Gebruik de Cisco IOS XE-hardwaregids

Inhoud

Inleiding

Dit document beschrijft informatie om uw Cisco IOS® XE-systeemapparaten te beveiligen, waardoor de algehele beveiliging van uw netwerkdocumentatie wordt verhoogd.

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

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 verwante items.

De drie functionele vlakken van een netwerk: beheervlak, controlevlak en dataplaat bieden elk verschillende functionaliteit die moet worden beveiligd.

1. Management Plan - het beheervliegtuig beheert verkeer dat naar het Cisco IOS XE-apparaat wordt verzonden en bestaat uit toepassingen en protocollen zoals Secure Shell (SSH) en Simple Network Management Protocol (SNMP).
2. Beheerplane: de beheerplane van een netwerkapparaat verwerkt het verkeer dat essentieel is voor de doorlopende werking van de netwerkinfrastructuur. Het besturingsplane bestaat uit toepassingen en protocollen tussen netwerkapparaten, waaronder het BGP-protocol (Border Gateway Protocol), evenals de Interior Gateway Protocols (IGP's) zoals het Enhanced Interior Gateway Routing Protocol (EIGRP) en Open Shortest Path First (OSPF).
3. Dataplane: de dataplane stuurt gegevens door via een netwerkapparaat. Het gegevensvlak bevat geen verkeer dat naar het lokale Cisco IOS XE-apparaat wordt verzonden.

   De dekking van veiligheidseigenschappen in dit document verstrekt vaak genoeg detail voor u om de eigenschap te vormen. In gevallen waarin dit niet het geval is, wordt de functie op een zodanige manier uitgelegd dat u kunt beoordelen of extra aandacht voor de functie vereist is. Waar mogelijk en passend bevat dit document aanbevelingen die, indien geïmplementeerd, helpen een netwerk te beveiligen.

Veilige werkzaamheden

Beveiligde netwerkactiviteiten is een belangrijk onderwerp. Hoewel het grootste deel van dit document is gewijd aan de beveiligde configuratie van een Cisco IOS XE-apparaat, wordt een netwerk niet volledig beveiligd door configuraties alleen. De operationele procedures die in gebruik zijn op het netwerk, dragen net zoveel bij aan de beveiliging als de configuratie van de onderliggende apparaten.

Deze onderwerpen bevatten operationele aanbevelingen die u wordt geadviseerd te implementeren. Deze onderwerpen lichten specifieke essentiële gebieden van netwerkactiviteiten uit en zijn niet allesomvattend.

Cisco-beveiligingsadvies en -reacties bewaken

Het Cisco Product Security Incident Response Team (PSIRT) maakt en onderhoudt publicaties, ook wel PSIRT Advisories genoemd, voor beveiligingsgerelateerde problemen in Cisco-producten. De gebruikte methode voor communicatie van minder ernstige problemen is de Cisco Security Response. Security Advisories en antwoorden zijn beschikbaar bij Cisco Security Advisories en antwoorden

Aanvullende informatie over deze communicatievoertuigen is beschikbaar in het Cisco Security Vulnerability Policy

Om een veilig netwerk te kunnen onderhouden, moet u bekend zijn met de beveiligingsadviezen en antwoorden van Cisco die zijn vrijgegeven. U moet op de hoogte zijn van een kwetsbaarheid voordat de dreiging die deze op een netwerk kan hebben, kan worden geëvalueerd. Raadpleeg Risicotriage voor aankondigingen van beveiligingsincidenten voor hulp bij dit evaluatieproces.

Verificatie, autorisatie en accounting inzetten

Het AAA-framework (verificatie, autorisatie en accounting) is essentieel voor beveiligde netwerkapparaten. Het AAA-framework biedt verificatie van beheersessies en kan ook gebruikers beperken tot specifieke, door beheerders gedefinieerde opdrachten en alle opdrachten vastleggen die door alle gebruikers worden ingevoerd. Bekijk het gedeelte Verificatie, autorisatie en accounting van dit document voor meer informatie over hoe u AAA kunt inzetten.

Logboekverzameling en monitoring centraliseren

Om kennis te verkrijgen over actuele, opkomende en historische gebeurtenissen die verband houden met beveiligingsincidenten, moet uw organisatie een uniforme strategie hebben voor gebeurtenisvastlegging en correlatie. Deze strategie moet gebruik maken van vastlegging vanaf alle netwerkapparaten en gebruik maken van voorverpakte en aanpasbare correlatiemogelijkheden.

Nadat gecentraliseerde vastlegging is geïmplementeerd, moet u een gestructureerde aanpak voor loganalyse en incidenttracering ontwikkelen. Aan de hand van de behoeften van uw organisatie kan deze aanpak variëren van een eenvoudige zorgvuldige beoordeling van logboekgegevens tot geavanceerde op regels gebaseerde analyse.

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

Beveiligde protocollen gebruiken wanneer mogelijk

Veel protocollen worden gebruikt om gevoelige netwerkbeheergegevens over te dragen. U moet waar mogelijk gebruik maken van beveiligde protocollen. Een beveiligde protocolkeuze omvat het gebruik van SSH in plaats van Telnet zodat zowel de verificatiegegevens als de beheerinformatie worden versleuteld. Daarnaast moet u beveiligde 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 de sectie Secure Interactive Management Sessies van dit document voor meer informatie over het beveiligde beheer van Cisco IOS XE-apparaten.

Verkeersinzicht krijgen met NetFlow

Met NetFlow kunt u verkeersstromen in het netwerk bewaken. Oorspronkelijk bedoeld om verkeersinformatie naar netwerkbeheertoepassingen uit te voeren, kan NetFlow ook worden gebruikt om stroominformatie over een router te tonen. Met deze mogelijkheid kunt u in real-time zien welk verkeer door het netwerk beweegt. Ongeacht of stroominformatie wordt geëxporteerd naar een externe collector, wordt u aangeraden om netwerkapparaten te configureren voor NetFlow zodat het reactief kan worden gebruikt indien nodig.

Meer informatie over deze functie is beschikbaar in de sectie Traffic Identification and Traceback van dit document en op Cisco IOS NetFlow (alleen geregistreerde gebruikers).

Configuratiebeheer

Configuratiebeheer is een proces waarmee configuratiewijzigingen worden voorgesteld, beoordeeld, goedgekeurd en geïmplementeerd. Binnen de context van een Cisco IOS XE-apparaatconfiguratie zijn twee extra aspecten van configuratiebeheer van cruciaal belang: configuratie, archivering en beveiliging.

U kunt configuratie archieven gebruiken om veranderingen terug te rollen die aan netwerkapparaten worden gemaakt. In een beveiligingscontext kunnen ook configuratie-archieven worden gebruikt om te bepalen welke beveiligingswijzigingen zijn aangebracht en wanneer deze wijzigingen hebben plaatsgevonden. In combinatie met AAA-loggegevens kan deze informatie helpen bij de veiligheidscontrole van netwerkapparaten.

De configuratie van een Cisco IOS XE-apparaat bevat veel gevoelige informatie. Gebruikersnamen, wachtwoorden en de inhoud van toegangscontrolelijsten zijn voorbeelden van dit soort informatie. De opslagplaats die u gebruikt om Cisco IOS XE-apparaatconfiguraties te archiveren moet worden beveiligd. Onbeveiligde toegang tot deze informatie kan de beveiliging van het volledige netwerk ondermijnen.

Beheerplane

De beheerplane bestaat uit functies die de beheerdoelen van het netwerk behalen.

Hieronder vallen interactieve beheersessies die SSH gebruiken, evenals statistiekverzameling met SNMP of NetFlow. Wanneer u de veiligheid van een netwerkapparaat overweegt, is het kritiek dat het beheervliegtuig wordt beschermd. Als een veiligheidsincident de functies van het beheervliegtuig kan ondermijnen, kan het voor u onmogelijk zijn om het netwerk terug te krijgen of te stabiliseren.

In deze secties worden de beveiligingsfuncties en -configuraties in detail beschreven die beschikbaar zijn in Cisco IOS XE-software die helpt het beheervlak te verstevigen.

Versterking algemene beheerplane

Het beheervliegtuig wordt gebruikt om toegang te hebben tot, een apparaat te vormen en te beheren, evenals zijn verrichtingen en het netwerk te controleren waarop het wordt opgesteld. Het managementvliegtuig is het vliegtuig dat verkeer ontvangt en verstuurt voor de werking van deze functies. U moet zowel het managementvliegtuig als het bedieningsvliegtuig van een apparaat beveiligen, omdat de handelingen van het bedieningsvliegtuig rechtstreeks van invloed zijn op de handelingen van het managementvliegtuig. Deze lijst van protocollen wordt gebruikt door het managementvliegtuig:

1. Simple Network Management Protocol
2. Telnet
3. Secure Shell Protocol
4. File Transfer Protocol
5. Hyper Text Transfer Protocol/Secure Hyper Text Transfer Protocol
6. Trivial File Transfer Protocol
7. Secure Copy Protocol
8. TACACS +
9. RADIUS
10. NetFlow
11. Network Time Protocol
12. Syslog

> Er moeten stappen worden ondernomen om ervoor te zorgen dat de beheer- en besturingsplane beveiligingsincidenten doorstaan. Als een van deze vliegtuigen met succes wordt geëxploiteerd, kunnen alle vliegtuigen worden gecompromitteerd.

Wachtwoordbeheer

Wachtwoorden beheren de toegang tot bronnen of apparaten. Dit wordt bereikt door de definitie van een wachtwoord of geheim dat wordt gebruikt om verzoeken te authentificeren. Wanneer een verzoek om toegang tot een middel of een apparaat wordt ontvangen, wordt het verzoek betwist voor controle van het wachtwoord en de identiteit, en de toegang kan worden verleend, worden

ontkend, of worden beperkt gebaseerd op het resultaat. Als aanbevolen procedure voor beveiliging moeten wachtwoorden worden beheerd met een TACACS+- of RADIUS-verificatieserver. Houd er echter rekening mee dat een lokaal ingesteld wachtwoord voor geprivilegieerde toegang nog steeds nodig is in geval van een storing van de TACACS+- of RADIUS-services. Op een apparaat kan ook andere wachtwoordinformatie aanwezig zijn binnen de configuratie, zoals een NTP-sleutel, SNMP-communitystring of Routing Protocol-sleutel.

De opdracht Laat geheim toe wordt gebruikt om het wachtwoord in te stellen dat bevoorrechte administratieve toegang tot het Cisco IOS XE-systeem verleent. De opdracht enable secret moet worden gebruikt in plaats van de oudere opdracht enable password. De opdracht enable password gebruikt een zwak versleutelingsalgoritme.

Als geen inschakelen geheim is ingesteld en een wachtwoord is ingesteld voor de console tty line, kan het console wachtwoord worden gebruikt om geprivilegieerde toegang te ontvangen, zelfs vanaf een externe virtuele tty (vty) sessie. Deze actie is bijna zeker ongewenst en het is nog een reden om te zorgen voor configuratie van de opdracht enable secret.

De globale configuratieopdracht Service Password-encryptie geeft de Cisco IOS XE-software de opdracht de wachtwoorden, Challenge Handshake Authentication Protocol (CHAP)-geheimen en soortgelijke gegevens te versleutelen die in het configuratiebestand zijn opgeslagen. Een dergelijke codering is nuttig om te voorkomen dat toevallige waarnemers wachtwoorden kunnen lezen, bijvoorbeeld wanneer zij over het scherm van een beheerder kijken. Het algoritme dat wordt gebruikt door de opdracht service password-encryption is echter een eenvoudige Vigen re-codering. Het algoritme is niet ontworpen om configuratiebestanden te beschermen tegen aanzienlijke analyse door zelfs enigszins geavanceerde aanvallers en mag niet voor dit doel worden gebruikt. Alle Cisco IOS XE-configuratiebestanden die versleutelde wachtwoorden bevatten, moeten met dezelfde zorg worden behandeld als die welke wordt gebruikt voor een duidelijke lijst met dezelfde wachtwoorden.

Hoewel dit zwakke versleutelingsalgoritme niet wordt gebruikt door de opdracht enable secret, wordt het wel gebruikt door de globale configuratie-opdracht enable password, evenals door de lijnconfiguratie-opdracht password. Wachtwoorden van dit type moeten worden verwijderd en de optie Laat geheime opdracht toe of de optie Verbeterde wachtwoordbeveiliging moet worden gebruikt.

De opdracht enable secret en de functie Verbeterde wachtwoordbeveiliging gebruiken Message Digest 5 (MD5) voor wachtwoordhashing. Dit algoritme heeft aanzienlijke publieke beoordeling ondergaan en staat niet bekend als omkeerbaar. Het algoritme heeft echter te maken met 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 beveiligd worden opgeslagen en alleen worden gedeeld met vertrouwde personen.

Verbeterde wachtwoordbeveiliging

Met de functie Enhanced Password Security, die sinds de eerste release van Cisco IOS XE-softwarerelease 16.6.4 is gebruikt, kan een beheerder MD5-hashing van wachtwoorden

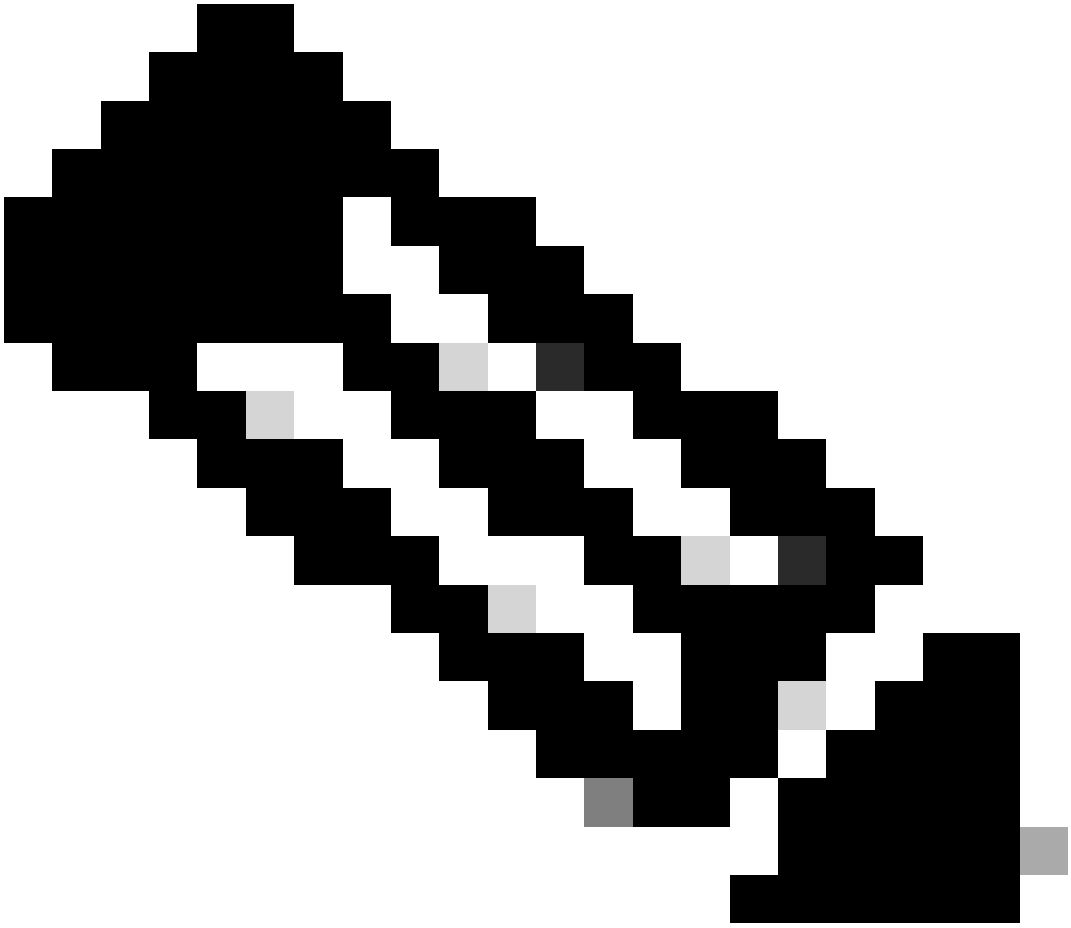
configureren voor de opdracht gebruikersnaam. Voorafgaand aan deze functie waren er twee soorten wachtwoorden: Type 0, dat een cleartext wachtwoord is, en Type 7, dat het algoritme van het Vigen re algoritme gebruikt. De functie Verbeterde wachtwoordbeveiliging kan niet worden gebruikt met protocollen die vereisen dat het leesbare wachtwoord op te halen is, zoals CHAP.

Om een gebruikerswachtwoord te versleutelen met MD5-hashing, moet u de opdracht voor de wereldwijde configuratie van de gebruikersnaam en het geheime wachtwoord opgeven.

gebruikersnaam <naam> geheim <wachtwoord>

Blokkering voor opnieuw aanmelden met wachtwoord

Met de functie voor opnieuw proberen met een wachtwoord voor inloggen, die al sinds de eerste release van Cisco IOS XE-softwarerelease 16.6.4 is uitgevoerd, kunt u een lokale gebruikersaccount uitsluiten na een ingesteld aantal onsuccesvolle inlogpogingen. Wanneer een gebruiker is geblokkeerd, is het account van deze gebruiker vergrendeld totdat u dit ontgrendelt. Een geautoriseerde gebruiker die is geconfigureerd met prioriteitsniveau 15 kan niet worden uitgesloten met deze functie. Het aantal gebruikers met voorrangsniveau 15 moet tot een minimum worden beperkt.



Opmerking: geautoriseerde gebruikers kunnen zichzelf uitsluiten van een apparaat als het aantal niet-succesvolle inlogpogingen wordt bereikt. Bovendien kan een kwaadwillende gebruiker een DoS-voorwaarde (denial of service) maken met herhaalde pogingen voor verificatie met een geldige gebruikersnaam.

Dit voorbeeld laat zien hoe u de functie 'Blokkering voor opnieuw aanmelden met wachtwoord' kunt inschakelen:

aaa nieuw-model aaa lokale verificatiepogingen max-fail <max-pogingen> aaa verificatie login standaard lokaal

gebruikersnaam <naam> geheim <wachtwoord>

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

Geen service wachtwoordherstel

In Cisco IOS XE-softwarerelease 16.6.4 en hoger kan met de functie Geen wachtwoord voor serviceherstel niemand met consoletoegang onveilig toegang krijgen tot de apparaatconfiguratie en het wachtwoord wissen. Ook wordt voorkomen dat kwaadwillende gebruikers de configuratieregisterwaarde wijzigen en toegang krijgen tot NVRAM.

Geen service wachtwoordherstel

Cisco IOS XE-software biedt een procedure voor wachtwoordherstel die afhankelijk is van toegang tot ROM Monitor Mode (ROMMON) en die de toets Break tijdens het opstarten van het systeem gebruikt. In ROMMON kan de apparaatsoftware worden herladen om een nieuwe systeemconfiguratie met een nieuw wachtwoord te starten.

Met de huidige wachtwoordherstelprocedure heeft iedereen met consoletoegang toegang tot het apparaat en het bijbehorende netwerk. Met de functie 'Geen service wachtwoordherstel' wordt het voltooien van de Break-toetscombinatie en het invoeren van ROMMON tijdens systeemopstart voorkomen.

Als op een apparaat geen wachtwoordherstel voor de service is ingeschakeld, wordt aanbevolen om een offline kopie van de apparaatconfiguratie op te slaan en een oplossing voor configuratie-archivering te implementeren. Als het wachtwoord van een Cisco IOS XE-apparaat moet worden hersteld nadat deze functie is ingeschakeld, wordt de gehele configuratie verwijderd.

Ongebruikte services uitschakelen

Als best practice op het gebied van beveiliging moet alle overbodige service worden uitgeschakeld. Deze onnodige diensten, vooral die die het Protocol van het Datagram van de Gebruiker (UDP) gebruiken, worden niet vaak gebruikt voor wettige doeleinden maar kunnen worden gebruikt om Dos en andere aanvallen te lanceren die anders door pakketfiltering worden verhinderd.

De kleine TCP- en UDP-services moeten worden uitgeschakeld. Deze services zijn onder andere:

1. echo (poortnummer 7)
2. discard (poortnummer 9)
3. daytime (poortnummer 13)
4. chargen (poortnummer 19)

   Hoewel misbruik van de kleine diensten kan worden voorkomen of minder gevaarlijk kan worden gemaakt door 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 XE-softwarereleases 16.6.4 en hoger. In eerdere software kunnen de globale configuratieopdrachten geen service-TCP-small-servers en geen service-udp-small-servers worden gegenereerd om ze uit te schakelen.

   Dit is een lijst van aanvullende diensten die moeten worden uitgeschakeld als ze niet worden gebruikt:
5. Geef de opdracht globale configuratie zonder ip finger uit om de Finger-service uit te schakelen. Cisco IOS XE-softwarereleases later dan 16.1 schakelt deze service standaard

uit.

6. Geef de globale configuratieopdracht geen ip bootp server uit om Bootstrap Protocol (BOOTP) uit te schakelen. Cisco IOS XE-softwarereleases later dan 16.1 schakelt deze service standaard uit.
7. In Cisco IOS XE-softwarerelease 16.6.4 en hoger wordt de opdracht IP-DHCP-bootp negeren in globale configuratiemodus uitgegeven om BOOTP uit te schakelen. Hiermee blijven DHCP-services (Dynamic Host Configuration Protocol) ingeschakeld.
8. DHCP-services kunnen worden uitgeschakeld als DHCP-relayservices niet vereist zijn. Start de opdracht no service dhcp in globale configuratiemodus.
9. Geef de opdracht no mop enabled uit in de modus voor interfaceconfiguratie om de MOP-service (Maintenance Operation Protocol) uit te schakelen.
10. Geef de opdracht globale configuratie zonder IP-domein-lookup uit om de resolutieservices van Domain Name System (DNS) uit te schakelen.
11. Geef de opdracht geen servicepad uit in globale configuratiemodus om Packet Assembler/Disassembler (PAD) service uit te schakelen. Deze service wordt gebruikt voor X.25-netwerken.
12. De HTTP-server kan worden uitgeschakeld met de opdracht no ip http server in globale configuratiemodus, en HTTPS-server (Secure HTTP) kan worden uitgeschakeld met de globale configuratie-opdracht no ip http secure-server.
13. Tenzij Cisco IOS XE-apparaten tijdens het opstarten configuraties uit het netwerk ophalen, moet de opdracht Geen service configuratie wereldwijd worden gebruikt. Dit voorkomt dat het Cisco IOS XE-apparaat een poging doet om een configuratiebestand op het netwerk te vinden met TFTP.
14. Cisco Discovery Protocol (CDP) is een netwerkprotocol dat wordt gebruikt om andere CDP-apparaten te detecteren voor buurnabijheid en netwerktopologie. CDP kan worden gebruikt door Network Management Systems (NMS) of tijdens probleemoplossing. CDP moet worden uitgeschakeld voor alle interfaces die zijn verbonden met onbetrouwbare netwerken. Dit wordt gedaan met de interface-opdracht no cdp enable. CDP kan ook globaal worden uitgeschakeld met de globale configuratie-opdracht no cdp run. Merk op dat CDP door een kwaadaardige gebruiker kan worden gebruikt voor verkenning en netwerkmapping.
15. Link Layer Discovery Protocol (LLDP) is een IEEE-protocol dat in 802.1AB is gedefinieerd. LLDP is gelijk aan CDP. Dit protocol zorgt echter voor interoperabiliteit tussen andere apparaten die CDP niet ondersteunen. LLDP moet op dezelfde manier worden behandeld als CDP en worden uitgeschakeld op alle interfaces die verbinding maken met niet-vertrouwde netwerken. Om dit te bereiken, geef no lldp uit verzenden en geen lldp ontvangen de bevelen van de interfaceconfiguratie. Geef de no lldp run global configuratie commando uit om LLDP globaal uit te schakelen. LLDP kan ook door een kwaadaardige gebruiker worden gebruikt voor verkenning en netwerkmapping.
16. Voor switches die opstarten vanaf sdflash ondersteunen, kan de beveiliging worden verbeterd door te starten vanaf flitser en sdflash uitschakelen met de opdracht no sdflash configuratie.

EXEC-time-out

Om het interval in te stellen dat de EXEC-opdrachttolk wacht op gebruikersinvoer voordat een sessie wordt beëindigd, moet u de opdracht voor configuratie van de exec-tijdlijn uitgeven. De

opdracht exec-timeout moet worden gebruikt om sessies uit te loggen op vty of tty lijnen die niet worden gebruikt. Standaard wordt de verbinding van sessies na tien minuten inactiviteit verbroken.

regel con 0

Exec-time-out <minuten> [seconden]

lijn vty 0 4

Exec-time-out <minuten> [seconden]

Keepalives voor TCP-sessies

Met de globale configuratie-opdrachten service tcp-keepalives-in en service tcp-keepalives-out kan een apparaat TCP-keepalives verzenden voor TCP-sessies. Deze configuratie moet worden gebruikt om TCP-keepalives op inkomende verbindingen met het apparaat en uitgaande verbindingen vanaf het apparaat in te schakelen. Dit waarborgt dat het apparaat op het verre eind van de verbinding nog toegankelijk is en dat de half-open of orphaned verbindingen worden verwijderd uit het lokale Cisco IOS XE apparaat.

service-tcp-keepalives-in

Service-TCP-keepalives-out

Gebruik van beheerinterface

De beheerplane van een apparaat wordt in-band of out-of-band geopend op een fysieke of logische beheerinterface. Idealiter bestaat zowel in-band als out-of-band beheertoegang voor elk netwerkapparaat zodat het beheervliegtuig kan worden benaderd tijdens netwerkuitval.

Een van de meest voorkomende interfaces die gebruikt worden voor in-band toegang tot een apparaat is de logische loopback interface. Loopback-interfaces zijn altijd actief, terwijl fysieke interfaces van status kunnen veranderen, en de interface mogelijk niet toegankelijk is. Aanbevolen wordt om een loopback-interface als beheerinterface aan elk apparaat toe te voegen en deze uitsluitend voor het beheervlak te gebruiken. Zo kan de beheerder beleidsregels toepassen in het netwerk voor de beheerplane. Zodra de loopbackinterface op een apparaat is geconfigureerd, kan deze worden gebruikt door beheerplatformprotocollen zoals SSH, SNMP en syslog om verkeer te verzenden en ontvangen.

interface-Loopback0

IP-adres 192.168.1.1 255.255.255.0

Meldingen voor geheugendrempel

Met de melding "Memory Drempel" van de functie, die in Cisco IOS XE-softwarerelease 16.6.4 is toegevoegd, kunt u omstandigheden met weinig geheugen op een apparaat verzachten. Om dit voor elkaar te krijgen gebruikt deze functie twee methoden: Memory Threshold Notification en

Memory Reservation.

Memory Threshold Notification genereert een logbericht om aan te geven dat het vrije geheugen op een apparaat is gedaald tot onder de ingestelde drempelwaarde. Dit configuratievoorbeeld laat zien hoe u deze functie kunt inschakelen met de globale configuratie-opdracht memory free low-watermark. Zo kan een apparaat een melding genereren wanneer beschikbaar geheugen een lager niveau bereikt dan de opgegeven drempelwaarde, en opnieuw wanneer beschikbaar geheugen weer vijf procent hoger is dan de opgegeven drempelwaarde.

geheugenvrije low-watermark processor <drempelwaarde>

geheugenvrij low-watermark-io <drempelwaarde>

Geheugenreservering wordt gebruikt zodat er voldoende geheugen beschikbaar is voor kritische meldingen. Dit configuratievoorbeeld toont aan hoe deze eigenschap toe te laten. Dit zorgt ervoor dat de beheerprocessen blijven functioneren wanneer het geheugen van het apparaat is uitgeput.

essentiële geheugenreserve <waarde>

Melding voor CPU-drempel

Geïntroduceerd in Cisco IOS XE-softwarerelease 16.6.4, kunt u met de functie CPU-melding van drempels detecteren en hiervan op de hoogte worden gesteld wanneer de CPU-belasting op een apparaat een ingestelde drempel overschrijdt. Wanneer de drempelwaarde wordt overschreden, genereert en verzendt het apparaat een SNMP-trapbericht. Twee methoden voor het toepassen van CPU-drempels worden ondersteund op Cisco IOS XE-software: verhoging van drempels en verlaging van drempels.

Deze voorbeeldconfiguratie laat zien hoe de drempelwaarden voor het opstijgen en dalen kunnen worden ingeschakeld die een melding van een CPU-drempelwaarde genereren:

SNMP-server inschakelen traps cpu drempel

SNMP-server host <host-address> <community-string> cpu

procescpu drempeltype <type> stijgend <percentage>-interval <seconden> [dalend <percentage>-interval <seconden>]

proceskopstatistieken beperken entry-percentage <number> [size <seconden>]

Network Time Protocol

Het Network Time Protocol (NTP) is geen bijzonder gevaarlijke service, maar elke onnodige service kan een aanvalsvector vertegenwoordigen. Als NTP wordt gebruikt, is het belangrijk om expliciet een vertrouwde tijdbron te configureren en de juiste verificatie te gebruiken. Nauwkeurige en betrouwbare tijd is nodig voor syslogdoeleinden, zoals tijdens forensisch onderzoek naar mogelijke aanvallen, en voor succesvolle VPN-connectiviteit die afhankelijk is van certificaten voor fase 1-verificatie.

1. NTP Time Zone - Wanneer u NTP configureert, moet de tijdzone zo worden geconfigureerd dat tijdstempels nauwkeurig gecorreleerd kunnen worden. Er zijn gewoonlijk twee benaderingen om de tijdzone voor apparaten in een netwerk met een globale aanwezigheid te vormen. De ene methode is het configureren van alle netwerkapparaten met de Coordinated Universal Time (UTC) (voorheen Greenwich Mean Time (GMT)). De andere benadering is netwerkapparaten met de lokale tijdzone te configureren. Meer informatie over deze functie vindt u in de tijdzone van de klok in de Cisco-productdocumentatie.
2. NTP-verificatie: als u NTP-verificatie configureert, biedt dit garantie dat NTP-berichten worden uitgewisseld tussen vertrouwde NTP-peers.

   Voorbeeldconfiguratie die NTP-verificatie gebruikt:

   Klant:

   (configuratie)#ntp authenticeren

   (config)#ntp 5 md5 ciscotime verificatiesleutel

   (configuratie)#ntp vertrouwde sleutel 5

   (configuratie)#ntp server 172.16.1.5 sleutel 5 server:

   (configuratie)#ntp authenticeren

   (config)#ntp 5 md5 ciscotime verificatiesleutel

   (configuratie)#ntp vertrouwde sleutel 5

Toegang tot het netwerk beperken met infrastructuur-ACL's

Ontworpen om onbevoegde directe communicatie met netwerkapparaten te voorkomen, zijn toegangscontrolelijsten voor infrastructuur (iACL's) een van de meest kritieke beveiligingscontroles die in netwerken kunnen worden geïmplementeerd. De hefboomwerking van ACLs van de infrastructuur het idee dat bijna al netwerkverkeer het netwerk oversteekt en niet aan het netwerk zelf bestemd is.

Een iACL wordt geconstrueerd en toegepast om verbindingen van gastheren of netwerken te specificeren die aan netwerkapparaten moeten worden toegestaan. Veel voorkomende voorbeelden van deze typen verbindingen zijn eBGP, SSH en SNMP. Nadat de vereiste verbindingen zijn toegestaan, wordt al het andere verkeer naar de infrastructuur expliciet geweigerd. Al het doorvoerverkeer dat door het netwerk gaat en niet is bedoeld voor infrastructuurapparaten, wordt dan expliciet toegestaan.

De beschermingen die worden geboden door iACL's zijn relevant voor zowel de beheer- als besturingsplane. De implementatie van iACL's kan worden vergemakkelijkt door het gebruik van verschillende adressering voor netwerkinfrastructuurapparaten. Raadpleeg een security

georiënteerde benadering van IP-adressering voor meer informatie over de veiligheidsimplicaties van IP-adressering.

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

IP-toegangslijst met uitgebreide ACL-INFRASTRUCTUUR-IN

— Vereiste verbindingen voor routing van protocollen en netwerkbeheer toestaan

license tcp host <usted-ebgp-peer> host <local-ebgp-address> eq 179

license tcp host <usted-ebgp-peer> eq 179 host <lokaal-ebgp-adres>

Laat TCP-host toe <Trusted-Management-stations> elke willekeurige eq 22

Laat UDP-host toe <Trusted-netmmt-servers> een willekeurige eq 161

— al het andere IP-verkeer naar een netwerkapparaat weigeren

Geen <infrastructuur-adres-ruimte> <wildcard-masker>

— Vergunning voor transitoverkeer

de vergunninghouder elke

Wanneer de iACL is gemaakt, moet deze worden toegepast op alle interfaces die te maken krijgen met niet-infrastructuurapparaten. Hieronder vallen interfaces die verbinding maken met andere organisaties, externe toegangssegmenten, gebruikerssegmenten en segmenten in datacenters.

Raadpleeg Uw core beschermen: Access Control Lists voor infrastructuurbescherming voor meer informatie over Infrastructuur-ACL's.

ICMP-pakketfiltering

Het Internet Control Message Protocol (ICMP) is ontworpen als een IP-besturingsprotocol. Als zodanig kunnen de berichten die worden overgebracht verreikende gevolgen hebben voor de TCP- en IP-protocollen in het algemeen. Terwijl de hulpmiddelen van het netwerkoplossen van problemen pingelen en traceroute gebruik ICMP, is de externe connectiviteit ICMP zelden nodig voor de juiste verrichting van een netwerk.

Cisco IOS XE-software biedt functionaliteit om ICMP-berichten specifiek te filteren op naam of type en code. Deze voorbeeld-ACL, die moet worden gebruikt met de access control entries (ACE's) van eerdere voorbeelden, biedt de mogelijkheid voor pings van vertrouwde beheerstations en NMS-servers en blokkeert alle andere ICMP-pakketten:

IP-toegangslijst met uitgebreide ACL-INFRASTRUCTUUR-IN

— Licentie voor ICMP Echo (ping) van vertrouwde beheerstations en servers

Laat ICMP-host <Trusted-Management-stations> toe om het even welke echo

Laat icmp host <vertrouwde-netmgmt-servers> elke echo toe

— al het andere IP-verkeer naar een netwerkapparaat weigeren

Geen <infrastructuur-adres-ruimte> <wildcard-masker>

— Vergunning voor transitoverkeer

de vergunninghouder elke

IP-fragmenten filteren

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

In deze voorbeeldconfiguratie, als een TCP-pakket dat bestemd is voor 192.168.1.1 op poort 22 gefragmenteerd is tijdens het transport, wordt het eerste fragment gedropt zoals verwacht door het tweede ACE op basis van Layer 4-informatie binnen het pakket. Alle resterende (niet-initiële) fragmenten worden echter toegestaan door de eerste ACE, volledig gebaseerd op Layer 3-informatie in het pakket en ACE. Het scenario wordt in deze configuratie getoond:

IP-toegangslijst uitgebreid ACL-FRAGMENT-VOORBEELD

vergunning tcp elke gastheer 192.168.1.1 eq 80

TCP elke host 192.168.1.1 eq 22 weigeren

Vanwege de niet-intuïtieve aard van fragmentverwerking, worden IP-fragmenten vaak onbedoeld toegestaan door ACL's. Fragmentatie wordt ook vaak gebruikt in pogingen om detectie te ontwijken door intrusiedetectiesystemen. Het is om deze redenen dat IP fragmenten vaak in aanvallen worden gebruikt, en waarom zij uitdrukkelijk bij de bovenkant van om het even welke gevormde iACLs moeten worden gefiltreerd. Dit voorbeeld ACL omvat uitgebreide filtering van IP-fragmenten. De functionaliteit uit dit voorbeeld moet worden gebruikt in combinatie met de functionaliteit van de voorgaande voorbeelden.

IP-toegangslijst met uitgebreide ACL-INFRASTRUCTUUR-IN

— IP-fragmenten weigeren die protocolspecifieke ACE’s gebruiken om te helpen bij

— classificatie van aanvalsverkeer

TCP geen fragmenten te weigeren

eventuele fragmenten te weigeren

geen scherven

eventuele fragmenten te weigeren

— al het andere IP-verkeer naar een netwerkapparaat weigeren

Geen <infrastructuur-adres-ruimte> <wildcard-masker>

— Vergunning voor transitoverkeer

de vergunninghouder elke

Raadpleeg Access Control Lists en IP-fragmenten voor meer informatie over hoe ACL omgaat met gefragmenteerde IP-pakketten.

Ondersteuning van ACL voor filtering van IP-opties

Cisco IOS XE-softwarerelease 16.6.4 voegde ondersteuning toe voor het gebruik van ACL's om IP-pakketten te filteren op basis van de IP-opties die in het pakket aanwezig zijn. IP-opties zijn een beveiligingsuitdaging voor netwerkapparaten omdat deze opties moeten worden verwerkt als uitzonderingspakketten. Dit vereist een CPU-inspanningsniveau dat niet vereist is voor normale pakketten die over het netwerk worden verzonden. De aanwezigheid van IP-opties in een pakket kan ook wijzen op een poging om beveiligingscontroles in het netwerk te omzeilen of op een andere manier de transitkenmerken van een pakket te wijzigen. Om deze redenen moeten pakketten met IP-opties aan de rand van het netwerk worden gefilterd.

Dit voorbeeld moet met de ACE's van eerdere voorbeelden worden gebruikt om volledige filtering van IP-pakketten met IP-opties te omvatten:

IP-toegangslijst met uitgebreide ACL-INFRASTRUCTUUR-IN

— IP-pakketten met IP-opties weigeren

geen enkele optie voor willekeurige opties

— al het andere IP-verkeer naar een netwerkapparaat weigeren

Geen <infrastructuur-adres-ruimte> <wildcard-masker>

— Vergunning voor transitoverkeer

de vergunninghouder elke

ACL-ondersteuning om te filteren op TTL-waarde

Ondersteuning van Cisco IOS XE-softwarerelease 16.6.4 voegde ACL toe om IP-pakketten te filteren op basis van de waarde van Time to Live (TTL). De TTL-waarde van een IP-datagram wordt verlaagd door elk netwerkapparaat wanneer een pakket van bron naar bestemming stroomt.

Hoewel de aanvankelijke waarden per besturingssysteem verschillen, moet het pakket worden gedropt als de TTL van een pakket op nul komt. Het apparaat dat decrements de TTL aan nul, en daarom het pakket laat vallen, wordt vereist om een Overschreden bericht van de Tijd te produceren en te verzenden ICMP aan de bron van het pakket.

Het genereren en overdragen van deze berichten is een uitzonderingsproces. Routers kunnen deze functie uitvoeren wanneer het aantal IP-pakketten dat verloopt, laag is, maar als het aantal pakketten dat verloopt hoog is, kunnen generatie en transmissie van deze berichten alle beschikbare CPU-bronnen gebruiken. Dit duidt op een DoS-aanvalsvector. Het is om deze reden dat de apparaten tegen aanvallen moeten worden gehard van Dos die een hoog tarief IP pakketten gebruiken die zullen verlopen.

Het wordt aanbevolen dat organisaties IP-pakketten met lage TTL-waarden aan de rand van het netwerk filteren. Volledig filteren van pakketten met TTL-waarden onvoldoende om het netwerk te doorkruisen, beperkt de dreiging van op TTL gebaseerde aanvallen.

In dit voorbeeld filtert ACL pakketten met TTL-waarden van minder dan zes. Dit biedt bescherming tegen TTL-vervalaanvallen voor netwerken van maximaal vijf hops in de breedte.

IP-toegangslijst met uitgebreide ACL-INFRASTRUCTUUR-IN

— IP-pakketten weigeren met TTL-waarden die niet volstaan om het netwerk te doorkruisen

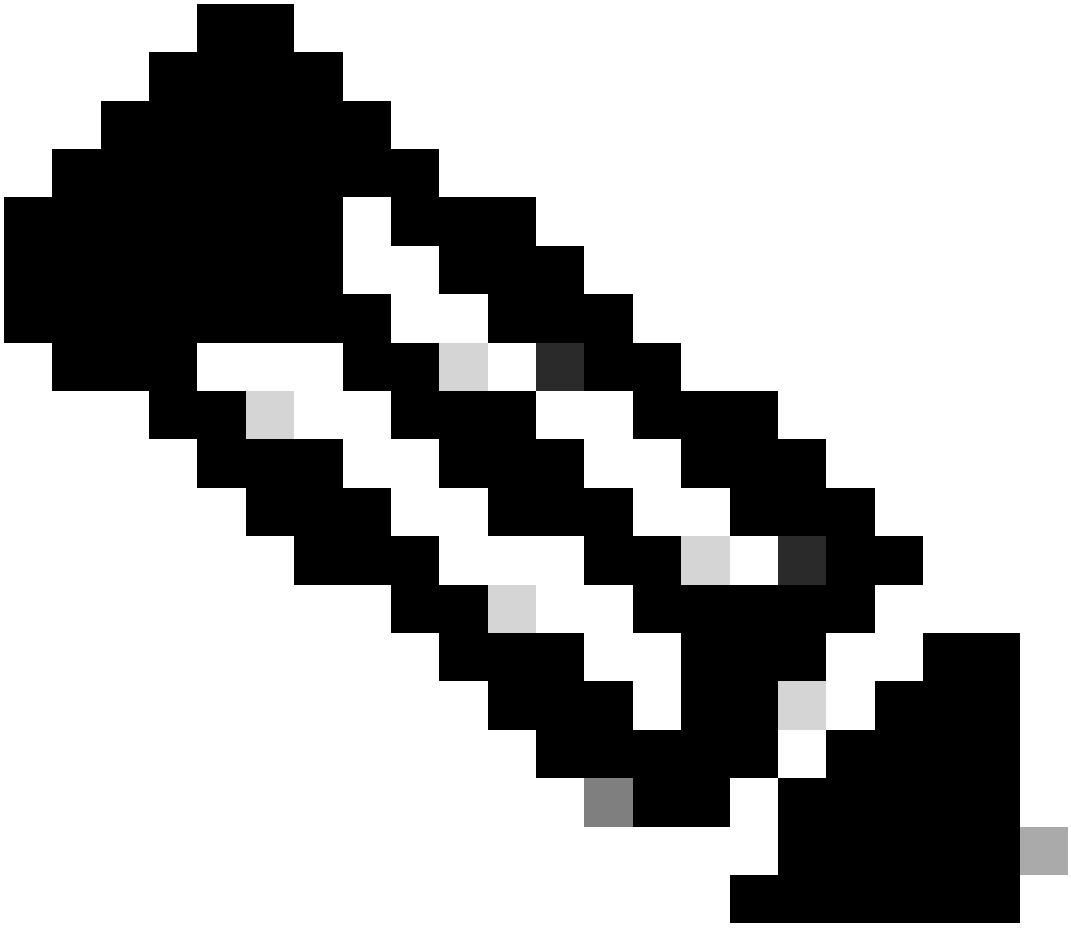
Ip geen enkele tellt LT6

— al het andere IP-verkeer naar een netwerkapparaat weigeren

Geen <infrastructuur-adres-ruimte> <masker>

— Vergunning voor transitoverkeer

de vergunninghouder elke



Opmerking: sommige protocollen maken legitiem gebruik van pakketten met lage TTL-waarden. eBGP is zo'n protocol. Raadpleeg de identificatie en beperking van TTL-aanvallen bij verlopen voor meer informatie over het beperken van op TTL-aanvallen op basis van vervaldata.

Beveiligde interactieve beheersessies

Beheersessies voor apparaten stellen u in staat om informatie over een apparaat en de werking ervan te bekijken en te verzamelen. Als deze informatie aan een kwaadwillige gebruiker wordt onthuld, kan het apparaat het doel van een aanval worden, gecompromitteerd, en gebruikt om extra aanvallen uit te voeren. Iedereen met bevoegde toegang tot een apparaat heeft de mogelijkheid voor volledige beheerderscontrole over dat apparaat. Het is absoluut noodzakelijk om beheersessies te beveiligen om de openbaarmaking van informatie en ongeoorloofde toegang te voorkomen.

Bescherming van beheerplane

In Cisco IOS XE-softwarerelease 16.6.4 en hoger kan met de functie Management Plane Protection (MPP) een beheerder beperken op welke interfaces beheerverkeer door een apparaat kan worden ontvangen. Zo heeft de beheerder meer controle over een apparaat en over hoe toegang wordt verkregen tot het apparaat.

Dit voorbeeld laat zien hoe u MPP kunt inschakelen om alleen SSH en HTTPS op de Gigabit Ethernet0/1 interface toe te staan:

bedieningsvliegtuig-host

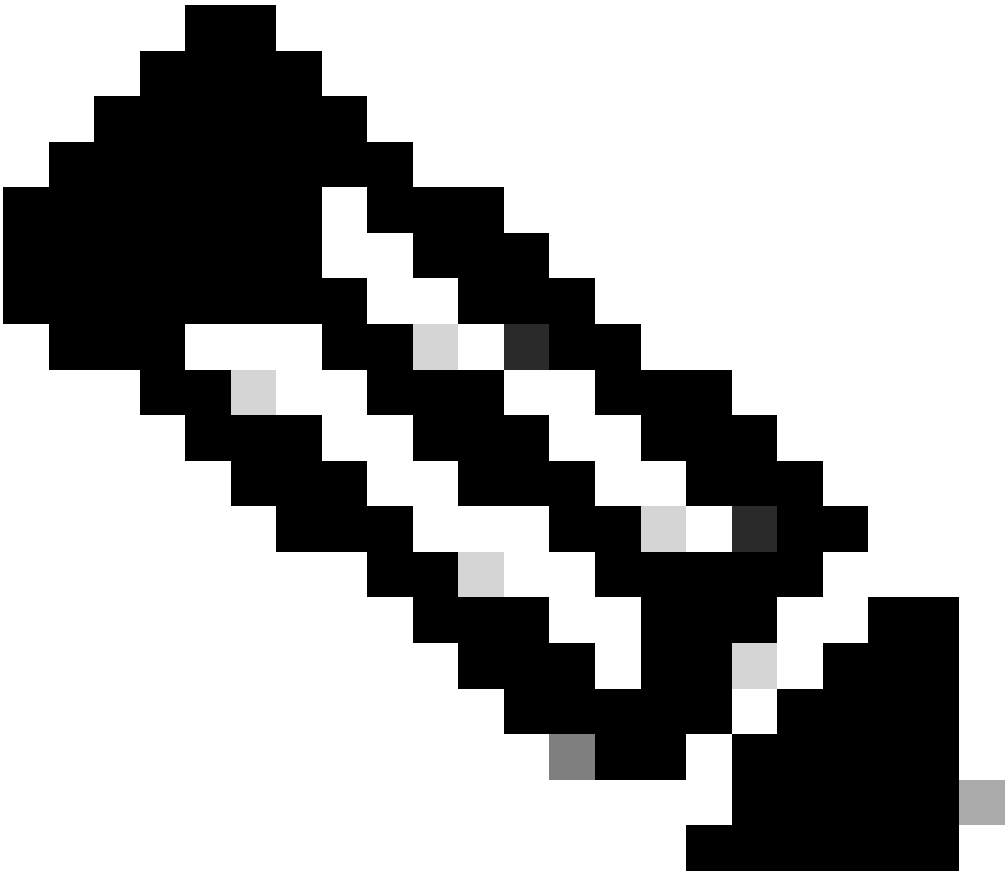
Gigabit Ethernet 10/1 beheerinterface voor SSH https

Bescherming van besturingsplane

Control Plane Protection (CPPr) bouwt voort op de functionaliteit van Control Plane Policing om vliegtuigverkeer te beperken en te controleren dat is bestemd voor de routeprocessor van het IOS-XE apparaat. CPPr verdeelt het bedieningsvlak in afzonderlijke categorieën van het bedieningsvlak die subinterfaces worden genoemd. Er bestaan drie subinterfaces van de besturingsplane: host, Transit en CEF-Exception. Daarnaast omvat CPPr deze extra beveiligingskenmerken van het bedieningsvlak:

1. Poortfiltering - Deze functie biedt de mogelijkheid om pakketten die naar een gesloten of niet-luisterende TCP- of UDP-poort gaan, te controleren of te laten vallen.
2. Queue-drempel beleidsfunctie - Deze functie beperkt het aantal pakketten voor een gespecificeerd protocol die zijn toegestaan in de IP-invoerwachtrij van het besturingsplane.

   CPPr staat een beheerder toe om verkeer te classificeren, te controleren en te beperken dat naar een apparaat voor beheersdoeleinden met de gastheer subinterface wordt verzonden. De voorbeelden van pakketten die voor de categorie van de gastheersubinterface worden geclassificeerd omvatten beheersverkeer zoals SSH of Telnet en het verpletteren van protocollen.



Opmerking: CPPr biedt geen ondersteuning voor IPv6 en is beperkt tot het IPv4-invoerpad.

Raadpleeg Control Plane Policing voor meer informatie over de Cisco CPPr-functie.

Beheersessies versleutelen

Omdat de informatie in een interactieve beheerszitting kan worden onthuld, moet dit verkeer worden versleuteld zodat een kwaadwillige gebruiker geen toegang kan krijgen tot de gegevens die worden doorgegeven. Verkeersversleuteling zorgt voor een beveiligde externe toegangsverbinding met het apparaat. Als het verkeer voor een beheersessie via het netwerk in leesbare tekst wordt verzonden, kan een aanvaller gevoelige informatie over het apparaat en het netwerk verkrijgen.

Een beheerder kan een versleutelde en beveiligde externe toegangsbeheerverbinding tot stand brengen met een apparaat met de functies SSH of Secure Hypertext Transfer Protocol (HTTPS). Cisco IOS XE-software ondersteunt SSH versie 2.0 (SSHv2) en HTTPS die Secure Sockets Layer (SSL) en Transport Layer Security (TLS) gebruikt voor verificatie en gegevenscodering.

Cisco IOS XE-software ondersteunt ook het Secure Copy Protocol (SCP), waarmee een

versleutelde en beveiligde verbinding tot stand wordt gebracht om apparaatconfiguraties of softwareafbeeldingen te kopiëren. SCP vertrouwt op SSH.

Deze voorbeeldconfiguratie maakt SSH op een Cisco IOS XE-apparaat mogelijk:

IP-domeinnaam example.com

crypto-sleutelgeneratie rsa modulus 2048

IP-time-out 60

IP Ssh-verificatie - opnieuw geprobeerd 3

IP-sh-broninterface Gigabit Ethernet 10/10

lijn vty 0 4

vervoersinvoer

Dit configuratievoorbeeld maakt SCP-services mogelijk:

IP-scp server inschakelen

Dit is een configuratievoorbeeld voor HTTPS-services:

crypto-sleutelgeneratie rsa modulus 2048

IP-http: beveiligde server

SSHv2

De SSHv2-functie is in Cisco IOS XE geïntroduceerd in de allereerste release 16.6.4 waarmee een gebruiker SSHv2 kan configureren. SSH wordt uitgevoerd bovenop een betrouwbare transportlaag en biedt sterke verificatie- en versleutelingsmogelijkheden. Het enige betrouwbare transport dat is gedefinieerd voor SSH is TCP. SSH biedt een middel om opdrachten op een andere computer of ander apparaat veilig via een netwerk te openen en uit te voeren. De Secure Copy Protocol (SCP)-functie die via SSH is getunneld, maakt een veilige overdracht van bestanden mogelijk.

Als de opdracht ip sh versie 2 niet expliciet is geconfigureerd, laat Cisco IOS XE SSH versie 1.9 toe. SSH-versie 1.99 zorgt voor zowel SSHv1- als SSHv2-verbindingen. SSHv1 wordt als onveilig beschouwd en kan nadelige effecten op het systeem hebben. Als SSH is ingeschakeld, wordt aangeraden om SSHv1 uit te schakelen met behulp van de opdracht ip sh versie 2.

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

hostname router

IP-domeinnaam example.com

crypto-sleutelgeneratie rsa modulus 2048

IP-time-out 60

IP Ssh-verificatie - opnieuw geprobeerd 3

IP-sh-broninterface Gigabit Ethernet 10/10

IP sh versie 2

lijn vty 0 4

vervoersinvoer

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

SSHv2-verbeteringen voor RSA-sleutels

Cisco IOS XE SHv2 ondersteunt toetsenbord-interactieve en op een wachtwoord gebaseerde verificatiemethoden. De functie 'SSHv2-verbeteringen voor RSA-sleutels' ondersteunt ook op RSA gebaseerde openbare sleutelverificatie voor de client en server.

Voor gebruikersverificatie gebruikt op RSA gebaseerde gebruikersverificatie een privé/openbaar sleutelpaar gekoppeld aan elke gebruiker voor verificatie. De gebruiker moet een privaat/publiek sleutelpaar op de client genereren en een openbare sleutel op de Cisco IOS XE SSH-server configureren om de verificatie te voltooien.

Een SSH-gebruiker die probeert de aanmeldgegevens in te stellen biedt een versleutelde handtekening met de privésleutel. De handtekening en de openbare sleutel van de gebruiker worden verzonden naar de SSH-server voor verificatie. De SSH-server berekent een hash over de openbare sleutel die door de gebruiker is verstrekt. De hash wordt gebruikt om te bepalen of de server een item heeft dat overeenkomt. Als een overeenkomst is gevonden, wordt een op RSA gebaseerde berichtverificatie uitgevoerd met de openbare sleutel. De gebruiker wordt dus geverifieerd of de toegang wordt geweigerd op basis van de versleutelde handtekening.

Voor serververificatie moet de Cisco IOS XE SSH-client een hostsleutel voor elke server toewijzen. Wanneer de client probeert een SSH-sessie met een server op te stellen, ontvangt deze de handtekening van de server als onderdeel van het bericht voor sleuteluitwisseling. Als de strikte vlag voor het controleren van de hostsleutel op de client is ingeschakeld, controleert de client of de host-sleutelvermelding die overeenkomt met de vooraf ingestelde server, aanwezig is. Als een overeenkomst wordt gevonden, probeert de client de handtekening te valideren met behulp van de serverhostsleutel. Als de server is geverifieerd, wordt doorgegaan met het tot stand brengen van de sessie; anders wordt deze beëindigd en wordt een bericht Serververificatie mislukt weergegeven.

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

Configureer een hostnaam voor het apparaat

hostname router

Een domeinnaam configureren

IP-domeinnaam example.com

Schakel de SSH-server in voor lokale en externe verificatie op de router die deze gebruikt

de opdracht "crypto key generation".

Voor SSH versie 2 moet de modulusgrootte minimaal 768 bits zijn

crypto-sleutel genereren rsa-gebruikstoetsen label shkeys modulus 2048

Specificeer de naam van het RSA-sleutelpaar (in dit geval "sleutels") dat voor SSH moet worden gebruikt

ip ssh rsa sleutelpaar-naam sleutels

Configureer een time-out voor de sh (in seconden).

De volgende output laat een onderbreking van 120 seconden voor SSH verbindingen toe.

IP-time-out 120

Configureer de limiet van vijf herhalingspogingen voor verificatie.

IP-sh-verificatie - opnieuw geprobeerd 5

Configureer SSH versie 2.

IP sh versie 2

Raadpleeg Ondersteuning voor Secure Shell versie 2 voor RSA-sleutels voor meer informatie over het gebruik van RSA-sleutels met SSHv2.

Met deze voorbeeldconfiguratie kan de Cisco IOS XE SSH-server RSA-gebaseerde gebruikersverificatie uitvoeren. De gebruikersverificatie lukt als de openbare RSA-sleutel die is opgeslagen op de server, wordt geverifieerd met het openbare of privé sleutelpaar dat is opgeslagen op de client.

Configureer een hostnaam voor het apparaat.

hostname router

Configureer een domeinnaam.

IP-domeinnaam cisco.com

Genereert RSA-sleutelparen die een modulus van 2048 bits gebruiken.

crypto-sleutelgeneratie rsa modulus 2048

Configureer de SSH-RSA-toetsen voor gebruiker- en serververificatie op de SSH-server.

ip ssh pubkey-chain

Configureer de SSH-gebruikersnaam.

Configureer de SSH-RSA-toetsen voor gebruiker- en serververificatie op de SSH-server.

ip ssh pubkey-chain

Configureer de SSH-gebruikersnaam.

gebruikersnaam sh-user

Geef de openbare RSA-sleutel van de externe peer op.

U moet dan de key-string opdracht configureren

(gevolgd door de openbare RSA-sleutel van de peer op afstand) of de

key-hash commando (gevolgd door het SSH-sleuteltype en de versie).

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

Met deze voorbeeldconfiguratie kan de Cisco IOS XE SSH-client RSA-gebaseerde serververificatie uitvoeren.

hostname router

IP-domeinnaam cisco.com

Genereer RSA-sleutelparen.

crypto-sleutelgeneratie rsa

Configureer de SSH-RSA-toetsen voor gebruiker- en serververificatie op de SSH-server.

ip ssh pubkey-chain

Schakel de SSH-server in voor openbare verificatie op de router.

naam van SSH-server van de server

Specificeer de RSA public-key van de remote peer.

U moet dan de key-string opdracht configureren

(gevolgd door de openbare RSA-sleutel van de peer op afstand) of thea

key-hash <key-type> <key-name>-opdracht (gevolgd door de SSH-toets)

type en versie).

Zorg ervoor dat de serververificatie plaatsvindt - De verbinding is

beëindigd op een storing.

ip ssh stricthostkeycheck

Raadpleeg Cisco IOS XE 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 XE-apparaten zijn console- en hulppoorten (AUX) asynchrone lijnen die kunnen worden gebruikt voor lokale en externe toegang tot een apparaat. U moet zich ervan bewust zijn dat consolepoorten op Cisco-apparaten speciale rechten hebben. Deze bevoegdheden zorgen er met name voor dat een beheerder de wachtwoordherstelprocedure kan uitvoeren. Om wachtwoordherstel uit te voeren, zou een niet-geverifieerde aanvaller toegang tot de consolepoort en de mogelijkheid om de voeding van het apparaat te onderbreken of het apparaat te laten crashen moeten hebben.

Elke methode die wordt gebruikt om toegang te krijgen tot de consolepoort van een apparaat moet worden beveiligd op een manier die gelijk is aan de beveiliging die wordt afgedwongen voor bevoorrechte toegang tot een apparaat. De methodes die worden gebruikt om toegang te beveiligen moeten het gebruik van AAA, exec-timeout, en modemwachtwoorden omvatten als een modem aan de console in bijlage is.

Als wachtwoordherstel niet nodig is, kan een beheerder de mogelijkheid verwijderen om de wachtwoordherstelprocedure uit te voeren die gebruikmaakt van de opdracht geen wachtwoord herstellen globale configuratie; zodra de opdracht geen wachtwoord herstellen is ingeschakeld, kan een beheerder echter geen wachtwoordherstel meer uitvoeren op een apparaat.

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

regel aux 0

transport input geen

vervoeroutput geen

geen exec exec-time-out 0 1

geen wachtwoord

Vty- en tty-lijnen beheren

Interactieve beheersessies in Cisco IOS XE-software maken gebruik van een ty of Virtual Tty (vty). Een tty is een lokale asynchrone lijn waaraan een terminal kan worden verbonden voor lokale toegang tot het apparaat of tot een modem voor inbeltoegang tot een apparaat. Let op: tty's kunnen worden gebruikt voor verbindingen met consolepoorten van andere apparaten. Deze functie zorgt ervoor dat een apparaat met tty-lijnen kan handelen als een consoleserver waarop verbindingen tot stand kunnen worden gebracht in het netwerk met de consolepoorten van apparaten die zijn verbonden met de tty-lijnen. De tty-lijnen voor deze omgekeerde verbindingen over het netwerk moeten ook worden beheerd.

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

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 vty-lijnen omdat ze via het netwerk toegankelijk zijn. Een tty-lijn die is aangesloten op een modem die wordt gebruikt voor externe toegang tot het apparaat, of een tty-lijn die is aangesloten op de consolepoort van andere apparaten, zijn ook toegankelijk via het netwerk. Andere vormen van vty- en tty-toegangscontroles kunnen worden afgedwongen met de configuratie-opdrachten transport input of access-class, met het gebruik van de functies CoPP en CPPr, of als u toegangslijsten toepast op interfaces op het apparaat.

Verificatie kan worden afgedwongen via het gebruik van AAA. Dit is de aanbevolen methode voor geverifieerde toegang tot een apparaat, met het gebruik van de lokale gebruikersdatabase, of door eenvoudige wachtwoordverificatie direct geconfigureerd op de vty- of tty-lijn.

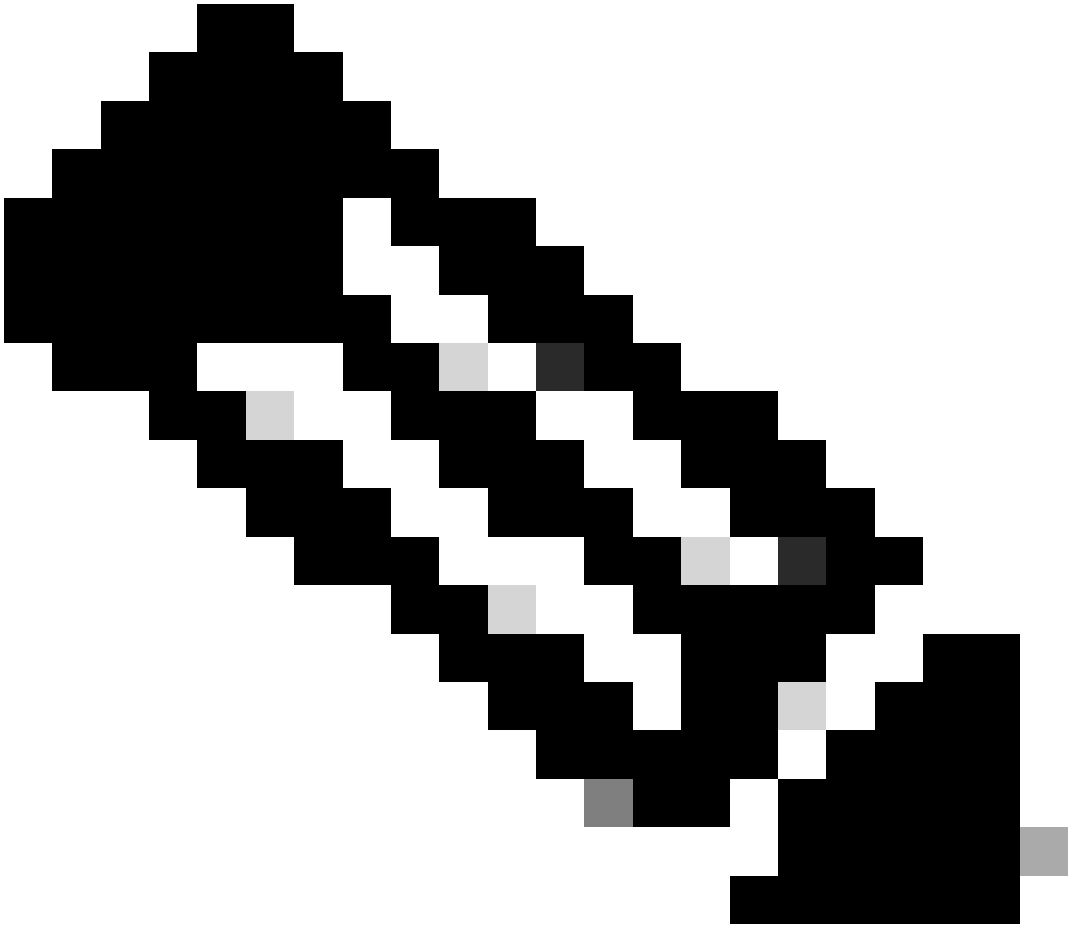
De opdracht exec-timeout moet worden gebruikt om sessies uit te loggen op vty of tty lijnen die niet worden gebruikt. De opdracht service-tcp-keepalives-in moet ook worden gebruikt om TCP-keepalives op inkomende verbindingen met het apparaat in te schakelen. Dit waarborgt dat het apparaat op het verre eind van de verbinding nog toegankelijk is en dat de half-open of orphaned verbindingen worden verwijderd uit het lokale apparaat IOS-XE.

Transport voor vty- en tty-lijnen beheren

Een vty en tty kan worden geconfigureerd om alleen versleutelde en beveiligde externe toegangsbeheerverbindingen naar het apparaat of via het apparaat te accepteren als het wordt gebruikt als een consoleserver. In dit gedeelte worden tty's besproken omdat dergelijke lijnen kunnen worden aangesloten op consolepoorten op andere apparaten, waarmee de tty toegankelijk is via het netwerk. In een poging om informatieopenbaarmaking of onbevoegde toegang tot de

gegevens te voorkomen die tussen de beheerder en het apparaat worden verzonden, kunnen transport-ingangssh worden gebruikt in plaats van clear-text protocollen, zoals Telnet en rlogin. De transport input geen configuratie kan worden ingeschakeld op een tty, die in feite het gebruik van de tty line voor reverse-console verbindingen verbiedt.

Met zowel vty- als tty-lijnen kan de beheerder verbinding maken met andere apparaten. Om het type transport te beperken dat een beheerder kan gebruiken voor uitgaande verbindingen, gebruikt u de opdracht voor configuratie van de uitvoerlijn. Als er geen uitgaande verbindingen nodig zijn, kan geen transportoutput worden gebruikt. Als echter uitgaande verbindingen zijn toegestaan, kan een versleutelde en beveiligde externe toegangsmethode voor de verbinding worden afgedwongen door het gebruik van transport output ssh.



Opmerking: IPSec kan worden gebruikt voor versleutelde en beveiligde externe toegangsverbindingen met een apparaat, indien ondersteund. Als u IPSec gebruikt, wordt ook aanvullende CPU-overhead toegevoegd aan het apparaat. SSH moet echter nog steeds als transport worden afgedwongen, zelfs als IPSec wordt gebruikt.

Waarschuwingsbanners

In sommige rechtsgebieden kan het onmogelijk zijn kwaadwillige gebruikers te vervolgen en illegaal te controleren, tenzij ze op de hoogte zijn gesteld dat ze het systeem niet mogen gebruiken. Een methode om dit bericht te geven is om deze informatie in een bannerbericht te plaatsen dat is geconfigureerd met de Cisco IOS XE-software-bannerinlogopdracht.

De wettelijke kennisgevingsvereisten zijn complex, variëren per jurisdictie en situatie en kunnen met juridische adviseurs worden besproken. Zelfs binnen rechtsgebieden kunnen juridische meningen verschillen. In samenwerking met een adviseur kan een banner deze informatie geheel of gedeeltelijk verstrekken:

1. Kennisgeving dat mensen zich moeten aanmelden bij het systeem of dat het alleen mag worden gebruikt door specifiek bevoegd personeel en mogelijk informatie over wie gebruik kan autoriseren.
2. Kennisgeving dat elk onbevoegd gebruik van het systeem onwettig is en onderhevig kan zijn aan civiele of strafrechtelijke boetes.
3. Bericht dat elk gebruik van het systeem zonder verdere kennisgeving kan worden geregistreerd of gecontroleerd en dat de resulterende logbestanden als bewijs in de rechtbank kunnen worden gebruikt.
4. Specifieke kennisgevingen vereist door lokale wetgeving.

   Vanuit een veiligheidsperspectief, eerder dan wettelijk, kan een login banner geen specifieke informatie over de routernaam, het model, de software, of het eigendom bevatten. Deze informatie kan worden misbruikt door kwaadwillende gebruikers.

Verificatie, autorisatie en accounting

Het AAA-kader (Verificatie, autorisatie en accounting) is essentieel om interactieve toegang tot netwerkapparaten te beveiligen. Het AAA-framework biedt een zeer configureerbare omgeving die op maat kan worden gesneden op basis van de behoeften van het netwerk.

TACACS+-verificatie

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

TACACS+-verificatie, of meer algemeen AAA-verificatie, biedt de mogelijkheid om afzonderlijke gebruikersaccounts te gebruiken voor elke netwerkbeheerder. Wanneer u niet afhankelijk bent van een enkel gedeeld wachtwoord, wordt de beveiliging van het netwerk verbeterd en uw verantwoordelijkheid versterkt.

RADIUS is een protocol dat in doel vergelijkbaar is met TACACS+; het versleutelt echter alleen het wachtwoord dat door het netwerk wordt verzonden. In tegenstelling tot het voorgaande versleutelt TACACS+ de volledige TCP-payload, die zowel de gebruikersnaam als het wachtwoord omvat. Daarom kan TACACS+ bij voorkeur worden gebruikt in plaats van RADIUS wanneer

TACACS+ wordt ondersteund door de AAA-server. Raadpleeg Vergelijking van TACACS+ en RADIUS voor een gedetailleerdere vergelijking van deze twee protocollen.

U kunt TACACS+ verificatie inschakelen op een Cisco IOS XE-apparaat met een configuratie die vergelijkbaar is met dit voorbeeld:

aaa new-model

aaa verificatie login standaardgroep tacacs+

tacacs-server <server_name>

adres ipv4 <tacacs_server_ip_address>

Sleutel <toets>

De vorige configuratie kan worden gebruikt als startpunt voor een organisatiespecifieke AAA-verificatiesjabloon.

Een methodelijst is een sequentiële lijst die de verificatiemethoden beschrijft die moeten worden opgevraagd om een gebruiker te verifiëren. Met methodelijsten kunt u een of meer beveiligingsprotocollen aanwijzen die voor de verificatie moeten worden gebruikt, en zo een back-upsysteem voor verificatie garanderen voor het geval dat de eerste methode mislukt. Cisco IOS XE-software gebruikt de eerste methode die met succes een gebruiker accepteert of afwijst. Latere methoden worden alleen geprobeerd in gevallen waarin eerdere methoden falen vanwege serveronbeschikbaarheid of onjuiste configuratie.

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

Verificatie-fallback

Als alle geconfigureerde TACACS+ servers niet beschikbaar worden, kan een Cisco IOS XE-apparaat vertrouwen op secundaire verificatieprotocollen. Typische configuraties zijn onder andere het gebruik van lokaal of inschakelen van verificatie als alle geconfigureerde TACACS+-servers onbeschikbaar zijn.

De volledige lijst van opties voor verificatie op het apparaat omvat enable, local en line. Elk van deze opties heeft voordelen. Het gebruik van het Enable geheim heeft de voorkeur omdat het geheim is gehakt met een unidirectioneel algoritme dat inherent veiliger is dan het encryptie algoritme dat met de Type 7 wachtwoorden voor lijn of lokale authentificatie wordt gebruikt.

Op Cisco IOS XE-softwarereleases die het gebruik van geheime wachtwoorden voor lokaal gedefinieerde gebruikers ondersteunen, kan een terugval naar lokale verificatie echter wenselijk zijn. Hierdoor kan een lokaal gedefinieerde gebruiker worden gemaakt voor een of meer netwerkbeheerders. Als TACACS+ volledig onbeschikbaar zou worden, kan elke beheerder zijn lokale gebruikersnaam en wachtwoord gebruiken. Hoewel deze actie de verantwoordelijkheid van netwerkbeheerders bij TACACS+-storingen verhoogt, wordt de beheerderslast aanzienlijk verhoogd omdat lokale gebruikersaccounts op alle netwerkapparaten moeten worden

onderhouden.

Dit configuratievoorbeeld bouwt voort op het vorige TACACS+ verificatievoorbeeld om fall-back-verificatie op te nemen in het wachtwoord dat lokaal is geconfigureerd met de opdracht Laat geheime opdracht toe:

geheime <wachtwoord> inschakelen

aaa new-model

Aa verificatie inlognaam standaardgroep tacacs+ inschakelen

tacacs-server <server_name>

adres ipv4 <tacacs_server_ip_address>

Sleutel <toets>

Raadpleeg Verificatie configureren voor meer informatie over het gebruik van fallback-verificatie met AAA.

Gebruik van Type 7-wachtwoorden

Oorspronkelijk ontworpen om snelle decryptie van opgeslagen wachtwoorden mogelijk te maken, zijn Type 7 wachtwoorden geen veilige vorm van wachtwoordopslag. Er zijn veel tools beschikbaar die deze wachtwoorden gemakkelijk kunnen decoderen. Het gebruik van wachtwoorden van type 7 kan worden vermeden, tenzij dit vereist is door een functie die in gebruik is op het Cisco IOS XE-apparaat.

Type 9 (crypt) kan waar mogelijk worden gebruikt:

gebruikersnaam <gebruikersnaam> privilege 15 algoritme-type encryptie geheim <geheim>

Het verwijderen van wachtwoorden van dit type kan worden vergemakkelijkt door AAA-verificatie en het gebruik van de functie Enhanced Password Security, waarmee geheime wachtwoorden kunnen worden gebruikt met gebruikers die lokaal zijn gedefinieerd via de opdracht Gebruikersnaam global configuratie. Als u het gebruik van Type 7-wachtwoorden niet volledig kunt voorkomen, beschouw deze wachtwoorden dan als verhuld, niet als versleuteld.

Raadpleeg het gedeelte Versterking algemene beheerplane van dit document voor meer informatie over het verwijderen van Type 7-wachtwoorden.

TACACS+-opdrachtautorisatie

Opdrachtautorisatie met TACACS+ en AAA biedt een mechanisme waarmee elke opdracht die wordt ingevoerd door een beheerdersgebruiker wordt toegestaan of geweigerd. Wanneer de gebruiker EXEC-opdrachten invoert, stuurt Cisco IOS XE elke opdracht naar de geconfigureerde AAA-server. De AAA-server gebruikt vervolgens het ingestelde beleid om de opdracht voor die specifieke gebruiker toe te staan of te weigeren.

Deze configuratie kan aan het vorige AAA-verificatievoorbeeld worden toegevoegd om opdrachtautorisatie te implementeren:

aaa-autorisatie exec standaardgroep tacacs+ geen

aaa-autorisatieopdrachten 0 standaardgroep tacacs+ geen

aaa-autorisatieopdrachten 1 standaardgroep tacacs+ geen

aaa-autorisatieopdrachten 15 standaard groep tacacs+ geen

Raadpleeg Autorisatie configureren voor meer informatie over opdrachtautorisatie.

TACACS+-opdrachtaccounting

Indien geconfigureerd stuurt AAA-opdrachtaccounting informatie over elke EXEC-opdracht die is ingevoerd op de geconfigureerde TACACS+-servers. De informatie die naar de TACACS+ server wordt verzonden omvat het uitgevoerde bevel, de datum het werd uitgevoerd, en de gebruikersbenaming van de gebruiker die het bevel ingaat. Opdrachtaccounting wordt niet ondersteund met RADIUS.

Deze voorbeeldconfiguratie schakelt AAA-opdrachtaccounting in voor EXEC-opdrachten ingevoerd op bevoegdheidsniveaus nul, één en 15. Deze configuratie bouwt voort op eerdere voorbeelden, waaronder de configuratie van de TACACS-servers.

aaa accounting exec standaard start-stop groep tacacs+

aaa accounting commando's 0 standaard start-stop groep tacacs+

aaa boekhoudingsbevelen 1 standaard start-stop groep tacacs+

aaa boekhoudingsbevelen 15 standaard start-stop groep tacacs+

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

Overbodige AAA-servers

De AAA-servers die worden ingezet in een omgeving, kunnen overbodig zijn en worden geïmplementeerd op een manier die fouten tolereert. Zo wordt ervoor gezorgd dat interactieve beheertoegang, zoals SSH, mogelijk is als een AAA-server onbeschikbaar is.

Wanneer u een overbodige AAA-serveroplossing ontwerpt of implementeert, onthoud dan deze overwegingen:

1. Beschikbaarheid van AAA-servers tijdens mogelijke netwerkstoringen
2. Geografisch verspreide plaatsing van AAA-servers
3. Belasting op afzonderlijke AAA-servers bij stabiele en storingsomstandigheden
4. Netwerklatentie tussen Network Access Servers en AAA-servers

5. Synchronisatie van AAA-serverdatabases

Raadpleeg De Access Control Servers implementeren voor meer informatie.

Het Simple Network Management Protocol versterken

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

SNMP-communitystrings

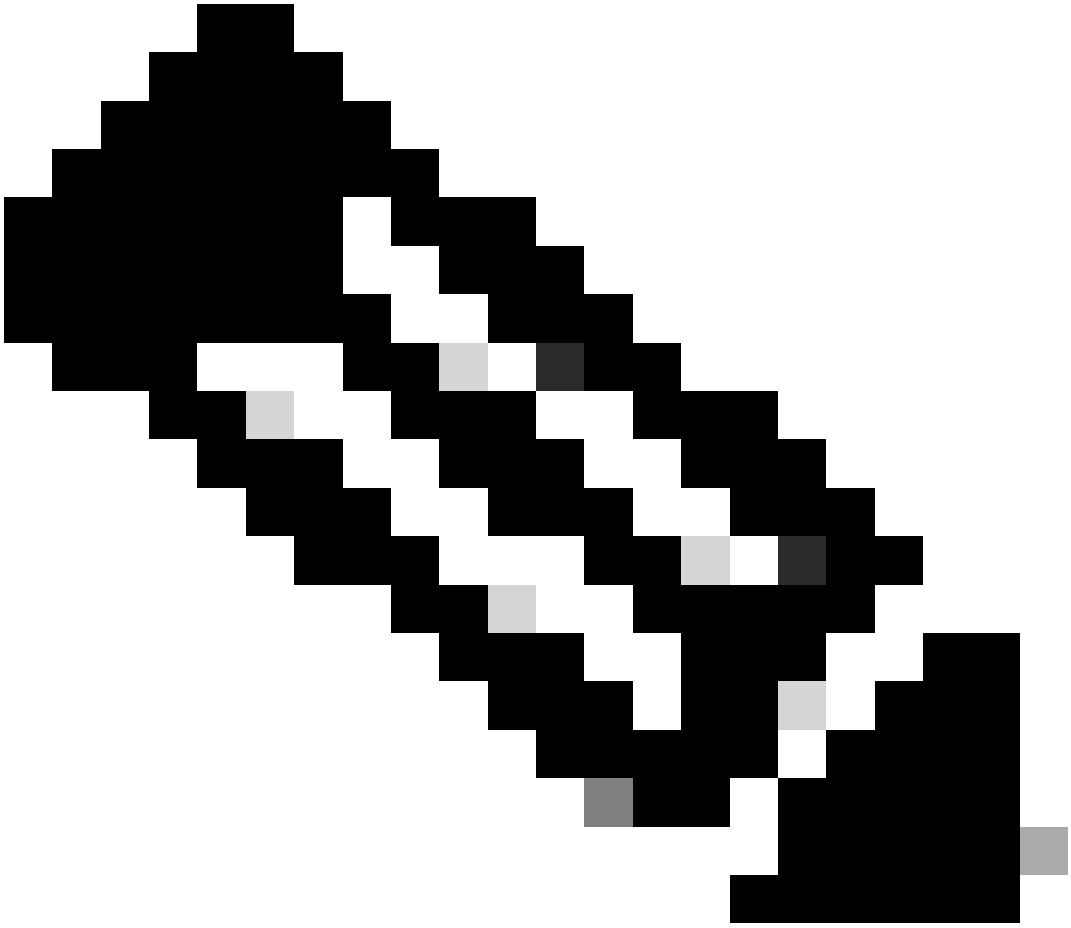
Community-strings zijn wachtwoorden die worden toegepast op een IOS-XE-apparaat om toegang, zowel alleen-lezen als lezen-schrijven, tot de SNMP-gegevens op het apparaat te beperken. Deze community-strings kunnen, net als alle wachtwoorden, zorgvuldig worden gekozen om te voorkomen dat ze onbelangrijk zijn. Communitytekenreeksen kunnen op gezette tijden en in overeenstemming met het beleid voor netwerkbeveiliging worden gewijzigd.

De strings kunnen bijvoorbeeld worden gewijzigd wanneer een netwerkbeheerder rollen wijzigt of het bedrijf verlaat.

Deze configuratielijnen configureren een alleen-lezen communitystring READONLY en een lezen-en-schrijven communitystring READWRITE:

SNMP-servercommunity READONLY RO

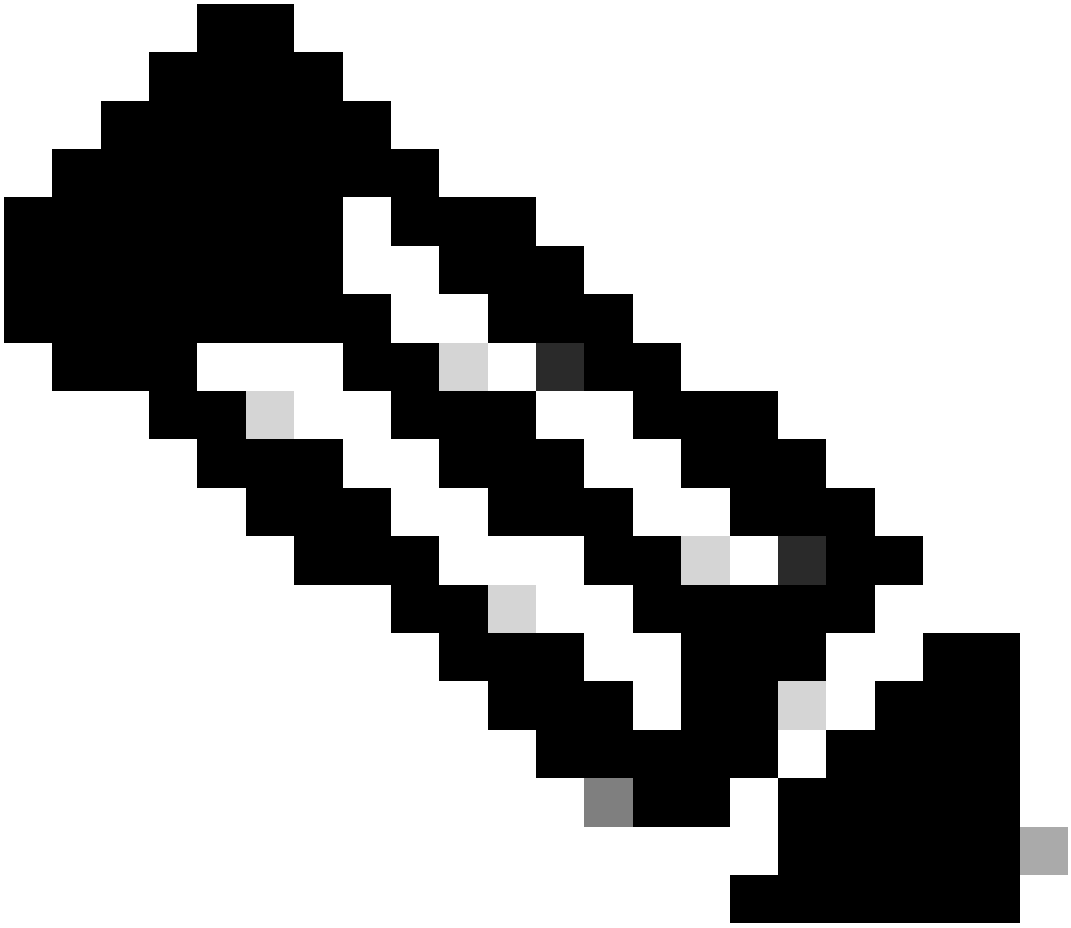
SNMP-servercommunity LEESSCHRIJF-RW



Opmerking: de vorige community string voorbeelden zijn gekozen om het gebruik van deze strings duidelijk te verklaren. Voor productieomgevingen kunnen community-strings 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 de selectie van niet-onbeduidende wachtwoorden.

SNMP-communitystrings met ACL's

Naast de community-string kan een ACL worden toegepast die de SNMP-toegang verder beperkt tot een selecte groep IP-bronadressen. Deze configuratie beperkt SNMP alleen-lezen toegang tot eindhostapparaten die zich in de adresruimte van 192.168.100.0/24 bevinden en beperkt SNMP-leestoegang tot alleen het eindhostapparaat op 192.168.100.1.



Opmerking: de apparaten die door deze ACL's zijn toegestaan, hebben de juiste community-string nodig om toegang te krijgen tot de gevraagde SNMP-informatie.

toegangslijst 98 vergunning 192.168.100.0 0.0.0.255

toegangslijst 99 vergunning 192.168.100.1

SNMP-servercommunity READONLY RO 98

SNMP-servercommunity MET READWrite RW 99

Raadpleeg de SNMP-servercommunity in de Cisco IOS XE Network Management Command Reference voor meer informatie over deze functie.

Infrastructuur-ACL's

Infrastructuur ACL's (iACL's) kunnen worden geïmplementeerd om ervoor te zorgen dat alleen eindhosts met vertrouwde IP-adressen SNMP-verkeer naar een IOS-XE-apparaat kunnen

verzenden. Een iACL kan een beleid bevatten dat onbevoegde SNMP-pakketten op UDP-poort 161 ontkent.

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

SNMP-weergaven

SNMP-weergaven zijn een beveiligingsfunctie die toegang tot bepaalde SNMP MIB's kan toestaan of weigeren. Zodra een weergave is gemaakt en toegepast op een community string met de snmp-server community string view global configuratie commando's, als u toegang hebt tot MIB data, bent u beperkt tot de permissies die zijn gedefinieerd door de view. Indien van toepassing wordt u aangeraden om weergaven te gebruiken om gebruikers van SNMP te beperken tot de gegevens die ze nodig hebben.

Dit configuratievoorbeeld beperkt SNMP-toegang met de communitystring LIMITED tot de MIB-gegevens die zich in de systeemgroep bevinden:

SNMP-serverweergave <view_name> <mib_view_family_name> [opnemen/uitsluiten]

SNMP-servercommunity <community_string>view <view_name> RO

Raadpleeg 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 beveiligde toegang tot apparaten omdat dit pakketten via het netwerk verifieert en optioneel versleutelt. Waar ondersteund, kan SNMPv3 worden gebruikt om een andere beveiligingslaag toe te voegen wanneer u SNMP implementeert. SNMPv3 bestaat uit drie primaire configuratie-opties:

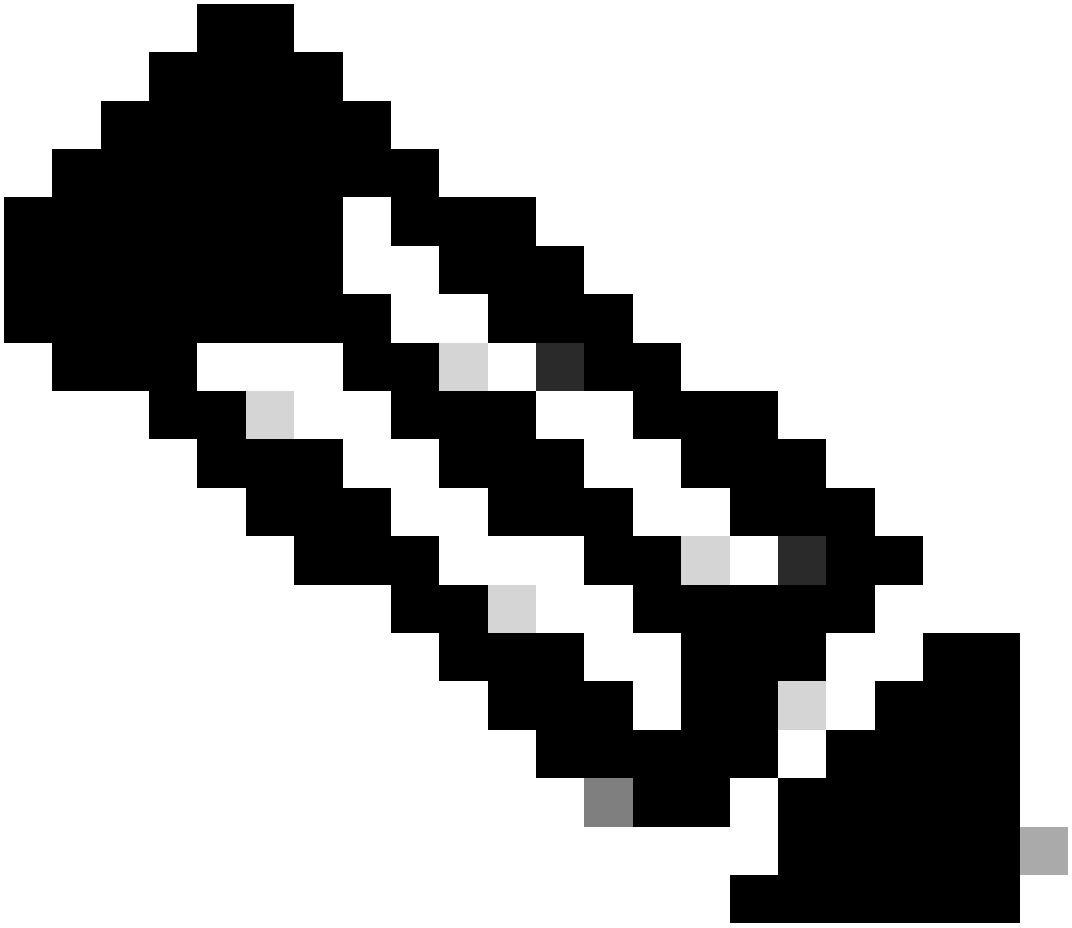
1. geen auth - Voor deze modus is geen verificatie of codering van SNMP-pakketten vereist.
2. auth - Voor deze modus is verificatie van het SNMP-pakket zonder codering vereist.
3. priv - Deze modus vereist zowel verificatie als codering (privacy) van elk SNMP-pakket.

   Er moet een gezaghebbende engine-ID bestaan om de SNMPv3 security mechanismes authenticatie of authenticatie en encryptie te gebruiken - om SNMP-pakketten te verwerken; standaard wordt de engine-ID lokaal gegenereerd. De engine-ID kan worden weergegeven met de opdracht show snmp engineID zoals weergegeven in dit voorbeeld:

   router#show snmp engineID

Lokale SNMP-engine-id: 800000090300000152BD35496

Remote Engine ID IP-adrespoort



Opmerking: als de engine-ID wordt gewijzgd, moeten alle SNMP-gebruikersaccounts opnieuw worden geconfigureerd.

De volgende stap is het configureren van een SNMPv3-groep. Met deze opdracht wordt een Cisco IOS XE-apparaat voor SNMPv3 met een SNMP-servergroep AUTHGROUP geconfigureerd en is alleen verificatie voor deze groep met het wachtwoordsleutelwoord mogelijk:

SNMP-servergroep AUTHGROUP v3 auth

Met deze opdracht wordt een Cisco IOS XE-apparaat voor SNMPv3 met een SNMP-servergroep geconfigureerd.

PRIVGROUP en maakt zowel verificatie als codering voor deze groep met het priv-sleutelwoord mogelijk:

SNMP-servergroep PRIVGROUP v3 priv

Deze opdracht configureert een SNMPv3-gebruiker snmpv3user met een MD5-verificatiewachtwoord authpassword en een 3DES-versleutelingswachtwoord privpassword:

snmp-server gebruiker snmpv3user PRIVGROUP v3 auth md5 authpassword priv 3des private password

Houd er rekening mee dat configuratieopdrachten voor snmp-servers niet worden weergegeven in de configuratie-uitgang van het apparaat, zoals vereist door RFC 3414; daarom kan het gebruikerswachtwoord niet worden weergegeven in de configuratie. Om de gevormde gebruikers te bekijken, ga het bevel van de show snmp gebruiker zoals in dit voorbeeld in:

router#show snmp-gebruiker

Gebruikersnaam: snmpv3user Engine ID: 800000090300000152BD35496

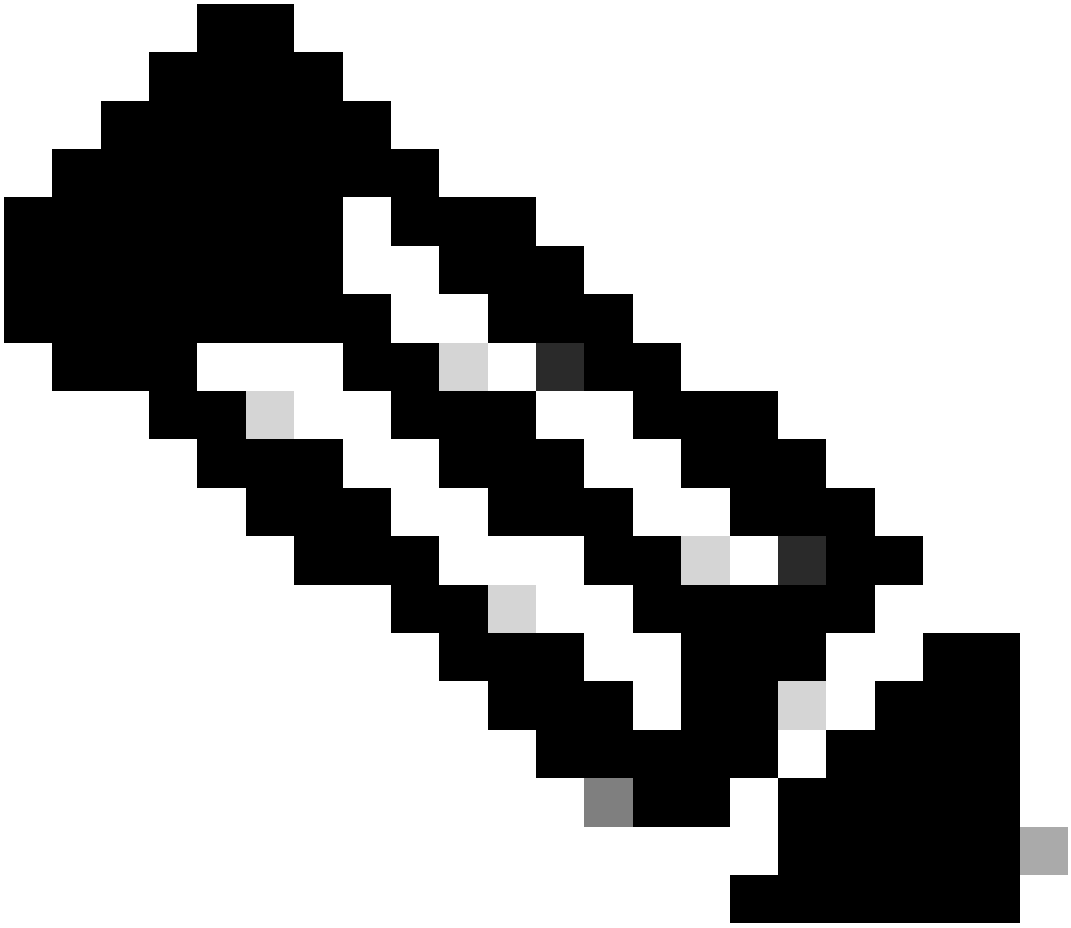
opslagtype: niet-vluchtig actief

Verificatieprotocol: MD5
Privacy Protocol: 3DES
Groepsnaam: PRIVGROUP

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

Bescherming van beheerplane

De functie Management Plane Protection (MPP) in Cisco IOS XE-software kan worden gebruikt om beveiligde SNMP te ondersteunen, omdat deze de interfaces beperkt waardoor SNMP-verkeer op het apparaat kan eindigen. Met de MPP-functie kan een beheerder een of meer interfaces toewijzen als beheerinterfaces. Beheerverkeer mag alleen via deze beheerinterfaces op een apparaat binnenkomen. Nadat MPP is ingeschakeld, accepteren alleen toegewezen beheerinterfaces netwerkverkeer dat bestemd is voor het apparaat.



> Opmerking: MPP is een subset van de CPPr-functie en vereist een versie van IOS die CPPr ondersteunt. Raadpleeg Inzicht in Control Plane Protection voor meer informatie over CPPr.

In dit voorbeeld wordt MPP gebruikt om SNMP- en SSH-toegang tot alleen de Fast Ethernet 0/0-interface te beperken:

bedieningsvliegtuig-host

beheer-interface FastEthernet0/0 toestaan ssh SNMP

Raadpleeg Functiehandleiding voor Management Plane Protection voor meer informatie.

Aanbevolen procedures bij logboekregistratie

Met gebeurtenisvastlegging kunt u inzicht krijgen in de werking van een Cisco IOS XE-apparaat en in het netwerk waarin het wordt geïmplementeerd. Cisco IOS XE-software biedt verschillende

flexibele registratieopties die kunnen helpen de doelstellingen voor netwerkbeheer en zichtbaarheid van een organisatie te realiseren.

Deze secties bieden enkele basis best practices voor vastlegging die een beheerder kunnen helpen met succes vastlegging te gebruiken en de impact van vastlegging op een Cisco IOS XE-apparaat te minimaliseren.

Logboeken verzenden naar een centrale locatie

U wordt geadviseerd logboekinformatie naar een verre syslog server te verzenden. Als u dit doet, kunnen netwerk- en beveiligingsgebeurtenissen op netwerkapparaten effectiever worden gecorreleerd en geaudit. Houd er rekening mee dat syslog-berichten onbetrouwbaar worden verzonden door UDP en in cleartext. Om deze reden kan elke bescherming die een netwerk biedt aan beheerverkeer (bijvoorbeeld codering of out-of-band toegang) uitgebreid worden met syslog verkeer.

In dit configuratievoorbeeld wordt een Cisco IOS XE-apparaat geconfigureerd om logboekinformatie naar een externe syslogserver te verzenden:

logboekhost <ip-adres>

Raadpleeg Incidenten identificeren met Firewall- en IOS-XE Router Syslog-gebeurtenissen voor meer informatie over logcorrelatie.

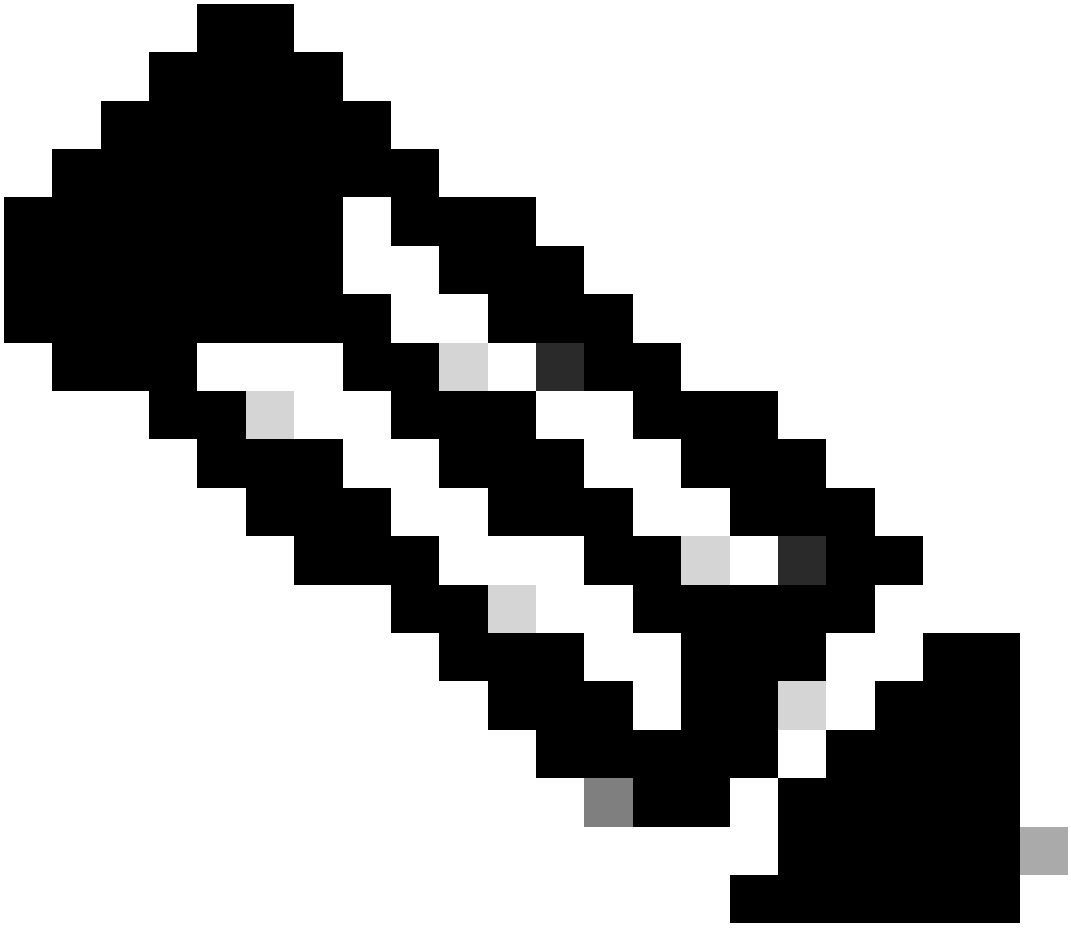
Met de functie Vastlegging aan lokale niet-vluchtige opslag (ATA-schijf) kunnen meldingen van systeemvastlegging worden opgeslagen op een geavanceerde technologie bijlage (ATA) flitsschijf. Berichten die zijn opgeslagen op een ATA-schijf blijven staan nadat een router opnieuw wordt opgestart.

Deze configuratielijnen configureren 134.217.728 bytes (128 MB) van logberichten naar de syslog-map van de ATA-flitser (disk0) en specificeert een bestandsgrootte van 16.384 bytes:

loggen gebufferd.

logboekpersistente url-schijf0:/syslog-grootte 134217728 bestand 16384

Alvorens berichten te registreren worden geschreven naar een bestand op de ATA-schijf, controleert Cisco IOS XE-software of er voldoende schijfruimte is. Als dit niet het geval is wordt het oudste bestand met logberichten (door tijdstempel) verwijderd en wordt het huidige bestand opgeslagen. De bestandsnaamnotatie is log_month:day:year::time.



Opmerking: een ATA-flashstation heeft beperkte schijfruimte en moet dus worden onderhouden om te voorkomen dat de opgeslagen gegevens worden overspannen.

Dit voorbeeld laat zien hoe u logberichten van de router ATA-flitsschijf naar een externe schijf op FTP-server 192.168.1.129 kopieert als onderdeel van onderhoudsprocedures:

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

Raadpleeg Vastlegging aan lokale niet-vluchtige opslag voor meer informatie over deze functie.

Logboekregistratieniveau

Elk logbericht dat door een Cisco IOS XE-apparaat wordt gegenereerd, wordt toegewezen aan een van de acht reeksen die variëren van niveau 0, Noodsituaties, tot niveau 7, Debug. Tenzij specifiek vereist, wordt u aangeraden om vastlegging op niveau 7 te vermijden. Vastlegging op niveau 7 resulteert in een verhoogde CPU-belasting op het apparaat, wat kan leiden tot instabiliteit van apparaat en netwerk.

Het globale niveau van de logboekval van het configuratiebevel wordt gebruikt om te specificeren welke logboekberichten naar verre syslog servers worden verzonden. Het opgegeven niveau geeft het laagste ernstbericht aan dat wordt verzonden. Voor gebufferde logboekregistratie wordt de opdracht logging buffered level gebruikt.

Dit configuratievoorbeeld beperkt logberichten die naar externe syslog-servers en de lokale logbuffer worden verzonden naar severities 6 (informatie) door 0 (noodgevallen):

logboekregistratie 6

houtkap gebufferd 6

Niet registreren op console- of bewakingssessies

Met Cisco IOS XE-software is het mogelijk om logberichten naar monitorsessies te verzenden - monitorsessies zijn interactieve beheersessies waarin de EXEC-opdrachtterminalmonitor is uitgegeven - en naar de console. Dit kan echter de CPU-belasting van een IOS-XE-apparaat verhogen en wordt daarom niet aanbevolen. In plaats daarvan, wordt u geadviseerd om registrereninformatie naar de lokale logboekbuffer te verzenden, die met het bevel van het showregistreren kan worden bekeken.

Gebruik de globale configuratiebevelen op logboekconsole en geen logboekmonitor om het registreren aan de console onbruikbaar te maken en zittingen te controleren. Dit configuratievoorbeeld toont het gebruik van deze opdrachten:

geen logboekconsole

geen logboekmonitor

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

Opgeslagen vastlegging gebruiken

Cisco IOS XE-software ondersteunt het gebruik van een lokale logbuffer, zodat een beheerder lokaal gegenereerde logberichten kan bekijken. Het gebruik van gebufferde logboekregistratie wordt ten zeerste aanbevolen in vergelijking met logboekregistratie voor de console- of monitorsessies.

Er zijn twee configuratieopties die relevant zijn bij het configureren van gebufferde logboekregistratie: de grootte van de logboekbuffer en de berichtbeveiliging die in de buffer is opgeslagen. De grootte van de logging buffer wordt geconfigureerd met de globale configuratie-opdracht logging buffered size. De laagste strengheid die in de buffer is opgenomen, wordt geconfigureerd met de opdracht "logging buffered severity". Een beheerder kan de inhoud van de logboekbuffer bekijken met de opdracht logboekregistratie EXEC.

Dit configuratievoorbeeld omvat de configuratie van een logboekbuffer van 16384 bytes, evenals een strengheid van 6, informatie, die erop wijst dat de berichten op niveaus 0 (noodgevallen) door

6 (informatie) worden opgeslagen:

houtkap gebufferd 16384 6

Raadpleeg Cisco IOS XE voor het instellen van het Berichtendisplay voor meer informatie over gebufferde vastlegging.

Broninterface voor logboekregistratie configureren

Om een verhoogd niveau van consistentie te bieden wanneer u logberichten verzamelt en beoordeelt, wordt u aangeraden om een logboekbroninterface statisch te configureren.

Voltooid via de logboekbron-interface-interfaceopdracht, zorgt statisch het vormen van een logboekbroninterface ervoor dat het zelfde IP adres in alle logboekberichten verschijnt die van een individueel Cisco IOS-apparaat worden verzonden. Voor extra stabiliteit, wordt u geadviseerd om een loopback interface als registrerenbron te gebruiken.

Dit configuratievoorbeeld illustreert het gebruik van het globale configuratiebevel van de logboekbron-interface interface om te specificeren dat het IP adres van loopback 0 interface voor alle logboekberichten wordt gebruikt:

Logboekbron-interface met logboekregistratie Loopback 0

Raadpleeg de Cisco IOS XE Embedded System Manager voor meer informatie.

Vastlegtijdstempels configureren

De configuratie van logboektijdstempels helpt u gebeurtenissen over netwerkapparaten te correleren. Het is belangrijk om een correcte en consistente logboektijdstempelconfiguratie te implementeren om ervoor te zorgen dat u logboekgegevens kunt correleren. Vastlegtijdstempels kunnen worden geconfigureerd om de datum en tijd met milliseconde precisie te omvatten en om de tijdzone in gebruik op het apparaat te omvatten.

Dit voorbeeld omvat de configuratie van logtijdstempels met milliseconde precisie binnen de gecoördineerde universele tijdzone (UTC):

service tijdstempels log datetime msec show-tijdzone

Als u liever geen tijden met betrekking tot UTC vastlegt, kunt u een specifieke tijdzone configureren en instellen dat informatie aanwezig moet zijn in gegenereerde logboekberichten. Dit voorbeelt toont een apparaatconfiguratie voor de zone Pacific Standard Time (PST):

klok tijdzone PST -8

service tijdstempels log datetime msec localtime show-tijdzone

Cisco IOS XE-softwareconfiguratiebeheer

Cisco IOS XE-software bevat verschillende functies die een vorm van configuratiebeheer op een

Cisco IOS XE-apparaat mogelijk kunnen maken. Dergelijke functies omvatten functionaliteit om configuraties te archiveren en de configuratie terug te draaien naar een vorige versie en een gedetailleerd logboek van de configuratieverandering te maken.

Configuratie vervangen en terugdraaiactie voor configuratie

In Cisco IOS XE-softwarerelease 16.6.4 en hoger kunt u met de functies Configuration Replace and Configuration Rollback de Cisco IOS XE-apparaatconfiguratie op het apparaat archiveren. De configuraties in dit archief, die handmatig of automatisch worden opgeslagen, kunnen worden gebruikt om de huidige actieve configuratie te vervangen door de opdracht Vervang bestandsnaam. Dit staat in contrast met de opdracht copy filename running-config. De opdracht Configure replace filename vervangt de actieve configuratie in plaats van de samenvoeging die wordt uitgevoerd door de opdracht Copy.

U wordt geadviseerd deze functie op alle Cisco IOS XE-apparaten in het netwerk in te schakelen. Als deze optie is ingeschakeld, kan een beheerder ervoor zorgen dat de huidige actieve configuratie wordt toegevoegd aan het archief met de opdracht archiefconfiguratie geprivilegieerd EXEC. De gearchiveerde configuraties kunnen worden weergegeven met de EXEC-opdracht show archive.

Dit voorbeeld illustreert de configuratie van automatische configuratie archivering. Het instrueert ook het Cisco IOS XE-apparaat om gearchiveerde configuraties op te slaan als bestanden met de naam archived-config-N op de disk0: bestandssysteem, om maximaal 14 back-ups te maken, en om één keer per dag te archiveren (1440 minuten) en wanneer een beheerder de opdracht schrijfgeheugen EXEC uitgeeft.

archiveren

pad disk0:archiveren-configureren

maximaal 14

periode 1440

Hoewel de configuratie-archieffunctionaliteit maximaal 14 back-upconfiguraties kan opslaan, wordt u aangeraden om rekening te houden met de ruimtevereisten voordat u de maximale opdracht gebruikt.

Exclusieve configuratiewijzigingstoegang

Toegevoegd aan Cisco IOS XE-softwarerelease 16.6.4, zorgt de functie Exclusive Configuration Change Access ervoor dat slechts één beheerder op een bepaald moment configuratiewijzigingen aanbrengt in een Cisco IOS XE-apparaat. Met deze functie wordt de ongewenste invloed van gelijktijdige wijzigingen die worden aangebracht aan gerelateerde configuratiecomponenten weggenomen. Deze functie is geconfigureerd met de globale configuratie commando configuratie modus exclusieve mode en werkt in een van de twee modi: auto en handleiding. In de automatische modus wordt de configuratie automatisch vergrendeld wanneer een beheerder de EXEC-opdracht configure terminal gebruikt. In handmatige modus, gebruikt de beheerder de

configuratie terminal lock commando om de configuratie te vergrendelen wanneer het de configuratie modus invoert.

Dit voorbeeld toont de configuratie van deze functie voor automatische configuratievergrendeling:

configuratie modus exclusief

Digitaal ondertekende Cisco-software

Toegevoegd in Cisco IOS XE-softwarerelease 16.1 en hoger, vergemakkelijkt de functie Digitaal ondertekende Cisco-software het gebruik van Cisco IOS XE-software die digitaal wordt ondertekend en dus vertrouwd, met het gebruik van beveiligde asymmetrische (public-key) cryptografie.

Een digitaal ondertekende installatiekopie bevat een versleutelde (met een privésleutel) hash van zichzelf. Na controle, het apparaat decrypteert de hash met de bijbehorende openbare sleutel van de sleutels het heeft in zijn belangrijkste winkel en berekent ook zijn eigen hash van het beeld. Als de ontsleutelde hash overeenkomt met de berekende installatiekopie-hash, is er niet geknoeid met de installatiekopie en kan deze worden vertrouwd.

Digitaal ondertekende Cisco-softwaresleutels worden geïdentificeerd door het type en de versie van de sleutel. Een sleutel kan een productie-, rollover- of speciaal sleuteltype zijn. Productie en speciale sleuteltypen hebben een gekoppelde sleutelversie die alfabetisch toeneemt wanneer de sleutel wordt ingetrokken en vervangen. ROMMON en reguliere Cisco IOS XE-afbeeldingen worden beide ondertekend met een speciale of productiesleutel wanneer u de functie Digitaal Ondertekende Cisco-software gebruikt. De ROMMON-installatiekopie kan worden geüpgraded en moet worden ondertekend met dezelfde sleutel als de productie- of speciale installatiekopie die is geladen.

Deze opdracht verifieert de integriteit van de afbeelding isr4300-universalk9.16.06.04.SPA.bin in flitser met de toetsen in het apparaattoetsarchief:

toon software authenticiteit bestand bootflash:isr4300-universalk9.16.06.04.SPA.bin

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

Een nieuw beeld (isr4300-universalk9.16.10.03.SPA.bin) kan dan worden gekopieerd naar de te laden flitser en de handtekening van het beeld wordt geverifieerd met de nieuw toegevoegde speciale sleutel

kopiëren/verifiëren tftp://<server_ip>/isr4300-universalk9.16.10.03.SPA.bin-flitser:

Melding en logboekregistratie van configuratiewijziging

De voorziening Configuration Change Notification and Logging (Kennisgeving van wijzigingen in configuratie en vastlegging) die is toegevoegd in Cisco IOS XE-softwarerelease 16.6.4, maakt het mogelijk de configuratiewijzigingen te registreren die aan een Cisco IOS XE-apparaat zijn aangebracht. Het logbestand wordt onderhouden op het Cisco IOS XE-apparaat en bevat de

gebruikersinformatie van het individu dat de wijziging heeft aangebracht, het ingevoerde configuratiebevel en het tijdstip waarop de wijziging is aangebracht. Deze functionaliteit wordt ingeschakeld met de opdracht logging enable voor loggerconfiguratiemodus voor configuratiewijziging. De optionele opdrachten verbergen sleutels en logboekgrootte ingangen worden gebruikt om de standaardconfiguratie te verbeteren, omdat ze voorkomen dat wachtwoordgegevens worden vastgelegd en de lengte van het wijzigingslogbestand vergroten.

U wordt geadviseerd om deze functionaliteit in te schakelen zodat de geschiedenis van de configuratieverandering van een Cisco IOS XE-apparaat gemakkelijker te begrijpen is. Daarnaast is het raadzaam om de opdracht syslog configuratie op de hoogte stellen te gebruiken om het genereren van syslog berichten mogelijk te maken wanneer een configuratie wordt gewijzigd.

archiveren

logboekconfiguratie

logboekregistratie inschakelen

logboekgrootte 200

hoofdbedekking

syslog informeren

Nadat de optie Melding van wijzigingen in configuratie en vastlegging is ingeschakeld, toont de geprivilegieerde opdracht EXEC archieflogbestand dat alle kunnen worden gebruikt om het configuratielogboek te bekijken.

Besturingsplane

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

Het is belangrijk dat gebeurtenissen in de beheer- en dataplanes geen negatief effect hebben op de besturingsplane. Wanneer een dataplaat gebeurtenis zoals een DoS-aanval het besturingsplane raakt, kan het gehele netwerk instabiel worden. Deze informatie over Cisco IOS XE-softwarefuncties en -configuraties kan de veerkracht van het besturingsplane helpen garanderen.

Versterking algemene besturingsplane

Bescherming van het bedieningsvlak van een netwerkapparaat is van cruciaal belang omdat het bedieningsvlak ervoor zorgt dat de besturings- en dataplanen worden onderhouden en operationeel zijn. Als het besturingsplane tijdens een veiligheidsincident 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 de transmissie van bepaalde types van berichten op een interface onbruikbaar maken om de hoeveelheid cpu lading te minimaliseren die wordt vereist om onnodige pakketten te verwerken.

IP ICMP-omleidingen

Een ICMP-omleidingsbericht kan worden gegenereerd door een router wanneer een pakket op dezelfde interface wordt ontvangen en verzonden. In deze situatie stuurt de router het pakket door en stuurt een ICMP-omleidingsbericht naar de afzender van het oorspronkelijke pakket. Dankzij dit gedrag kan de afzender de router omzeilen en toekomstige pakketten direct doorsturen naar de bestemming (of naar een router dichterbij de bestemming). In een goed functionerend IP-netwerk stuurt een router omleidingen alleen naar hosts op zijn eigen lokale subnetten. Met andere woorden, ICMP-omleidingen kunnen nooit verder gaan dan een Layer 3-grens.

Er zijn twee typen ICMP-omleidingsberichten: omleiden voor een hostadres en omleiden voor een volledig subnet. Een kwaadwillige gebruiker kan de capaciteit van de router exploiteren om ICMP te verzenden omleidt door voortdurend pakketten naar de router te verzenden, die de router dwingt om met ICMP te antwoorden om berichten om te leiden, en resulteert in een negatief effect op de CPU en de prestaties van de router. Om te voorkomen dat de router ICMP-omleidingen verstuurt, gebruikt u de opdracht geen ip-omleidingen voor interfaceconfiguratie.

ICMP onbereikbare apparaten

Het filtreren met een lijst van de interfacetoegang brengt de transmissie van onbereikbare berichten ICMP terug naar de bron van het gefilterde verkeer teweeg. De generatie van deze berichten kan CPU-gebruik op het apparaat verhogen. In Cisco IOS XE-software is de onbereikbare ICMP-generatie standaard beperkt tot één pakket per 500 milliseconden. Het genereren van berichten 'ICMP onbereikbaar' kan worden uitgeschakeld met de interfaceconfiguratie-opdracht no ip unreachables. ICMP-onbereikbare snelheidsbeperking kan worden gewijzigd ten opzichte van de standaardinstelling met de onbereikbare interval-in-ms-grens van het globale configuratiebevel.

Proxy-ARP

Proxy ARP is de techniek waarin één apparaat, gewoonlijk een router, ARP verzoeken beantwoordt die voor een ander apparaat bedoeld zijn. Door zijn identiteit te veinzen, neemt de router verantwoordelijkheid op zich voor het routing van pakketten naar de echte bestemming. Proxy ARP kan machines op een subnetnetwerk op afstand helpen zonder routing of een standaardgateway te configureren. Proxy ARP is gedefinieerd in RFC 1027 .

Er zijn verscheidene nadelen aan volmachtARP gebruik. Het kan leiden tot een toename in de hoeveelheid ARP-verkeer op het netwerksegment en bronuitputting en man-in-the-middle-aanvallen. Proxy ARP is een aanvalsvector voor bronuitputting omdat elke ARP-aanvraag waarvoor een proxy is uitgevoerd, een kleine hoeveelheid geheugen verbruikt. Een aanvaller kan al beschikbaar geheugen uitputten als het een groot aantal ARP verzoeken verzendt.

Man-in-the-middle aanvallen stellen een host op het netwerk in staat om het MAC-adres van de

router te parodiëren, wat resulteert in nietsvermoedende hosts die verkeer naar de aanvaller verzenden. Proxy ARP kan worden uitgeschakeld met de interfaceconfiguratie-opdracht no ip proxy-arp.

Raadpleeg Proxy-ARP in- en uitschakelen voor meer informatie over deze functie.

NTP-controleberichten

NTP Control Message queries zijn functies van NTP die ondersteund hebben in Network Management (NM) functies voordat betere NM's werden gemaakt en gebruikt. Tenzij uw organisatie nog steeds NTP voor NM-functies gebruikt, zijn de best practices van Network Security om ze allemaal samen volledig uit te schakelen. Als u ze gebruikt, kunnen ze een interne netwerk alleen type service die wordt geblokkeerd door firewall of ander extern apparaat. Ze zijn zelfs verwijderd uit alle standaard IOS- en IOS-XE versies, omdat IOS-XR en NX-OS ze niet ondersteunen.

Als u ervoor kiest om deze functie uit te schakelen, is de opdracht

```
Router (config)# geen ntp staat modemcontrole toe
```

Dit commando verschijnt dan in het in werking stellen-configuratie als ntp geen mode control 0 toestaat. Door dit te doen, hebt u NTP Control Berichten op het apparaat uitgeschakeld en het apparaat tegen aanvallen beveiligen.

CPU-impact van besturingsplaneverkeer beperken

Bescherming van de besturingsplane is essentieel. Omdat de toepassingsprestaties en de eindgebruikerservaring zonder de aanwezigheid van gegevens en beheersverkeer kunnen lijden, zorgt de overlevingskans van het controlevliegtuig ervoor dat de andere twee vliegtuigen worden gehandhaafd en operationeel zijn.

Inzicht in besturingsplaneverkeer

Om het besturingsplane van het Cisco IOS XE-apparaat goed te beveiligen, is het essentieel om de typen verkeer te begrijpen die door de CPU worden verwerkt. Het proces switched verkeer bestaat normaal uit twee verschillende typen verkeer. Het eerste type verkeer wordt geleid naar het Cisco IOS XE-apparaat en moet rechtstreeks worden verwerkt door het Cisco IOS XE-apparaat CPU. Dit verkeer bestaat uit de categorie Aangrenzend verkeer ontvangen. Dit verkeer bevat een ingang in de CEF-tabel (Cisco Express Forwarding) waarin de volgende routerhop het apparaat zelf is, dat wordt aangegeven door de term Ontvangen in de CLI-uitvoer van de show ip cef. Deze indicatie is het geval voor elk IP-adres waarvoor directe verwerking door de Cisco IOS XE-apparaatprocessor vereist is, inclusief IP-interfaceadressen, multicast adresruimte en broadcast-adresruimte.

Het tweede type verkeer dat door de CPU wordt verwerkt, is datavliegverkeer - verkeer met een bestemming buiten het Cisco IOS XE-apparaat zelf - waarvoor een speciale verwerking door de CPU is vereist. Hoewel dit geen uitputtende lijst van CPU's is die van invloed is op het verkeer van

dataplaten, worden deze typen verkeer via een proces geschakeld en kunnen deze daarom de werking van het besturingsplane beïnvloeden:

1. Vastlegging toegangscontrolelijst - ACL-logverkeer bestaat uit alle pakketten die zijn gegenereerd vanwege een overeenkomst (licentie of ontkenning) met een ACE waarop het logwoord wordt gebruikt.
2. Unicast Reverse Path Forwarding (Unicast RPF) - Unicast RPF, gebruikt in combinatie met een ACL, kan resulteren in de processwitching van bepaalde pakketten.
3. IP-opties: alle IP-pakketten met opties moeten worden verwerkt door de CPU.
4. Fragmentatie: elk IP-pakket waarvoor fragmentatie is vereist, moet worden doorgegeven aan de CPU voor verwerking.
5. Time-to-live (TTL) Verval - Voor pakketten met een TTL-waarde van minder dan of gelijk aan één is het nodig dat de tijd voor het Internet Control Message Protocol (ICMP Type 11, Code 0) wordt overschreden, wat resulteert in CPU-verwerking.
6. ICMP-onbereikbare bestanden - Pakketten die resulteren in ICMP-onbereikbare berichten als gevolg van routing, MTU of filtering worden verwerkt door de CPU.
7. Verkeer dat een ARP-verzoek vereist - Bestemmingen waarvoor geen ARP-ingang bestaat, moeten worden verwerkt door de CPU.
8. Niet-IP-verkeer: al het niet-IP-verkeer wordt verwerkt door de CPU.

   Deze lijst detailleert verschillende methoden om te bepalen welke typen verkeer door de Cisco IOS XE-apparaat-CPU worden verwerkt:
9. De opdracht show ip cef biedt de volgende hop-informatie voor elk IP-prefix dat in de CEF-tabel is opgenomen. Zoals eerder aangegeven, ontvangen de items die bevatten als de Next Hop worden beschouwd als ontvangstnabijheid en geven aan dat verkeer rechtstreeks naar de CPU moet worden verzonden.
10. De opdracht show interface switching biedt informatie over het aantal pakketten waarvoor een proces-switch wordt uitgevoerd door een apparaat.
11. De opdracht IP-verkeer tonen biedt informatie over het aantal IP-pakketten: met een lokale bestemming (namelijk nabijheidsverkeer ontvangen) met opties die fragmentatie vereisen en naar broadcast-adresruimte worden verzonden die naar multicast-adresruimte wordt verzonden.
12. Ontvangstaangrenzend verkeer kan worden geïdentificeerd met de opdracht show ip cache flow. Alle stromen die bestemd zijn voor het Cisco IOS XE-apparaat hebben een doelinterface (DstIf) van lokaal.
13. Control Plane Policing kan worden gebruikt om het type en de snelheid van het verkeer te bepalen dat het besturingsplane van het Cisco IOS XE-apparaat bereikt. Controle van het vliegtuig toezicht kan worden uitgevoerd door het gebruik van granulaire classificatie ACLs, vastlegging, en het gebruik van de show beleid-kaart controle-vlak opdracht.

Infrastructuur-ACL's

Infrastructuur-ACL's (iACL's) beperken externe communicatie tot de apparaten van het netwerk.

ACL’s voor infrastructuur worden uitgebreid behandeld in de sectie Toegang tot netwerk met infrastructuur-ACL’s van dit document.

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

Ontvangst-ACL's

De rACL beschermt het apparaat tegen schadelijk verkeer voordat het verkeer invloed heeft op de routeprocessor. Ontvang ACL's zijn ontworpen om alleen het apparaat te beschermen waarop het is geconfigureerd en het transitverkeer wordt niet beïnvloed door een rACL. Dientengevolge, verwijst het bestemmingsIP adres om het even welk die in de voorbeeldACL ingangen wordt gebruikt slechts naar de fysieke of virtuele IP adressen van de router. Ontvang ACL's worden ook beschouwd als best practice voor netwerkbeveiliging en kunnen worden beschouwd als een lange-termijntoevoeging aan een goede netwerkbeveiliging.

Dit is de ontvangstpad-ACL die wordt geschreven om SSH-verkeer (TCP-poort 22) van vertrouwde hosts op het 192.168.100.0/24-netwerk toe te staan:

— SH van vertrouwde hosts toestaan aan het apparaat.

toegangslijst 151 vergunning tcp 192.168.100.0 0.0.255 elke eq 22

— SSH uit alle andere bronnen aan de referentieprijs ontzeggen.

access-list 151 deny tcp any eq 22

— al het andere verkeer naar het apparaat toe te laten.

— overeenkomstig het beveiligingsbeleid en de beveiligingsconfiguraties.

toegang-lijst 151 vergunning ip elke

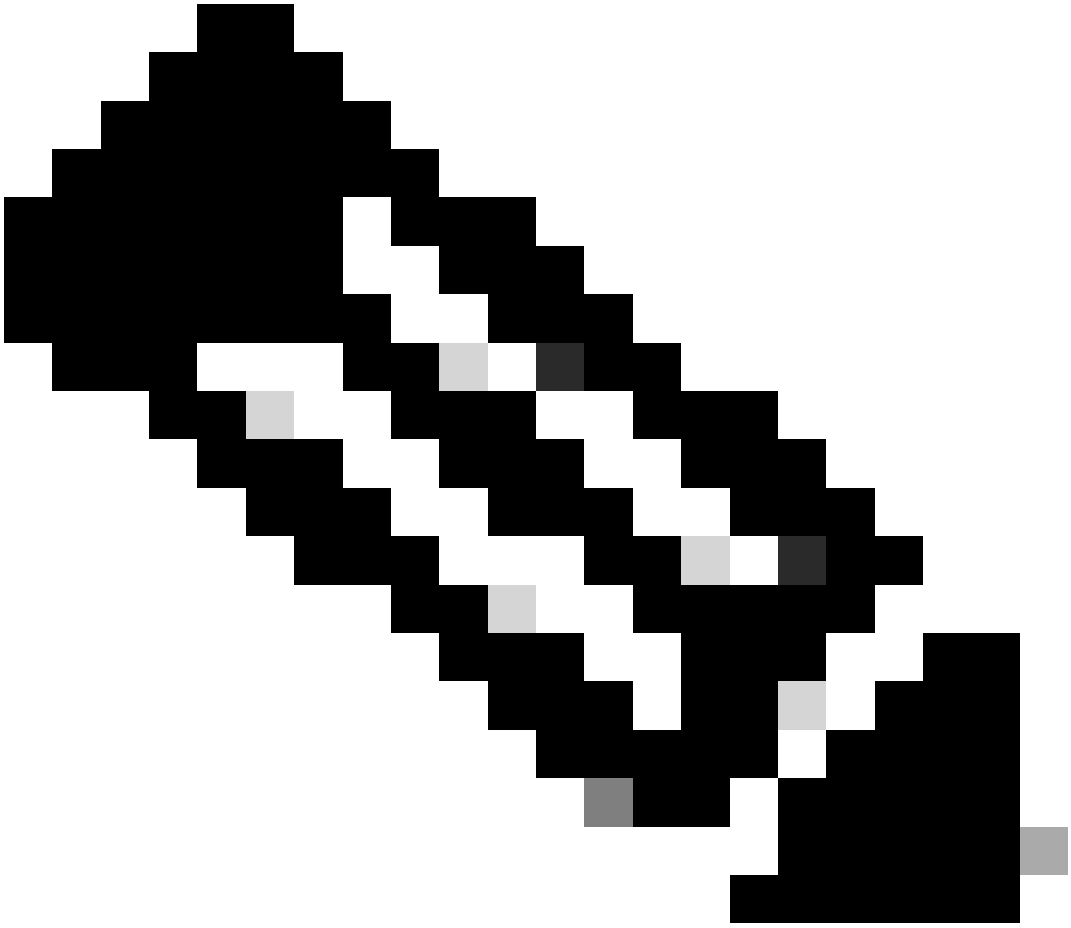
— Pas deze toegangslijst toe op het ontvangstpad.

IP ontvangt toegangslijst 151

Raadpleeg Toegangscontrolelijsten om legitiem verkeer naar een apparaat te identificeren en toe te staan en alle ongewenste pakketten te ontkennen.

CoPP

De CoPP-functie kan ook worden gebruikt om IP-pakketten die bestemd zijn voor het infrastructuurapparaat, te beperken. In dit voorbeeld mag alleen SSH-verkeer van vertrouwde hosts de Cisco IOS XE-apparaat CPU bereiken.



Opmerking: als u verkeer laat vallen van onbekende of onbetrouwbare IP-adressen, kunnen hosts met dynamisch toegewezen IP-adressen geen verbinding maken met het Cisco IOS XE-apparaat.

---

access-list 152 deny TCP <vertrouwde-adressen> <mask> een willekeurige eq 22

toegangslijst 152 vergunning tcp elke willekeurige eq 22

access-list 152

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

beleid-kaart COPP-INPUT-POLICY klasse COPP-BEKEND-UNDESIRABLE drop

Control-plane service-policy-ingangssignaal COPP-INPUT-POLICY

In het vorige CoPP-voorbeeld leiden de ACL-vermeldingen die overeenkomen met de onbevoegde pakketten met de toestemmingsactie tot het verwijderen van deze pakketten door de

functie 'policy-map drop', terwijl pakketten die overeenkomen met de weigeringsactie niet worden beïnvloed door de functie 'policy-map drop'.

CoPP is beschikbaar in Cisco IOS XE-softwarerelease.

Raadpleeg Control Plane Policing voor meer informatie over de configuratie en het gebruik van de CoPP-functie.

Bescherming van besturingsplane

Control Plane Protection (CPPr), geïntroduceerd in Cisco IOS XE-softwarerelease 16.6.4, kan worden gebruikt om vliegtuigverkeer dat bestemd is voor de CPU van het Cisco IOS XE-apparaat, te beperken of te bewaken. Hoewel vergelijkbaar met CoPP, CPPr heeft de mogelijkheid om verkeer te beperken met fijnere granulariteit. CPPr verdeelt het geaggregeerde controlevlak in drie afzonderlijke categorieën van bedieningsvlakken, bekend als subinterfaces. Subinterfaces bestaan voor de verkeerscategorieën Host, Doorgifte en CEF-uitzondering. Bovendien bevat CPPr de volgende beschermingsfuncties voor besturingsplanes:

1. Poortfiltering - Deze functie voorziet in toezicht op en uitval van pakketten die worden verzonden naar gesloten of niet-luisterende TCP- of UDP-poorten.
2. Queue-dorsing-functie - Deze functie beperkt het aantal pakketten voor een gespecificeerd protocol die zijn toegestaan in de wachtrij voor IP-ingangen van het besturingsplatform.

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

Begrenzers voor hardwaresnelheid

Cisco Catalyst 6500 Series Supervisor Engine 32 en Supervisor Engine 720 ondersteunen platform-specifieke, op hardware gebaseerde snelheidsbegrenzers (HWRL's) voor speciale netwerkscenario's. Deze hardwaresnelheidsbegrenzers worden ook wel snelheidsbegrenzers voor speciale scenario's genoemd omdat ze een specifieke vooraf gedefinieerde set IPv4-, IPv6-, unicast- en multicast-DoS-scenario's dekken. HWRL's kunnen het Cisco IOS XE-apparaat beveiligen tegen een verscheidenheid aan aanvallen waarvoor pakketten moeten worden verwerkt door de CPU.

Beveiligde BGP

De Border Gateway Protocol (BGP) is de routeringsfundering van internet. Dat betekent dat elke organisatie met meer dan bescheiden connectiviteitsvereisten vaak BGP gebruikt. BGP wordt vaak geviseerd door aanvallers vanwege zijn alomtegenwoordigheid en de set en vergeet de aard van BGP-configuraties in kleinere organisaties. Er zijn echter veel BGP-specifieke beveiligingsfuncties die kunnen worden gebruikt om de beveiliging van een BGP-configuratie te verbeteren.

Dit geeft een overzicht van de belangrijkste BGP-beveiligingsfuncties. Indien van toepassing worden aanbevelingen voor de configuratie gedaan.

Op TTL gebaseerde beveiligingsbeschermingen

Elk IP-pakket bevat een veld van 1-byte dat bekendstaat als de Time to Live (TTL). Elk apparaat waar een IP-pakket doorheen beweegt, vermindert deze waarde met één. De startwaarde varieert per besturingssysteem en varieert doorgaans van 64 tot 255. Een pakket wordt verwijderd wanneer de TTL-waarde nul bereikt.

Gekend als zowel het Generalized TTL-gebaseerde Security Mechanism (GTSM) als BGP TTL Security Hack (BTSH), benut een op TTL gebaseerde security bescherming de TTL-waarde van IP-pakketten om ervoor te zorgen dat de BGP-pakketten die worden ontvangen van een direct aangesloten peer afkomstig zijn. Deze optie vereist vaak coördinatie van peering routers; echter, eenmaal ingeschakeld, kan het veel TCP-gebaseerde aanvallen tegen BGP volledig verslaan.

GTSM voor BGP wordt ingeschakeld met de optie ttl-security voor de configuratie-opdracht neighbor van de BGP-router. Dit voorbeeld toont de configuratie van deze functie:

router bgp <asn>

buurtnaam <ip-adres> extern-als <afstandsbediening>

TW-hops voor buur <ip-adres> <hop-count>

Aangezien BGP-pakketten worden ontvangen, wordt de TTL-waarde gecontroleerd. Deze moet groter of gelijk zijn aan 255 min de opgegeven hoptelling.

BGP-peerverificatie met MD5

Peer-verificatie met MD5 maakt een MD5-digest van elk pakket verzonden als onderdeel van een BGP-sessie. Met name delen van de IP en TCP headers, TCP payload en een geheime key worden gebruikt om de vertering te genereren.

De gemaakte digest wordt vervolgens opgeslagen in TCP-optie Kind 19, die specifiek voor dit doel is gemaakt door RFC 2385 . De ontvangende BGP-luidspreker gebruikt hetzelfde algoritme en dezelfde geheime sleutel om de berichtsamenvatting te regenereren. Als de ontvangen en berekende digests niet identiek zijn, wordt het pakket verwijderd

Peer-verificatie met MD5 wordt geconfigureerd met de optie password op de configuratie-opdracht neighbor van de BGP-router. Het gebruik van deze opdracht wordt als volgt geïllustreerd:

router bgp <asn>-buur <ip-adres> op afstand als <afstandsbediening>

buur <ip-adres> wachtwoord <geheim>

Raadpleeg Verificatie van aangrenzende router voor meer informatie over BGP-peerverificatie met MD5.

Maximale prefixes configureren

BGP-prefixes worden door een router opgeslagen in het geheugen. Hoe meer prefixes een router

moet bevatten, hoe meer geheugen BGP moet verbruiken. In sommige configuraties, kan een ondergroep van alle prefixes van Internet, zoals in configuraties worden opgeslagen die hefboomwerking slechts een standaardroute of routes voor de gebruikersnetwerken van een leverancier.

Om geheugenuitputting te voorkomen, is het belangrijk om het maximale aantal prefixes te configureren dat per peer wordt geaccepteerd. Aanbevolen wordt om voor elke BGP-peer een limiet te configureren.

Wanneer u deze functie configureert met de opdracht voor routerconfiguratie van de buurmaximum-prefix BGP, is één argument vereist: het maximale aantal prefixes dat wordt geaccepteerd voordat een peer wordt uitgeschakeld. U kunt ook een cijfer van 1 tot 100 invoeren. Dit getal vertegenwoordigt het percentage van de maximale waarde voor prefixes waarop een logbericht wordt verzonden.

router bgp <asn>-buur <ip-adres> op afstand als <afstandsbediening>

<ip-adres> maximum-prefix <shutdown-drempel> <log-percent>

Raadpleeg De functie BGP maximale prefix configureren voor meer informatie over maximale prefixes per peer.

BGP-prefixes filteren met prefix-lijsten

Met prefixlijsten kan een netwerkbeheerder specifieke prefixes toestaan of weigeren die via BGP worden verzonden of ontvangen. Er kunnen waar mogelijk prefixlijsten worden gebruikt om er zeker van te zijn dat netwerkverkeer via de bedoelde paden wordt verzonden. De prefixlijsten kunnen op elke eBGP peer in zowel de inkomende als uitgaande richting worden toegepast.

De gevormde prefixlijsten beperken de prefixes die worden verzonden of ontvangen naar die specifiek toegelaten door het routeringsbeleid van een netwerk. Als dit niet haalbaar is vanwege het grote aantal ontvangen prefixes, kan een prefixlijst worden geconfigureerd om bekende slechte prefixes specifiek te blokkeren. Deze bekende slechte prefixes omvatten niet-toegewezen IP-adresruimte en netwerken die zijn gereserveerd voor interne of testdoeleinden door RFC 330. Uitgaande prefixlijsten kunnen worden geconfigureerd om alleen de prefixes toe te staan die een organisatie wil adverteren.

Dit configuratievoorbeeld gebruikt prefix-lijsten om de geleerde en geadverteerde routes te beperken. Alleen een standaardroute is inkomend toegestaan door prefix-lijst BGP-PL-INBOUND, en de prefix 192.168.2.0/24 is de enige route die mag worden geadverteerd door BGP-PL-OUTBOUND.

ip prefix-lijst BGP-PL-INBOUND sequentiekaart 0.0.0.0/0

IP-prefixlijst BGP-PL-OUTBOUND volgnummer 5, vergunning 192.168.2.0/24

router bgp <asn>

buur <ip-adres> prefix-lijst BGP-PL-INBOUND in

buur <ip-adres> prefix-lijst BGP-PL-OUTBOUND

Raadpleeg Prefix-gebaseerde uitgaande routefiltering voor volledige dekking van BGP-prefixfiltering.

BGP-prefixes filteren met autonome toegangslijsten voor systeempad

BGP-toegangslijsten voor autonoom systeem (AS)-pad maken het de gebruiker mogelijk om ontvangen en geadverteerde prefixes te filteren op basis van het AS-path attribuut van een prefix. Dit kan worden gebruikt in combinatie met prefixlijsten om een robuuste reeks filters te definiëren.

Dit configuratievoorbeeld gebruikt AS-toegangslijsten om inkomende prefixes te beperken tot prefixes die door de externe AS en uitgaande prefixes zijn gegenereerd tot prefixes die door het lokale autonome systeem zijn gegenereerd. Prefixes die afkomstig zijn van alle andere autonome systemen worden gefilterd en niet geïnstalleerd in de routeringstabel.

IP as-path access-list 1-vergunning

IP as-path access-list 2-vergunning

router bgp <asn>

naaister <ip-adres> op afstand 65501

buurt<ip-adres>, filterlijst 1

buurtcode <ip-adres>, filterlijst 2

Beveiligde Interior Gateway Protocols

De capaciteit van een netwerk om verkeer behoorlijk door:sturen en van topologieveranderingen of fouten terug te krijgen is afhankelijk van een nauwkeurige mening van de topologie. U kunt vaak een Interior Gateway Protocol (IGP) uitvoeren om deze weergave te bieden. IGP's zijn standaard dynamisch en ontdekken aanvullende routers die communiceren met de specifieke IGP die in gebruik is. IGP's ontdekken ook routes die kunnen worden gebruikt tijdens een netwerkverbindingsfout.

Deze subsecties bieden een overzicht va de belangrijkste IGP-beveiligingsfuncties.

Aanbevelingen voor en voorbeelden van Routing Information Protocol Version 2 (RIPv2), Enhanced Interior Gateway Routing Protocol (EIGRP) en Open Shortest Path First (OSPF) worden indien nodig geboden.

Authenticatie en verificatie van routingprotocol met Message Digest 5

Als de uitwisseling van routeringsinformatie niet wordt beveiligd, kan een aanvaller ongeldige

routeringsinformatie in het netwerk plaatsen. Door wachtwoordverificatie te gebruiken met routerprotocollen tussen routers, kunt u de beveiliging van het netwerk verbeteren. Deze verificatie wordt verzonden als leesbare tekst en daarom kan het heel eenvoudig zijn voor een aanvaller om deze beveiligingscontrole te ondermijnen.

Wanneer u MD5-hashmogelijkheden aan het verificatieproces toevoegt, bevatten routingupdates geen duidelijke wachtwoorden meer en is de volledige inhoud van de routingupdate beter bestand tegen manipulatie. MD5-authenticatie is echter nog steeds vatbaar voor brute kracht en woordenboekaanvallen indien er zwakke wachtwoorden worden gekozen. Aangeraden wordt om wachtwoorden met voldoende willekeur te gebruiken. MD5-verificatie is een stuk veiliger in vergelijking met wachtwoordverificatie en daarom zijn deze voorbeelden specifiek voor MD5-verificatie. IPSec kan ook worden gebruikt om routeringsprotocollen te valideren en te beveiligen, maar deze voorbeelden geven geen details over het gebruik ervan.

EIGRP en RIPv2 gebruiken sleutelketens als deel van de configuratie. Raadpleeg sleutel voor meer informatie over de configuratie en het gebruik van sleutelketens.

Dit is een voorbeeldconfiguratie voor EIGRP-routerverificatie die MD5 gebruikt:

sleutelketen <key-name>

toets <key-identifier>

key-string <wachtwoord>

interface <interface> IP-verificatie modus eigrp <as-number> md5

IP-verificatie-sleutelhanger voor eigrp <as-number> <key-name>

Dit is een voorbeeld van configuratie van MD5-routerverificatie voor RIPv2. RIPv1 biedt geen ondersteuning voor verificatie.

sleutelketen <key-name>

toets <key-identifier>

key-string <wachtwoord>

interface <interface> IP-rip-verificatiemodus md5

IP-rip verificatie-sleutelhanger <naam van sleutel>

Dit is een voorbeeldconfiguratie voor OSPF-routerverificatie die MD5 gebruikt. OSPF gebruikt geen sleutelketens.

interface <interface> IP ospf bericht-samenvatting-sleutel <key-id> md5 <wachtwoord>

router ospf <proces-id>

netwerk 10.0.0.0 0.255.255.255 gebied 0 gebied 0 authenticatie bericht-samenvatting

Raadpleeg OSPF configureren voor meer informatie.

Passive-interface-opdrachten

De lekken van de informatie, of de introductie van valse informatie in een IGP, kunnen door gebruik van het passief-interfacebevel worden verlicht dat in controle van de reclame van het verpletteren van informatie bijstaat. U wordt geadviseerd om geen informatie aan netwerken te adverteren die buiten uw administratieve controle zijn.

Dit voorbeeld laat het gebruik van deze functie zien:

router eigrp <as-number> standaard passieve interface

geen passieve interface <interface>

Routes filteren

Om de mogelijkheid te verminderen dat u valse routerinformatie in het netwerk introduceert, moet u Routerfiltering gebruiken. In tegenstelling tot de opdracht voor routerconfiguratie met passieve interfaces, vindt routing op interfaces plaats zodra routefiltering is ingeschakeld, maar de informatie die wordt geadverteerd of verwerkt, is beperkt.

Voor EIGRP en RIP beperkt het gebruik van de opdracht verdeel-lijst met het uit sleutelwoord welke informatie wordt geadverteerd, terwijl het gebruik van de in sleutelwoord beperkt welke updates worden verwerkt. De distribute-list opdracht is beschikbaar voor OSPF, maar het voorkomt niet dat een router gefilterde routes verspreidt. In plaats daarvan kan de opdracht area filter-list worden gebruikt.

Dit EIGRP-voorbeeld filtert uitgaande advertenties met de opdracht distribute-list en een prefix-lijst:

IP-prefixlijst <naam van lijst>

volgende 10-vergunning <prefix>

router eigrp <as-number>

passieve interface-standaard

geen passieve interface <interface>

prefix voor distributielijst <lijst-naam> out <interface>

Dit EIGRP-voorbeeld filtert inkomende updates met een prefix-lijst:

IP-prefixlijst <list-name> volgende 10 vergunningen <prefix>

router eigrp <as-number>

passieve interface-standaard

geen passieve interface <interface>

prefix voor distributielijst <naam van lijst> in <interface>

Verwijs naar het filteren van de Route EIGRP voor meer informatie over hoe te om de reclame en de verwerking van het verpletteren van updates te controleren.

Dit OSPF-voorbeeld gebruikt een prefix-lijst met de OSPF-specifieke opdracht area filter-list:

IP-prefixlijst <list-name> volgende 10 vergunningen <prefix>

router ospf <proces-id>

gebied <gebied-id>, prefix <naam-lijst> in

Gebruik van procesbronnen routeren

Routing Protocol prefixes worden opgeslagen door een router in het geheugen, en het resourceverbruik neemt toe met extra prefixes die een router moet houden. Om middeluitputting te verhinderen, is het belangrijk om het routeringsprotocol te vormen om middelconsumptie te beperken. Dit kan worden uitgevoerd met OSPF als u de functie 'Bescherming van databaseoverbelasting linkstatus' gebruikt.

Dit voorbeeld toont de configuratie van de OSPF-functie 'Bescherming van databaseoverbelasting linkstatus':

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

Raadpleeg Het aantal zelfgenererende LSA's beperken voor een OSPF-proces voor meer informatie over OSPF Bescherming van databaseoverbelasting linkstatus.

First Hop Redundancy Protocols beveiligen

First Hop Redundancy Protocols (FHRP's) bieden veerkracht en redundantie voor apparaten die functioneren als standaardgateways. Deze situatie en deze protocollen zijn standaard in omgevingen waarin een set Layer 3-apparaten standaardgateway-functionaliteit biedt voor een netwerksegment of set VLAN's die servers of werkstations bevatten.

Het Gateway Load-Balancing Protocol (GLBP), Hot Standby Router Protocol (HSRP) en Virtual Router Redundancy Protocol (VRRP) zijn allemaal FHRP's. Standaard communiceren deze protocollen met niet-geverifieerde communicaties. Dit soort communicatie kan een aanvaller toestaan om te poseren als een FHRP-sprekend apparaat om de standaardgatewayrol op het netwerk over te nemen. Deze overname zou een aanvaller in staat stellen een man-in-the-middle aanval uit te voeren en al het gebruikersverkeer dat het netwerk verlaat, te onderscheppen.

Om dit type aanval te voorkomen, bevatten alle FHRP's die worden ondersteund door Cisco IOS XE-software een verificatiemogelijkheid met MD5 of tekststrings. Vanwege de dreiging van niet-geverifieerde FHRP's wordt aanbevolen dat exemplaren van deze protocollen MD5-verificatie

gebruiken. Dit configuratievoorbeeld toont het gebruik van GLBP-, HSRP- en VRRP MD5-verificatie.

interface Fast Ethernet 1

beschrijving *** GLBP-***

glbp 1 authenticatie md5 key-string <glbp-geheim>

Gbps 1 ip 10.1.1.1

interface Fast Ethernet 2

beschrijving *** HSRP-***

stand-by 1 verificatie md5 key-string <hsrp-secret>

stand-by 1 ip 10.2.2.1

interface Fast Ethernet 3

beschrijving *** VRRP-***

VRP 1 authenticatie md5 key-string <vrp-geheim>

vrp 1 ip 10.3.3.1

Dataplane

Hoewel het gegevensvlak verantwoordelijk is voor het verplaatsen van gegevens van bron naar bestemming, is binnen de context van veiligheid het gegevensvlak het minst belangrijke van de drie vlakken. Daarom is het belangrijk om de beheer- en besturingsplanen te beschermen in plaats van het dataplane wanneer u een netwerkapparaat beveiligen.

Binnen de dataplane zelf zijn er echter veel functies en configuratie-opties die kunnen helpen bij het beveiligen van verkeer. In deze secties worden deze functies en opties gedetailleerd, zodat u uw netwerk eenvoudiger kunt beveiligen.

Versterking algemene dataplane

De overgrote meerderheid van de verkeersstromen van het dataplatform over het netwerk zoals bepaald door de routerconfiguratie van het netwerk. IP-netwerkfunctionaliteit is echter aanwezig om het pad van pakketten door het netwerk te wijzigen. Functies zoals IP-opties, met name de optie voor bronrouting, vormen een beveiligingsuitdaging in de huidige netwerken.

Het gebruik van transitACL's is ook relevant voor de verharding van het gegevensvlak.

Raadpleeg het gedeelte Overgangsverkeer filteren met overgangs-ACL's van dit document voor meer informatie.

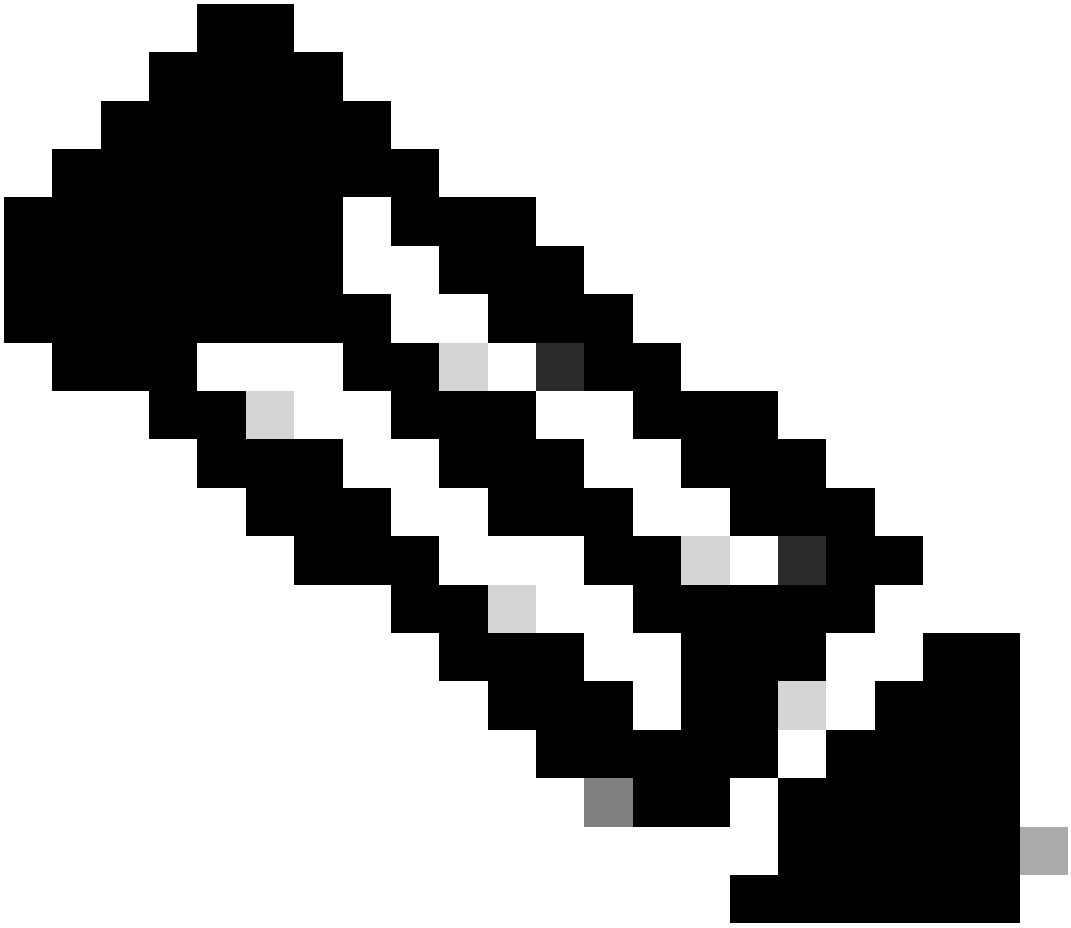
IP-opties selectief verlies

IP-opties kennen twee beveiligingskwesties. Verkeer dat IP-opties bevat, moet via proces worden geschakeld door Cisco IOS XE-apparaten, wat kan leiden tot een hogere CPU-lading. IP-opties bevatten ook de functionaliteit om het pad te wijzigen dat het verkeer door het netwerk neemt, waardoor het mogelijk beveiligingscontroles kan omkeren.

Vanwege deze kwesties is de globale configuratie-opdracht ip options {drop | Negeren} is toegevoegd aan Cisco IOS XE-softwarereleases 16.6.4 en hoger. In de eerste vorm van deze opdracht, ip-opties drop, worden alle IP-pakketten die IP-opties bevatten die worden ontvangen door het Cisco IOS XE-apparaat gedropt. Hiermee wordt de verhoogde CPU-belasting en de mogelijke ondermijning van beveiligingscontroles voorkomen die door IP-opties mogelijk kunnen worden.

De tweede vorm van deze opdracht, ip-opties negeren, configureert het Cisco IOS XE-apparaat om IP-opties die in ontvangen pakketten zitten, te negeren. Terwijl dit de bedreigingen met betrekking tot IP opties voor het lokale apparaat verlicht, is het mogelijk dat de stroomafwaartse apparaten door de aanwezigheid van IP opties zouden kunnen worden beïnvloed. Het is om deze reden dat de drop vorm van deze opdracht wordt ten zeerste aanbevolen. Dit wordt aangetoond in het configuratievoorbeeld:

daling ip-opties



Opmerking: sommige protocollen, bijvoorbeeld de RSVP, maken rechtmatig gebruik van IP-opties. De functionaliteit van deze protocollen wordt beïnvloed door deze opdracht.

Als IP Options Selective Drop eenmaal is ingeschakeld, kan de opdracht IP traffic EXEC worden gebruikt om het aantal pakketten te bepalen dat vanwege de aanwezigheid van IP-opties wordt verbroken. Deze informatie is aanwezig in de teller voor gedwongen verwijderingen.

Raadpleeg ACL IP-opties selectief verlies voor meer informatie over deze functie.

IP-bronroutering uitschakelen

IP-bronrouting maakt gebruik van de opties Loose Source Route en Record Route in tandem of de strikte bronroute samen met de optie Record Route om de bron van het IP-datagram in staat te stellen het netwerkpad te specificeren dat een pakket neemt. Deze functionaliteit kan worden gebruikt in pogingen om verkeer rond veiligheidscontroles in het netwerk te leiden.

Als IP-opties niet volledig zijn uitgeschakeld via de functie IP-opties selectieve drop, is het

belangrijk dat IP-bronrouting is uitgeschakeld. IP-bronrouting, die standaard is ingeschakeld in alle Cisco IOS XE-softwarereleases, is uitgeschakeld via de opdracht geen globale configuratie vanaf IP-bron.

Dit configuratievoorbeeld toont het gebruik van deze opdracht:

geen IP-bronroute

ICMP-omleidingen uitschakelen

ICMP-omleidingen worden gebruikt om een netwerkapparaat te informeren over een beter pad naar een IP-bestemming. Standaard wordt met de Cisco IOS XE-software een redirect verzonden als het een pakket ontvangt dat moet worden doorgestuurd via de interface die het heeft ontvangen.

In sommige situaties, kan het voor een aanvaller mogelijk zijn om het apparaat van Cisco IOS XE te veroorzaken om vele ICMP te verzenden opnieuw richt berichten, die in een verhoogde lading van cpu resulteren. Om deze reden wordt aanbevolen om de transmissie van ICMP-omleidingen uit te schakelen. ICMP-omleidingen zijn uitgeschakeld met de interfaceconfiguratie op IP-omleidingen, zoals in de voorbeeldconfiguratie:

interface Fast Ethernet 0

no ip redirects

IP-omgeleide uitzendingen uitschakelen of beperken

IP-omgeleide uitzendingen zorgen voor dat een IP-uitzendpakket naar een extern IP-subnet kan worden verzonden. Zodra het het externe netwerk bereikt, verstuurt het doorsturen IP-apparaat het pakket als Layer 2-uitzending naar alle stations op het subnetnetwerk. Deze direct uitgezonden functionaliteit is gebruikt als een versterker en reflectie hulp in verschillende aanvallen waaronder de smurf aanval.

Bij de huidige versies van Cisco IOS XE-software is deze functionaliteit standaard uitgeschakeld. U kunt deze echter inschakelen via de opdracht voor de configuratie van de IP-interface met geregelde uitzending. Releases van Cisco IOS XE-software vóór 12.0 hebben deze functionaliteit standaard ingeschakeld.

Als een netwerk absoluut doorgestuurde uitzendfunctionaliteit vereist, kan het gebruik ervan worden gecontroleerd. Dit is mogelijk met het gebruik van een toegangscontrolelijst als optie voor de ip directed-broadcast-opdracht. Dit configuratievoorbeeld beperkt geleide uitzendingen tot die UDP-pakketten die afkomstig zijn van een vertrouwd netwerk, 192.168.1.0/24:

toegangslijst 100 vergunning udp 192.168.1.0 0.0.0.255 elke

interface Fast Ethernet 0

IP direct-broadcast 100

Overgangsverkeer filteren met overgangs-ACL's

Het is mogelijk om te beheren welk verkeer door het netwerk beweegt met het gebruik van overgangs-ACL's (tACL's). Dit in tegenstelling tot infrastructuur ACL's die verkeer willen filteren dat bestemd is voor het netwerk zelf. Het filteren door tACL's is gunstig wanneer het wenselijk is om verkeer te filteren op een bepaalde groep apparaten of verkeer die het netwerk doorvoert.

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

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

Raadpleeg het gedeelte Beschermingen voor anti-spoofing van dit document voor meer informatie.

Raadpleeg Transit Access Control Lists: filteren aan uw zijde voor meer informatie over tACL's.

ICMP-pakketfiltering

Het Internet Control Message Protocol (ICMP) is ontworpen als een beheerprotocol voor IP. Als zodanig kunnen de berichten die worden overgebracht verreikende gevolgen hebben voor de TCP- en IP-protocollen in het algemeen. ICMP wordt gebruikt door de tools voor netwerkprobleemoplossing ping en traceroute en door Path MTU Discovery; externe ICMP-connectiviteit is echter zelden nodig voor een juiste werking van een netwerk.

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

IP-toegangslijst uitgebreid ACL-TRANSIT-IN

— Laat ICMP-pakketten alleen toe vanuit vertrouwde netwerken

vergunning icmp host <vertrouwde-netwerken> elke

— al het andere IP-verkeer naar een netwerkapparaat weigeren

de icmp niet toestaan

IP-fragmenten filteren

Zoals eerder in de sectie Toegang tot netwerk met infrastructuur-ACL's van dit document is uiteengezet, kan het filteren van gefragmenteerde IP-pakketten een uitdaging vormen voor beveiligingsapparaten.

Vanwege de niet-intuïtieve aard van fragmentverwerking worden IP-fragmenten vaak onbedoeld

toegestaan door ACL's. Fragmentatie wordt ook vaak gebruikt in pogingen om detectie te ontwijken door intrusiedetectiesystemen. Het is om deze redenen dat IP fragmenten vaak in aanvallen worden gebruikt en bij om het even welke gevormde tACLs uitdrukkelijk kunnen worden gefiltreerd.

ACL omvat uitgebreide filtering van IP-fragmenten. De functionaliteit die in dit voorbeeld wordt geïllustreerd, moet worden gebruikt in combinatie met de functionaliteit van de voorgaande voorbeelden:

IP-toegangslijst uitgebreid ACL-TRANSIT-IN

— IP-fragmenten weigeren die protocolspecifieke ACE's gebruiken om te helpen bij

— classificatie van aanvalsverkeer

TCP geen fragmenten te weigeren

eventuele fragmenten te weigeren

geen scherven

eventuele fragmenten te weigeren

Raadpleeg Verwerking van fragmenten in toegangslijsten voor meer informatie over ACL-verwerking van gefragmenteerde IP-pakketten.

Ondersteuning van ACL voor filtering van IP-opties

In Cisco IOS XE-softwarerelease 16.6.4 en hoger ondersteunt Cisco IOS XE-software het gebruik van ACL's om IP-pakketten te filteren op basis van de IP-opties die in het pakket aanwezig zijn. De aanwezigheid van IP-opties in een pakket kan wijzen op een poging om beveiligingscontroles in het netwerk te omzeilen of op een andere manier de transitkenmerken van een pakket te wijzigen. Om deze redenen kunnen pakketten met IP-opties aan de rand van het netwerk worden gefilterd.

Dit voorbeeld moet met de inhoud van eerdere voorbeelden worden gebruikt om volledige filtering van IP-pakketten met IP-opties te omvatten:

IP-toegangslijst uitgebreid ACL-TRANSIT-IN

— IP-pakketten met IP-opties weigeren

geen enkele optie voor willekeurige opties

Beschermingen voor anti-spoofing

Veel aanvallen gebruiken spoofing van bron-IP-adressen om effectief te zijn of om de echte bron van een aanval te verhullen en goede traceback te verhinderen. Cisco IOS XE-software biedt Unicast RPF en IP Source Guard (IPSG) om aanvallen te voorkomen die afhankelijk zijn van IP-

bronadresspoofing. Bovendien worden ACL's en null-routering vaak geïmplementeerd als handmatige methode om spoofing te voorkomen.

IP Source Guard werkt aan het minimaliseren van spoofing voor netwerken die onder directe bestuurlijke controle staan door switch poort, MAC-adres en bronadresverificatie uit te voeren. Unicast RPF biedt verificatie van het bronnetwerk en kan gespoofde aanvallen van netwerken die niet onder directe administratieve controle staan, verminderen. Poortbeveiliging kan worden gebruikt om MAC-adressen op de toegangslaag te valideren. Dynamic Address Resolution Protocol (ARP) Inspection (DAI) vermindert aanvalsvectoren die ARP-poisoning op lokale segmenten gebruiken.

Unicast RPF

Unicast PDF stelt een apparaat in staat om te verifiëren dat het bronadres van een doorgestuurd pakket kan worden bereikt via de interface die het pakket heeft ontvangen. U mag niet vertrouwen op Unicast RPF als de enige bescherming tegen spoofing. Verspoofde pakketten konden het netwerk via een Unicast RPF-interface invoeren als er een geschikte retourroute naar het IP-adres van de bron bestaat. Unicast RPF vertrouwt erop dat u Cisco Express Forwarding inschakelt op elk apparaat en wordt op interfacebasis geconfigureerd.

Unicast RPF kan in twee modi worden geconfigureerd: vrij of strikt. Wanneer er sprake is van asymmetrische routering, heeft de vrije modus de voorkeur omdat van de strikte modus bekend is dat in deze situaties pakketten worden verwijderd. Tijdens de configuratie van de interfaceconfiguratie-opdracht ip verify configureert het trefwoord any de vrije modus terwijl het trefwoord rx de strikte modus configureert.

Dit voorbeeld toont de configuratie van deze functie:

ip cef

interface <interface>

IP-verificatie van unicastbron bereikbaar-via <mode>

Raadpleeg Inzicht in Unicast Reverse Path Forwarding voor meer informatie over de configuratie en het gebruik van Unicast RPF.

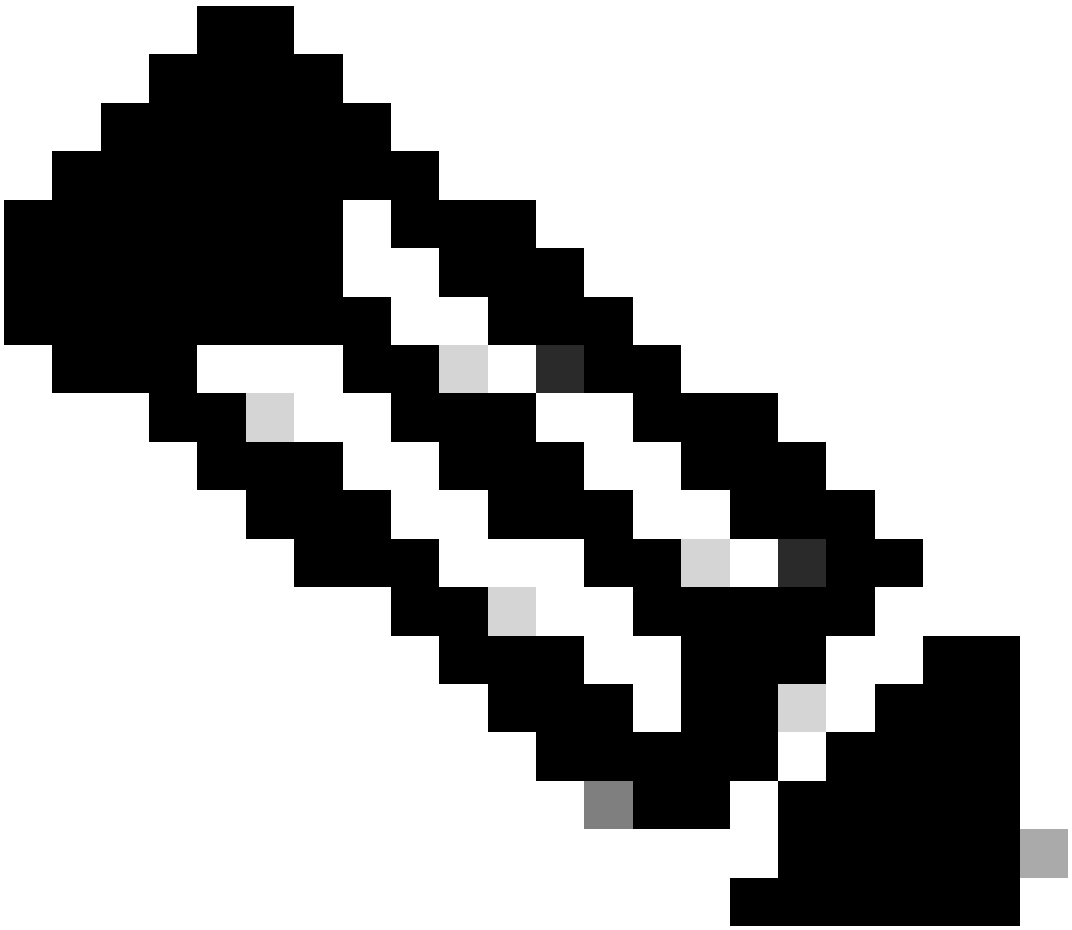
IP-bronbewaker

IP-bronbewaker is een effectieve methode voor spoofing-preventie die kan worden gebruikt als u het beheer over Layer 2-interfaces hebt. IP Source Guard gebruikt informatie van DHCP-controle om dynamisch een poorttoegangscontrolelijst (PACL) op Layer 2-interface te configureren en ontkent daarbij elk verkeer vanaf IP-adressen die niet in de bindende IP-brontabel zijn gekoppeld.

IP Source Guard kan worden toegepast op Layer 2-interfaces die behoren tot DHCP-snooping-enabled VLAN’s. Deze opdrachten maken DHCP-snooping mogelijk:

IP DHCP-snuffelen

IP DHCP-snooping VLAN <VLAN-bereik>



Opmerking: om IP Source Guard te ondersteunen, heeft het chassis/de router een Layer-2-switchingmodule nodig.

Poortbeveiliging kan worden ingeschakeld met de opdracht van de configuratie van de IP-verify-bronpoortbeveiliging. Hiervoor is de globale configuratie-opdracht ip dhcp snooping information option vereist; bovendien moet de DHCP-server DHCP-optie 82 ondersteunen.

Raadpleeg IP Source Guard voor meer informatie over deze functie.

Poortbeveiliging

Poortbeveiliging wordt gebruikt om MAC-adresspoofing op de toegangsinterface te beperken. Poortbeveiliging kan dynamisch geleerde (persistente) MAC-adressen gebruiken om de initiële configuratie eenvoudiger te maken. Zodra poortbeveiliging een MAC-overtreding heeft vastgesteld, kan deze functie een van de vier overtredingsmodi gebruiken. Deze modi zijn VLAN

beveiligen, beperken, afsluiten en afsluiten. Bij gevallen wanneer een poort alleen toegang biedt voor een enkel werkstation met het gebruik van standaardprotocollen, kan een maximaal aantal van één voldoende zijn. Protocollen die gebruik maken van virtuele MAC-adressen zoals HSRP werken niet wanneer het maximum aantal is ingesteld op één.

interface <interface>-switchpoort

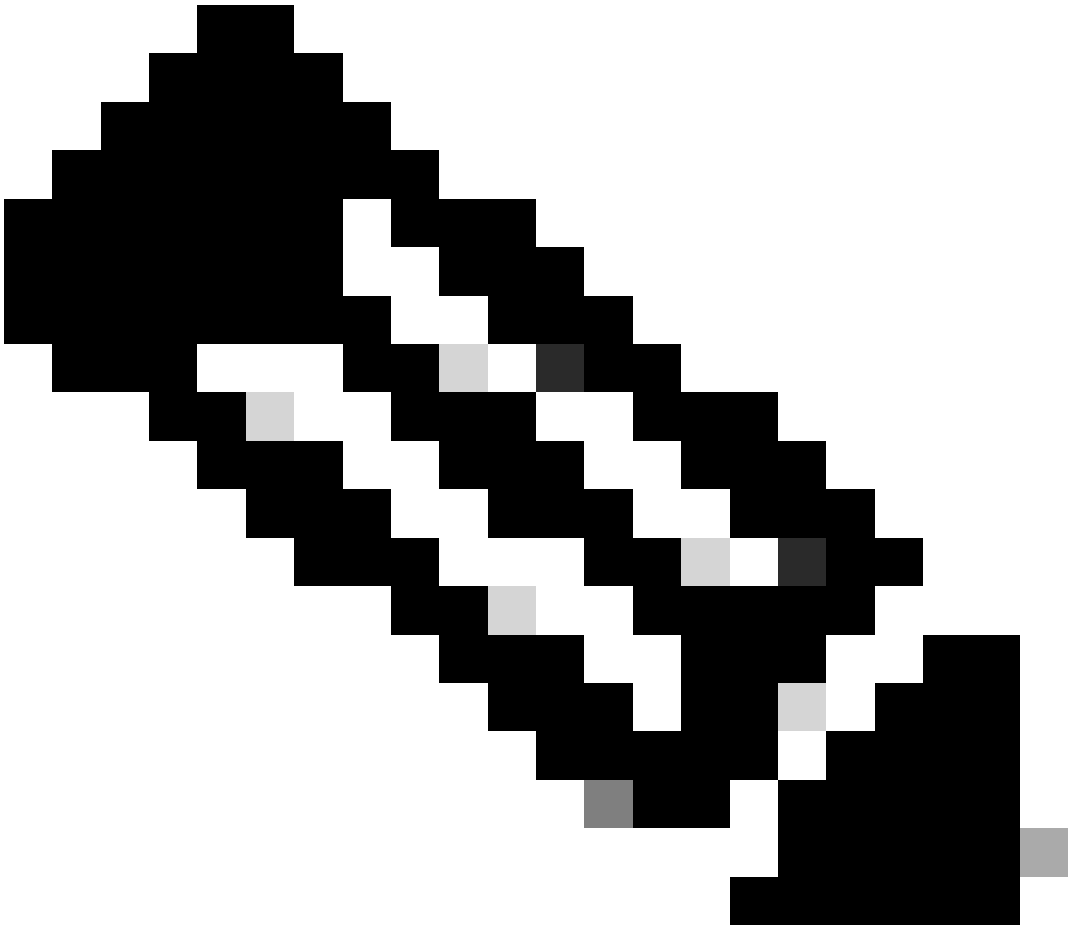
toegang tot switchport-modus

switchport-poortbeveiliging

switchport poort-security mac-adres sticky

switchpoort poort-beveiligingsmaximum <nummer>

switchport-poortbeveiligingsschending <violation-mode>



Opmerking: ter ondersteuning van poortbeveiliging heeft het chassis/de router een Layer-2-switchingmodule nodig.

Raadpleeg Poortbeveiliging configureren voor meer informatie over de poortbeveiligingsconfiguratie.

Anti-Spoofing ACL's

Handmatig geconfigureerde ACL's kunnen statische anti-spoofing-bescherming bieden tegen aanvallen die bekende ongebruikte en niet-vertrouwde adresruimte gebruiken. Deze anti-spoofing ACL's worden vaak toegepast op inkomend verkeer bij netwerkgrenzen als een component van een grotere ACL. Anti-spoofing ACL's vereisen regelmatige bewaking omdat ze vaak kunnen veranderen. Spoofing kan worden geminimaliseerd in verkeer dat zijn oorsprong heeft in het lokale netwerk als u uitgaande ACL's toepast die het verkeer naar geldige lokale adressen beperken.

Dit voorbeeld toont aan hoe ACL's kunnen worden gebruikt om IP-spoofing te beperken. Deze ACL wordt inkomend toegepast op de gewenste interface. De ACE's waaruit deze ACL bestaat, zijn niet allesomvattend. Als u deze typen ACL's configureert, zoekt u een actuele referentie die beslissend is.

IP-toegangslijst uitgebreid ACL-ANTISPOOF-IN

geen ip 10.0.0 0.255.255.255

geen ip 192.168.0.0 0.0.255.255

interface <interface>

IP-toegangsgroep ACL-ANTISPOOF-IN

Raadpleeg IPv4 ACL's configureren voor meer informatie over het configureren van toegangscontrolelijsten.

CPU-impact van dataplaneverkeer beperken

Het primaire doel van routers en switches is om pakketten en frames via het apparaat door te sturen naar eindbestemmingen. Deze pakketten, die door de apparaten bewegen die zijn geïmplementeerd in het netwerk, kunnen invloed hebben op de CPU-activiteiten van een apparaat. Het dataplatform, dat bestaat uit verkeer dat het netwerkapparaat doorkruist, kan worden beveiligd om de werking van de beheer- en besturingsplanen te waarborgen. Indien het transitoverkeer ertoe kan leiden dat een switch het verkeer verwerkt, kan dit gevolgen hebben voor het controlevlak van een inrichting, wat kan leiden tot een verstoring van de werking.

Functies en verkeerstypen die invloed hebben op de CPU

Hoewel niet uitputtend, omvat deze lijst types van gegevensvliegtuigverkeer die speciale verwerking van cpu vereisen en door cpu proces geschakeld zijn:

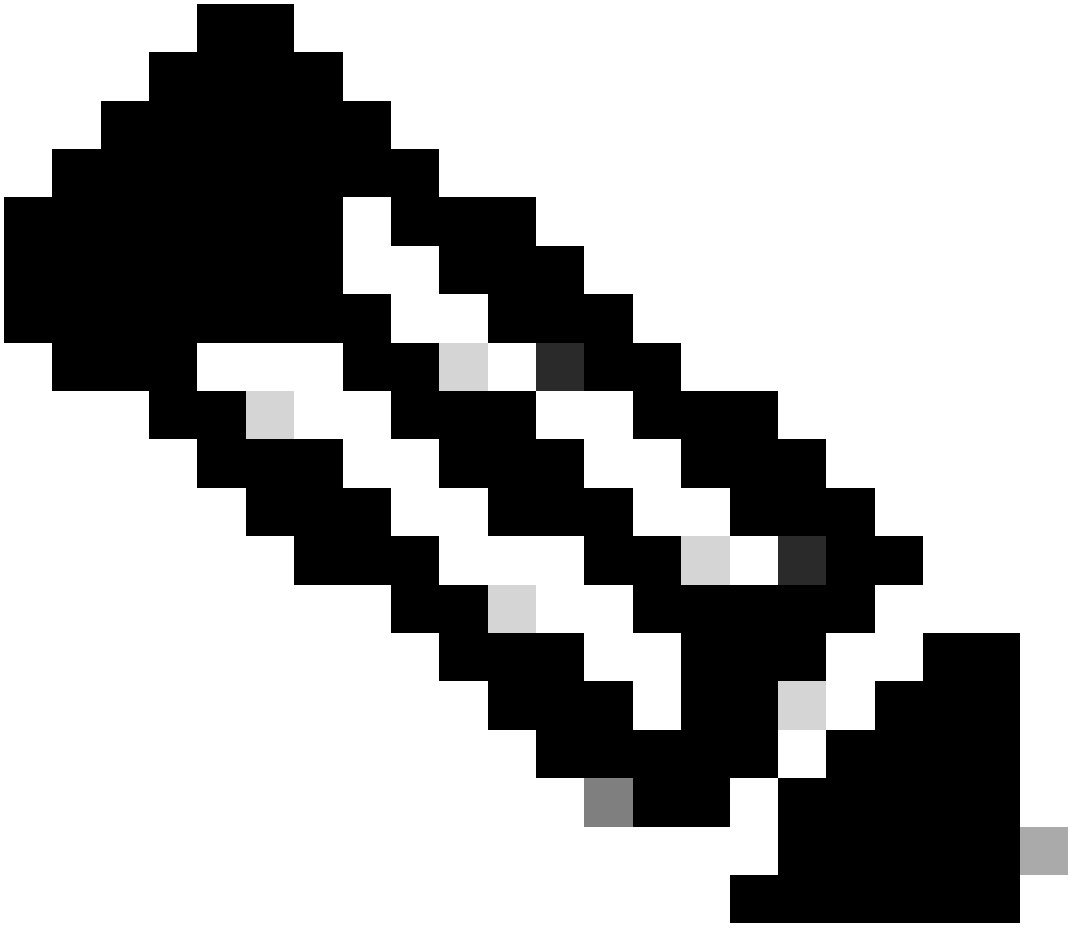
1. ACL-vastlegging - ACL-logverkeer bestaat uit alle pakketten die zijn gegenereerd vanwege een overeenkomst (licentie of ontkenning) met een ACE-bestand waarop het logwoord wordt gebruikt.

2. Unicast RPF - Unicast RPF gebruikt in combinatie met een ACL kan resulteren in de procesomschakeling van bepaalde pakketten.
3. IP-opties: alle IP-pakketten met opties moeten worden verwerkt door de CPU.
4. Fragmentatie: elk IP-pakket waarvoor fragmentatie is vereist, moet worden doorgegeven aan de CPU voor verwerking.
5. Vervaldatum van time-to-live (TTL): pakketten met een TTL-waarde lager dan of gelijk aan 1 vereisen dat berichten 'Tijd verstreken voor Internet Control Message Protocol' (ICMP-type 11, Code 0) worden verzonden. Dit leidt tot CPU-verwerking.
6. ICMP Onbereikbaar - Pakketten die resulteren in ICMP onbereikbare berichten als gevolg van routing, MTU of filtering worden verwerkt door de CPU.
7. Verkeer dat een ARP-verzoek vereist - Bestemmingen waarvoor geen ARP-vermelding bestaat, moeten worden verwerkt door de CPU.
8. Niet-IP-verkeer: al het niet-IP-verkeer wordt verwerkt door de CPU.

   Raadpleeg het gedeelte Versterking algemene dataplane van dit document voor meer informatie over versterking van dataplane.

Filteren op TTL-waarde

U kunt de ACL-ondersteuning voor filtering op TTL-waarde, geïntroduceerd in Cisco IOS XE-softwarerelease 16.6.4, in een uitgebreide IP-toegangslijst gebruiken om pakketten te filteren op basis van TTL-waarde. Deze functie kan worden gebruikt om een apparaat te beveiligen dat transitoverkeer ontvangt wanneer de TTL-waarde een nul of een is. Filterpakketten op basis van TTL-waarden kunnen ook worden gebruikt om ervoor te zorgen dat de TTL-waarde niet lager is dan de diameter van het netwerk, zodat het controlevlak van stroomafwaartse infrastructuurapparaten wordt beschermd tegen TTL-expiratieaanvallen.



Opmerking: Sommige toepassingen en tools zoals traceroute gebruiken TTL-vervalpakketten voor test- en diagnostische doeleinden. Sommige protocollen, zoals IGMP, gebruiken op een legitieme manier een TTL-waarde van één.

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

— ACL-beleid maken waarmee IP-pakketten met een TTL-waarde worden gefilterd.

— minder dan 6

IP-toegangslijst uitgebreid ACL-TRANSIT-IN

Ip geen enkele tellt LT6

de vergunninghouder elke

— Toegangslijst toepassen op interface in de ingangsrichting.

interface Gigabit Ethernet 0/0

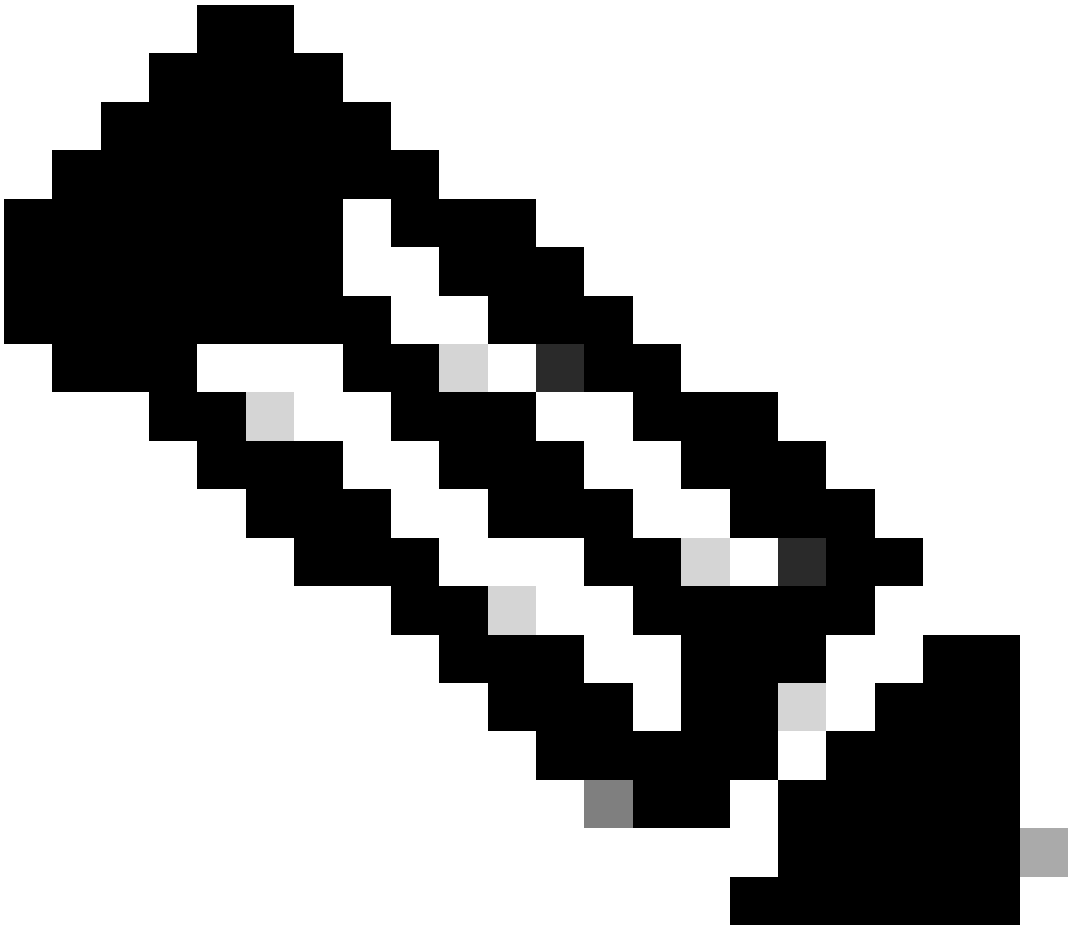
IP-toegangsgroep ACL-TRANSIT-IN

Raadpleeg de TTL-pakketidentificatie en -beperking voor meer informatie over filtreerpakketten op basis van de TTL-waarde.

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

Filteren op de aanwezigheid van IP-opties

In Cisco IOS XE-softwarerelease 16.6.4 en hoger kunt u de ACL-ondersteuning voor de functie Filterende IP-opties in een benoemde, uitgebreide IP-toegangslijst gebruiken om IP-pakketten met aanwezige IP-opties te filteren. Filterende IP-pakketten die zijn gebaseerd op de aanwezigheid van IP-opties kunnen ook worden gebruikt om te voorkomen dat het besturingsplane van infrastructurele apparaten deze pakketten op CPU-niveau moet verwerken.



Opmerking: de functie ACL-ondersteuning voor filtering van IP-opties kan alleen worden gebruikt met benoemde, uitgebreide ACL's.

Het kan ook worden opgemerkt dat RSVP, Multiprotocol Label Switching Traffic Engineering, IGMP versies 2 en 3 en andere protocollen die IP-optiepakketten gebruiken, niet goed kunnen functioneren als pakketten voor deze protocollen worden gedropt. Als deze protocollen in het netwerk worden gebruikt, kan de ACL-ondersteuning voor IP-filtering worden gebruikt. De functie voor selectieve drop van ACL-opties kan dit verkeer echter laten vallen en deze protocollen kunnen niet goed functioneren. Als er geen protocollen in gebruik zijn die IP-opties vereisen, is 'ACL IP-opties selectief verlies' de voorkeursmethode om deze pakketten te verwijderen.

Dit ACL-voorbeeld stelt een beleid op waarmee IP-pakketten worden gefilterd die IP-opties bevatten:

IP-toegangslijst uitgebreid ACL-TRANSIT-IN

geen enkele optie voor willekeurige opties

de vergunninghouder elke

interface Gigabit Ethernet 0/0

IP-toegangsgroep ACL-TRANSIT-IN

Deze voorbeeld-ACL toont een beleid dat IP-pakketten met vijf specifieke IP-opties filtert. Pakketten die deze opties bevatten, worden geweigerd:

1. 0 End of Options List (eool)
2. 7 Record Route (record-route)
3. 68 Time Stamp (timestamp)
4. 131 - Loose Source Route (lsr)
5. 137 - Strict Source Route (ssr)

IP-toegangslijst uitgebreid ACL-TRANSIT-IN

geen optie koel

geen optie record-route

geen optie tijdstempel

geen optie sr

geen optie ssr

de vergunninghouder elke

interface Gigabit Ethernet 0/0

IP-toegangsgroep ACL-TRANSIT-IN

Zie het gedeelte General Data Plane Hardening van dit document voor meer informatie over selectieve drop van ACL-opties.

Een andere functie in Cisco IOS XE-software die kan worden gebruikt om pakketten met IP-opties te filteren is CoPP. In Cisco IOS XE-softwarerelease 16.6.4 en hoger staat CoPP een beheerder toe om de verkeersstroom van pakketten voor besturingsplanten te filteren. Een apparaat dat CoPP en ACL-ondersteuning voor filtering van IP-opties ondersteunt, dat is geïntroduceerd in Cisco IOS XE-softwarerelease 16.6.4, kan een toegangslijstbeleid gebruiken om pakketten te filteren die IP-opties bevatten.

Dit CoPP-beleid verwijdert overgangspakketten die worden ontvangen door een apparaat wanneer er IP-opties aanwezig zijn:

IP-toegangslijst uitgebreide ACL-IP-OPTIONS-ANY

laat ip om het even welke optie om het even welke opties toe

class-map ACL-IP-OPTIONS-CLASS

overeenkomende toegangsgroepnaam ACL-IP-OPTIONS-ANY

beleidsmap COPP-POLICY

class ACL-IP-OPTIONS-CLASS

politie 80000 conform verzenden overschrijdt drop

controlevlak

Service-policy input-COPP-POLICY !

Dit CoPP-beleid verwijdert overgangspakketten die worden ontvangen door een apparaat wanneer deze IP-opties aanwezig zijn:

1. 0 End of Options List (eool)
2. 7 Record Route (record-route)
3. 68 Time Stamp (timestamp)
4. 131 Loose Source Route (lsr)
5. 137 Strict Source Route (ssr)

IP-toegangslijst met uitgebreide ACL-IP-OPTIES

Laat ip om het even welke optie koel toe

vergunning ip om het even welke optie record-route

Laat ip om het even welke optie tijdstempel toe

Laat ip om het even welke optie toe lsr

Laat ip om het even welke optie ssr toe

class-map ACL-IP-OPTIONS-CLASS

overeenkomende toegangsgroepnaam voor ACL-IP-OPTIES

beleidsmap COPP-POLICY

class ACL-IP-OPTIONS-CLASS

politie 80000 conform verzenden overschrijdt drop

controlevlak

Service-policy input-COPP-BELEID

In het vorige CoPP beleid, resulteren de ingangen van de toegangscontrolelijst (ACEs) die pakketten met de vergunningsactie aanpassen in deze pakketten die door de beleid-kaart drop-functie worden verworpen, terwijl de pakketten die de ontkennen actie (niet getoond) aanpassen niet door de beleid-kaart drop-functie worden beïnvloed.

Raadpleeg Control Plane Policing implementeren voor meer informatie over de CoPP-functie.

Bescherming van besturingsplane

In Cisco IOS XE-softwarerelease 16.6.4 en hoger kan CPPr (Control Plane Protection) worden gebruikt om vliegverkeer via de CPU van een Cisco IOS XE-apparaat te beperken of te bewaken. Hoewel vergelijkbaar met CoPP, CPPr heeft de mogelijkheid om verkeer te beperken of te controleren dat fijnere granulariteit gebruikt dan CoPP. CPPr verdeelt de geaggregeerde besturingsplane in drie afzonderlijke planecategorieën, bekend als subinterfaces: de subinterfaces Host, Transit en CEF-Exception bestaan.

Dit CPPr-beleid verwijdert overgangspakketten die zijn ontvangen door een apparaat wanneer de TTL-waarde lager is dan 6, en overgangs- of niet-overgangspakketten die zijn ontvangen door een apparaat wanneer de TTL-waarde nul of één is. Het CPPr-beleid verwijdert ook pakketten met geselecteerde IP-opties ontvangen door het apparaat.

IP-toegangslijst met uitgebreide ACL-IP-TTL-0/1

vergunning ip om het even welk ttl eq 0 1

class-map ACL-IP-TTL-0/1-CLASS

ACL-IP-TTL-0/1-naam van toegangsgroep

IP-toegangslijst met uitgebreide ACL-IP-TTL-LOW

vergunningverlening ip (ip) alle ttl lt 6

class-map ACL-IP-TTL-LOW-CLASS

overeenkomende toegangsgroepnaam ACL-IP-TTL-LOW

IP-toegangslijst met uitgebreide ACL-IP-OPTIES

Laat ip om het even welke optie koel toe

vergunning ip om het even welke optie record-route

Laat ip om het even welke optie tijdstempel toe

Laat ip om het even welke optie toe lsr

Laat ip om het even welke optie ssr toe

class-map ACL-IP-OPTIONS-CLASS

overeenkomende toegangsgroepnaam voor ACL-IP-OPTIES

policy-map CPPR-CEF-EXCEPTION-POLICY

klasse ACL-IP-TTL-0/1-KLASSE

politie 80000 nalevingsdruppel

class ACL-IP-OPTIONS-CLASS

politie 8000 conforme-actie drop

policy-map CPPR-TRANSIT-POLICY

klasse ACL-IP-TTL-LOW-CLASS

politie 8000 conforme-actie drop

transit in het controlevliegtuig

Service-Policy invoer CVR-TRANSIT-BELEID

In het vorige CPPr beleid, de ingangen van de toegangscontrolelijst die pakketten met het

resultaat van de vergunningsactie aanpassen in deze pakketten die door de beleid-kaart drop-functie worden verworpen, terwijl de pakketten die de ontkennen actie (niet getoond) aanpassen niet door de beleid-kaart drop-functie worden beïnvloed.

Raadpleeg Control Plane Policing voor meer informatie over de CPPr-functie.

Verkeersidentificatie en traceback

Soms moet u netwerkverkeer snel identificeren en traceback, vooral tijdens incidentele respons of slechte netwerkprestaties. NetFlow en Classificatie ACL's zijn de twee primaire methoden om dit te bereiken met Cisco IOS XE-software. NetFlow kan inzicht in al het verkeer op het netwerk bieden. Bovendien kan NetFlow worden geïmplementeerd met verzamelaars die langdurige trending en geautomatiseerde analyse kunnen leveren. Classificatie-ACL's zijn een component van ACL's en vereisen pre-planning om specifiek verkeer en handmatige interventie tijdens analyse te identificeren. Deze gedeelten bieden een kort overzicht van elke functie.

NetFlow

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

CEF, of gedistribueerde CEF, is een vereiste om NetFlow in te schakelen. NetFlow kan worden geconfigureerd op routers en switches.

Dit voorbeeld illustreert de basisconfiguratie van deze functie. In vorige releases van Cisco IOS XE-software is de opdracht om NetFlow in te schakelen op een interface de IP-route-cache stroom in plaats van de IP-flow {toegang | egress}.

IP-stroom-exportbestemming <ip-adres> <p-poort>

IP-flow-export versie <versie>

interface <interface>

IP-flow <invoer|uitgang>

Dit is een voorbeeld van NetFlow-uitvoer van de CLI. Het SrcIf-kenmerk kan helpen bij de traceback.

router#show ip cache flow IP-pakketgrootteverdeling (26662860 totale pakketten):

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

512 544 576 1024 1536 2048 2560 3072 3584 4096 4608

0,000 000 0,001 007 039 000 000 0 000 0 0 000 0 000 0 000

IP Flow Switching Cache, 4456704 bytes

55 actief, 65481 inactief, 1014683 toegevoegd

41000680 peilingen, geen storingen in stroomtoewijzing

Active flows time-out in 2 minuten

Inactieve flow-timeout in 60 seconden

IP Sub Flow Cache, 336520 bytes

110 actief, 16274 inactief, 2029366 toegevoegd, 1014683 toegevoegd aan flow

0 alloc failures, 0 force free 1 chunk, 15 chunks toegevoegd laatste clearing van statistieken nooit

Protocol totale stromen pakketten met bytes actieve pakketten (sec) inactivum (sec)

-------- stromen /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 0,0 240 0,0 0,0 60,8

TCP-BGP 114 0,0 1 40 0,0 0,0 62,4

TCP/NTP 120.0 1.42 0.0 0.7 61.4

TCP-andere 556070 0,6 8 318 6,0 8,2 38,3

UDP-DNS 130909 0,1 2 5 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 1405 0,0 0,0 86,8

UDP — overige 86247 0,1 226 29 24,0 31,4 54,3

ICMP 19989 0,0 37 33 0,9 26,0

IP-overig 193 0,0 1 22 0,0 3,0 78,2

Totaal: 1014637 1,2 26 99 32,8 13,8 43,9

SRCAls SRCIP-adres DSTif DSTIP-adres Pr SRCp DstP-poorten

Gi0/1 192.168.128.21 Lokaal 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 Lokaal 192.168.206.20 01 000 0303 11

Gi0/0 10.89.17.146 Gi0/1 192.168.150.60 06 07F1 0016 1

Raadpleeg Flexibel NetFlow voor meer informatie over NetFlow-functies.

Classificatie-ACL's

Classificatie-ACL's bieden inzicht in verkeer dat door een interface beweegt. Classificatie-ACL's wijzigen het beveiligingsbeleid van een netwerk niet en worden normaal gesproken opgebouwd om afzonderlijke protocollen, bronadressen of bestemmingen te classificeren. Een ACE die bijvoorbeeld al het verkeer toestaat, kan worden gescheiden in specifieke protocollen of poorten. Deze meer granulaire classificatie van verkeer in specifieke ACE's kan helpen om een begrip van het netwerkverkeer te geven omdat elke verkeerscategorie zijn eigen hit teller heeft. Een beheerder kan impliciet ook scheiden ontkent aan het eind van een ACL in korrelige ACE's om te helpen de types van ontkend verkeer identificeren.

Een beheerder kan een incidentele reactie versnellen door gebruik van classificatie ACL's met de show access-list en duidelijke IP access-list tellers EXEC commando's.

Dit voorbeeld illustreert de configuratie van een classificatie ACL om SMB verkeer te identificeren voorafgaand aan een gebrek ontkennen:

IP-toegangslijst uitgebreide ACL-SMB-CLASSIFY

Opmerking Bestaande inhoud van ACL

Opmerking Classificatie van SMB-specifiek TCP-verkeer

tcp geen cq 139

TCP niet opgeven 445

geen toegang

Om het verkeer te identificeren dat een classificatie ACL gebruikt, gebruik de show access-list acl-naam

EXEC-opdracht. De ACL-tellers kunnen worden gewist met de duidelijke IP-toegangslijst tellers met de naam EXEC-opdracht.

router#show access-list ACL-SMB-CLASSIFY Uitgebreide IP-toegangslijst ACL-SMB-CLASSIFY

10 ontken tcp een willekeurige eq 139 (10 wedstrijden)

20 ontkennen tcp een willekeurige eq 445 (9 wedstrijden)

30 Geen i.p.v. (184 overeenkomsten)

Raadpleeg Logboekregistratie toegangscontrolelijst begrijpen voor meer informatie over het inschakelen van registratiemogelijkheden binnen ACL's.

Toegangscontrole met PACL's

PACL's kunnen alleen worden toegepast op de inkomende richting op Layer 2 fysieke interfaces van een switch. Net zoals VLAN-kaarten bieden PACL's toegangscontrole op niet-gerouteerd Layer 2-verkeer. De syntaxis voor het maken van PACL's, die prioriteit heeft over VLAN-kaarten en router-ACL's, is hetzelfde als router-ACL's. Als een ACL is toegepast op een Layer 2-interface, wordt hiernaar verwezen met PACL.

Configuratie omvat het maken van een IPv4, IPv6 of MAC-ACL en toepassing hiervan op de Layer 2-interface.

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

IP-toegangslijst uitgebreid met <acl-name>-vergunning <protocol> <bron-adres> <bron-port> <bestemming-adres> <bestemming-port>!

interface <type> <sleuf/poort> switchport mode access switchport access vlan <vlan_number> IP access-group <acl-name> in !

Raadpleeg het gedeelte Port ACL van Configuration Network Security with Port ACL's voor meer informatie over de configuratie van PAL's.

Geïsoleerde VLAN's

De configuratie van een secundair VLAN als geïsoleerd VLAN voorkomt volledig communicatie tussen apparaten in het secundaire VLAN. Er kan slechts één geïsoleerd VLAN per primair VLAN zijn, en slechts kunnen de promiscuous poorten met poorten in een geïsoleerd VLAN communiceren. Geïsoleerde VLAN's kunnen worden gebruikt op niet-vertrouwde netwerken zoals netwerken die ondersteuning bieden voor gasten.

Dit configuratievoorbeeld configureert VLAN 11 als een geïsoleerde VLAN en koppelt deze aan de primaire VLAN, VLAN 20. In dit voorbeeld wordt ook de interface Fast Ethernet 1/1 als een geïsoleerde poort in VLAN 11 geconfigureerd:

VLAN 11 geïsoleerd voor privé-VLAN

VLAN 20 privaat-VLAN primaire privaat-VLAN-associatie 11

interface FastEthernet 1/1 beschrijving *** poort in geïsoleerd VLAN *** switchport mode privaat-VLAN host-switchport privaat-VLAN host-associatie 20.11

Community-VLAN's

Een secundair VLAN dat als gemeenschap VLAN wordt gevormd staat communicatie onder leden van VLAN evenals met om het even welke promiscuous havens in primair VLAN toe. Er is echter geen communicatie mogelijk tussen twee community-VLAN's of van een community-VLAN naar een geïsoleerde VLAN. Community VLAN’s moeten worden gebruikt om servers te groeperen die onderlinge connectiviteit nodig hebben, maar waarbij verbinding met alle andere apparaten in het VLAN niet nodig is. Dit scenario is gemeenschappelijk in een openbaar toegankelijk netwerk of overal dat de servers inhoud aan onbetrouwbare cliënten verstrekken.

Dit voorbeeld configureert een enkele community-VLAN en configureert switch-poort FastEthernet 1/2 als een lid van die VLAN. De community-VLAN, VLAN 12, is een secundaire VLAN voor primaire VLAN 20.

VLAN 12 privaat-VLAN-community

VLAN 20 privaat-VLAN primaire privaat-VLAN-associatie 12

interface FastEthernet 1/2 beschrijving *** poort in Community VLAN *** switchport mode privaat-VLAN host-switchport privaat-VLAN host-associatie 20.12

Conclusie

Dit document geeft u een breed overzicht van de methoden die kunnen worden gebruikt om een Cisco IOS XE-systeemapparaat te beveiligen. Als u de apparaten beveiligen, verhoogt het de algemene veiligheid van de netwerken die u beheert. In dit overzicht worden bescherming van de beheer-, besturing- en dataplanes besproken en worden aanbevelingen verstrekt voor configuratie. Waar mogelijk wordt voldoende detail geboden voor de configuratie van elke gekoppelde functie. In alle gevallen worden echter uitgebreide referenties geboden zodat u beschikt over de benodigde informatie voor verdere evaluatie.

Dankwoord

Sommige functiebeschrijvingen in dit document zijn geschreven door informatie-ontwikkelingsteams van Cisco.

Bijlage: Cisco IOS XE-controlelijst voor apparaatverharding

Deze controlelijst is een verzameling van alle verhardende stappen die in deze handleiding

worden weergegeven.

Beheerders kunnen het gebruiken als een herinnering aan alle verhardende functies die worden gebruikt en overwogen voor een Cisco IOS XE-apparaat, zelfs als een functie niet is geïmplementeerd omdat deze niet van toepassing was. Beheerders worden geadviseerd om elke optie te evalueren op potentiële risico's voordat ze de optie implementeren.

Beheerplane

1. Wachtwoorden
   MD5-hashing inschakelen (geheime optie) voor inschakelen en lokale gebruikerswachtwoorden instellenWachtwoord opnieuw proberen om wachtwoord in te schakelenWachtwoordherstel uitschakelen (rekening houdend met risico)
2. Niet-gebruikte services uitschakelen
3. TCP-keepalives voor beheersessies configureren
4. Meldingen voor geheugen en CPU-drempel instellen
5. Configureren
   Geheugen en CPU drempel meldingen Reserveer geheugen voor console toegang Geheugen lek detector Buffer overflow detectie Uitgebreide crash info verzameling
6. iACL's gebruiken om beheertoegang te beperken
7. Filteren (overweeg risico)
   ICMP-pakkettenIP-fragmentenIP-optiesTTL-waarde in pakketten
8. Bescherming van besturingsplane
   Poortfiltering configurerenWachtrijdrempels configureren
9. Beheertoegang
   Gebruik Management Plane Protection om beheerinterfaces te beperkenStel uitvoertijd inGebruik een versleuteld transportprotocol (zoals SSH) voor CLI access Control transport voor vty en tty lines (access class optie)Waarschuwing dat u banners gebruikt
10. AAA
    Gebruik AAA voor verificatie en reserveGebruik AAA (TACACS+) voor opdrachtautorisatieGebruik AAA voor accountingGebruik redundante AAA-servers
11. SNMP
    SNMPv2-gemeenschappen configureren en ACL’s toepassen SNMPv3 configureren
12. Logboekregistratie
    Gecentraliseerde logboekniveaus instellen voor alle relevante componentenLogboekbroninterface instellenTijdstempelgranulariteit van logboekregistratie instellen
13. Configuratiebeheer
    Replace and rollbackExclusive Configuration Change AccessSoftware veerkracht configuratieConfiguration wijzigingsmeldingen.

Besturingsplane

1. Uitschakelen (overweeg risico)
   ICMP-omleidingenICMP onbereikbaarProxy-ARP

2. NTP-verificatie configureren als NTP wordt gebruikt
3. Configuratie van toezicht op besturingsplane/bescherming (poortfiltering, wachtrijdrempels)
4. Beveiligde routeringsprotocollen
   BGP (TTL, MD5, maximale prefixes, prefixlijsten, systeempad-ACL’s)IGP (MD5, passieve interface, routefiltering, resourceconsumptie)
5. Begrenzers voor hardwaresnelheid configureren
6. First Hop Redundancy Protocols beveiligen (GLBP, HSRP, VRRP)

Dataplane

1. IP-opties selectief verlies configureren
2. Uitschakelen (overweeg risico)
   IP-bronroutingIP directed BroadcastsICMP-omleidingen
3. IP-omgeleide uitzendingen beperken
4. tACL's configureren (overweeg risico)
   Filter ICMPFilter IP fragmentenFilter IP-optiesFilter TTL-waarden
5. Vereiste beschermingen voor anti-spoofing configureren
   ACL’sIP Source Guard Dynamische ARP-inspectieUnicast RPFP-poortbeveiliging
6. Control Plane Protection (control-plane cef-exception)
7. NetFlow en classificatie-ACL's configureren voor verkeersidentificatie
8. Vereiste toegangscontrole-ACL's configureren (VLAN-kaarten, PACL's, MAC)
9. Privé-VLAN's configureren

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.