

Unicast RPF kan in een van twee modi worden ingesteld: los of streng. In gevallen waar er een asymmetrische routing is, heeft deze vrije modus de voorkeur omdat de strikte modus bekend is om pakketten in deze situaties te laten vallen. Tijdens configuratie van de **ip** de opdracht van de interfaceconfiguratie **verifieert**, **vormt** het sleutelwoord **om het even welke** losse modus terwijl het sleutelwoord **rx** strikte wijze vormt.

Dit voorbeeld illustreert de configuratie van deze functie:

```
!

ip cef
!

interface <interface>
ip verify unicast source reachable-via <mode>
!
```

Raadpleeg het gedeelte Unicast omgekeerde pad doorsturen voor meer informatie over de configuratie en het gebruik van Unicast RPF.

IP-bronbewaking

IP Source Guard is een effectief middel om spoofing preventie te voorkomen die kan worden gebruikt als u controle over Layer 2 interfaces hebt. IP Source Guard gebruikt informatie van DHCP-spionage om dynamisch een Port Access Control List (PACL) op de Layer 2-interface te configureren en elk verkeer van IP-adressen te ontkennen die niet in de IP-bronbindende tabel zijn gekoppeld.

IP Source Guard kan worden toegepast op Layer 2-interfaces die behoren tot DHCP snooping-enabled VLAN's. Met deze opdrachten kan DHCP-snooping worden uitgevoerd:

```
!

ip dhcp snooping
ip dhcp snooping vlan <vlan-range>
!
```

Nadat DHCP-snooping is ingeschakeld, schakelen deze opdrachten IPSG in:

```
!
interface <interface-id>
ip verify source
!
```

Poortbeveiliging kan worden ingeschakeld met de opdracht **voor het** configureren **van** de **bronpoortbeveiliging**. Dit vereist de **optie** voor **informatie over** het **snuffelen** van **IP-dhcp** van de configuratie; Bovendien moet de DHCP-server DHCP-optie 82 ondersteunen.

Raadpleeg de DHCP-functies en IP-bronbewaking voor meer informatie over deze functie.

Poortbeveiliging

Poortbeveiliging wordt gebruikt om het MAC-adres spoofing op de toegangsinterface te beperken. Poortbeveiliging kan dynamisch geleerde (kleverige) MAC-adressen gebruiken om de eerste configuratie te vergemakkelijken. Zodra de havenveiligheid een MAC schending heeft bepaald, kan het één van de vier overschrijvingswijzen gebruiken. Deze modi zijn VLAN beveiligen, beperken, afsluiten en sluiten. In gevallen waarin een poort slechts toegang biedt voor één werkstation met het gebruik van standaardprotocollen, kan een maximum aantal van één voldoende zijn. Protocols die virtuele MAC-adressen maken zoals HSRP, werken niet wanneer het maximum aantal wordt ingesteld op één.

```
!

interface <interface>
switchport
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum <number>
switchport port-security violation <violation-mode>
!
```

Raadpleeg Port Security *configureren* voor meer informatie over de poortbeveiliging.

Dynamische ARP-inspectie

Dynamic ARP Inspection (DAI) kan worden gebruikt om ARP-vergiftigingsaanvallen op lokale segmenten te verzachten. Een ARP-vergiftigingsaanval is een methode waarbij een aanvaller vervalste ARP-informatie naar een lokaal segment stuurt. Deze informatie wordt ontworpen om het ARP cache van andere apparaten te corrumperen. Vaak gebruikt een aanvaller ARP-vergiftiging om een man-in-de-middenaanval uit te voeren.

DAI onderschept en bevestigt de IP-to-MAC adresverhouding van alle ARP pakketten op onvertrouwde poorten. In DHCP-omgevingen gebruikt DAI de gegevens die gegenereerd worden door de DHCP-snooping functie. ARP-pakketten die op vertrouwde interfaces worden ontvangen, worden niet gevalideerd en ongeldige pakketten op onvertrouwde interfaces worden vernietigd. In niet-DHCP-omgevingen is het gebruik van ARP ACL's vereist.

Met deze opdrachten kan DHCP-snooping worden uitgevoerd:

```
!
ip dhcp snooping
ip dhcp snooping vlan <vlan-range>
!
```

Nadat DHCP-snooping is ingeschakeld, schakelen deze opdrachten DAI in:

```
!
ip arp inspection vlan <vlan-range>
!
```

In niet DHCP-omgevingen zijn ARP ACL's vereist om DAI in te schakelen. Dit voorbeeld demonstreert de basisconfiguratie van DAI met ARP ACL's:

```
!

arp access-list <acl-name>
permit ip host <sender-ip> mac host <sender-mac>
!

ip arp inspection filter <arp-acl-name> vlan <vlan-range>
!
```

DAi kan ook per interface worden ingeschakeld, waar dat wordt ondersteund.

```
ip arp inspection limit rate <rate_value> burst interval <interval_value>
```

Raadpleeg Dynamische ARP-inspectie configureren voor meer informatie over de manier waarop u DAI kunt configureren.

Anti-Spoofing ACL's

Handmatig geconfigureerd ACL's kunnen statische anti-spoofing bescherming bieden tegen aanvallen die bekende ongebruikte en onvertrouwde adresruimte gebruiken. Deze anti-spoofing ACL's worden vaak toegepast op toegangsverkeer op netwerkgrenzen als onderdeel van een grotere ACL-toegangscontrolelijst. Anti-spoofing ACL's vereisen regelmatige controle omdat ze vaak kunnen veranderen. Spoofing kan in verkeer worden geminimaliseerd dat van het lokale netwerk afkomstig is als u uitgaande ACL's toepast die het verkeer beperken tot geldige lokale adressen.

Dit voorbeeld laat zien hoe ACLs kan worden gebruikt om IP spoofing te beperken. Dit ACL wordt

binnenkomend op de gewenste interface toegepast. De ACE's die uit deze ACL bestaan zijn niet uitgebreid. Als u deze typen ACL's configureren hebt u een actuele referentie nodig die beslissend is.

```
!

ip access-list extended ACL-ANTISPOOF-IN
deny ip 10.0.0.0 0.255.255.255 any
deny ip 192.168.0.0 0.0.255.255 any
!

interface <interface>
ip access-group ACL-ANTISPOOF-IN in
!
```

Raadpleeg de veelgebruikte IP-ACL's configureren voor meer informatie over het configureren van toegangscontrolelijsten.

De officiële lijst van niet toegewezen internetadressen wordt door Team Cymru bewaard. Aanvullende informatie over het filteren van ongebruikte adressen is beschikbaar op de Bogon Referentiepagina.

Limiet CPU-effect van verkeer van datacenters

Het primaire doel van routers en switches is pakketten en frames door het apparaat naar eindbestemmingen te sturen. Deze pakketten, die de apparaten die door het netwerk worden gebruikt, kunnen de operaties van CPU van een apparaat beïnvloeden. Het gegevensvliegtuig, dat bestaat uit verkeer dat het netwerkapparaat overbrengt, moet worden vastgezet om de werking van het beheers- en besturingsplane te garanderen. Indien het transitoverkeer een inrichting kan doen om het switchverkeer te verwerken, kan het bedieningsvlak van een inrichting worden beïnvloed, hetgeen tot een operationele verstoring kan leiden.

Functies en verkeerstypen die van invloed zijn op de CPU

Hoewel deze lijst niet volledig is, bevat deze lijst ook soorten gegevensverkeer die speciale CPU-verwerking vereisen en die door de CPU worden geschakeld:

- **Vastlegging ACL** - Het logverkeer van ACL bestaat uit om het even welke pakketten die door een overeenkomst (vergunning of ontkenning) van een ACE worden gegenereerd waarop het **logsleutelwoord** wordt gebruikt.
- **Unicast RPF** - Unicast RPF die in combinatie met ACL wordt gebruikt kan in het proces van het overschakelen van bepaalde pakketten resulteren.
- **IP-opties** - Alle IP-pakketten met opties moeten door de CPU worden verwerkt.
- **Fragmentation** - Elk IP-pakket dat fragmentatie vereist, moet aan de CPU worden doorgegeven voor verwerking.
- **Time-to-Live (TTL)** Vervaldatum - Packets met een TTL-waarde minder of gelijk aan 1 vereisen dat de **Multiservice** Message Protocol Time Overschot (ICMP Type 11, Code 0) wordt verzonden, wat resulteert in CPU-verwerking.

- **ICMP Onbereikbaar** - pakketten die in ICMP onbereikbare berichten door routing, MTU of filtering opleveren worden door de CPU verwerkt.

- **Verkeer dat een ARP-aanvraag wordt ingediend** - Bestanden waarvoor een ARP-vermelding niet bestaat, moeten worden verwerkt door de CPU.

- **Niet-IP verkeer** - al het niet-IP verkeer wordt door de CPU verwerkt.

Zie het gedeelte General Data Plane Hardening van dit document voor meer informatie over het hardmaken van datacenters.

Filteren op TTL-waarde

U kunt de ACL-ondersteuning gebruiken voor filtering op TTL-waarde, geïntroduceerd in Cisco IOS-softwarerelease 12.4(2)T, in een uitgebreide IP-toegangslijst naar filterpakketten op basis van TTL-waarde. Deze optie kan worden gebruikt om een apparaat te beschermen dat doorvoerverkeer ontvangt wanneer de TTL-waarde een nul of één is. Filtering van pakketten die op TTL-waarden zijn gebaseerd, kan ook worden gebruikt om te verzekeren dat de TTL-waarde niet lager is dan de diameter van het netwerk, en zo het besturingsplane van stroomafwaarts gerichte infrastructuren tegen TTL-aanvallen wordt beschermd.

Merk op dat sommige toepassingen en hulpmiddelen zoals **Traceroute** TTL pakketten voor test en diagnostische doeleinden gebruiken. Sommige protocollen, zoals IGMP, gebruiken legaal een TTL-waarde van één.

Dit ACL-voorbeeld maakt een beleid dat IP-pakketten filtert waarop de TTL-waarde minder dan 6 is.

```
!
!--- Create ACL policy that filters IP packets with a TTL value
!--- less than 6
!

ip access-list extended ACL-TRANSIT-IN
deny ip any any ttl lt 6
permit ip any any
!
!--- Apply access-list to interface in the ingress direction
!

interface GigabitEthernet 0/0
ip access-group ACL-TRANSIT-IN in
!
```

Raadpleeg de TTL *Vertaalde* Attack Identification and Mitigation voor meer informatie over het filteren van pakketten op basis van de TTL-waarde.

Raadpleeg ACL-ondersteuning voor filtering op TTL-waarde voor meer informatie over deze functie.

In Cisco IOS-softwarerelease 12.4(4)T en later stelt Flexibel Packet matching (FPM) een beheerder in om op willekeurige bits van een pakket te overeenkomen. Dit FPM-beleid druppelt pakketten in met een TTL-waarde van minder dan zes.

```
!

load protocol flash:ip.phdf
!

class-map type access-control match-all FPM-TTL-LT-6-CLASS
match field IP ttl lt 6
!

policy-map type access-control FPM-TTL-LT-6-DROP-POLICY
class FPM-TTL-LT-6-CLASS
drop
!

interface FastEthernet0
service-policy type access-control input FPM-TTL-LT-6-DROP-POLICY
!
```

Raadpleeg Flexibele pakketmatching, op de Cisco IOS Flexibele Packet matching startpagina voor meer informatie over de functie.

Filteren op aanwezigheid van IP-opties

In Cisco IOS-softwarerelease 12.3(4)T en later kunt u de ACL-ondersteuning gebruiken voor de filtering van IP-opties in een genoemde, uitgebreide IP-toegangslijst om IP-pakketten met huidige opties te filteren. IP-pakketten filteren die zijn gebaseerd op de aanwezigheid van IP-opties, kunnen ook worden gebruikt om te voorkomen dat het besturingsplane van infrastructuurapparaten deze pakketten op het CPU-niveau moet verwerken.

Merk op dat de ACL-ondersteuning voor het filteren van IP-opties alleen gebruikt kan worden met benoemde, uitgebreide ACL's. Houd er ook rekening mee dat RSVP, Multiprotocol Label Switching Traffic Engineering, IGMP versies 2 en 3 en andere protocollen die IP-opties gebruiken, mogelijk niet goed kunnen werken als pakketten voor deze protocollen worden verzonden. Als deze protocollen in het netwerk worden gebruikt, kan de ACL-ondersteuning voor filtering van IP-opties worden gebruikt. Maar de ACL IP Opties Selective Drop kan dit verkeer wel laten vallen en deze protocollen kunnen niet goed werken. Als er geen protocollen in gebruik zijn die IP-opties vereisen, is de selectieve Drop van ACL-opties de gewenste methode om deze pakketten te laten vallen.

Dit ACL-voorbeeld maakt een beleid dat IP-pakketten filtreert die IP-opties bevatten:

```
!

ip access-list extended ACL-TRANSIT-IN
deny ip any any option any-options
permit ip any any
!

interface GigabitEthernet 0/0
ip access-group ACL-TRANSIT-IN in
!
```

Dit voorbeeld ACL demonstreert een beleid dat IP pakketten met vijf specifieke IP opties filtert. Pakketten die deze opties bevatten worden geweigerd:

- 0 Einde opties (pool)

- 7 Record Route (record-route)
- 68 Time Stamp (tijdstempel)
- 131 - losse bronrouter (LSR)
- 137 - Streng Source Route (ssr)

```
!

ip access-list extended ACL-TRANSIT-IN
deny ip any any option eool
deny ip any any option record-route
deny ip any any option timestamp
deny ip any any option lsr
deny ip any any option ssr
permit ip any any
!

interface GigabitEthernet 0/0
ip access-group ACL-TRANSIT-IN in
!
```

Zie het gedeelte General Data Plane Hardening van dit document voor meer informatie over ACL IP Opties Selective Drop.

Raadpleeg Transit Access Control Lists: Filtering aan Uw Rand voor meer informatie over het filteren van douanevervoer en randverkeer.

Een andere optie in Cisco IOS-software die kan worden gebruikt om pakketten met IP-opties te filteren, is CoPP. In Cisco IOS-softwarerelease 12.3(4)T en later staat CoPP een beheerder toe om de verkeersstroom van besturingsplannen pakketten te filteren. Een apparaat dat Ondersteuning van CoPP en ACL ondersteunt voor het filteren van IP-opties, geïntroduceerd in Cisco IOS-softwarerelease 12.3(4)T, kan een toegangslijstbeleid gebruiken om pakketten te filteren die IP-opties bevatten.

Dit CoP-beleid daalt de doorvoerpakketten die door een apparaat worden ontvangen wanneer er IP-opties aanwezig zijn:

```
!

ip access-list extended ACL-IP-OPTIONS-ANY
permit ip any any option any-options
!

class-map ACL-IP-OPTIONS-CLASS
match access-group name ACL-IP-OPTIONS-ANY
!

policy-map COPP-POLICY
class ACL-IP-OPTIONS-CLASS
drop
!

control-plane
```

```
service-policy input COPP-POLICY
!
```

Dit CoP-beleid vermindert doorvoerpakketten die door een apparaat worden ontvangen wanneer deze IP-opties aanwezig zijn:

- 0 Einde opties (pool)
- 7 Record Route (record-route)
- 68 Time Stamp (tijdstempel)
- 1310 LASSE Bron-router (LSR)
- 1370 strikte bronrouter (ssr)

```
!

ip access-list extended ACL-IP-OPTIONS
permit ip any any option eool
permit ip any any option record-route
permit ip any any option timestamp
permit ip any any option lsr
permit ip any any option ssr
!

class-map ACL-IP-OPTIONS-CLASS
match access-group name ACL-IP-OPTIONS
!

policy-map COPP-POLICY
class ACL-IP-OPTIONS-CLASS
drop
!

control-plane
service-policy input COPP-POLICY
!
```

In het voorgaande CoPP beleid, leiden de Access Control List items (ACEs) die pakketten met de vergunningsactie vergelijken, ertoe dat deze pakketten worden verwijderd door de beleidsmap-platenfunctie, terwijl pakketten die overeenkomen met de ontkenningsactie (niet weergegeven) niet worden beïnvloed door de beleidsmap-vervolgfunctie.

Raadpleeg Toezicht besturingsplane implementeren voor meer informatie over de CoPP-functie.

Bescherming van besturingsplane

In Cisco IOS-softwarerelease 12.4(4)T en hoger kan CPPr (Control Plane Protection) worden gebruikt om vliegtuigverkeer door de CPU van een Cisco IOS-apparaat te beperken of te controleren. Hoewel vergelijkbaar met CoPP, is CPPr in staat om verkeer te beperken of te controleren met behulp van fijnere granulariteit dan CoPP. CPPr verdeelt het geaggregeerde bedieningspaneel in drie verschillende categorieën van besturingsvlakken die als subinterfaces bekend staan: Host, Transit, en CEF-Exception subinterfaces bestaan.

Dit CPPr-beleid daalt de door een apparaat ontvangen transitpakketten waar de TTL-waarde

minder dan 6 is en transito- of niet-doorvoerpakketten die worden ontvangen door een apparaat waar de TTL-waarde nul of één is. Het CPPr beleid daalt ook pakketten met geselecteerde IP opties die door het apparaat worden ontvangen.

```
!

ip access-list extended ACL-IP-TTL-0/1
permit ip any any ttl eq 0 1
!

class-map ACL-IP-TTL-0/1-CLASS
match access-group name ACL-IP-TTL-0/1
!

ip access-list extended ACL-IP-TTL-LOW
permit ip any any ttl lt 6
!

class-map ACL-IP-TTL-LOW-CLASS
match access-group name ACL-IP-TTL-LOW
!

ip access-list extended ACL-IP-OPTIONS
permit ip any any option eool
permit ip any any option record-route
permit ip any any option timestamp
permit ip any any option lsr
permit ip any any option ssr
!

class-map ACL-IP-OPTIONS-CLASS
match access-group name ACL-IP-OPTIONS
!

policy-map CPPR-CEF-EXCEPTION-POLICY
class ACL-IP-TTL-0/1-CLASS
drop
class ACL-IP-OPTIONS-CLASS
drop
!

!-- Apply CPPr CEF-Exception policy CPPR-CEF-EXCEPTION-POLICY to
!-- the CEF-Exception CPPr sub-interface of the device

!

control-plane cef-exception
service-policy input CPPR-CEF-EXCEPTION-POLICY
!

policy-map CPPR-TRANSIT-POLICY
class ACL-IP-TTL-LOW-CLASS
drop
!

control-plane transit
service-policy input CPPR-TRANSIT-POLICY
!
```

In het vorige CPPr beleid, leiden de toegangs controle lijstingangen die pakketten met de de vergunnings actie aanpassen tot deze pakketten die door de beleid-kaart druppelfunctie worden verworpen, terwijl pakketten die de ontkennende actie (niet getoond) aanpassen niet door de

beleid-kaart druppelfunctie worden beïnvloed.

*Raadpleeg*Understanding *tussen* besturingsplane en bescherming van besturingsplane voor meer informatie over de CPPr-functie.

Verkeersidentificatie en -tracering

Soms moet u netwerkverkeer snel identificeren en traceren, vooral tijdens de respons van het incident of slechte netwerkprestaties. NetFlow en Classifier ACL's zijn de twee primaire methoden om dit met Cisco IOS-software te bereiken. NetFlow kan zicht bieden in al het verkeer op het netwerk. Daarnaast kan NetFlow worden geïmplementeerd met verzamelaars die lange termijn trending en geautomatiseerde analyse kunnen bieden. Classificatie ACL's zijn een onderdeel van ACL's en vereisen voorafgaande planning om specifiek verkeer en handmatige interventie tijdens analyse te identificeren. Deze secties geven een kort overzicht van elk onderdeel.

NetFlow

NetFlow identificeert een abnormale en aan veiligheid gerelateerde netwerkactiviteit door netwerkstromen te volgen. NetFlow-gegevens kunnen via de CLI worden bekeken en geanalyseerd, of de gegevens kunnen voor aggregatie en analyse worden geëxporteerd naar een commerciële NetFlow-Collector of naar een Virtual NetFlow-verzamelaar. NetFlow Collectors, door lange termijn trending, kunnen netwerkgedrag en gebruiksanalyse verstrekken. NetFlow functioneert door analyse uit te voeren op specifieke eigenschappen binnen IP-pakketten en stromen te maken. Versie 5 is de meest gebruikte versie van NetFlow, maar versie 9 is uitbreidbaar. NetFlow-stromen kunnen worden gecreëerd met steekproefsgewijze verkeersgegevens in omgevingen met een hoog volume.

CEF, of gedistribueerde CEF, is een voorwaarde om NetFlow mogelijk te maken. NetFlow kan op routers en switches worden geconfigureerd.

Dit voorbeeld illustreert de basisconfiguratie van deze functie. In vorige releases van Cisco IOS-software is de opdracht om NetFlow op een interface in te schakelen **ip route-cache flow** in plaats van **ip flow {ingress |** Vers.

```
!

ip flow-export destination <ip-address> <udp-port>
ip flow-export version <version>
!

interface <interface>
ip flow <ingess|egress>
!
```

Dit is een voorbeeld van NetFlow output van de CLI. De eigenschap srcIf kan helpen in tracback.

```
router#show ip cache flow
IP packet size distribution (26662860 total packets):
1-32 64 96 128 160 192 224 256 288 320 352 384 416 448 480
.741 .124 .047 .006 .005 .005 .002 .008 .000 .000 .003 .000 .001 .000 .000

512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
.000 .000 .001 .007 .039 .000 .000 .000 .000 .000 .000
```

```
IP Flow Switching Cache, 4456704 bytes
55 active, 65481 inactive, 1014683 added
41000680 ager polls, 0 flow alloc failures
Active flows timeout in 2 minutes
Inactive flows timeout in 60 seconds
IP Sub Flow Cache, 336520 bytes
110 active, 16274 inactive, 2029366 added, 1014683 added to flow
0 alloc failures, 0 force free
1 chunk, 15 chunks added
last clearing of statistics never
Protocol Total Flows Packets Bytes Packets Active(Sec) Idle(Sec)
-------- Flows /Sec /Flow /Pkt /Sec /Flow /Flow
TCP-Telnet 11512 0.0 15 42 0.2 33.8 44.8
TCP-FTP 5606 0.0 3 45 0.0 59.5 47.1
TCP-FTPD 1075 0.0 13 52 0.0 1.2 61.1
TCP-WWW 77155 0.0 11 530 1.0 13.9 31.5
TCP-SMTP 8913 0.0 2 43 0.0 74.2 44.4
TCP-X 351 0.0 2 40 0.0 0.0 60.8
TCP-BGP 114 0.0 1 40 0.0 0.0 62.4
TCP-NNTP 120 0.0 1 42 0.0 0.7 61.4
TCP-other 556070 0.6 8 318 6.0 8.2 38.3
UDP-DNS 130909 0.1 2 55 0.3 24.0 53.1
UDP-NTP 116213 0.1 1 75 0.1 5.0 58.6
UDP-TFTP 169 0.0 3 51 0.0 15.3 64.2
UDP-Frag 1 0.0 1 1405 0.0 0.0 86.8
UDP-other 86247 0.1 226 29 24.0 31.4 54.3
ICMP 19989 0.0 37 33 0.9 26.0 53.9
IP-other 193 0.0 1 22 0.0 3.0 78.2
Total: 1014637 1.2 26 99 32.8 13.8 43.9

SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts
Gi0/1 192.168.128.21 Local 192.168.128.20 11 CB2B 07AF 3
Gi0/1 192.168.150.60 Gi0/0 10.89.17.146 06 0016 101F 55
Gi0/0 10.89.17.146 Gi0/1 192.168.150.60 06 101F 0016 9
Gi0/1 192.168.150.60 Local 192.168.206.20 01 0000 0303 11
Gi0/0 10.89.17.146 Gi0/1 192.168.150.60 06 07F1 0016 1
```

Raadpleeg Cisco IOS NetFlow voor meer informatie over NetFlow-functies.

Raadpleeg Een inleiding tot Cisco IOS NetFlow - een technisch overzicht voor een technisch overzicht van NetFlow.

Classificatie ACL's

Classificatie ACL's bieden zichtbaarheid in verkeer dat een interface overschrijdt. Classificatie ACL's wijzigen het beveiligingsbeleid van een netwerk niet en zijn doorgaans geconstrueerd om afzonderlijke protocollen, bronadressen of bestemmingen te classificeren. Bijvoorbeeld, een ACE die al verkeer toelaat zou in specifieke protocollen of havens kunnen worden gescheiden. Deze meer gedetailleerde classificatie van verkeer in specifieke ACE's kan helpen om het netwerkverkeer te begrijpen omdat elke verkeerscategorie zijn eigen slagteller heeft. Een beheerder kan impliciet ontkennen aan het eind van ACL in granulaire ACE's ook scheiden om de types van ontkend verkeer te helpen identificeren.

Een beheerder kan een invallingsreactie versnellen door classificatie s met de **tonen toegang-lijst** en **de** opdrachten **van de IP toegang-lijst tellers** EXEC **te gebruiken**.

Dit voorbeeld illustreert de configuratie van een classificatie ACL om het verkeer van MKB voorafgaand aan een standaard te identificeren ontkent:

```
!

ip access-list extended ACL-SMB-CLASSIFY
remark Existing contents of ACL
remark Classification of SMB specific TCP traffic
deny tcp any any eq 139
deny tcp any any eq 445
deny ip any any
!
```

Om het verkeer te identificeren dat een classificatie ACL gebruikt, gebruik de opdracht ACL-naam (**toegangslijst)** EXEC. De ACL-tellers kunnen worden gewist door met de **heldere IP access-list tellers** ACL-naam EXEC opdracht.

```
router#show access-list ACL-SMB-CLASSIFY
Extended IP access list ACL-SMB-CLASSIFY
10 deny tcp any any eq 139 (10 matches)
20 deny tcp any any eq 445 (9 matches)
30 deny ip any any (184 matches)
```

Raadpleeg de modus Toegangscontrolelijst *begrijpen* voor meer informatie over het mogelijk maken van blogfuncties binnen ACL's.

Toegangsbeheer met VLAN-kaarten en poorttoegangscontrolelijsten

VLAN Access Control Lists (VACL's) of VLAN-kaarten en PACL's (PACL's) bieden de mogelijkheid om toegangscontrole op niet-routed Traffic Engineering uit te voeren die dichter bij endpointapparaten ligt dan toegangscontrolelijsten die op routed interfaces worden toegepast.

Deze secties bieden een overzicht van de eigenschappen, voordelen en potentiële gebruiksccenario's van VACL's en PACL's.

Toegangsbeheer met VLAN-kaarten

VACL's (VACL's) of VLAN-kaarten die van toepassing zijn op alle pakketten die het VLAN invoeren, bieden de mogelijkheid om toegangscontrole op verkeer binnen VLAN af te dwingen. Dit is niet mogelijk met ACL's op routed interfaces. Bijvoorbeeld, zou een kaart van VLAN kunnen worden gebruikt om hosts te voorkomen die binnen hetzelfde VLAN ingesloten zijn door met elkaar te communiceren, wat mogelijkheden voor lokale aanvallers of wormen reduceert om een host op het zelfde netwerksegment te exploiteren. Om pakketten te ontkennen van het gebruiken van een kaart van VLAN, kunt u een toegangscontrolelijst (ACL) maken die het verkeer aanpast en, in de kaart van VLAN, de te laten vallen actie instellen. Zodra een VLAN-map is geconfigureerd worden alle pakketten die LAN invoeren, achtereenvolgens geëvalueerd aan de hand van de geconfigureerde VLAN-kaart. VLAN-toegangskaarten ondersteunen IPv4- en MAC-toegangslijsten; zij ondersteunen echter geen houtkap of IPv6 ACL's.

Dit voorbeeld gebruikt een uitgebreide genoemde toegangslijst die de configuratie van deze eigenschap illustreert:

```
!

ip access-list extended <acl-name>
permit <protocol> <source-address> <source-port> <destination-address>
<destination-port>
```

```
!

vlan access-map <name> <number>
match ip address <acl-name>
action <drop|forward>
!
```

Dit voorbeeld demonstreert het gebruik van een kaart van VLAN om TCP poorten 139 en 445 evenals het protocol van de wijnstok te ontkennen:

```
!

ip access-list extended VACL-MATCH-ANY
permit ip any any
!

ip access-list extended VACL-MATCH-PORTS
permit tcp 192.168.1.0 0.0.0.255 192.168.1.0 0.0.0.255 eq 445
permit tcp 192.168.1.0 0.0.0.255 192.168.1.0 0.0.0.255 eq 139
!

mac access-list extended VACL-MATCH-VINES
permit any any vines-ip
!

vlan access-map VACL 10
match ip address VACL-MATCH-VINES
action drop
!

vlan access-map VACL 20
match ip address VACL-MATCH-PORTS
action drop
!

vlan access-map VACL 30
match ip address VACL-MATCH-ANY
action forward
!

vlan filter VACL vlan 100
!
```

Raadpleeg Netwerkbeveiliging configureren met ACL's voor meer informatie over de configuratie van VLAN-kaarten.

Toegangsbeheer met PACL's

PACL's kunnen alleen worden toegepast op de inkomende richting op Layer 2 fysieke interfaces van een switch. Overeenkomstig met VLAN-kaarten bieden PACL's toegangscontrole op niet-routed of Layer 2-verkeer. De syntaxis voor het maken van PACL's, die voorrang heeft op kaarten van VLAN en router ACL's, is hetzelfde als router ACL's. Als ACL op een Layer 2-interface wordt toegepast, wordt deze naar PACL verwezen. Configuratie omvat de creatie van een IPv4, IPv6, of MAC ACL en de toepassing van het op Layer 2 interface.

Dit voorbeeld gebruikt een uitgebreide genoemde toegangslijst om de configuratie van deze eigenschap te illustreren:

```
!
```

```
ip access-list extended <acl-name>
permit <protocol> <source-address> <source-port> <destination-address>
<destination-port>
!

interface <type> <slot/port>
switchport mode access
switchport access vlan <vlan_number>
ip access-group <acl-name> in
!
```

Raadpleeg het gedeelte Port ACL-netwerkbeveiliging met ACL's voor meer informatie over de configuratie van PACL's.

Toegangsbeheer met MAC

MAC-toegangscontrolelijsten of uitgebreide lijsten kunnen worden toegepast op IP-netwerk met behulp van deze opdracht in interfacemodus:

```
Cat6K-IOS(config-if)#mac packet-classify
```

> Opmerking: Layer 3-pakketten classificeren als Layer 2-pakketten. De opdracht wordt ondersteund in Cisco IOS-softwarerelease 12.2(18)SXD (voor Sup 720) en Cisco IOS-softwarereleases 12.2(33)SRA of hoger.

Deze interfaceopdracht moet worden toegepast op de ingangsinterface en het geeft de verzendmotor op om de IP-header niet te controleren. Het resultaat is dat u een MAC-toegangslijst in de IP-omgeving kunt gebruiken.

Private VLAN-toepassing

Private VLAN's (PVLAN's) zijn een Layer 2-beveiligingsfunctie die de connectiviteit tussen werkstations of servers in een VLAN beperkt. Zonder PVLAN's kunnen alle apparaten op Layer 2 VLAN's vrij communiceren. Netwerksituaties bestaan waarin de beveiliging kan worden ondersteund door de communicatie tussen apparaten op één VLAN te beperken. Bijvoorbeeld, PVLAN's worden vaak gebruikt om communicatie tussen servers in een openbaar toegankelijk net te verbieden. Mocht één server gecompromitteerd raken, kan het gebrek aan connectiviteit met andere servers door de toepassing van PVLAN's het compromis tot één server helpen beperken.

Er zijn drie typen Private VLAN's: geïsoleerde VLAN's, community VLAN's en primaire VLAN's. De configuratie van PVLAN's maakt gebruik van primaire en secundaire VLAN's. Het primaire VLAN bevat alle veelbelovende havens, die later worden beschreven, en omvat één of meer secundaire VLAN's, die of geïsoleerd of communautair VLANs kunnen zijn.

Geïntegreerde VLAN's

De configuratie van een secundair VLAN als geïsoleerd VLAN voorkomt volledig communicatie tussen apparaten in het secundaire VLAN. Er zou slechts één geïsoleerd VLAN per primair VLAN kunnen zijn, en alleen veelbelovende havens kunnen met havens in een geïsoleerd VLAN communiceren. Isolated VLAN's moeten op onvertrouwde netwerken zoals netwerken die gasten ondersteunen, worden gebruikt.

Dit configuratievoorbeeld vormt VLAN 11 als geïsoleerd VLAN en associeert het met het primaire VLAN, VLAN 20. Het voorbeeld hieronder vormt ook interface FastEthernet 1/1 als een geïsoleerde poort in VLAN 11:

```
!

vlan 11
private-vlan isolated
!

vlan 20
private-vlan primary
private-vlan association 11
!

interface FastEthernet 1/1
description *** Port in Isolated VLAN ***
switchport mode private-vlan host
switchport private-vlan host-association 20 11
!
```

Community-VLAN's

Een secundair VLAN dat als gemeenschap VLAN wordt gevormd staat communicatie tussen leden van het VLAN zowel als met om het even welke veelbelovende havens in het primaire VLAN toe. Nochtans, is geen communicatie mogelijk tussen om het even welke twee gemeenschap VLAN's of van een gemeenschap VLAN aan een geïsoleerd VLAN. Community VLAN's moeten worden gebruikt om servers te groeperen die connectiviteit met elkaar nodig hebben, maar waar de connectiviteit met alle andere apparaten in het VLAN niet vereist is. Dit scenario is gebruikelijk in een openbaar toegankelijk netwerk of overal waar servers content leveren aan onvertrouwde klanten.

Dit voorbeeld vormt één enkel gemeenschap VLAN en vormt de schakelaar van poort FastEthernet 1/2 als lid van dat VLAN. De gemeenschap VLAN, VLAN 12, is een secundair VLAN aan primair VLAN 20.

```
!

vlan 12
private-vlan community
!

vlan 20
private-vlan primary
private-vlan association 12
!

interface FastEthernet 1/2
description *** Port in Community VLAN ***
switchport mode private-vlan host
switchport private-vlan host-association 20 12
!
```

Promiscueuze poorten

Switch-poorten die in het primaire VLAN worden geplaatst, zijn bekend als veelbelovende poorten. Promiscueuze poorten kunnen met alle andere poorten communiceren in de primaire en

secundaire VLAN's. De router of firewallinterfaces zijn de meest gebruikelijke apparaten die op deze VLAN's worden gevonden.

Dit configuratievoorbeeld combineert de vorige geïsoleerde en community VLAN-voorbeelden en voegt de configuratie van interface FastEthernet 1/12 toe als een veelbelovende poort:

```
!

vlan 11
private-vlan isolated
!

vlan 12
private-vlan community
!

vlan 20
private-vlan primary
private-vlan association 11-12
!

interface FastEthernet 1/1
description *** Port in Isolated VLAN ***
switchport mode private-vlan host
switchport private-vlan host-association 20 11
!

interface FastEthernet 1/2
description *** Port in Community VLAN ***
switchport mode private-vlan host
switchport private-vlan host-association 20 12
!

interface FastEthernet 1/12
description *** Promiscuous Port ***
switchport mode private-vlan promiscuous
switchport private-vlan mapping 20 add 11-12
!
```

Wanneer u PVLAN's implementeert, is het van belang om ervoor te zorgen dat de Layer 3-configuratie op zijn plaats de beperkingen ondersteunt die door PVLAN's worden opgelegd en niet toestaat dat de PVLAN-configuratie wordt ondersteboven. Layer 3 filtering met een router ACL of firewall kan de subversie van de PVLAN-configuratie verhinderen.

Raadpleeg Private VLAN's (PVLAN's) - Promiscuous, Isolated, Community, sted op de LAN Security startpagina, voor meer informatie over het gebruik en de configuratie van Private VLAN's.

Conclusie

Dit document geeft u een breed overzicht van de methoden die kunnen worden gebruikt om een Cisco IOS-systeemapparaat te beveiligen. Als u de apparaten veilig stelt, verhoogt het de algemene veiligheid van de netwerken die u beheert. In dit overzicht wordt gesproken over de bescherming van het beheer, de controle en de dataplannen en worden er aanbevelingen voor de configuratie gegeven. Waar mogelijk wordt voldoende details verstrekt voor de configuratie van elke bijbehorende functie. In alle gevallen worden echter uitgebreide verwijzingen verstrekt om u de informatie te verschaffen die nodig is voor verdere evaluatie.

ERKENNING

Sommige functiebeschrijvingen in dit document zijn geschreven door Cisco-informatieteams.

Bijlage: Cisco IOS-controlelijst voor apparaten

Deze controlelijst is een verzameling van alle verhardende stappen die in deze handleiding worden gepresenteerd. De beheerders kunnen het als herinnering aan alle verhardende die eigenschappen gebruiken en voor een Cisco IOS apparaat worden overwogen, zelfs als een eigenschap niet werd geïmplementeerd omdat het niet van toepassing was. Administrateurs wordt aangeraden elke optie voor het potentiële risico te evalueren voordat zij de optie implementeren.

beheermaatschappij

- Wachtwoorden

  Schakel MD5-hashing (geheime optie) in om wachtwoorden voor gebruikers en lokale gebruikers in te schakelenConfigureer de wachtwoord door de uitsluiting opnieuw uit te voerenWachtwoordherstel uitschakelen (denk aan risico)

- Ongebruikte services uitschakelen

- Configureer TCP-keepaliën voor beheersessies

- Meldingen voor geheugen en CPU-drempels instellen

- Configureren

  Meldingen van geheugen- en CPU-drempelsReserve-geheugen voor console-toegangGeheugenlekkagedetectorDetectie van buffer-overflowUitgebreide verzameling crashinformatie

- Gebruik iACL's om beheertoegang te beperken

- Filteren (risico overwegen)

  ICMP-pakkettenIP-fragmentenIP-optiesTTL-waarde in pakketten

- Bescherming van besturingsplane

  Poortfiltering configurerenLijstdrempels instellen

- Toegang tot beheer

  Gebruik de bescherming van het beheersplan om beheerinterfaces te beperkenUitgangspunt instellenGebruik een versleuteld transportprotocol (zoals SSH) voor CLI-toegangBeheer van transport voor vty- en tty-lijnen (optie toegangsklasse)Waarschuwen met spandoeken

- AAA

  Gebruik AAA voor verificatie en back-upGebruik AAA (TACACS+) voor toestemming voor opdrachtGebruik AAA voor accountingRedundante AAA-servers gebruiken

- SNMP

  SNMPv2-gemeenschappen configureren en ACL's toepassenSNMPv3 configureren

- Vastlegging

  Gecentraliseerde vastlegging configurerenVastleggingsniveaus voor alle relevante onderdelenOpslagbron-interface instellenGranulariteit van logtijdstempel configureren

- Configuratie-beheer

  Vervangen en terugdraaienToegang tot exclusieve configuratieConfiguratie van softwareMeldingen voor configuratie-wijziging

besturingsplane

- Uitschakelen (risico overwegen)

  ICMP-omleidingenICMP onbereikbaarProxy ARP

- NTP-verificatie configureren als NTP wordt gebruikt

- Toezicht/bescherming van besturingsplane configureren (poortfiltering, wachtrijdrempels)

- Secure-routingprotocollen

  BGP (TTL, MD5, maximum prefixes, voorvoegsellijsten, systeempad ACL's)IGP (MD5, passieve interface, routefiltering, hulpbronconsumptie)

- hardwaresnelheidsbeperkingen instellen

- Secure First hop-redundantieprotocollen (GLBP, HSRP, VRRP)

datacentrum

- IP-opties selecteren

- Uitschakelen (risico overwegen)

  IP-bronroutingIP-gerichte broadcastICMP-omleidingen

- Beperkte IP-gerichte broadcast
- ACL’s configureren (risico overwegen)

  ICMP-filterIP-fragmenten filterenIP-opties filterenTTL-waarden filteren
- Vereiste bescherming tegen spoofing configureren

  ACL’sIP-bronbewakingDynamische ARP-inspectieUnicast RPFPoortbeveiliging
- Bescherming van het besturingsplane (met uitzondering van het besturingsplane)
- NetFlow en classificatie ACL’s configureren voor traffic identificatie
- Configureer verplichte toegangscontrole ACL’s (VLAN-kaarten, PACL’s, MAC)
- Private VLAN’s configureren