Cisco IOS XE-Härtungsleitfaden verwenden

Inhalt

Einleitung

In diesem Dokument werden Informationen zum Schutz Ihrer Cisco IOS® XE-Systemgeräte beschrieben, die die Sicherheit Ihrer Netzwerkdokumentation erhöhen.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Dieses Dokument umfasst drei Ebenen, in die die Funktionen eines Netzwerkgeräts eingeteilt werden können. Es enthält eine Übersicht über die einzelnen Funktionen sowie Verweise auf zugehörige Elemente.

Die drei Funktionsebenen eines Netzwerks - Verwaltungsebene, Kontrollebene und Datenebene - bieten jeweils unterschiedliche Funktionen, die geschützt werden müssen.

1. Verwaltungsebene - Die Verwaltungsebene verwaltet den an das Cisco IOS XE-Gerät gesendeten Datenverkehr, der aus Anwendungen und Protokollen wie Secure Shell (SSH) und Simple Network Management Protocol (SNMP) besteht.
2. Steuerfläche - Die Steuerfläche eines Netzgerätes verarbeitet den Verkehr, der entscheidend ist, die Funktionalität der Netzwerk-Infrastruktur beizubehalten. Die Steuerfläche besteht Anwendungen und Protokollen zwischen Netzgeräten, die das Border Gateway Protocol (BGP) umfasst, sowie aus den Innenkommunikationsrechner-Protokollen (IGP) wie das erhöhte Innenkommunikationsrechner-Wegewahl-Protokoll (EIGRP) und offenes Shortest-Path zuerst (OSPF).
3. Daten-Fläche - Die Daten der Datenfläche vorwärts durch ein Netzgerät. Die Datenebene enthält keinen Datenverkehr, der an das lokale Cisco IOS XE-Gerät gesendet wird.

   Die Dichte von Sicherheitsmerkmalen in diesem Dokument stellt häufig genügend Detail bereit, damit Sie das Merkmal konfigurieren. Jedoch in den Fällen wo es nicht tut, wird das Merkmal erklärt, sodass Sie auswerten können, ob zusätzliche Aufmerksamkeit zum Merkmal erfordert wird. Wo möglich und verwenden Sie, dieses Dokument enthält

Empfehlungen, die, wenn sie eingeführt werden, sicher einem Netz helfen.

Sichern Sie Operationen

Sichere Netzoperationen ist ein erhebliches Thema. Obwohl der Großteil dieses Dokuments der sicheren Konfiguration eines Cisco IOS XE-Geräts gewidmet ist, bieten Konfigurationen allein noch keinen vollständigen Schutz für ein Netzwerk. Die Arbeitsabläufe, die im Netz gebräuchlich sind, tragen so viel zur Sicherheit wie die Konfiguration der zugrunde liegenden Geräte bei.

Diese Themen enthalten Betriebsempfehlungen, denen Ihnen geraten werden einzuführen. Diese Themen markieren kritische Bereiche des Besonderen von Netzoperationen und sind nicht umfassend.

Überwachen Sie Cisco-Sicherheits-Advisories und Antworten

Das Cisco-Produkt-Sicherheits-Vorfall-Warteteam (PSIRT) erstellt und behält die Veröffentlichungen bei, geläufig gekennzeichnet als PSIRT-Advisories, für sicherheitsbezogene Fragen in Cisco-Produkten. Die Methode, die für Kommunikation von weniger schweren Fragen angewendet wird, ist die Cisco-Sicherheits-Antwort. Sicherheitsempfehlungen und -antworten finden Sie unter Cisco Security Advisories and Responses.

Weitere Informationen zu diesen Kommunikationsmitteln finden Sie in der Cisco Security Vulnerability Policy.

Zwecks ein sicheres Netz beizubehalten, müssen Sie die Cisco-Sicherheitsadvisories und -antworten berücksichtigen die freigegeben worden sind. Sie müssen Wissen einer Verwundbarkeit haben, bevor die Drohung, die sie zu einem Netz aufwerfen kann, ausgewertet werden kann. Hinweise zu diesem Bewertungsprozess finden Sie auf der Webseite zur Risikoselektierung bei Bekanntgabe von Sicherheitslücken.

Setzen Sie Authentisierung, Ermächtigung und Buchhaltung wirksam ein

Der Authentisierungs-, Ermächtigungs- und Buchhaltungs(AAA) Rahmen ist wesentlich, Netzgeräte zu sichern. Der aaa-Rahmen liefert Authentisierung von Managementsitzungen und kann Benutzer auf die spezifischen, Verwalter-definierten Befehle auch begrenzen und alle Befehle protokollieren, die von allen Benutzern eingegeben werden. Sehen Sie das Authentisierungs-, Ermächtigungs- und Buchhaltungskapitel dieses Dokuments zu mehr Information über, wie man AAA wirksam einsetzt.

Zentralisieren Sie Log-Sammlung und Überwachung

Um Informationen über aktuelle, neue und historische Ereignisse im Zusammenhang mit Sicherheitsvorfällen zu erhalten, benötigt Ihr Unternehmen eine einheitliche Strategie für die Ereignisprotokollierung und -korrelation. Diese Strategie muss das Protokollieren von allen

Netzgeräten wirksam einsetzen und die verpackten und kundengerechten Wechselbeziehungsfähigkeiten verwenden.

Nachdem das zentralisierte Protokollieren eingeführt ist, müssen Sie eine strukturierte Annäherung entwickeln, um den Analyse- und Vorfallgleichlauf zu protokollieren. Basiert auf dem Bedarf Ihrer Organisation, kann diese Annäherung von einer einfachen sorgfältigen Zusammenfassung von Journaldaten bis zu hoch entwickelter Regel-basierter Analyse reichen.

Im Abschnitt Best Practices für die Protokollierung dieses Dokuments finden Sie weitere Informationen zur Implementierung der Protokollierung auf Cisco IOS XE-Netzwerkgeräten.

Verwenden Sie sichere Protokolle, wenn möglich

Viele Protokolle werden verwendet, um empfindliche Netzführungsdaten zu tragen. Sie müssen sichere Protokolle verwenden, wann immer möglich. Eine sichere Protokollwahl umfasst den Gebrauch SSHs anstelle telnet, damit Authentisierungsdaten und Managementinformationen verschlüsselt werden. Darüber hinaus müssen Sie sichere Dateiübertragungsprotokolle verwenden, wenn Sie Konfigurationsdaten kopieren. Ein Beispiel ist der Gebrauch von dem sicheren Kopien-Protokoll (SCP) anstelle ftp oder TFTPS.

Weitere Informationen zur sicheren Verwaltung von Cisco IOS XE-Geräten finden Sie im Abschnitt Sichere interaktive Management-Sitzungen dieses Dokuments.

Gewinnen Sie Verkehrs-Sicht mit NetFlow

NetFlow aktiviert Sie, Verkehrsströme in das Netz zu überwachen. Beabsichtigte ursprünglich, Verkehrsinformation in Netzführungsanwendungen zu exportieren, NetFlow kann auch verwendet werden, um Flussinformationen über einen Router zu zeigen. Diese Fähigkeit erlaubt Ihnen, zu sehen, welcher Verkehr das Netz in der Istzeit überquert. Unabhängig davon, ob Flussinformationen in einen Fernkollektor exportiert werden, werden Sie geraten, Netzgeräte für NetFlow zu konfigurieren, damit es reaktiv verwendet werden kann, wenn es benötigt wird.

Weitere Informationen zu dieser Funktion finden Sie im Abschnitt Traffic Identification and Traceback (Identifizierung und Rückverfolgung von Datenverkehr) dieses Dokuments sowie unter Cisco IOS NetFlow (nur für registrierte Benutzer).

Konfigurationsverwaltung

Konfigurationsverwaltung ist ein Prozess, durch den Konfigurationsänderungen vorgeschlagen, wiederholt, genehmigt und eingesetzt werden. Im Zusammenhang mit einer Cisco IOS XE-Gerätekonfiguration sind zwei weitere Aspekte des Konfigurationsmanagements wichtig: Konfigurationsarchivierung und Sicherheit.

Sie können Konfigurationsarchive benutzen, um Änderungen zurück zu rollen, die zu den Netzgeräten vorgenommen werden. In einem Sicherheitskontext können Konfigurationsarchive auch benutzt werden, um zu bestimmen, welche Sicherheitsänderungen vorgenommen wurden

und als diese Änderungen eintraten. In Verbindung mit AAA-Journaldaten können diese Informationen in der Sicherheitsrevidierung von Netzgeräten unterstützen.

Die Konfiguration eines Cisco IOS XE-Geräts enthält viele vertrauliche Details. Benutzernamen, Passwörter und der Inhalt von Zugriffskontrolllisten ist Beispiele dieses Typen der Informationen. Das Repository, das Sie zur Archivierung von Cisco IOS XE-Gerätekonfigurationen verwenden, muss gesichert werden. Unsicherer Zugriff zu diesen Informationen kann die Sicherheit des gesamten Netzes untergraben.

Management-Fläche

Die Managementfläche besteht aus Funktionen, die die Managementziele des Netzes erzielen.

Dieses schließt interaktive Managementsitzungen, die SSH verwenden, sowie mit SNMP oder NetFlow Statistik-erfassen ein. Wenn Sie die Sicherheit eines Netzgerätes betrachten, ist es kritisch, dass die Managementfläche geschützt wird. Wenn ein Sicherheitsvorfall in der Lage ist, die Funktionen der Managementfläche zu untergraben, kann es für Sie unmöglich sein, das Netz wieder herzustellen oder zu stabilisieren.

In diesen Abschnitten werden die Sicherheitsfunktionen und -konfigurationen der Cisco IOS XE Software zur Konsolidierung der Verwaltungsebene beschrieben.

Geschäftsleitungs-Flächen-Verhärtung

Die Managementfläche wird benutzt, um auf ein Gerät zuzugreifen, zu konfigurieren und zu handhaben sowie seine Operationen und das Netz überwacht, auf denen es eingesetzt wird. Die Managementfläche ist die Fläche, die Verkehr für Operationen dieser Funktionen empfängt und sendet. Sie müssen die Managementfläche und Steuerfläche eines Gerätes sichern, weil Betrieb der Steuerfläche direkt Betrieb der Managementfläche beeinflußt. Diese Liste von Protokollen wird durch die Managementfläche benutzt:

1. Simple Network Management Protocol
2. Telnet
3. Sichern Sie Shell Protocol
4. File Transfer Protocol
5. Hyper Text Transfer Protocol/Secure Hyper Text Transfer Protocol
6. Triviales File Transfer Protocol
7. Sichern Sie Kopien-Protokoll
8. TACACS+
9. RADIUS
10. NetFlow
11. Network Time Protocol
12. Syslog

Schritte müssen unternommen werden, um das Überleben des Managements sicherzustellen und Flächen während der Sicherheitsvorfälle zu steuern. Wenn eine dieser

Flächen erfolgreich ausgenutzt wird, können alle Flächen kompromittiert werden.

Passwortverwaltung

Passwortsteuerzugriff zu den Betriebsmitteln oder zu den Geräten. Dies wird durch die Definition eines Kennworts oder Geheimnisses erreicht, das zur Authentifizierung von Anforderungen verwendet wird. Wenn eine Anfrage für Zugriff zu einer Ressource oder zu einem Gerät empfangen wird, wird die Anfrage für Überprüfung des Passwortes und der Identität angefochten, und Zugriff kann bewilligt sein, verweigert sein, oder begrenzt sein basiert worden auf dem Ergebnis. Als Sicherheitsoptimales verfahren müssen Passwörter mit Server einer TACACS+- oder RADIUS-gehandhabt werden Authentisierung. Jedoch beachten Sie, dass ein lokal konfiguriertes Passwort für privilegierten Zugriff noch im Falle der Störung der TACACS+- oder RADIUS-Dienstleistungen benötigt wird. Ein Gerät kann andere Passwortinformationen auch haben, die innerhalb seiner Konfiguration, wie eine NTP-Tasten-, SNMP-Gemeinschaftszeichenkette oder Wegewahl-Protokolltaste vorhanden sind.

Mit dem Befehl enable secret wird das Kennwort festgelegt, das dem Cisco IOS XE-System einen privilegierten Administratorzugriff gewährt. Der geheime Befehl des Aktivierunges muss verwendet werden, eher, als die älteren Passwortbefehl aktivieren. Der Aktivierungspasswortbefehl verwendet einen Algorithmus der schwachen Verschlüsselung.

Wenn kein Geheimnis ist gesetzt aktivieren Sie und ein Passwort wird für die Konsole tty-Zeile, das Konsolenpasswort kann verwendet werden, um privilegierten Zugriff, sogar von einer virtuellen (vty) entferntsitzung tty zu empfangen konfiguriert. Diese Aktion ist fast zweifellos unerwünscht und ist ein anderer Grund, Konfiguration eines Aktivierungsgeheimnisses sicherzustellen.

Der globale Konfigurationsbefehl service password-encryption weist die Cisco IOS XE-Software an, die Kennwörter, CHAP-Schlüssel (Challenge Handshake Authentication Protocol) und ähnliche Daten, die in der Konfigurationsdatei gespeichert sind, zu verschlüsseln. Solche Verschlüsselung ist nützlich, um zufällige Beobachter an den Lesepasswörtern, wie zu verhindern, wenn sie den Bildschirm über der Musterung eines Verwalters betrachten. Jedoch ist der Algorithmus, der durch den Service-Passwortverschlüsselungsbefehl verwendet wird, ein einfaches Vigen bezüglich der Ziffer. Der Algorithmus wird, um konzipiert Konfigurationsdateien gegen ernste Analyse zu schützen nicht von sogar etwas hoch entwickelten Angreifern und darf nicht zu diesem Zweck verwendet werden. Jede Cisco IOS XE-Konfigurationsdatei, die verschlüsselte Kennwörter enthält, muss mit der gleichen Sorgfalt behandelt werden, die auch für eine Klartextliste dieser Kennwörter verwendet wird.

Während dieser Algorithmus der schwachen Verschlüsselung nicht durch den geheimen Befehl des Aktivierunges verwendet wird, wird er durch den globalen Konfigurationsbefehl des Aktivierungspasswortes sowie die Passwortzeile Konfigurationsbefehl verwendet. Passwörter dieses Typen müssen beseitigt werden und der geheime Befehl des Aktivierunges oder das erhöhte Passwort-Sicherheitsmerkmal muss benutzt werden.

Der geheime Befehl des Aktivierunges und das erhöhte Passwort-Sicherheitsmerkmal benutzen Meldungs-Auswahl 5 (MD5) für Passwort Hashing. Dieser Algorithmus hat beträchtliche

allgemeine Zusammenfassung gehabt und nicht bekannt, um umschaltbar zu sein. Jedoch ist der Algorithmus abhängig von Wörterbuchangriffen. In einem Wörterbuchangriff versucht ein Angreifer jedes Wort in einem Wörterbuch oder andere Liste von Bewerberpasswörtern, um eine Abgleichung zu finden. Deshalb müssen Konfigurationsdateien mit verlässlichen Einzelpersonen sicher gespeichert werden und nur geteilt werden.

Erhöhte Passwort-Sicherheit

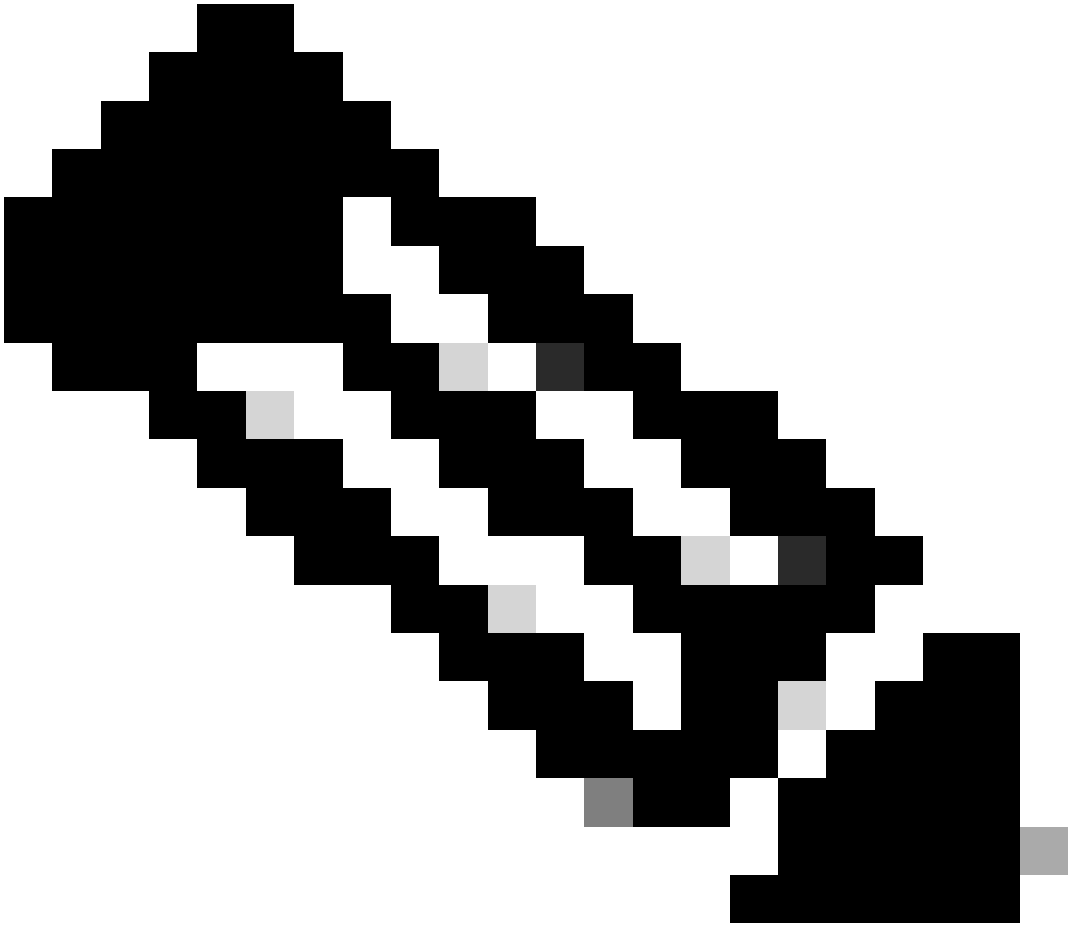
Die Funktion "Enhanced Password Security" (Erweiterte Kennwortsicherheit), die seit der ersten Version der Cisco IOS XE Software, Version 16.6.4, funktioniert, ermöglicht es einem Administrator, das MD5-Hashing von Kennwörtern für den Benutzernamen-Befehl zu konfigurieren. Vor dieser Funktion gab es zwei Arten von Passwörtern: Typ 0, der ein Klartext-Passwort ist, und Typ 7, der den Algorithmus der Vigen re-Verschlüsselung verwendet. Das erhöhte Passwort-Sicherheitsmerkmal kann nicht mit Protokollen, die das Klartextpasswort, benötigen wieder gutzumachend zu sein, wie TYPEN benutzt werden.

Zwecks ein Benutzerpasswort mit Hashing MD5 zu verschlüsseln, geben Sie den geheimen globalen Konfigurationsbefehl username heraus.

username <Name> secret <Kennwort>

LOGON-Passwort-Wiederholungs-Aussperrung

Mit der Funktion zum erneuten Abmelden (Login Password Retry Lockout), die seit der ersten Version der Cisco IOS XE Software 16.6.4 funktioniert, können Sie ein lokales Benutzerkonto nach einer konfigurierten Anzahl erfolgloser Anmeldeversuche sperren. Sobald ein Benutzer heraus gesperrt wird, ist ihr Konto verschlossen, bis Sie es freisetzen. Ein berechtigter Benutzer, der mit Privilegstufe 15 konfiguriert wird, kann nicht mit diesem Merkmal heraus gesperrt werden. Die Anzahl von Benutzern mit Privilegstufe 15 muss zu einem Minimum gehalten werden.



Hinweis: Autorisierte Benutzer können sich von einem Gerät ausschließen, wenn die Anzahl der erfolglosen Anmeldeversuche erreicht wird. Zusätzlich kann ein böswilliger Benutzer eine Leistungsverweigerung (DOS) Zustand mit wiederholten Versuchen erstellen, mit einem gültigen username zu beglaubigen.

Dieses Beispiel zeigt, wie man das LOGON-Passwort-Wiederholungs-Ausrück-Merkmal aktiviert:

aaa new-model aaa lokale Authentifizierung Versuche max-fail <max-attempts> aaa Authentifizierung Anmeldung default lokal

username <Name> secret <Kennwort>

Dieses Merkmal trifft auch auf Authentisierungsmethoden wie TYPEN und Passwort-Authentisierungs-Protokoll zu (BREI).

Kein Service-Passwort-Wiederanlauf

In Cisco IOS XE Software, Version 16.6.4 und höher, ermöglicht die Funktion zur

Wiederherstellung von Service-Passwörtern niemandem mit Konsolenzugriff einen unsicheren Zugriff auf die Gerätekonfiguration und das Löschen des Passworts. Es auch erlaubt nicht böswilligen Benutzern, den Konfigurationsregisterwert zu ändern und auf NVRAM zuzugreifen.

kein service-passwort-wiederanlauf

Die Cisco IOS XE Software stellt ein Verfahren zur Kennwortwiederherstellung bereit, das auf den ROM Monitor Mode (ROMMON)-Zugriff angewiesen ist und beim Systemstart die Taste "Break" (Unterbrechung) verwendet. In ROMMON kann die Gerätsoftware neu geladen werden, um eine neue Anlagenkonfiguration aufzufordern, die ein neues Passwort umfasst.

Die aktuelle PasswortWiederherstellungsprozedur aktiviert jedermann mit Konsolenzugriff, das Gerät und auf sein Netz zuzugreifen. Das kein Service-Passwort-Wiederanlaufmerkmal verhindert die Fertigstellung der Unterbrechungstastereihenfolge und das Hereinkommen von ROMMON während des Einschaltens der Anlage.

Wenn kein Service-Passwortwiederanlauf auf einem Gerät aktiviert wird, wird es empfohlen, dass eine Offline-Kopie der Geräteausstattung gesichert wird und dass eine Konfiguration, die Lösung archiviert, eingeführt wird. Wenn das Kennwort eines Cisco IOS XE-Geräts wiederhergestellt werden muss, nachdem diese Funktion aktiviert wurde, wird die gesamte Konfiguration gelöscht.

Sperrungs-unbenutzte Dienstleistungen

Als Sicherheitsoptimales verfahren muss jeder unnötige Service behindert sein. Diese nicht benötigten Dienstleistungen, besonders die, die User Datagram Protocol (UDP) verwenden, werden selten verwendet, für legitime Zwecke aber können verwendet werden, um DOS und andere Angriffe zu starten, die andernfalls verhindert werden, indem man Paketfiltert.

Die kleinen Dienstleistungen TCPs und UDP müssen behindert sein. Diese Dienstleistungen umfassen:

1. Echo (Anschlussnummer 7)
2. verwerfen Sie (Anschlussnummer 9)
3. Tageszeit (Anschlussnummer 13)
4. chargen (Anschlussnummer 19)

   Obgleich Missbrauch der kleinen Dienstleistungen durch anti-spoofing Zugriffslisten vermieden werden oder weniger gefährlich gemacht werden kann, müssen die Dienstleistungen auf jedem möglichem Gerät deaktiviert werden, das innerhalb des Netzes zugänglich ist. Die kleinen Services sind in Cisco IOS XE Software, Version 16.6.4 und höher, standardmäßig deaktiviert. In der früheren Software können die keine Service-TCP-kleinservers und keine globalen Konfigurationsbefehle der Service-UDP-kleinservers herausgegeben werden, um sie zu deaktivieren.

   Dieses ist eine Liste von zusätzlichen Dienstleistungen, die behindert sein müssen, wenn nicht verwendet:
5. Geben Sie den keinen globalen Konfigurationsbefehl IP-Fingers heraus, um Fingerservice zu deaktivieren. Spätere Cisco IOS XE Software-Versionen als 16.1 deaktivieren diesen

Service standardmäßig.

6. Geben Sie den keinen globalen Konfigurationsbefehl IPbootp-Servers heraus, um Urladen-Protokoll (BOOTP) zu deaktivieren. Spätere Cisco IOS XE Software-Versionen als 16.1 deaktivieren diesen Service standardmäßig.
7. Führen Sie in Cisco IOS XE Software, Version 16.6.4 und höher, den Befehl ip dhcp bootp ignore im globalen Konfigurationsmodus aus, um BOOTP zu deaktivieren. Dieses lässt Dienstleistungen des dynamischer Hauptrechner-Konfigurations-Protokolls (DHCP) aktiviert.
8. DHCP-Dienstleistungen können behindert sein, wenn DHCP-Relaisdienstleistungen nicht benötigt werden. Geben Sie den keinen Service-DHCP-Befehl im globalen Konfigurationsmodus heraus.
9. Geben Sie den keinen Mopp aktivierten Befehl im Schnittstellenkonfigurationsmodus heraus, um den Service des Pflege-Operations-Protokolls zu deaktivieren (MOPP).
10. Geben Sie den keinen IP-Gebietlook-up globalen Konfigurationsbefehl heraus, um Auflösungsdienstleistungen des Domain Name System (DNS) zu deaktivieren.
11. Geben Sie den keinen Service-Auflagenbefehl im globalen Konfigurationsmodus heraus, um Paket-Assembler-/Disassembler(AUFLAGE) Service zu deaktivieren, der für Netze X.25 verwendet wird.
12. Der HTTP-Server kann mit dem keinem IPhttp-Serverbefehl im globalen Konfigurationsmodus deaktiviert werden, und sicherer Server HTTP (HTTPS) kann mit dem keinem globalen Konfigurationsbefehl IPhttp-sicher-Servers deaktiviert werden.
13. Wenn Cisco IOS XE-Geräte beim Start keine Konfigurationen aus dem Netzwerk abrufen, muss der globale Konfigurationsbefehl no service config verwendet werden. Dadurch wird verhindert, dass das Cisco IOS XE-Gerät versucht, eine Konfigurationsdatei über TFTP im Netzwerk zu finden.
14. Cisco-Entdeckungs-Protokoll (Verdichteraustrittsdruck) ist ein Vermittlungsprotokoll, das verwendet wird, um andere Verdichteraustrittsdruck aktivierte Geräte für Nachbarumgebungs- und Netztopologie zu entdecken. Verdichteraustrittsdruck kann durch Netzführungs-Systeme (Nanometer) oder während der Störungssuche verwendet werden. Verdichteraustrittsdruck muss auf allen Schnittstellen deaktiviert werden, die an untrusted Netze angeschlossen werden. Dieses wird mit dem keinem Verdichteraustrittsdruck aktivieren Schnittstellenbefehl vollendet. Wechselweise kann Verdichteraustrittsdruck mit dem keinem Verdichteraustrittsdruck ausgeführten globalen Konfigurationsbefehl global deaktiviert werden. Beachten Sie, dass Verdichteraustrittsdruck von einem böswilligen Benutzer für Untersuchung und das Netzabbilden verwendet werden kann.
15. Sicherungsschicht-Entdeckungs-Protokoll (LLDP) ist ein IEEE-Protokoll, das in 802.1AB definiert wird. LLDP ist Verdichteraustrittsdruck ähnlich. Jedoch erlaubt dieses Protokoll Interoperabilität zwischen anderen Geräten, die nicht Verdichteraustrittsdruck unterstützen. LLDP muss auf die gleiche Weise wie Verdichteraustrittsdruck behandelt werden und auf allen Schnittstellen deaktiviert werden, die an untrusted Netze anschließen. Zwecks dieses zu vollenden, geben Sie das kein lldp übertragen heraus und kein lldp empfangen Schnittstellenkonfigurationsbefehle. Geben Sie den keinen lldp ausgeführten globalen Konfigurationsbefehl heraus, um LLDP global zu deaktivieren. LLDP kann von einem böswilligen Benutzer für Untersuchung und das Netzabbilden auch verwendet werden.
16. Für Switches, die das Booten über sdflash unterstützen, kann die Sicherheit erhöht werden, indem vom Flash gebootet wird und sdflash mit dem Konfigurationsbefehl no sdflash deaktiviert wird.

LEITPROGRAMM Unterbrechung

Zwecks den Abstand einzustellen auf dem der Bedienungsaufruf- an den Ablaufteilinterpreter Benutzerinput wartet bevor er eine Sitzung abbricht, geben Sie die Leitprogrammunterbrechungszeile Konfigurationsbefehl heraus. Der Leitprogrammunterbrechungsbefehl muss verwendet werden, um sich Sitzungen auf den vty oder tty-Zeilen auszuloggen, die untätig gelassen werden. Standardmäßig sind Sitzungen nach zehn Minuten Untätigkeit getrennt.

Zeilensymbol 0

exec-timeout **<**Minuten**>** [Sekunden]

Zeile vty 0 4

exec-timeout **<**Minuten**>** [Sekunden]

Keepalives für TCP-Sitzungen

Der Service TCP-keepalives-in und globalen die Konfigurationsbefehle Service TCPKeepalives-heraus aktivieren ein Gerät, TCP-Keepalives für TCP-Sitzungen zu senden. Diese Konfiguration muss verwendet werden, um TCP-Keepalives auf Inlandsverbindungen zum Gerät und Auslandsverbindungen vom Gerät zu aktivieren. So wird sichergestellt, dass der Zugriff auf das Gerät am Remote-Ende der Verbindung weiterhin möglich ist und dass halb offene oder verwaiste Verbindungen vom lokalen Cisco IOS XE-Gerät entfernt werden.

service tcp-keepalives-in

service tcp-keepalives-out

Management-Schnittstellen-Gebrauch

Die Managementfläche eines Gerätes ist auf einer körperlichen oder logischen Managementschnittstelle erreichtes Inband- oder nicht auf Band aufgenommen. Ideal existiert Inband- und nicht auf Band aufgenommener Managementzugriff für jedes Netzgerät, damit die Managementfläche während der Netzausfälle erreicht werden kann.

Eine der geläufigsten Schnittstellen, die für Inbandzugriff zu einem Gerät benutzt wird, ist die logische Schleifenbetriebschnittstelle. Schleifenbetriebschnittstellen sind immer oben, während körperliche Schnittstellen Zustand ändern können und die Schnittstelle nicht zugänglich möglicherweise sein kann. Es wird empfohlen, um eine Schleifenbetriebschnittstelle jedem Gerät als Managementschnittstelle hinzuzufügen und das wird es ausschließlich für die Managementfläche verwendet. Dieses erlaubt dem Verwalter, Politik während des Netzes für die Managementfläche anzuwenden. Sobald die Schleifenbetriebschnittstelle auf einem Gerät konfiguriert wird, kann sie durch Managementflächenprotokolle, wie SSH, SNMP und syslog benutzt werden, um Verkehr zu senden und zu empfangen.

Schnittstelle Loopback0

ip address 192.168.1.1 255.255.255.0

Speicher-Schwellwert-Mitteilungen

Mit der Funktion "Memory Threshold Notification" (Benachrichtigung über Speicherschwellenwert), die in Version 16.6.4 der Cisco IOS XE-Software enthalten ist, können Sie die Auswirkungen von Speicherengpässen auf einem Gerät minimieren. Diese Funktion verwendet zwei Methoden, um dies zu erreichen: Speicherschwellenbenachrichtigung und Speicherreservierung.

Speicher-Schwellwert-Mitteilung legt eine Logmeldung fest, um anzuzeigen, dass freier Speicher auf einem Gerät niedriger als der konfigurierte Schwellwert gefallen ist. Dieses Konfigurationsbeispiel zeigt, wie man dieses Merkmal mit dem Konfigurationsbefehl NiedrigWaterMarks des Speichers freien globalen aktiviert. Dieses aktiviert ein Gerät, eine Mitteilung festzulegen, wenn verfügbarer freier Speicher niedriger als der spezifizierte Schwellwert fällt, und wieder, wenn verfügbarer freier Speicher auf fünf Prozent höher als der spezifizierte Schwellwert steigt.

speicherfreier Low-Watermark-Prozessor <threshold>

speicherfrei Low-Watermark io <threshold>

Speicher-Reservierung wird verwendet, damit genügender Speicher für kritische Mitteilungen verfügbar ist. Dieses Konfigurationsbeispiel zeigt, wie man dieses Merkmal aktiviert. Dieses garantiert, dass Managementprozesse fortfahren zu arbeiten, wenn der Speicher des Gerätes erschöpft wird.

memory reserve critical <Wert>

CPU-Thresholding-Mitteilung

Die Funktion "CPU Thresholding Notification", die in der Cisco IOS XE Software-Version 16.6.4 eingeführt wurde, ermöglicht es Ihnen, zu erkennen und benachrichtigt zu werden, wenn die CPU-Last auf einem Gerät einen konfigurierten Grenzwert überschreitet. Wenn der Schwellwert überschritten wird, legt das Gerät fest und sendet eine SNMP-Blockiermeldung. Die Cisco IOS XE-Software unterstützt zwei Grenzwertmethoden für die CPU-Auslastung: steigender und fallender Schwellenwert.

Shows dieser Beispielkonfiguration, wie man die steigenden und fallenden Schwellwerte aktiviert, die eine CPU-Schwellwertmitteilungsmeldung starten:

SNMP-server enable traps cpu threshold

snmp-server host <Host-Adresse> <Community-String> cpu

process cpu threshold type <type> rising <percentage> interval <seconds> [fallendes <percentage> interval <seconds>]

process cpu statistics limit entry-percentage <Nummer> [Größe <Sekunden>]

Network Time Protocol

Das Network Time Protocol (NTP) ist ein nicht besonders gefährlicher Service, aber jeder nicht benötigte Service kann einen Angriffsvektor darstellen. Wenn NTP benutzt wird, ist es wichtig, eine verlässliche Zeitquelle ausdrücklich zu konfigurieren und richtige Authentisierung zu verwenden. Für Syslog-Zwecke, wie etwa bei forensischen Untersuchungen potenzieller Angriffe, sowie für erfolgreiche VPN-Verbindungen, die von Zertifikaten für die Phase-1-Authentifizierung abhängen, ist ein genauer und zuverlässiger Zeitraum erforderlich.

1. NTP-Zeit-Zone - Wenn Sie NTP konfigurieren, muss die Zeitzone konfiguriert werden, damit Zeitstempel genau aufeinander bezogen werden können. Es gibt normalerweise zwei Ansätze, zum der Zeitzone für Geräte in einem Netz mit einer globalen Anwesenheit zu konfigurieren. Eine Methode ist, alle Netzgeräte mit der koordinierten Weltzeit (UTC) (vorher die Greenwich-Zeit (GMT) zu konfigurieren). Die andere Annäherung ist, Netzgeräte mit der Ortszeitzone zu konfigurieren. Weitere Informationen zu dieser Funktion finden Sie in der Zeitzone der Uhr in der Cisco Produktdokumentation.
2. NTP-Authentisierung - Wenn Sie NTP-Authentisierung konfigurieren, liefert sie Versicherung, dass NTP-Meldungen zwischen verlässlichen NTP-Gleichen ausgetauscht werden.

   Beispielkonfiguration, die NTP-Authentifizierung verwendet:

   Kunde:

   (config)#ntp authentifizieren

   (config)#ntp Authentifizierungsschlüssel 5 md5 ciscotime

   (config)#ntp Trusted-Key 5

   (config)#ntp server 172.16.1.5 key 5 Server:

   (config)#ntp authentifizieren

   (config)#ntp Authentifizierungsschlüssel 5 md5 ciscotime

   (config)#ntp Trusted-Key 5

Grenzzugriff zum Netz mit Infrastruktur ACLs

Geplant, um nicht autorisierte direkte Kommunikation zu den Netzgeräten zu verhindern, sind InfrastrukturZugriffskontrolllisten (iACLs) eine der kritischsten Sicherheitskontrollen, die in den Netzen eingeführt werden können. Infrastruktur ACLs-Hebelkraft die Idee, dass fast aller Netzwerkverkehr das Netz überquert und nicht zum Netz selbst vorgesehen wird.

Ein iACL wird konstruiert und angewendet, um Verbindungen von den Hauptrechnern oder von

den Netzen zu spezifizieren, die zu den Netzgeräten erlaubt werden müssen. Geläufige Beispiele dieser Typen der Verbindungen sind eBGP, SSH und SNMP. Nachdem die erforderlichen Verbindungen die Erlaubnis gehabt worden sind, weitere wird ganzer Verkehr zur Infrastruktur ausdrücklich verweigert. Aller Durchgangsverkehr, der das Netz kreuzt und nicht zu den Infrastrukturgeräten vorgesehen wird, wird dann ausdrücklich die Erlaubnis gehabt.

Der Schutz, der von den iACLs geboten wird, ist zum Management relevant und steuert Flächen. Die Implementierung von iACLs kann einfacher gemacht werden durch den Gebrauch von eindeutigem Wenden für Netzwerk-Infrastruktur-Geräte. Sprechen Sie eine Sicherheit orientierte Annäherung zu IP an, das zu mehr Information über die Sicherheitsauswirkungen von IPwenden sich wendet.

Diese Beispiel iACL Konfiguration veranschaulicht die Struktur, die als Ausgangspunkt benutzt werden muss, wenn Sie den iACL Implementierungsprozeß anfangen:

ip access-list extended ACL-INFRASTRUCTURE-IN

- Zulassen erforderlicher Verbindungen für Routing-Protokolle und das Netzwerkmanagement

permit tcp host <trusted-ebgp-peer> host <local-ebgp-address> eq 179

permit tcp host <trusted-ebgp-peer> eq 179 host <local-ebgp-address>

permit tcp host <vertrauenswürdige Management-Stationen> any eq 22

permit udp host <trusted-netmgmt-servers> any eq 161

- Anderen IP-Datenverkehr an jedes Netzwerkgerät ablehnen

deny ip any <Infrastruktur-Adressraum> <Platzhaltermaske>

— Transitverkehr zulassen

permit ip any any

Sobald erstellt, muss das iACL an allen Schnittstellen angewendet werden, die Nichtinfrastrukturgeräte gegenüberstellen. Dieses schließt Schnittstellen ein, die an andere Organisationen, Fernzugriffsegmente, Benutzersegmente und Segmente in den Rechenzentren anschließen.

Im Dokument zum Thema Schützen des Core mit Zugriffskontrolllisten für den Infrastrukturschutz finden Sie weitere Informationen zu Infrastruktur-ACLs.

ICMP-Paket-Entstörung

Das Internet Control Message Protocol (ICMP) ist als IP-Steuerprotokoll konzipiert. Als solches können die Meldungen, die es übermittelt, weit reichende Verzweigungen zu den TCP- und IP-Protokollen im Allgemeinen haben. Während das Netzstörungssuchewerkzeuge Klingeln und das traceroute ICMP benutzen, wird externe ICMP-Anschlussfähigkeit selten für die sinngemässe Funktion eines Netzes benötigt.

Die Cisco IOS XE Software bietet Funktionen, mit denen ICMP-Meldungen gezielt nach Name, Typ und Code gefiltert werden können. Dieses Beispiel ACL, das mit den Zugriffssteuerungseinträgen (Asse) von den vorhergehenden Beispielen verwendet werden muss, erlaubt Klingeln von den Vermögensverwaltungsstationen und VON Nanometer-Servers und blockt alle weiteren ICMP-Pakete:

ip access-list extended ACL-INFRASTRUCTURE-IN

— ICMP-Echo (Ping) von vertrauenswürdigen Verwaltungsstationen und Servern zulassen

icmp host <vertrauenswürdige Management-Stationen> jegliches Echo erlauben

permit icmp host <trusted-netmgmt-servers> any echo

- Anderen IP-Datenverkehr an jedes Netzwerkgerät ablehnen

deny ip any <Infrastruktur-Adressraum> <Platzhaltermaske>

— Transitverkehr zulassen

permit ip any any

Filter IP-Fragmente

Der Filterprozeß für zersplitterte IP-Pakete kann eine Herausforderung zu den Arten der Sicherheitsleistung darstellen. Dieses ist, weil die Informationen der Schicht 4, die verwendet wird, um TCP- und UDP-Pakete zu filtern, im Anfangsfragment nur anwesend sind. Die Cisco IOS XE Software verwendet eine bestimmte Methode, um nicht anfängliche Fragmente mit konfigurierten Zugriffslisten zu vergleichen. Die Cisco IOS XE-Software wertet diese nicht anfänglichen Fragmente anhand der ACL aus und ignoriert alle Layer-4-Filterinformationen. Dieses veranlaßt nicht-Anfangsfragmente, auf die Schicht nur ausgewertet zu werden 3 Teil von jedem möglichem konfigurierten ACE.

In dieser Beispielkonfiguration wenn ein TCP-Paket, das zu 192.168.1.1 auf Kanal 22 vorgesehen wird, bei dem Transport zersplittert wird, wird das Anfangsfragment wie erwartet durch zweite ACE fallen gelassen, das auf den Informationen der Schicht 4 innerhalb des Pakets basiert. Jedoch werden alle restlichen (nicht-Anfangs) Fragmente durch erste ACE erlaubt, das vollständig auf den Informationen der Schicht 3 im Paket und in ACE basiert. Das Szenario wird in der folgenden Konfiguration dargestellt:

ip access-list extended ACL-FRAGMENT-BEISPIEL

permit tcp any host 192,168.1,1 eq 80

deny tcp any host 192,168.1,1 eq 22

Wegen der nonintuitive Art des Fragments handhabend, werden IP-Fragmente häufig unbeabsichtigt durch ACLs die Erlaubnis gehabt. Fragmentierung ist auch in den Versuchen, Entdeckung durch EindringenErfassungssysteme auszuweichen häufig benutzt. Es ist aus diesen

Gründen, dass IP-Fragmente in den Angriffen häufig benutzt sind, und warum sie an der Spitze aller möglicher konfigurierten iACLs ausdrücklich gefiltert werden müssen. Dieses Beispiel ACL umfasst die umfassende Entstörung von IP-Fragmenten. Die Funktionalität von diesem Beispiel muss in Verbindung mit der Funktionalität der vorhergehenden Beispiele verwendet werden.

ip access-list extended ACL-INFRASTRUCTURE-IN

- Verweigern von IP-Fragmenten, die protokollspezifische ACEs verwenden, um

— Klassifizierung des Angriffsverkehrs

tcp alle Fragmente verweigern

udp alle Fragmente verweigern

icmp alle Fragmente verweigern

ip alle Fragmente verweigern

- Anderen IP-Datenverkehr an jedes Netzwerkgerät ablehnen

deny ip any <Infrastruktur-Adressraum> <Platzhaltermaske>

— Transitverkehr zulassen

permit ip any any

Siehe Zugriffskontrolllisten und IP-Fragmente zu mehr Information über, wie ACL zersplitterte IP-Pakete handhabt.

Acl-Support für die Entstörung von IP-Optionen

Die Cisco IOS XE Software, Version 16.6.4, bietet nun Unterstützung für die Verwendung von ACLs zum Filtern von IP-Paketen anhand der im Paket enthaltenen IP-Optionen. IP-Optionen stellen eine Sicherheitsherausforderung für Netzgeräte dar, weil diese Optionen als Ausnahmepakete verarbeitet werden müssen. Dieses benötigt ein Niveau von CPU-Bemühung, die nicht für typische Pakete benötigt wird, die das Netz überqueren. Das Vorhandensein von IP-Optionen innerhalb eines Pakets kann einen Versuch auch anzeigen, Sicherheitskontrollen im Netz umzustürzen oder die Durchfahrteigenschaften eines Pakets andernfalls zu ändern. Es ist aus diesen Gründen, dass Pakete mit IP-Optionen am Rand des Netzes gefiltert werden müssen.

Dieses Beispiel muss mit den Assen von den vorhergehenden Beispielen verwendet werden, um die komplette Entstörung von IP-Paketen einzuschließen, die IP-Optionen enthalten:

ip access-list extended ACL-INFRASTRUCTURE-IN

- IP-Pakete mit IP-Optionen verweigern

deny ip any option any option any options

- Anderen IP-Datenverkehr an jedes Netzwerkgerät ablehnen

deny ip any <Infrastruktur-Adressraum> <Platzhaltermaske>

— Transitverkehr zulassen

permit ip any any

Acl-Support, zum auf TTL-Wert zu filtern

Mit der Cisco IOS XE Software-Version 16.6.4 wurde die ACL-Unterstützung zum Filtern von IP-Paketen basierend auf dem TTL-Wert (Time to Live) erweitert. Der TTL-Wert eines IP datagram wird durch jedes Netzgerät verringert, während ein Paket von Quelle zu Zieleinheit fließt. Obgleich Anfangswerte durch Betriebssystem schwanken, wenn TTL eines Pakets null erreicht, muss das Paket fallen gelassen werden. Das Gerät, das TTL bis null und deshalb verringert, das Paket fallenläßt, um eine überstiegene Meldung ICMP Zeit zur Quelle des Pakets festzulegen und zu schicken benötigt wird.

Die Generation und die Übertragung dieser Meldungen ist ein Ausnahmeprozeß. Router können diese Aufgabe wahrnehmen, wenn die Anzahl von IP-Paketen, die ablaufen sollen, niedrig ist, aber, wenn die Anzahl von den Paketen, die passend sind abzulaufen, hoch ist, können Generation und Übertragung dieser Meldungen alle verfügbaren CPU-Betriebsmittel verbrauchen. Dieses stellt einen DOS-Angriffsvektor dar. Aus diesem Grunde müssen Geräte gegen DOS-Angriffe verhärtet werden, die eine hohe Kinetik von IP-Paketen verwenden, die ablaufen sollen.

Es wird empfohlen, dass Organisationen IP-Pakete mit niedrigen TTL-Werten am Rand des Netzes filtern. Pakete vollständig filtern mit TTL-Werten, die unzulänglich sind, das Netz zu überqueren, schwächt die Drohung von TTL-basierten Angriffen ab.

In diesem Beispiel filtert die ACL Pakete mit TTL-Werten unter sechs. Dieses bietet Schutz gegen TTL-Endangriffe für Netze bis zu fünf einsteigt Breite.

ip access-list extended ACL-INFRASTRUCTURE-IN

— IP-Pakete mit TTL-Werten, die nicht ausreichen, um das Netzwerk zu durchlaufen, werden abgelehnt

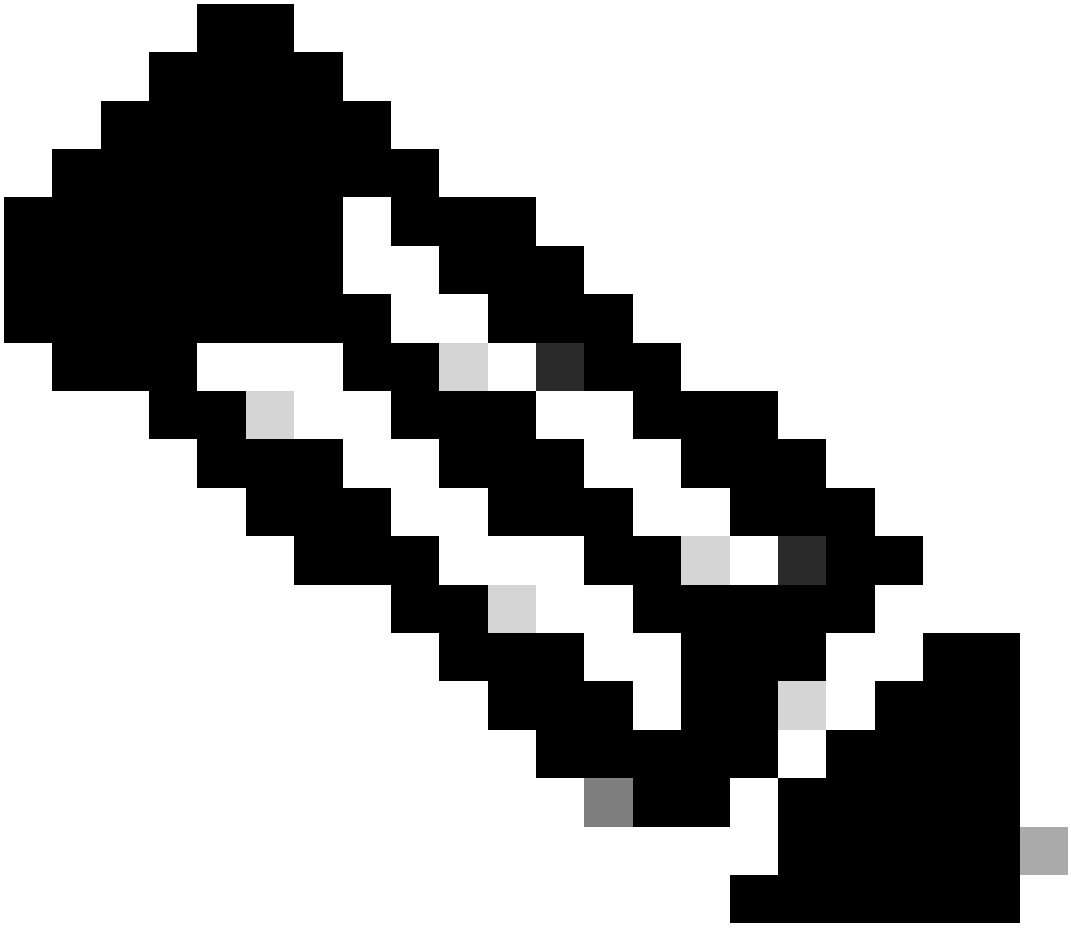
ip any ttl lt 6 verweigern

- Anderen IP-Datenverkehr an jedes Netzwerkgerät ablehnen

deny ip any <Infrastruktur-Adressraum> <Maske>

— Transitverkehr zulassen

permit ip any any



Hinweis: Bei einigen Protokollen werden Pakete mit niedrigen TTL-Werten zu legitimen Zwecken genutzt. eBGP ist ein solches Protokoll. Siehe TTL-Endangriffs-Kennzeichen und Abschwächung zu mehr Information über die Abschwächung von Ende-basierten Angriffen TTLs.

Sichern Sie interaktive Management-Sitzungen

Managementsitzungen zu den Geräten gestehen Ihnen die Fähigkeit zu, Informationen über ein Gerät und seine Operationen anzusehen und zu sammeln. Wenn diese Informationen zu einem böswilligen Benutzer bekannt gemacht werden, kann das Gerät das Ziel werden eines Angriffs, kompromittiert, und benutzt, um zusätzliche Angriffe durchzuführen. Jedermann mit privilegiertem Zugriff zu einem Gerät hat die Fähigkeit für volle Verwaltungskontrolle dieses Gerätes. Es ist zwingend, Managementsitzungen zu sichern, um Informationsdatenübermittlung und -unberechtigten Zugriff zu verhindern.

Management-flacher Schutz

In Cisco IOS XE Software, Version 16.6.4 und höher, können Administratoren mit der Funktion zum Schutz der Verwaltungsebene (Management Plane Protection, MPP) festlegen, auf welchen Schnittstellen der Verwaltungsdatenverkehr von einem Gerät empfangen werden kann. Dieses erlaubt die Verwalterzusätzliche kontrolle über einem Gerät und wie das Gerät erreicht wird.

Dieses Beispiel zeigt, wie man den MPP aktiviert, um SSH nur zu erlauben und HTTPS auf dem GigabitEthernet0/1 schließen an:

Control-Plane-Host

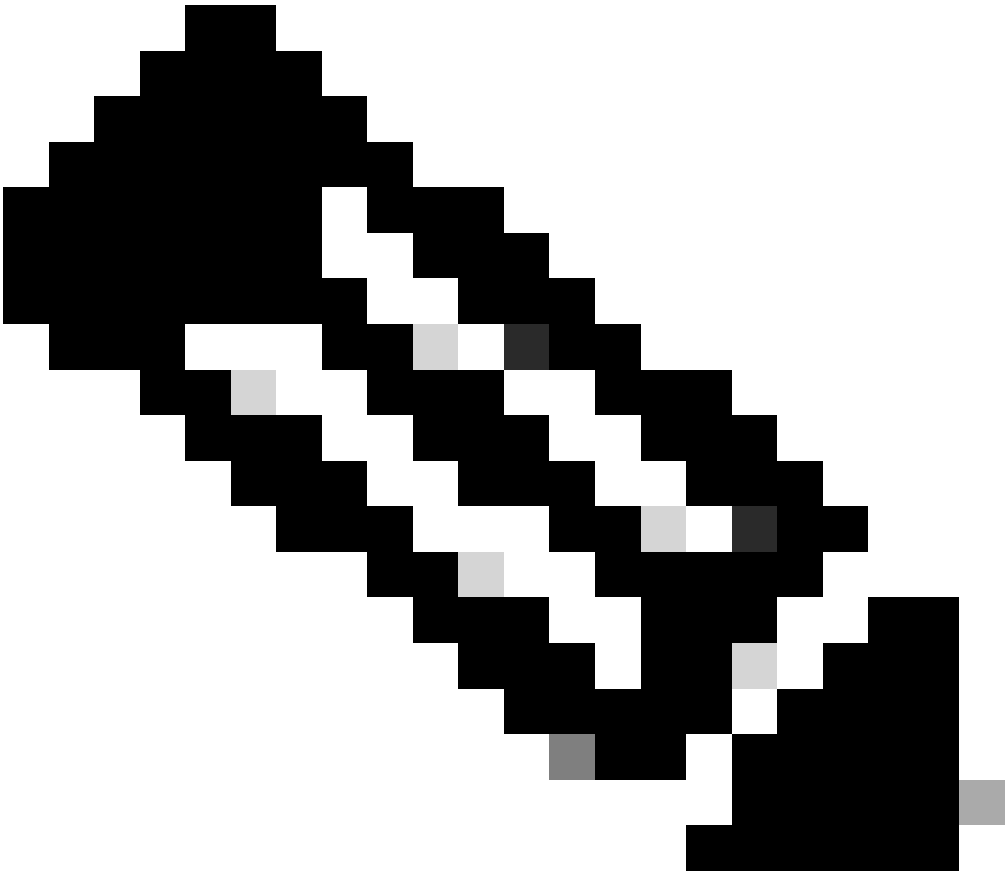
Management-Schnittstelle GigabitEthernet 0/1 SSH HTTPS zulassen

Steuern Sie flachen Schutz

Der Control Plane Protection (CPPr) baut auf der Funktionalität des Control Plane Policing auf, um den Datenverkehr auf der Kontrollebene, der an den Routingprozessor des IOS-XE-Geräts gerichtet ist, einzuschränken und zu regeln. CPPr teilt die Kontrollebene in separate Kontrollebenenkategorien auf, die als Subschnittstellen bezeichnet werden. Es gibt drei Subschnittstellen für die Steuerungsebene: Host, Transit und CEF-Exception. Darüber hinaus schließt CPPr diese Flächen-Schutzmerkmale der zusätzlichen Kontrolle ein:

1. Kanal-Entstörungsmerkmal - Dieses Merkmal stellt für das Polizeilich überwachen oder das Fallen von Paketen zur Verfügung, die zu geschlossenen oder nicht-hörenden TCP- und UDP-Kanälen gehen.
2. Warteschlange-Schwellwertpolitikmerkmal - Dieses Merkmal begrenzt die Anzahl von Paketen für ein spezifiziertes Protokoll, die in der Steuerfläche IP-Eingabewarteschlange erlaubt werden.

   CPPr erlaubt einem Verwalter, Verkehr zu klassifizieren, polizeilich zu überwachen und einzuschränken, der zu einem Gerät zu den Managementzwecken mit dem Hauptrechner Subinterface geschickt wird. Beispiele von Paketen, die für die Hauptrechner Subinterfacekategorie klassifiziert werden, umfassen Managementverkehr wie SSH oder telnet und Wegewahlprotokolle.



Hinweis: CPPr unterstützt IPv6 nicht und ist auf den IPv4-Eingabepfad beschränkt.

Weitere Informationen zur Cisco CPPr-Funktion finden Sie unter Control Plane Policing.

Verschlüsseln Sie Management-Sitzungen

Weil Informationen in einer interaktiven Managementsitzung bekannt gemacht werden können, muss dieser Verkehr verschlüsselt werden, damit ein böswilliger Benutzer nicht zu den Daten Zutritt erhalten kann, die übertragen wird. Verkehrsverschlüsselung erlaubt eine sichere Fernzugriffverbindung zum Gerät. Wenn der Verkehr für eine Managementsitzung über das Netz im Klartext gesendet wird, kann ein Angreifer vertrauliche Information über das Gerät und das Netz einholen.

Ein Administrator kann eine verschlüsselte und sichere Remote-Zugriffsmanagement-Verbindung zu einem Gerät mit SSH- oder HTTPS-Funktionen (Secure Hypertext Transfer Protocol) herstellen. Die Cisco IOS XE Software unterstützt SSH Version 2.0 (SSHv2) und HTTPS, das Secure Sockets Layer (SSL) und Transport Layer Security (TLS) für die Authentifizierung und Datenverschlüsselung verwendet.

Die Cisco IOS XE Software unterstützt auch das Secure Copy Protocol (SCP), das eine

verschlüsselte und sichere Verbindung ermöglicht, um Gerätekonfigurationen oder Software-Images zu kopieren. SCP beruht auf SSH.

In dieser Beispielkonfiguration wird SSH auf einem Cisco IOS XE-Gerät aktiviert:

ip domain-name example.com

crypto key generate rsa modulus 2048

ip ssh timeout 60

ip ssh authentication-retries 3

ip ssh source-interface GigabitEthernet 0/1

Zeile vty 0 4

Transporteingabe SSH

Dieses Konfigurationsbeispiel aktiviert SCP-Dienstleistungen:

IP SCP-Serveraktivierung

Dieses ist ein Konfigurationsbeispiel für HTTPS-Dienstleistungen:

crypto key generate rsa modulus 2048

ip http secure-server

SSHv2

Die SSHv2-Funktion wurde in Cisco IOS XE in der ersten Version 16.6.4 eingeführt, mit der ein Benutzer SSHv2 konfigurieren kann. SSH wird auf einer zuverlässigen Transportschicht ausgeführt und bietet Funktionen für starke Authentifizierung und Verschlüsselung. Der einzige zuverlässige Transport, der für SSH definiert wird, ist TCP. SSH liefert Durchschnitte, auf Befehle auf einem anderen Computer oder Gerät über einem Netz sicher zuzugreifen und sicher durchzuführen. Das sichere Merkmal des Kopien-Protokolls (SCP), das über SSH einen Tunnel angelegt wird, lässt die sichere Übertragung von Dateien zu.

Wenn der Befehl ip ssh version 2 nicht explizit konfiguriert ist, aktiviert Cisco IOS XE SSH Version 1.99. SSH-Version 1,99 erlaubt Verbindungen SSHv1 und SSHv2. SSHv1 wird als unsicher betrachtet und kann nachteilige Wirkungen auf das System haben. Wenn SSH aktiviert ist, wird empfohlen, SSHv1 mithilfe des Befehls ip ssh version 2 zu deaktivieren.

Mit dieser Beispielkonfiguration wird SSHv2 (bei deaktiviertem SSHv1) auf einem Cisco IOS XE-Gerät aktiviert:

Hostname-Router

ip domain-name example.com

crypto key generate rsa modulus 2048

ip ssh timeout 60

ip ssh authentication-retries 3

ip ssh source-interface GigabitEthernet 0/1

IP SSH Version 2

Zeile vty 0 4

Transporteingabe SSH

Sprechen Sie sicheren Support Shell Versions 2 zu mehr Information über den Gebrauch SSHv2 an.

Verbesserungen SSHv2 für RSA-Tasten

Cisco IOS XE SSHv2 unterstützt interaktive Authentifizierungsmethoden über die Tastatur und kennwortbasierte Authentifizierungsmethoden. Die Verbesserungen SSHv2 für RSA-Hauptmerkmal unterstützt auch RSA-basierte Authentisierung der allgemeinen Taste für den Kunden und den Server.

Für Benutzerauthentisierung verwendet RSA-basierte Benutzerauthentisierung ein privates/allgemeines Schlüsselpaar, das mit jedem Benutzer für Authentisierung verbunden ist. Der Benutzer muss auf dem Client ein Paar aus privaten und öffentlichen Schlüsseln generieren und auf dem Cisco IOS XE SSH-Server einen öffentlichen Schlüssel konfigurieren, um die Authentifizierung abzuschließen.

Ein SSH-Benutzer, der versucht, die Bescheinigungen herzustellen, versieht eine verschlüsselte Unterzeichnung mit der privaten Taste. Die Unterzeichnung und die allgemeine Taste des Benutzers werden zum SSH-Server für Authentisierung geschickt. Der SSH-Server berechnet ein Hasch über der allgemeinen Taste, die vom Benutzer zur Verfügung gestellt wird. Das Hasch wird benutzt, um zu bestimmen, wenn der Server einen Eintrag hat, der abgleicht. Wenn eine Abgleichung gefunden wird, wird RSA-basierte Meldungsüberprüfung mit der allgemeinen Taste durchgeführt. Folglich wird der Benutzer beglaubigt, oder verweigerter Zugriff basiert auf der verschlüsselten Unterzeichnung.

Für die Serverauthentifizierung muss der Cisco IOS XE SSH-Client jedem Server einen Host-Schlüssel zuweisen. Wenn der Kunde versucht, eine SSH-Sitzung mit einem Server herzustellen, empfängt er die Unterzeichnung des Servers als Teil der Schlüsselaustauschmeldung. Wenn die Schlüsselprüfungsflagge des strengen Hauptrechners auf dem Kunden aktiviert wird, überprüft der Kunde, ob sie den Hauptrechnerschlüsseleintrag hat, der dem vorkonfigurierten Server entspricht. Wenn eine Abgleichung gefunden wird, versucht der Kunde, die Unterzeichnung mit der Serverhauptrechnertaste zu validieren. Wenn der Server erfolgreich authentifiziert wird, wird der Sitzungsaufbau fortgesetzt. Andernfalls wird er mit einer Meldung zu einer fehlgeschlagenen Serverauthentifizierung beendet.

Diese Beispielkonfiguration ermöglicht die Verwendung von RSA-Schlüsseln mit SSHv2 auf einem Cisco IOS XE-Gerät:

Konfigurieren eines Hostnamens für das Gerät

Hostname-Router

Konfigurieren eines Domänennamens

ip domain-name example.com

Aktivieren Sie den SSH-Server für die lokale und die Remote-Authentifizierung auf dem Router, der verwendet

den Befehl "crypto key generate".

Für SSH-Version 2 muss die Modulgröße mindestens 768 Bit betragen.

crypto key generate rsa usage-keys label sshkeys modulus 2048

Geben Sie den Namen des RSA-Schlüsselpaars (in diesem Fall "sshkeys") an, das für SSH verwendet werden soll.

ip ssh rsa keypair-name sshkeys

Konfigurieren Sie ein SSH-Timeout (in Sekunden).

Die nächste Ausgabe ermöglicht eine Zeitüberschreitung von 120 Sekunden für SSH-Verbindungen.

ip ssh timeout 120

Konfigurieren Sie eine Beschränkung auf fünf Authentifizierungsversuche.

ip ssh authentication-retries 5

Konfigurieren Sie SSH Version 2.

IP SSH Version 2

Sprechen Sie sichere Shell Version 2 Verbesserungen für RSA-Tasten zu mehr Information über den Gebrauch von RSA-Tasten mit SSHv2 an.

Mit dieser Beispielkonfiguration kann der Cisco IOS XE SSH-Server eine RSA-basierte Benutzerauthentifizierung durchführen. Die Benutzerauthentisierung ist erfolgreich, wenn die allgemeine Taste RSA, die auf dem Server gespeichert wird, mit der Öffentlichkeit oder den privaten Schlüsselpaaren überprüft wird, die auf dem Kunden gespeichert werden.

Konfigurieren Sie einen Hostnamen für das Gerät.

Hostname-Router

Konfigurieren eines Domänennamens

ip domain name cisco.com

Generieren Sie RSA-Schlüsselpaare mit einem Modul von 2048 Bit.

crypto key generate rsa modulus 2048

Konfigurieren Sie die SSH-RSA-Schlüssel für die Benutzer- und Serverauthentifizierung auf dem SSH-Server.

ip ssh pubkey-chain

Konfigurieren Sie den SSH-Benutzernamen.

Konfigurieren Sie die SSH-RSA-Schlüssel für die Benutzer- und Serverauthentifizierung auf dem SSH-Server.

ip ssh pubkey-chain

Konfigurieren Sie den SSH-Benutzernamen.

Benutzername ssh-user

Geben Sie den öffentlichen RSA-Schlüssel des Remote-Peer an.

Sie müssen dann entweder den Befehl key-string konfigurieren,

(gefolgt vom öffentlichen RSA-Schlüssel des Remote-Peers) oder

key-hash-Befehl (gefolgt vom Typ und der Version des SSH-Schlüssels).

Weitere Informationen zur Verwendung von RSA-Schlüsseln mit SSHv2 finden Sie unter Configuring the Cisco IOS XE SSH Server to Perform RSA-Based User Authentication (Konfigurieren des Cisco IOS XE SSH-Servers zur Durchführung einer RSA-basierten Benutzerauthentifizierung).

Mit dieser Beispielkonfiguration kann der Cisco IOS XE SSH-Client eine RSA-basierte Serverauthentifizierung durchführen.

Hostname-Router

ip domain-name cisco.com

Generieren Sie RSA-Schlüsselpaare.

Kryptografieschlüssel RSA generieren

Konfigurieren Sie die SSH-RSA-Schlüssel für die Benutzer- und Serverauthentifizierung auf dem SSH-Server.

ip ssh pubkey-chain

Aktivieren Sie den SSH-Server für die Authentifizierung mit dem öffentlichen Schlüssel auf dem Router.

Server SSH-Servername

Geben Sie den öffentlichen RSA-Schlüssel des Remote-Peers an.

Sie müssen dann entweder den Befehl key-string konfigurieren,

(gefolgt vom öffentlichen RSA-Schlüssel des Remote-Peers) oder

key-hash <Schlüsseltyp> <Schlüsselname> (gefolgt vom SSH-Schlüssel)

Typ und Version).

Stellen Sie sicher, dass die Serverauthentifizierung stattfindet. Die Verbindung ist

aufgrund eines Fehlers beendet.

ip ssh stricthostkeycheck

Weitere Informationen zur Verwendung von RSA-Schlüsseln mit SSHv2 finden Sie unter Configuring the Cisco IOS XE SSH Client to Perform RSA-Based Server Authentication (Konfigurieren des Cisco IOS XE SSH-Clients zum Durchführen einer RSA-basierten Serverauthentifizierung).

Konsole und ZUSATZkanäle

Bei Cisco IOS XE-Geräten sind Konsolen- und AUX-Ports asynchrone Leitungen, die für den lokalen und Remote-Zugriff auf ein Gerät verwendet werden können. Sie müssen beachten, dass Konsolenports auf Cisco Geräten über spezielle Berechtigungen verfügen. Insbesondere erlauben diese Privilegien einem Verwalter, die PasswortWiederherstellungsprozedur durchzuführen. Zwecks Passwortwiederanlauf durchzuführen, würde ein unauthenticated Angreifer Zugriff zum Konsolenkanal und zur Fähigkeit haben müssen Energie zum Gerät zu unterbrechen oder das Gerät zu veranlassen abzubrechen.

Jede mögliche Methode, die angewendet wird, um auf den Konsolenkanal eines Gerätes zuzugreifen, muss in gewissem Sinne gesichert werden, das der Sicherheit gleich ist, die für privilegierten Zugriff zu einem Gerät erzwungen wird. Die Methoden, die angewendet werden, um Zugriff zu sichern, müssen den Gebrauch von AAA, Leitprogrammunterbrechung und Modempasswörtern umfassen, wenn ein Modem zur Konsole befestigt wird.

Wenn keine Kennwortwiederherstellung erforderlich ist, kann ein Administrator die Möglichkeit entfernen, das Kennwortwiederherstellungsverfahren durchzuführen, das den globalen Konfigurationsbefehl no service password-recovery verwendet. Sobald jedoch der Befehl no

service password-recovery aktiviert wurde, kann ein Administrator die Kennwortwiederherstellung nicht mehr auf einem Gerät durchführen.

In den meisten Situationen muss der ZUSATZkanal eines Gerätes behindert sein, um unberechtigten Zugriff zu verhindern. Ein ZUSATZkanal kann mit diesen Befehlen deaktiviert werden:

Anschluss aux 0

Transporteingabe keine

Transportleistung keine

no exec exec-timeout 0 1

Kein Kennwort

Steuern Sie die vty und tty-Zeilen

Bei interaktiven Verwaltungssitzungen in der Cisco IOS XE Software wird ein tty oder virtual tty (vty) verwendet. Ein tty ist eine lokale asynchrone Zeile, zu der ein Terminal für lokalen Zugriff zum Gerät oder zu einem Modem für Wählleitung zu einem Gerät befestigt werden kann. Beachten Sie, dass ttys für Verbindungen zu den Konsolenkanälen anderer Geräte benutzt werden können. Diese Funktion lässt ein Gerät mit tty-Zeilen als ein Konsolenserver, in dem auftreten Verbindungen über dem Netz hergestellt werden können zu den Konsolenkanälen von den Geräten, die an die tty-Zeilen angeschlossen werden. Die tty-Zeilen für diese Rückverbindungen über dem Netz müssen kontrolliert auch sein.

Eine vty Zeile wird für alle weiteren Netzs- mit größerer geographischer Ausdehnungverbindungen benutzt, die durch das Gerät, unabhängig davon Protokoll unterstützt werden (SSH, SCP oder telnet sind Beispiele). Zwecks zu garantieren dass ein Gerät über eine Sitzung der lokalen oder Fernverwaltung erreicht werden kann, müssen richtige Kontrollen auf den vty und tty-Zeilen erzwungen werden. Cisco IOS XE-Geräte haben eine begrenzte Anzahl von vty-Leitungen. Die Anzahl der verfügbaren Leitungen kann mit dem Befehl show line EXEC bestimmt werden. Wenn alle vty Zeilen gebräuchlich sind, können neue Managementsitzungen nicht hergestellt werden, das eine DOS-Zugangsbedingung zum Gerät erstellt.

Das einfachste Formular der Zugriffssteuerung zu einem vty oder des tty eines Gerätes ist durch den Gebrauch von Authentisierung auf allen Zeilen unabhängig davon den Gerätstandort innerhalb des Netzes. Dieses ist für vty Zeilen kritisch, weil sie über das Netz zugänglich sind. Eine tty-Zeile, die an ein Modem angeschlossen wird, das für Fernzugriff zum Gerät benutzt wird oder eine tty-Zeile, die an den Konsolenkanal anderer Geräte angeschlossen wird, sind auch über das Netz zugänglich. Andere Formulare von vty und tty-Zugriffssteuerungen können mit dem Transportinput oder Zugriff-klasseden konfigurationsbefehlen, mit dem Gebrauch von den Merkmalen CoPP und CPPr erzwungen werden oder, wenn Sie Zugriffslisten an den Schnittstellen auf dem Gerät anwenden.

Authentisierung kann durch den Gebrauch AAA erzwungen werden, der die empfohlene Methode

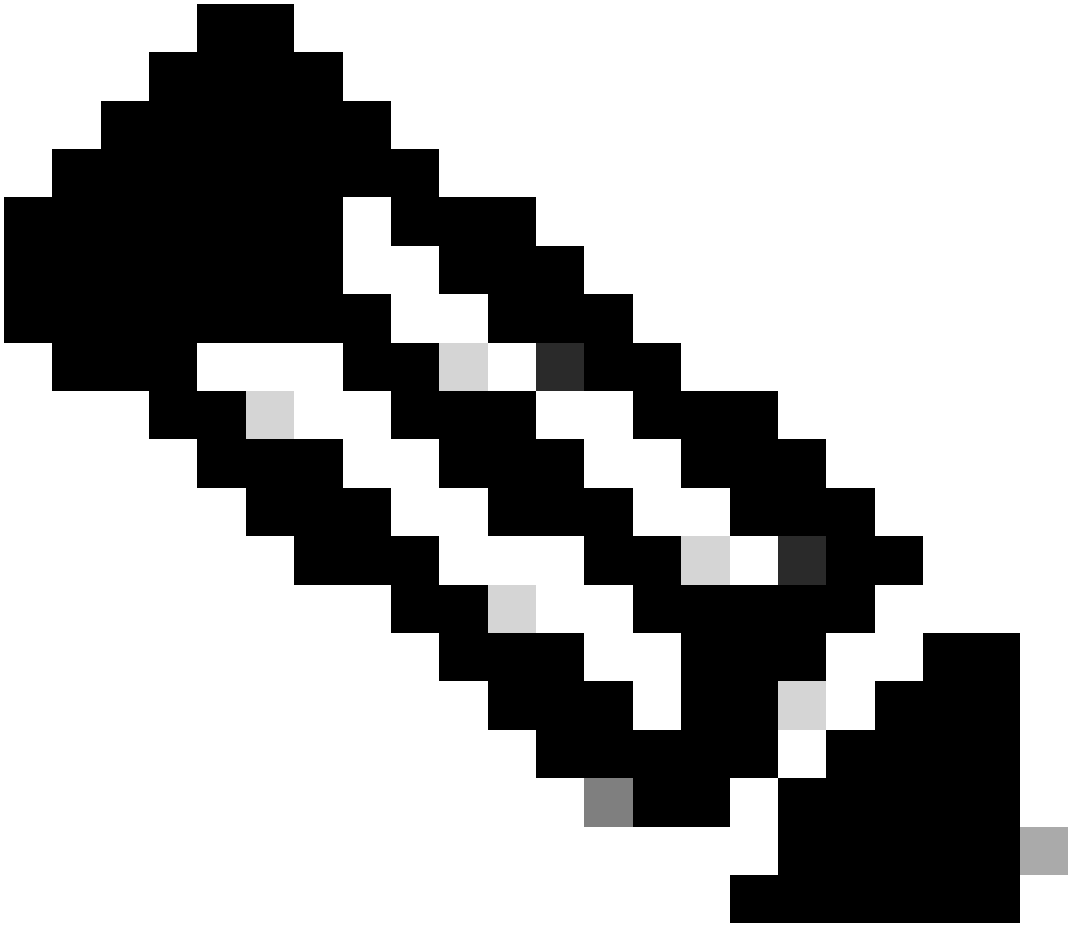
für beglaubigten Zugriff zu einem Gerät, mit dem Gebrauch von der lokalen Benutzerdatenbank oder durch die einfache Passwortauthentisierung ist, die direkt auf der vty oder tty-Zeile konfiguriert wird.

Der Leitprogrammunterbrechungsbefehl muss verwendet werden, um sich Sitzungen auf den vty oder tty-Zeilen auszuloggen, die untätig gelassen werden. Der Service TCP-keepalives-im Befehl muss auch verwendet werden, um TCP-Keepalives auf ankommenden Verbindungen zum Gerät zu aktivieren. Dadurch wird sichergestellt, dass das Gerät am Remote-Ende der Verbindung weiterhin zugänglich ist und halb offene oder verwaiste Verbindungen vom lokalen IOS-XE-Gerät entfernt werden.

Steuern Sie Transport für die vty und tty-Zeilen

Ein vty und tty können so konfiguriert werden, dass nur verschlüsselte und sichere Remote-Zugriffsmanagement-Verbindungen zum Gerät oder über das Gerät akzeptiert werden, wenn es als Konsolenserver verwendet wird. Dieses Kapitel adressiert ttys, weil solche Zeilen an Konsolenkanäle auf anderen Geräten angeschlossen werden können, die den tty über dem Netz zugänglich sein lassen. Um die Offenlegung von Informationen oder den unbefugten Zugriff auf die Daten zu verhindern, die zwischen dem Administrator und dem Gerät übertragen werden, kann anstelle von Klartext-Protokollen wie Telnet und rlogin die Transporteingabe ssh verwendet werden. Der Transport gab, das keine ein, kann Konfiguration auf einem tty aktiviert werden, der in Wirklichkeit den Gebrauch von der tty-Zeile für Rück-konsolenverbindungen deaktiviert.

erlauben vty und tty-Zeilen einem Verwalter, an andere Geräte anzuschließen. Zwecks den Typen des Transportes zu begrenzen den ein Verwalter für gehend Verbindungen benutzen kann, benutzen Sie die TransportAusgabeleitung Konfigurationsbefehl. Wenn keine ausgehenden Verbindungen benötigt werden, kann keine Transportausgabe verwendet werden. Wenn jedoch ausgehende Verbindungen zulässig sind, kann eine verschlüsselte und sichere Remote-Zugriffsmethode für die Verbindung mithilfe von Transport-Output-SSH durchgesetzt werden.



Hinweis: Sofern unterstützt, kann IPsec für verschlüsselte, sichere Remote-Zugriffsverbindungen zu einem Gerät verwendet werden. Wenn Sie IPSec verwenden, fügt es auch zusätzliche CPU-Unkosten dem Gerät hinzu. Jedoch muss SSH als der Transport noch erzwungen werden, selbst wenn IPSec verwendet wird.

Warnende Banner

In etwas Gerichtsbezirken zu verfolgen kann unmöglich sein und illegal, böswillige Benutzer zu überwachen, es sei denn, dass sie benachrichtigt worden sind, dass sie nicht die Erlaubnis gehabt werden, um das System zu benutzen. Eine Möglichkeit, diese Benachrichtigung bereitzustellen, besteht darin, diese Informationen in eine Bannermeldung zu schreiben, die mit dem Banner-Anmeldebefehl der Cisco IOS XE Software konfiguriert wurde.

Die gesetzlichen Mitteilungsanforderungen sind komplex, unterscheiden sich je nach Gerichtsbarkeit und Situation und können mit einem Rechtsbeistand besprochen werden. Sogar innerhalb der Rechtsprechungen, können sich Rechtsgutachten unterscheiden. In Zusammenarbeit mit Ratschlag kann ein Banner einiges oder alle diese Informationen zur

Verfügung stellen:

1. Beachten Sie, dass das System in protokolliert werden oder verwendet werden soll nur durch speziell berechtigtes Personal und möglicherweise Informationen über, wem Gebrauch autorisieren kann.
2. Beachten Sie, dass jede mögliche unbefugte Benutzung des Systems ungesetzlich ist und abhängig von den Zivil- und kriminellen Strafen sein kann.
3. Beachten Sie, dass jeder möglicher Gebrauch von dem System ohne weitere Ankündigung protokolliert werden oder überwacht werden kann und dass die resultierenden Logs als Beweis vor Gericht benutzt werden können.
4. Spezifische Begriffe benötigt durch örtliche Gesetze.

   Aus sicherheitstechnischer und nicht aus rechtlicher Sicht kann ein Anmeldebanner keine spezifischen Informationen über den Routernamen, das Modell, die Software oder den Besitzer des Routers enthalten. Diese Informationen können von den böswilligen Benutzern missbraucht werden.

Authentisierung, Ermächtigung und Buchhaltung

Der Authentisierungs-, Ermächtigungs- und Buchhaltungs(AAA) Rahmen ist kritisch, um interaktiven Zugriff zu den Netzgeräten zu sichern. Der aaa-Rahmen liefert eine in hohem Grade konfigurierbare Umgebung, die hergestellt werden kann basierte auf dem Bedarf des Netzes.

TACACS+-Authentisierung

TACACS+ ist ein Authentifizierungsprotokoll, das von Cisco IOS XE-Geräten für die Authentifizierung von Managementbenutzern gegenüber einem AAA-Remote-Server verwendet werden kann. Diese Managementbenutzer können über SSH, HTTPS, Telnet oder HTTP auf das IOS-XE-Gerät zugreifen.

TACACS+-Authentisierung oder im Allgemeinen AAA-Authentisierung, liefert die Fähigkeit, einzelnen Benutzer zu verwenden erklärt jeden Netzwerkadministrator. Wenn Sie nicht von einem einzelnen geteilten Passwort abhängen, wird die Sicherheit des Netzes verbessert und Ihre Verantwortlichkeit wird verstärkt.

RADIUS ist ein Protokoll, das TACACS+ ähnelt. Dabei wird jedoch nur das Kennwort verschlüsselt, das über das Netzwerk gesendet wird. Demgegenüber verschlüsselt TACACS+ die gesamte TCP-Nutzlast, die das username und Passwort einschließt. Aus diesem Grund kann TACACS+ anstelle von RADIUS verwendet werden, wenn TACACS+ vom AAA-Server unterstützt wird. Siehe TACACS+- und RADIUS-Vergleich für einen ausführlicheren Vergleich dieser zwei Protokolle.

Die TACACS+-Authentifizierung kann auf einem Cisco IOS XE-Gerät mit einer Konfiguration wie in diesem Beispiel aktiviert werden:

aaa neues Modell

aaa Authentifizierung Anmeldung Standardgruppe TACACS+

tacacs server <Servername>

address ipv4 <tacacs_server_ip_address>

Schlüssel <Schlüssel>

Die vorhergehende Konfiguration kann als Ausgangspunkt für eine Organisation-spezifische AAA-Authentisierungsschablone verwendet werden.

Eine Methodenliste ist eine sequenzielle Liste, die die, um einen beschreibt Benutzer zu beglaubigen abgefragt zu werden Authentisierungsmethoden. Methodenlisten aktivieren Sie, für Authentisierung verwendet zu werden Sicherheitsprotokolle zu kennzeichnen eine oder mehrere, und stellen folglich eine Ausweichanlage für Authentisierung sicher, falls die Anfangsmethode ausfällt. Die Cisco IOS XE Software verwendet die erste aufgelistete Methode, die einen Benutzer akzeptiert oder ablehnt. Folgende Methoden werden nur versucht, in den Fällen wo frühere Methoden wegen der Servernichtverfügbarkeit oder der falschen Konfiguration verlassen.

Sprechen Sie benannte Method Lists für Authentisierung zu mehr Information über die Konfiguration von benannter Method Lists an.

Authentisierungs-Reserve

Wenn alle konfigurierten TACACS+-Server nicht mehr verfügbar sind, kann sich ein Cisco IOS XE-Gerät auf sekundäre Authentifizierungsprotokolle verlassen. Typische Konfigurationen umfassen den Gebrauch des Einheimischen oder aktivieren Authentisierung, wenn alle konfigurierten TACACS+-Servers nicht verfügbar sind.

Die komplette Liste von Optionen für Aufgerätauthentisierung umfasst aktivieren, Einheimisches und Zeile. Jede dieser Optionen hat Vorteile. Der Gebrauch von dem Aktivierungsgeheimnis wird bevorzugt, weil das Geheimnis mit einem Einwegalgorithmus gehackt wird, der in sich selbst sicherer als der Verschlüsselungsalgorithmus ist, der mit dem Typen 7 Passwörter für Zeile oder lokale Authentisierung verwendet wird.

In Cisco IOS XE Software-Versionen, die die Verwendung geheimer Kennwörter für lokal definierte Benutzer unterstützen, kann jedoch ein Ausweichen auf die lokale Authentifizierung wünschenswert sein. Dieses darf einen lokal definierten Benutzer für eine oder mehrere Netzwerkadministratoren erstellt werden. Wenn TACACS+, vollständig nicht verfügbar zu werden waren, kann jeder Verwalter ihr lokales username und Passwort verwenden. Obgleich diese Aktion die Verantwortlichkeit von Netzwerkadministratoren in TACACS+-Ausfällen erhöht, erhöht sie erheblich die Verwaltungsbelastung, weil lokale Benutzerkonten auf allen Netzgeräten aufrechterhalten werden müssen.

Gestalten dieses Konfigurationsbeispiels nach dem vorhergehenden TACACS+-Authentisierungsbeispiel zwecks Reservenauthentisierung zum Passwort einschließen, das lokal mit dem geheimen Befehl des Aktivierunges konfiguriert wird:

enable secret <Kennwort>

aaa neues Modell

aaa authentication login default group tacacs+ enable

tacacs server <Servername>

address ipv4 <tacacs_server_ip_address>

Schlüssel <Schlüssel>

Sprechen Sie konfigurierende Authentisierung zu mehr Information über den Gebrauch von Reservenauthentisierung mit AAA an.

Gebrauch von Typen 7 Passwörter

Ursprünglich konzipiert, um schnelle Dekodierung von gespeicherten Passwörtern zu erlauben, sind Typ 7 Passwörter kein sicheres Formular des Passwortspeichers. Es gibt viele verfügbaren Werkzeuge, die diese Passwörter leicht entschlüsseln können. Die Verwendung von Typ-7-Passwörtern kann vermieden werden, es sei denn, dies ist aufgrund einer Funktion erforderlich, die auf dem Cisco IOS XE-Gerät verwendet wird.

Typ 9 (Verschlüsselung) kann nach Möglichkeit immer verwendet werden:

username <benutzername> privilege 15 algorithmus-type scrypt secret <geheim>

Der Abbau von Passwörtern dieses Typen kann durch AAA-Authentisierung und den Gebrauch von dem erhöhten Passwort-Sicherheitsmerkmal erleichtert werden, das erlaubt, dass geheime Passwörter mit Benutzern verwendet werden, die lokal über den globalen Konfigurationsbefehl username definiert werden. Wenn Sie den Gebrauch von Typen 7 Passwörter nicht völlig verhindern können, betrachten Sie diese Passwörter als verdunkelt, nicht verschlüsselt.

Sehen Sie das flache Verhärtungskapitel der Geschäftsleitung dieses Dokuments zu mehr Information über den Abbau des Typen 7 Passwörter.

TACACS+-Befehls-Ermächtigung

Befehlsermächtigung mit TACACS+ und AAA liefert einen Mechanismus, der ermöglicht oder verweigert jeden Befehl, der von einem Verwaltungsbenutzer eingegeben wird. Wenn der Benutzer EXEC-Befehle eingibt, sendet Cisco IOS XE jeden Befehl an den konfigurierten AAA-Server. Der aaa-Server verwendet dann seine konfigurierte Politik, um den Befehl für diesen bestimmten Benutzer zu ermöglichen oder zu verweigern.

Diese Konfiguration kann dem vorhergehenden AAA-Authentisierungsbeispiel hinzugefügt werden, um Befehlsermächtigung einzuführen:

aaa, Autorisierung, exec, Standardgruppe, TACACS+ keine

aaa, Autorisierungsbefehle 0 default group tacacs+ none

aaa, Autorisierungsbefehle 1 Standardgruppentaka+ keine

aaa, Autorisierungsbefehle 15 Standardgruppentaketen+ keine

Sprechen Sie konfigurierende Ermächtigung zu mehr Information über Befehlsermächtigung an.

TACACS+-Befehls-Buchhaltung

Wenn sie konfiguriert wird, sendet AAA-Befehlsbuchhaltung Informationen über jeden Bedienungsaufruf an den Ablaufteil, der zu den konfigurierten TACACS+-Servers eingegeben wird. Die Informationen, die zum TACACS+-Server geschickt werden, umfassen den durchgeführten Befehl, das Datum, die er durchgeführt wurde und das username des Benutzers, der den Befehl eingibt. Befehlsbuchhaltung wird nicht mit RADIUS unterstützt.

Diese Beispielkonfiguration aktiviert AAA-Befehl die erklärenden Bedienungsaufrufe an den Ablaufteil, die auf Privilegstufen null, eine und 15 eingegeben werden. Gestalten dieser Konfiguration nach vorhergehenden Beispielen, die Konfiguration der TACACS-Servers umfassen.

aaa accounting exec default start-stop group tacacs+

aaa accounting-Befehle 0 default start-stop group tacacs+

aaa accounting-Befehle 1 standardmäßige Start-Stopp-Gruppe tacacs+

aaa accounting-Befehle 15 standardmäßige Start-Stopp-Gruppe tacacs+

Siehe das Konfigurieren, mehr Informationen über die Konfiguration von AAA-Buchhaltung ausmachend.

Überflüssige AAA-Servers

Die in einer Umgebung genutzten AAA-Server können redundant und fehlertolerant bereitgestellt werden. Dieses hilft, zu garantieren, dass interaktiver Managementzugriff, wie SSH, möglich ist, wenn ein AAA-Server nicht verfügbar ist.

Wenn Sie eine überflüssige AAA-Serverlösung konzipieren oder einführen, erinnern Sie sich an diese Erwägungen:

1. Verfügbarkeit von AAA-Servers während der möglichen Netzstörungen
2. Geographisch zerstreute Platzierung von AAA-Servers
3. Laden Sie auf einzelnen AAA-Servers im Dauerzustand und in den Bruchbedingungen
4. Netzlatenzzeit zwischen Netzzugang-Servers und AAA-Servers
5. Aaa-Serverdatenbank- Synchronisierung

Sprechen Sie einsetzen die Zugriffssteuerungs-Servers zu mehr Information an.

Verstärken Sie das Simple Network Management Protocol

In diesem Abschnitt werden verschiedene Methoden beschrieben, mit denen die Bereitstellung von SNMP auf IOS-XE-Geräten abgesichert werden kann. Es ist kritisch, dass SNMP richtig gesichert wird, um die Vertraulichkeit, die Integrität und die Verfügbarkeit der Netzdaten und der Netzgeräte zu schützen, durch die diese Daten durchfahren. SNMP versieht Sie mit einer Fülle von Informationen auf der Gesundheit von Netzgeräten. Diese Informationen können vor böswilligen Benutzern geschützt werden, die diese Daten für Angriffe auf das Netzwerk nutzen möchten.

SNMP-Gemeinschaftszeichenketten

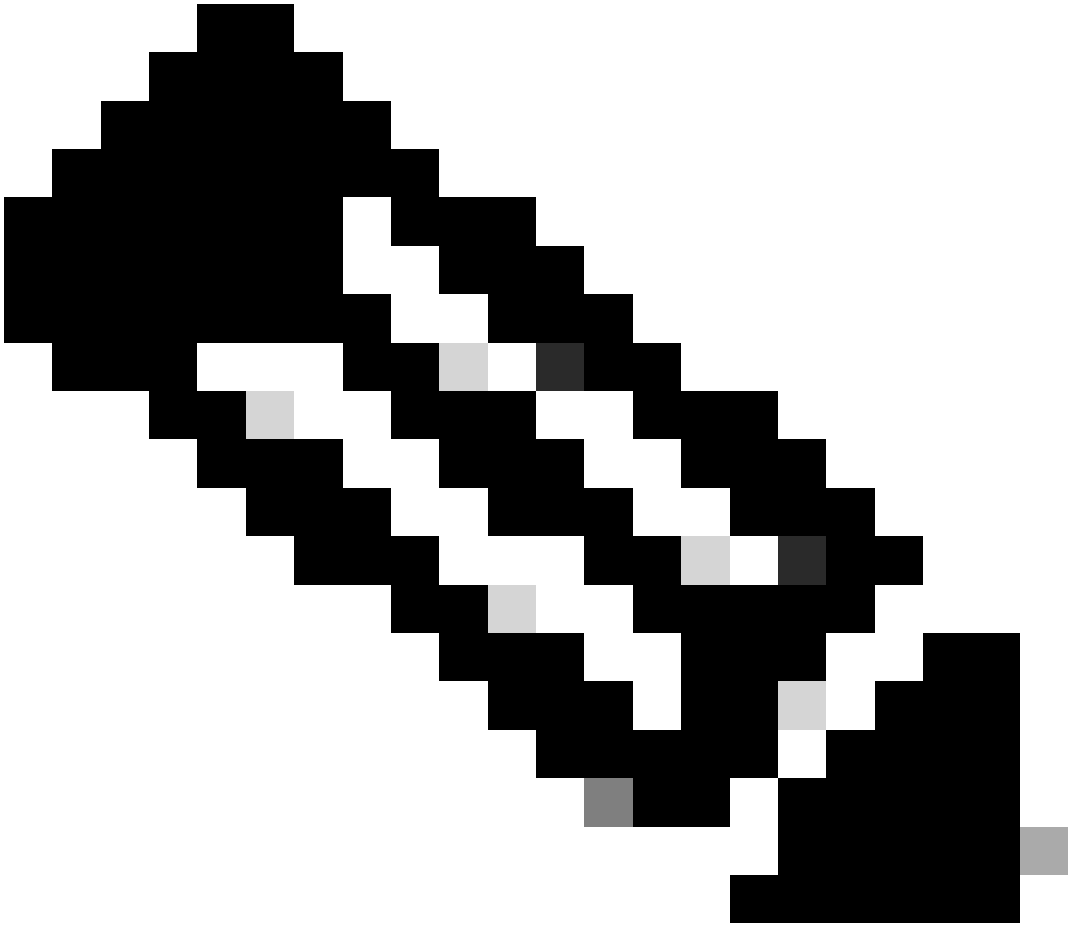
Community-Strings sind Kennwörter, die auf ein IOS-XE-Gerät angewendet werden, um den schreibgeschützten und den schreibgeschützten Zugriff auf die SNMP-Daten auf dem Gerät zu beschränken. Diese Community-Strings können, wie bei allen Passwörtern, sorgfältig ausgewählt werden, um sicherzustellen, dass sie nicht trivial sind. Community-Strings können in regelmäßigen Abständen und in Übereinstimmung mit Netzwerksicherheitsrichtlinien geändert werden.

Beispielsweise können die Zeichenfolgen geändert werden, wenn ein Netzwerkadministrator die Rolle ändert oder das Unternehmen verlässt.

Diese Konfigurationszeilen konfigurieren eine Read-only-Gemeinschaftszeichenkette von READ-ONLY und eine Lese-Schreibgemeinschaftszeichenkette von LESE-SCHREIB:

snmp-server community READONLY RO

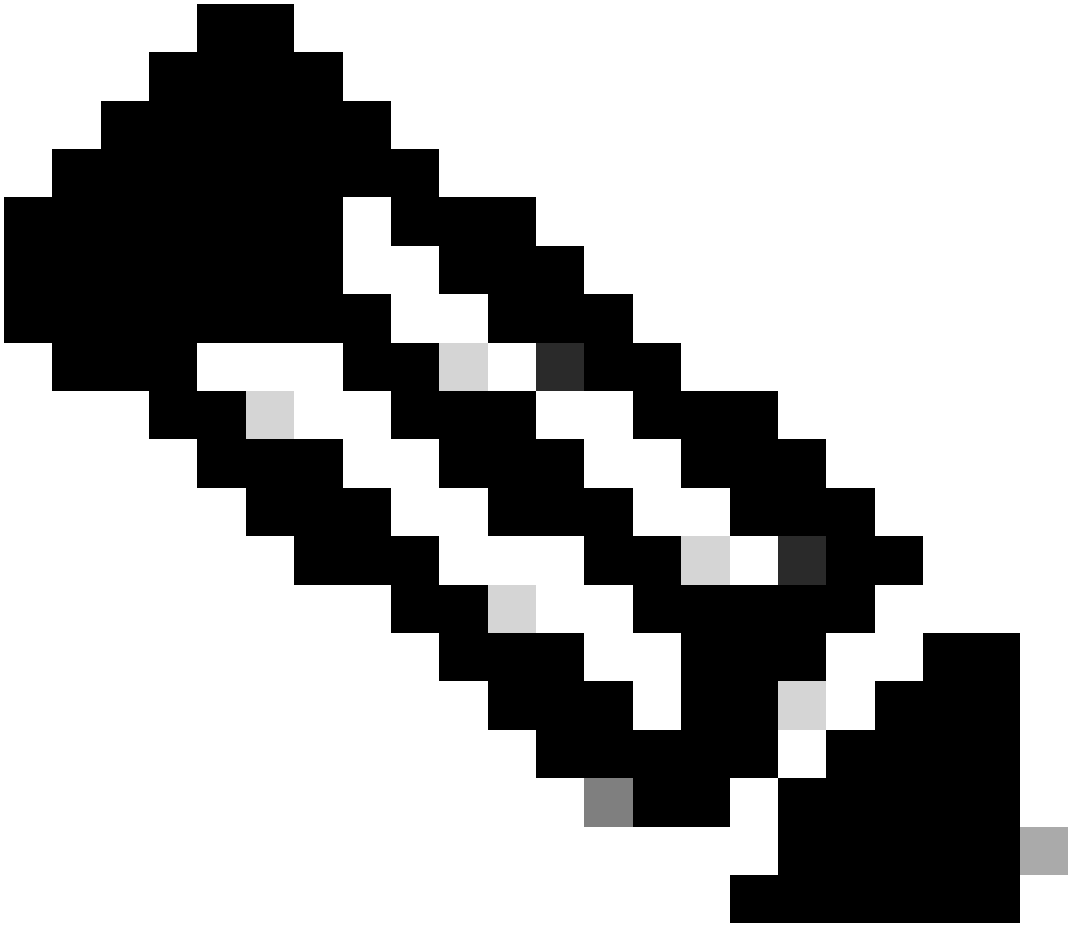
snmp-server community READWRITE RW



Hinweis: Die vorherigen Community-Stringbeispiele wurden ausgewählt, um die Verwendung dieser Strings klar zu erklären. In Produktionsumgebungen können Community-Strings mit Vorsicht ausgewählt werden und aus einer Reihe alphabetischer, numerischer und nicht alphanumerischer Symbole bestehen. Siehe Empfehlungen für das Erstellen von starken Passwörtern zu mehr Information über die Auswahl von nicht trivialen Passwörtern.

SNMP-Gemeinschaftszeichenketten mit ACLs

Zusätzlich zum Community-String kann eine ACL angewendet werden, die den SNMP-Zugriff weiter auf eine ausgewählte Gruppe von Quell-IP-Adressen beschränkt. Mit dieser Konfiguration wird der schreibgeschützte SNMP-Zugriff auf End-Host-Geräte im Adressbereich 192.168.100.0/24 und der schreibgeschützte SNMP-Zugriff auf das End-Host-Gerät unter 192.168.100.1 beschränkt.



Hinweis: Für die Geräte, die von diesen ACLs zugelassen werden, ist der korrekte Community String erforderlich, um auf die angeforderten SNMP-Informationen zugreifen zu können.

access-list 98 permit 192.168.100.0 0.0.0.255

access-list 99 permit 192.168.100.1

snmp-server community READONLY RO 98

snmp-server community READWRITE RW 99

Weitere Informationen zu dieser Funktion finden Sie in der snmp-server-Community in der Cisco IOS XE Network Management Command Reference.

Infrastruktur ACLs

Infrastruktur-ACLs (iACLs) können bereitgestellt werden, um sicherzustellen, dass nur End-Hosts

mit vertrauenswürdigen IP-Adressen SNMP-Datenverkehr an ein IOS-XE-Gerät senden können. Eine iACL kann eine Richtlinie enthalten, die nicht autorisierte SNMP-Pakete auf dem UDP-Port 161 verweigert.

Weitere Informationen zur Verwendung von iACLs finden Sie im Abschnitt Beschränken des Zugriffs auf das Netzwerk mit Infrastruktur-ACLs in diesem Dokument.

SNMP-Ansichten

SNMP-Ansichten sind ein Sicherheitsmerkmal, das Zugriff zu bestimmtem SNMP MIBs ermöglichen oder verweigern kann. Nachdem eine Ansicht erstellt und mit den Befehlen snmp-server community string view global configuration auf einen Community String angewendet wurde, sind Sie beim Zugriff auf MIB-Daten auf die von der Ansicht definierten Berechtigungen beschränkt. Wenn passend, werden Sie geraten, Ansichten zu verwenden, um Benutzer von SNMP auf die Daten zu begrenzen, die sie fordern.

Dieses Konfigurationsbeispiel schränkt SNMP-Zugriff mit der Gemeinschaftszeichenkette ein, die zu den MIB-Daten BEGRENZT ist, die in der Systemgruppe ist:

snmp-server view <view_name> <mib_view_family_name> [include/exclude]

snmp-server community <community_string>view <view_name> RO

Sprechen Sie konfigurierenden SNMP-Support zu mehr Information an.

SNMP-Version 3

SNMP-Version 3 (SNMPv3) wird durch RFC3410, RFC3411, RFC3412, RFC3413, RFC3414 und RFC3415 definiert und ist ein dialogfähiges Standard-basiertes Protokoll für Netzführung. SNMPv3 bietet sicheren Zugang zu den Geräten, weil es beglaubigt und beliebig Pakete über dem Netz verschlüsselt. Wo unterstützt, kann SNMPv3 verwendet werden, um eine andere Schicht Sicherheit hinzuzufügen, wenn Sie SNMP einsetzen. SNMPv3 besteht aus drei Primärkonfigurationsoptionen:

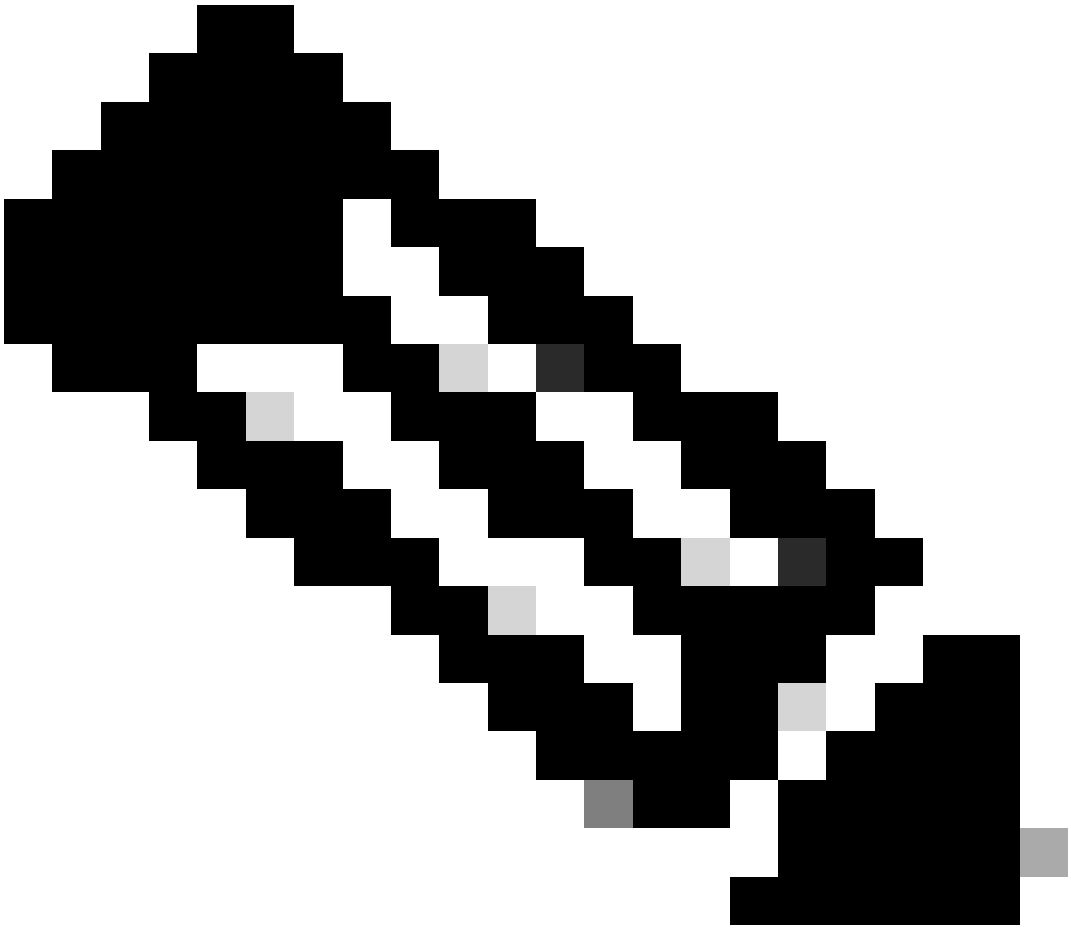
1. no auth - Dieser Modus erfordert keine Authentifizierung oder Verschlüsselung von SNMP-Paketen.
2. auth - Dieser Modus erfordert die Authentifizierung des SNMP-Pakets ohne Verschlüsselung.
3. priv - Dieser Modus erfordert sowohl Authentifizierung als auch Verschlüsselung (Datenschutz) jedes SNMP-Pakets.

   Es muss eine autoritative Engine-ID vorhanden sein, damit die SNMPv3-Sicherheitsmechanismen für Authentifizierung oder Authentifizierung und Verschlüsselung zur Verarbeitung von SNMP-Paketen verwendet werden können. Standardmäßig wird die Engine-ID lokal generiert. Die Maschine Identifikation kann mit dem Show-SNMP-engineID Befehl wie in diesem Beispiel gezeigt angezeigt werden:

   router#show snmp-Modul-ID

Lokale SNMP-Modul-ID: 800000090300000152BD35496

Remote Engine ID IP-Adresse-Port



> Hinweis: Wenn der Wert von engineID geändert wird, müssen alle SNMP-Benutzerkonten neu konfiguriert werden.

Der nächste Schritt ist, eine Gruppe SNMPv3 zu konfigurieren. Mit diesem Befehl wird ein Cisco IOS XE-Gerät für SNMPv3 mit einer SNMP-Servergruppe AUTHGROUP konfiguriert und nur die Authentifizierung für diese Gruppe mit dem Schlüsselwort auth aktiviert:

snmp-server group AUTHGROUP v3 auth

Mit diesem Befehl wird ein Cisco IOS XE-Gerät für SNMPv3 mit einer SNMP-Servergruppe konfiguriert.

PRIVGROUP und aktiviert sowohl Authentifizierung als auch Verschlüsselung für diese Gruppe mit dem priv-Schlüsselwort:

snmp-server gruppe PRIVGROUP v3 priv

Dieser Befehl konfiguriert einen SNMPv3 Benutzer snmpv3user mit einem Passwort der Authentisierung MD5 von authpassword und einem Passwort der Verschlüsselung 3DES von privpassword:

snmp-server benutzer snmpv3user PRIVGROUP v3 auth md5 authpassword priv 3des privpassword

Beachten Sie, dass die snmp-server-Benutzerkonfigurationsbefehle nicht wie in RFC 3414 vorgeschrieben in der Konfigurationsausgabe des Geräts angezeigt werden. Das Benutzerkennwort kann daher in der Konfiguration nicht angezeigt werden. Zwecks die konfigurierten Benutzer anzusehen, geben Sie den Show-SNMP-Benutzerbefehl wie in diesem Beispiel gezeigt ein:

router#show snmp-benutzer

Benutzername: snmpv3user Modul-ID: 800000090300000152BD35496

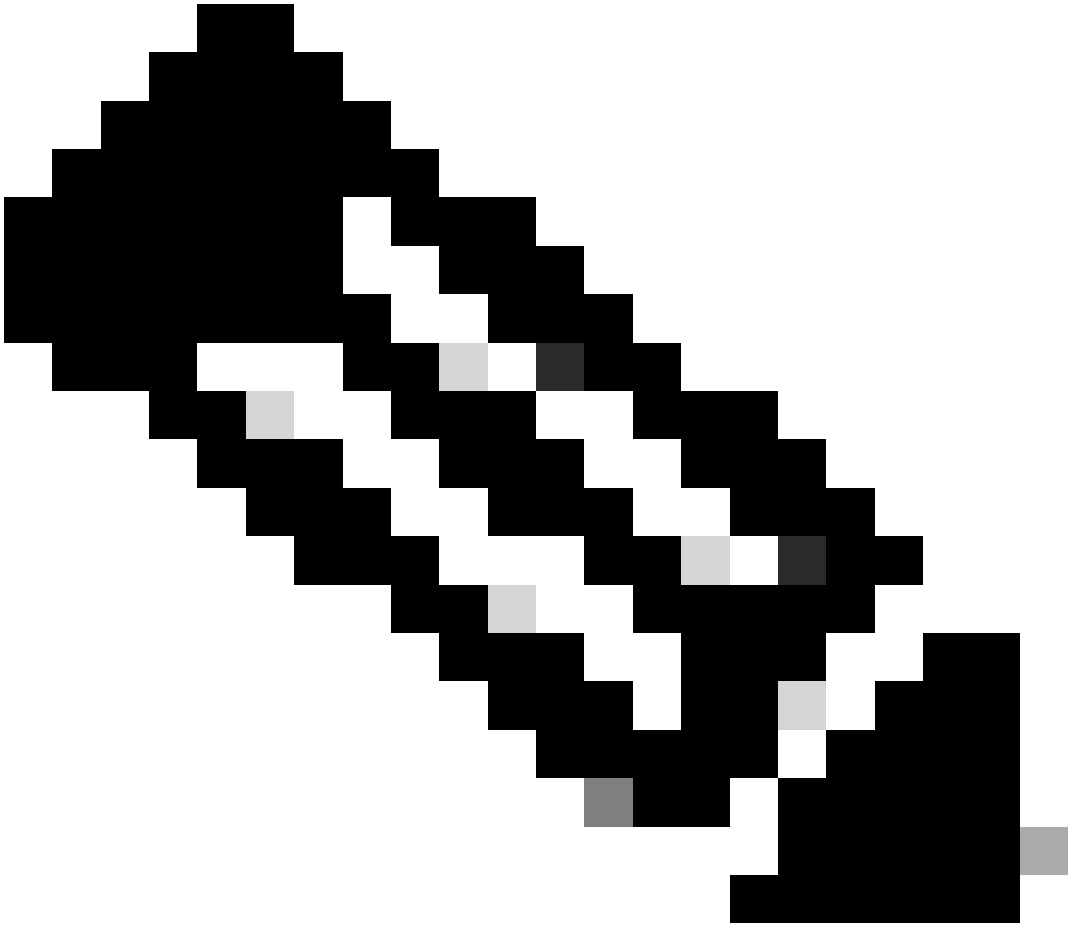
Speichertyp: nicht flüchtig aktiv

Authentifizierungsprotokoll: MD5
Datenschutzprotokoll: 3DES
Gruppenname: PRIVGROUP

Sprechen Sie konfigurierenden SNMP-Support zu mehr Information über dieses Merkmal an.

Management-flacher Schutz

Die Funktion zum Schutz der Verwaltungsebene (MPP) der Cisco IOS XE Software kann verwendet werden, um SNMP zu schützen, da sie die Schnittstellen einschränkt, über die SNMP-Datenverkehr auf dem Gerät terminiert werden kann. Das mpp-Merkmal erlaubt einem Verwalter, eine oder mehrere Schnittstellen als Managementschnittstellen zu kennzeichnen. Managementverkehr wird die Erlaubnis gehabt, um ein Gerät nur durch diese Managementschnittstellen einzutragen. Nachdem MPP aktiviert ist, keine Schnittstellen, ausgenommen gekennzeichnete Managementschnittstellen Netzführungsverkehr annehmen, der zum Gerät vorgesehen wird.



Hinweis: MPP ist ein Teil der CPPr-Funktion und erfordert eine IOS-Version, die CPPr unterstützt. Siehe Verständnis des Steuerflachen Schutzes zu mehr Information über CPPr.

In diesem Beispiel wird MPP verwendet, um SNMP- und SSH-Zugriff nur zum FastEthernet einzuschränken 0/0 Schnittstelle:

Control-Plane-Host

management-interface FastEthernet0/0 allow ssh snmp

Sprechen Sie Management-flache Schutz-Merkmals-Anleitung zu mehr Information an.

Protokollierende optimale Verfahren

Durch die Ereignisprotokollierung erhalten Sie einen Überblick über den Betrieb eines Cisco IOS XE-Geräts und über das Netzwerk, in dem es bereitgestellt wird. Die Cisco IOS XE Software bietet

verschiedene flexible Protokollierungsoptionen, mit denen die Netzwerkmanagement- und Transparenzziele eines Unternehmens erreicht werden können.

In diesen Abschnitten werden einige grundlegende Best Practices für die Protokollierung beschrieben, mit denen ein Administrator die Protokollierung erfolgreich nutzen und die Auswirkungen der Protokollierung auf ein Cisco IOS XE-Gerät minimieren kann.

Schicken Sie Logs zu einem zentralen Standort

Sie werden geraten, protokollierende Informationen zu einem Fernsyslog-Server zu schicken. Dieses macht es möglich, effektiv aufeinander zu beziehen und Revisionsnetz- und -sicherheitsereignisse über Netzgeräten. Beachten Sie, dass Syslog-Meldungen unzuverlässig von UDP und in Klartext übertragen werden. Aus diesem Grund können alle Schutzmaßnahmen, die ein Netzwerk für den Managementverkehr bietet (z. B. Verschlüsselung oder Out-of-Band-Zugriff), erweitert werden, um Syslog-Datenverkehr einzubeziehen.

In diesem Konfigurationsbeispiel wird ein Cisco IOS XE-Gerät konfiguriert, um Protokollinformationen an einen Remote-Syslog-Server zu senden:

logging host <IP-Adresse>

Weitere Informationen zur Protokollkorrelation finden Sie unter Identifying Incidents Using Firewall and IOS-XE Router Syslog Events (Identifizierung von Vorfällen mit Firewall- und IOS-XE-Router-Syslog-Ereignissen).

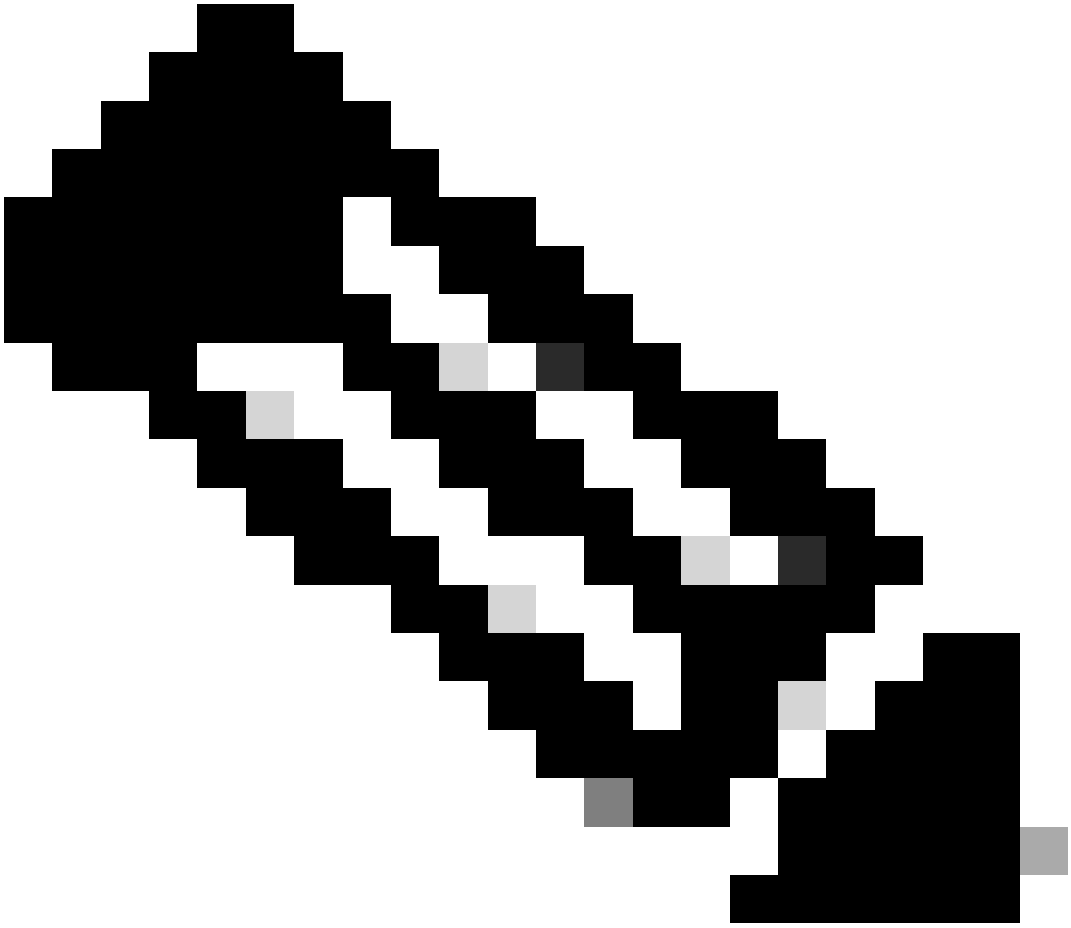
Die Funktion "Protokollierung bei lokalem nichtflüchtigem Speicher (ATA-Festplatte)" ermöglicht das Speichern von Systemprotokollierungsmeldungen auf einer Flash-Festplatte mit erweitertem Technologieanhang (ATA). Die Meldungen, die auf einem ATA-Laufwerk gesichert werden, bestehen weiter, nachdem ein Router neu geladen ist.

Mit diesen Konfigurationszeilen werden 134.217.728 Byte (128 MB) an Protokollmeldungen im Syslog-Verzeichnis des ATA-Flash-Laufwerks (disk0) konfiguriert. Außerdem wird eine Dateigröße von 16.384 Byte festgelegt:

logging buffered.

logging persistent url disk0:/syslog größe 134217728 dateigröße 16384

Bevor Protokollmeldungen in eine Datei auf dem ATA-Laufwerk geschrieben werden, überprüft die Cisco IOS XE Software, ob genügend Festplattenspeicher vorhanden ist. Wenn nicht, wird die älteste Datei von protokollierenden Meldungen (durch Zeitstempel) und die aktive Datei wird gesichert gelöscht. Das Format für den Dateinamen lautet Protokoll_Monat:Tag:Jahr::Zeit.



Hinweis: Ein ATA-Flash-Laufwerk hat nur begrenzten Speicherplatz und muss daher gewartet werden, um eine Überlastung gespeicherter Daten zu vermeiden.

Dieses Beispiel zeigt, wie man protokollierende Meldungen von der grellen Platte des Routers ATA zu einer externen Platte auf ftp server 192.168.1.129 als Teil der Instandhaltungsverfahren kopiert:

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

Weitere Informationen zu dieser Funktion finden Sie unter Protokollierung bei lokalem nichtflüchtigem Speicher.

Protokollierende Stufe

Jeder von einem Cisco IOS XE-Gerät generierten Protokollmeldung wird einer von acht Schweregraden zugewiesen, die von Stufe 0, Notfälle bis Stufe 7, Debuggen reichen. Es wird empfohlen, die Protokollierung auf Stufe 7 zu vermeiden, sofern dies nicht ausdrücklich

erforderlich ist. Protokollierung auf Ebene 7 erzeugt eine erhöhte CPU-Last auf dem Gerät, die zu Geräte- und Netzwerkinstabilität führen kann.

Die globale protokollierende Stufe des Konfigurationsbefehls Blockierwird benutzt, um zu spezifizieren, welche protokollierenden Meldungen zu Fernsyslog-Servers geschickt werden. Die spezifizierte Stufe zeigt die niedrigste Schweremeldung an, die gesendet wird. Für das gepufferte Protokollieren wird der protokollierende gepufferte waagerecht ausgerichtete Befehl verwendet.

Dieses Konfigurationsbeispiel begrenzt Logmeldungen, die zu Fernsyslog-Servers und zum lokalen Logbuffer zu den severities 6 (informatorisch) durch 0 geschickt werden (Not-):

Protokollierungsfalle 6

Protokollierung gepuffert 6

Protokollieren Sie nicht, um zu trösten oder Monitorläufe

Mit der Cisco IOS XE Software ist es möglich, Protokollmeldungen zur Überwachung von Sitzungen - Überwachungssitzungen sind interaktive Verwaltungssitzungen, in denen der EXEC-Befehl Terminal Monitor ausgegeben wurde - und zur Konsole zu senden. Dies kann jedoch die CPU-Last eines IOS-XE-Geräts erhöhen und wird daher nicht empfohlen. Stattdessen werden Sie geraten, protokollierende Informationen zum lokalen Logbuffer zu schicken, der mit dem protokollierenden Befehl der Show angesehen werden kann.

Verwenden Sie die globalen Konfigurationsbefehle keine protokollierende Konsole und kein protokollierender Monitor, um das Protokollieren zur Konsole und zu den Monitorläufen zu deaktivieren. Dieses Konfigurationsbeispiel zeigt den Gebrauch von diesen Befehlen:

Keine Protokollkonsole

Keine Protokollierungsüberwachung

Weitere Informationen zu globalen Konfigurationsbefehlen finden Sie in der Cisco IOS XE Network Management Command Reference.

Verwenden Sie das gepufferte Protokollieren

Die Cisco IOS XE Software unterstützt die Verwendung eines lokalen Protokollpuffers, sodass ein Administrator lokal generierte Protokollmeldungen anzeigen kann. Der Gebrauch von gepuffertem Protokollieren wird in hohem Grade gegen das Protokollieren entweder in den Konsolen- oder Monitorläufen empfohlen.

Für die Konfiguration der gepufferten Protokollierung gibt es zwei relevante Konfigurationsoptionen: die Größe des Protokollierungspuffers und die Nachrichtenschweregrade, die im Puffer gespeichert werden. Die Größe des protokollierenden Buffers wird mit der globalen protokollierenden Puffergröße des Konfigurationsbefehls konfiguriert. Die niedrigste Schwere, die im Buffer eingeschlossen ist, wird mit dem protokollierenden gepufferten Schwerebefehl konfiguriert. Ein Verwalter ist in der Lage, den Inhalt des protokollierenden Buffers durch den

Show protokollierenden Bedienungsaufruf an den Ablaufteil anzusehen.

Dieses Konfigurationsbeispiel umfasst die Konfiguration eines protokollierenden Buffers von 16384 Bytes sowie eine Schwere von 6, informatorisch, die anzeigt, dass Meldungen auf Stufen 0 (Not-) durch 6 (informatorisch) gespeichert wird:

Protokollierung gepuffert 16384 6

Weitere Informationen zur gepufferten Protokollierung finden Sie unter Cisco IOS XE Einstellen des Nachrichtenanzeige-Zielgeräts.

Konfigurieren Sie protokollierende Quellschnittstelle

Zwecks ein erhöhtes Niveau der Übereinstimmung zur Verfügung zu stellen wenn Sie Logmeldungen sammeln und wiederholen, werden Sie geraten eine protokollierende Quellschnittstelle statisch zu konfigurieren.

Wird der Befehl logging source-interface interface (Protokollierungsschnittstelle) verwendet, stellt die statische Konfiguration einer Protokollierungsschnittstelle sicher, dass in allen Protokollierungsmeldungen, die von einem einzelnen Cisco IOS-Gerät gesendet werden, dieselbe IP-Adresse angezeigt wird. Für hinzugefügte Stabilität werden Sie geraten, eine Schleifenbetriebschnittstelle als die protokollierende Quelle zu benutzen.

Dieses Konfigurationsbeispiel veranschaulicht den Gebrauch von dem protokollierenden globalen Konfigurationsbefehl der Quelleschnittstellenschnittstelle, um zu spezifizieren, dass das IP address der Schnittstelle des Schleifenbetriebs 0 für alle Logmeldungen verwendet wird:

Logging Source-Interface Loopback 0

Weitere Informationen finden Sie im integrierten Syslog-Manager von Cisco IOS XE.

Konfigurieren Sie protokollierende Zeitstempel

Die Konfiguration von protokollierenden Zeitstempeln hilft Ihnen, Ereignisse über Netzgeräten aufeinander zu beziehen. Es ist wichtig, eine korrekte und konsequente protokollierende Zeitstempelkonfiguration einzuführen, zu garantieren, dass Sie in der Lage sind, Journaldaten aufeinander zu beziehen. Protokollierungszeitstempel können so konfiguriert werden, dass Datum und Uhrzeit mit einer Genauigkeit von Millisekunden und die auf dem Gerät verwendete Zeitzone einbezogen werden.

Dieses Beispiel umfasst die Konfiguration von protokollierenden Zeitstempeln mit Millisekundenpräzision innerhalb der koordinierten Zone der Weltzeit (UTC):

service timestamps log datetime msec show-timezone

Wenn Sie, es vorziehen Zeiten nicht im Verhältnis zu UTC zu protokollieren, können Sie eine spezifische Ortszeitzone konfigurieren und diese Informationen konfigurieren, um in festgelegten Logmeldungen anwesend zu sein. Dieses Beispiel zeigt eine Geräteausstattung für die Zone der pazifischen Standardzeit (PST):

Zeitzone PST -8

service timestamps log datetime msec localtime show-timezone

Cisco IOS XE Software-Konfigurationsmanagement

Die Cisco IOS XE Software umfasst mehrere Funktionen, die eine Form des Konfigurationsmanagements auf einem Cisco IOS XE-Gerät ermöglichen. Solche Merkmale umfassen Funktionalität, um Konfigurationen und zur Preissenkung die Konfiguration zu einer vorhergehenden Version zu archivieren sowie ein ausführliches Konfigurationsänderungslog herzustellen.

Konfiguration ersetzen und Konfigurations-Preissenkung

In Cisco IOS XE Software, Version 16.6.4 und höher, ermöglichen Ihnen die Funktionen "Configuration Replace" (Konfigurationsersatz) und "Configuration Rollback" (Konfigurations-Rollback) die Archivierung der Cisco IOS XE-Gerätekonfiguration auf dem Gerät. Manuell oder automatisch gespeichert, können die Konfigurationen in diesem Archiv verwendet werden, um die aktuelle laufende Konfiguration durch das Konfigurierung zu ersetzen ersetzen Dateinamebefehl. Dieses ist im Gegensatz zu dem Kopiendateiname AusführenConfigbefehl. Das Konfigurierung ersetzen Dateinamebefehl ersetzt die laufende Konfiguration im Gegensatz zu dem Merge, das durch die Kopieanweisung durchgeführt wird.

Es wird empfohlen, diese Funktion auf allen Cisco IOS XE-Geräten im Netzwerk zu aktivieren. Sobald aktiviert, kann ein Verwalter die aktuelle laufende Konfiguration veranlassen, dem Archiv mit dem Archiv Config privilegierten Bedienungsaufruf an den Ablaufteil hinzugefügt zu werden. Die archivierten Konfigurationen können mit dem Showarchiv Bedienungsaufruf an den Ablaufteil angesehen werden.

Dieses Beispiel veranschaulicht die Konfiguration der automatischen Konfigurationsarchivierung. Außerdem wird das Cisco IOS XE-Gerät angewiesen, archivierte Konfigurationen als Dateien namens archived-config-N auf dem Dateisystem disk0: zu speichern, maximal 14 Sicherungen zu verwalten und einmal täglich (1440 Minuten) zu archivieren, wenn ein Administrator den Befehl write memory EXEC ausgibt.

Archiv

Pfad disk0:archivierte Konfiguration

max. 14

Zeitraum 1440

Obgleich die Konfigurationsarchivfunktionalität bis 14 Backup-Konfigurationen speichern kann, werden Sie geraten, den Platzbedarf zu betrachten, bevor Sie den maximalen Befehl verwenden.

Exklusiver Konfigurations-Änderungs-Zugriff

Zusätzlich zur Cisco IOS XE Software-Version 16.6.4 stellt die Funktion für den exklusiven Zugriff auf Konfigurationsänderungen sicher, dass jeweils nur ein Administrator Konfigurationsänderungen an einem Cisco IOS XE-Gerät vornimmt. Dieses Merkmal hilft, die unerwünschte Auswirkung von den simultanen Änderungen zu beseitigen, die an in Verbindung stehenden Konfigurationskomponenten vorgenommen werden. Diese Funktion wird mit dem globalen Konfigurationsbefehl Konfigurationsmodus Exklusivmodus konfiguriert und in einem von zwei Modi betrieben: auto und manual. Im Selbst-modus sperrt die Konfiguration automatisch, wenn ein Verwalter den Konfigurierung Terminalbedienungsaufruf an den Ablaufteil herausgibt. Im manuellen Arbeitsmodus verwendet der Verwalter den Konfigurierungsterminalverschlussbefehl, um die Konfiguration zu sperren, wenn er Konfigurationsmodus kommt.

Dieses Beispiel veranschaulicht die Konfiguration dieses Merkmals für das automatische Konfigurationssperrung:

Konfigurationsmodus exklusiv

Digital gekennzeichnete Cisco-Software

Zusätzlich zur Cisco IOS XE Software Version 16.1 und höher erleichtert die digital signierte Cisco Software-Funktion die Verwendung der Cisco IOS XE Software, die digital signiert und somit vertrauenswürdig ist, mithilfe einer sicheren asymmetrischen (öffentlichen) Verschlüsselung.

Ein digital gekennzeichnetes Bild trägt ein verschlüsseltes (mit einer privaten Taste) Hasch von sich. Nach Kontrolle entschlüsselt das Gerät das Hasch mit der entsprechenden allgemeinen Taste von den Tasten, die sie in seinem Schlüsselspeicher hat und auch sein eigenes Hasch des Bildes berechnet. Wenn das entschlüsselte Hasch das berechnete Bildhasch abgleicht, ist das Bild nicht mit abgegeben worden und kann vertraut werden.

Digital gekennzeichnete Cisco-Software-Tasten werden nach dem Typen und der Version der Taste identifiziert. Eine Taste kann ein Special, eine Produktion oder ein Unfallschlüsseltyp sein. Produktion und spezielle Schlüsseltypen haben eine verbundene Schlüsselversion, die alphabetisch erhöht, wann immer die Taste widerrufen und ersetzt wird. ROMMON- und reguläre Cisco IOS XE-Images werden bei Verwendung der Funktion für digital signierte Cisco Software mit einem Sonder- oder Produktionsschlüssel signiert. Das ROMMON-Bild ist erweiterungsfähig und muss mit der gleichen Taste wie das Special- oder Produktionsbild gekennzeichnet werden, das geladen wird.

Mit diesem Befehl wird die Integrität des Images isr4300-universalk9.16.06.04.SPA.bin im Flash-Speicher mit den Schlüsseln im Geräteschlüsselspeicher überprüft:

show software authentication file bootflash:isr4300-universalk9.16.06.04.SPA.bin

Sprechen Sie Digital gekennzeichnete Cisco-Software zu mehr Information über dieses Merkmal an.

Anschließend kann ein neues Image (isr4300-universalk9.16.10.03.SPA.bin) in den zu ladenden Flash-Speicher kopiert und die Signatur des Images mit dem neu hinzugefügten Spezialschlüssel überprüft werden.

copy /verify tftp://<server_ip>/isr4300-universalk9.16.10.03.SPA.bin flash:

Konfigurations-Änderungs-Mitteilung und protokollieren

Die Funktion zur Benachrichtigung und Protokollierung von Konfigurationsänderungen, die in Version 16.6.4 der Cisco IOS XE-Software hinzugefügt wurde, ermöglicht die Protokollierung der Konfigurationsänderungen, die an einem Cisco IOS XE-Gerät vorgenommen wurden. Das Protokoll wird auf dem Cisco IOS XE-Gerät verwaltet und enthält die Benutzerinformationen der Person, die die Änderung vorgenommen hat, den eingegebenen Konfigurationsbefehl und den Zeitpunkt der Änderung. Diese Funktionalität wird mit dem Protokollieren aktivieren Konfigurationsänderungs-Loggerkonfigurations-Modusbefehl aktiviert. Die optionalen Befehle blenden Schlüssel und Protokollierungsgrößeneinträge aus, um die Standardkonfiguration zu verbessern, da sie die Protokollierung von Kennwortdaten verhindern und die Länge des Änderungsprotokolls erhöhen.

Es wird empfohlen, diese Funktion zu aktivieren, damit der Änderungsverlauf der Konfiguration eines Cisco IOS XE-Geräts einfacher verständlich wird. Zusätzlich werden Sie geraten, den Benachrichtigung syslog-Konfigurationsbefehl zu verwenden, um die Generation von syslog-Meldungen zu aktivieren, wenn eine Konfigurationsänderung vorgenommen wird.

Archiv

Protokollkonfiguration

Protokollierung aktivieren

Protokollierungsgröße 200

Verstecke

Syslog benachrichtigen

Nach der Mitteilung und protokollierenden dem Merkmal der Konfigurations-Änderung ist, die privilegierten Bedienungsaufruf- an den Ablaufteilshow-Archivlog Config kann ganz verwendet werden, um das Konfigurationslog anzusehen aktiviert worden.

Steuern Sie Fläche

Steuerflache Funktionen bestehen den Protokollen und aus den Prozessen, die zwischen Netzgeräten in Verbindung stehen, um Daten von der Quelle auf Zieleinheit zu verschieben. Dieses schließt Wegewahlprotokolle wie das Border Gateway Protocol sowie Protokolle wie ICMP und das Ressourcen-Reservierungs-Protokoll ein (RSVP).

Es ist wichtig, dass Ereignisse in den Management- und Datenflächen nicht nachteilig die Steuerfläche beeinflussen. Wenn ein Ereignis auf Datenebene, wie z. B. ein DoS-Angriff, die Kontrollebene beeinträchtigt, kann das gesamte Netzwerk instabil werden. Diese Informationen zu den Funktionen und Konfigurationen der Cisco IOS XE Software können dabei helfen, die Ausfallsicherheit der Kontrollebene sicherzustellen.

Allgemeines Steuerflache Verhärtung

Schutz der Steuerfläche eines Netzgerätes ist- kritisch, weil die Steuerfläche garantiert, dass die Management- und Datenflächen gewartet und betrieblich sind. Wenn die Steuerfläche, während eines Sicherheitsvorfalls instabil zu werden waren-, kann es für Sie unmöglich sein, die Stabilität des Netzes wieder herzustellen.

In vielen Fällen können Sie die Aufnahme und die Übertragung von bestimmten Typen von Meldungen auf einer Schnittstelle deaktivieren, um die Menge von CPU-Eingabe herabzusetzen, die benötigt wird, um nicht benötigte Pakete zu verarbeiten.

IP-ICMP adressiert um

Ein ICMP adressieren Meldung kann durch einen Router festgelegt werden um, wenn ein Paket auf die gleiche Schnittstelle empfangen und übertragen wird. In dieser Situation sendet der Router vorwärts das Paket und ein ICMP umadressieren Meldung zurück zu dem Absender des ursprünglichen Pakets. Dieses Verhalten erlaubt dem Absender, den Router und die vorderen zukünftigen Pakete direkt zur Zieleinheit zu umgehen (oder zu einem Router näher an der Zieleinheit). In einem richtig arbeitenden IP-Netz sendet ein Router umadressiert nur zu den Hauptrechnern auf seinen eigenen lokalen Teilnetzen. Mit anderen Worten: ICMP-Umleitungen dürfen niemals über eine Layer-3-Grenze hinausgehen.

Es gibt zwei Arten von ICMP-Umleitungsnachrichten: die Umleitung für eine Host-Adresse und die Umleitung für ein komplettes Subnetz. Ein böswilliger Benutzer kann die Fähigkeit des Routers ausnutzen, ICMP zu senden umadressiert, indem er fortwährend Pakete zum Router schickt, der den Router erzwingt, um mit ICMP zu reagieren umadressieren Meldungen und Ergebnisse in einer nachteiligen Auswirkung auf die CPU und die Leistung des Routers. Zwecks zu verhindern dass der Router ICMP umadressiert, benutzt das kein IP umadressiert Schnittstellenkonfigurationsbefehl sendet.

ICMP Unreachables

Die Entstörung mit einer Schnittstellenzugriffsliste bekommt die Übertragung von nicht-erreichbaren Meldungen ICMP zurück zu der Quelle des gefilterten Verkehrs heraus. Die Generation dieser Meldungen kann CPU-Nutzung auf dem Gerät erhöhen. In der Cisco IOS XE Software ist die Erzeugung von nicht erreichbaren ICMP-Paketen standardmäßig auf ein Paket pro 500 Millisekunden beschränkt. Kann nicht-erreichbare Meldungsgeneration ICMP mit dem Schnittstellenkonfigurationsbefehl deaktiviert werden keine IP-unreachables. Kann die nicht-erreichbare Kinetikbegrenzung ICMP von der Nichterfüllung mit der globale Konfigurationsbefehls-IPicmp-Kinetikgrenznicht-erreichbaren Abstand-infrau geändert werden.

Proxy ARP

Proxy ARP ist die Technik in, welches Gerät, normalerweise ein Router, Antworten ARP-Anfragen, die für ein anderes Gerät bestimmt sind. Durch Fälschen seiner Identität übernimmt der Router die Verantwortung für das Routing von Paketen an das reale Ziel. Proxy ARP kann Maschinen auf

einem Teilnetze helfen, Fernteilnetze zu erreichen, ohne Wegewahl oder einen Nichterfüllungskommunikationsrechner zu konfigurieren. Proxy ARP wird in RFC 1027 definiert.

Es gibt einige Nachteile zur proxy- ARPnutzung. Es kann eine Zunahme der Menge von ARP-Verkehr auf der Netzsegment- und -ressourcenabführung und den Mann-in-d-mittleren Angriffen ergeben. Proxy ARP stellt einen Ressourcenabführungs-Angriffsvektor dar, weil jede proxied ARP-Anfrage eine kleine Menge des Speichers verbraucht. Ein Angreifer kann in der Lage sein, allen verfügbaren Speicher zu erschöpfen, wenn er viele ARP-Anfragen sendet.

Mann-in-d-mittlere Angriffe aktivieren einen Hauptrechner im Netz zur Parodie das MAC address des Routers, der die unverdächtigen Hauptrechner ergibt, die Verkehr zum Angreifer schicken. Proxy ARP kann mit dem Schnittstellenkonfigurationsbefehl deaktiviert werden kein IP-proxy ARP.

Weitere Informationen zu dieser Funktion finden Sie unter Aktivieren und Deaktivieren des Proxy-ARP.

NTP-Kontrollnachrichten

Abfragen von NTP-Kontrollnachrichten sind NTP-Funktionen, die Netzwerkmanagement-Funktionen (NM) unterstützten, bevor bessere NMs erstellt und verwendet wurden. Wenn Ihr Unternehmen NTP nicht weiterhin für NM-Funktionen verwendet, sollten Sie diese nach den besten Methoden für die Netzwerksicherheit vollständig deaktivieren. Wenn Sie sie verwenden, kann es sich um einen Service vom Typ Nur internes Netzwerk handeln, der durch eine Firewall oder ein anderes externes Gerät blockiert wird. Sie wurden sogar von allen Standard-IOS- und IOS-XE-Versionen entfernt, da IOS-XR und NX-OS sie nicht unterstützen.

Wenn Sie diese Funktion deaktivieren, lautet der Befehl

```
Router (Konfiguration)# keine NTP-Zulassungsmodussteuerung
```

Dieser Befehl wird dann in der Ausführungskonfiguration als no ntp allow mode control 0 angezeigt. Auf diese Weise haben Sie NTP-Kontrollnachrichten auf dem Gerät deaktiviert und das Gerät vor Angriffen geschützt.

Grenze-CPU-Auswirkung des Steuerflächen-Verkehrs

Schutz der Steuerfläche ist- kritisch. Weil Anwendungsleistungs- und -endbenutzererfahrung ohne das Vorhandensein des Daten- und Managementverkehrs leiden kann, garantiert die Empfindlichkeit der Steuerfläche, dass die anderen zwei Flächen gewartet und betrieblich sind.

Verstehen Sie Steuerflachen Verkehr

Um die Steuerungsebene des Cisco IOS XE-Geräts ordnungsgemäß zu schützen, müssen Sie die Arten des Datenverkehrs kennen, für den die CPU das Prozess-Switching durchführt. Verarbeiten Sie geschalteten Verkehr besteht normalerweise aus zwei verschiedenen Verkehrsarten. Die erste Art von Datenverkehr wird an das Cisco IOS XE-Gerät weitergeleitet und muss direkt von der CPU des Cisco IOS XE-Geräts verarbeitet werden. Dieser Verkehr besteht aus der

Empfangungsumgebungs-Verkehrskategorie. Dieser Verkehr enthält einen Eintrag in der Tabelle Eilbeförderung Ciscos (CEF), hingegen das folgende Routerhopfen das Gerät selbst ist, das durch den Ausdruck empfangen in der Show-IP-cef CLI Ausgabe angezeigt wird. Dieser Hinweis gilt für alle IP-Adressen, die direkt von der CPU des Cisco IOS XE-Geräts verarbeitet werden müssen. Dazu gehören IP-Schnittstellenadressen, Multicast-Adressraum und Broadcast-Adressraum.

Die zweite Art von Datenverkehr, der von der CPU verarbeitet wird, ist Datenverkehr auf Datenebene - Datenverkehr mit einem Ziel außerhalb des Cisco IOS XE-Geräts selbst -, der eine spezielle Verarbeitung durch die CPU erfordert. Obwohl es sich nicht um eine vollständige Liste der CPU handelt, die den Datenverkehr auf Datenebene beeinträchtigt, werden diese Datenverkehrsarten prozessgesteuert und können sich daher auf den Betrieb der Kontrollebene auswirken:

1. Access- Control Listprotokollieren - Protokollierender Verkehr ACL besteht aus allen möglichen Paketen, die an einer Abgleichung (Erlaubnis oder verweigert) von ACE festgelegtes liegen, auf denen das Logschlüsselwort verwendet wird.
2. Rückpfad-Versenden Unicast (Unicast RPF) - Unicast RPF, verwendet in Verbindung mit einem ACL, kann die Prozessschaltung von bestimmten Paketen ergeben.
3. IP-Optionen - Alle mögliche IP-Pakete mit den eingeschlossenen Optionen müssen durch die CPU verarbeitet werden.
4. Fragmentierung - Jedes mögliches IP-Paket, das Fragmentierung benötigt, muss zur CPU für die Verarbeitung geführt werden.
5. Ende des Time- to Live(TTL) - Pakete, die einen TTL-Wert weniger als oder Gleichgestelltes bis eins Internet- Control Message Protocolzeit fordern lassen, überstiegen (ICMP-Typ 11, Code 0) die gesendet zu werden Meldungen, das CPUverarbeitung ergibt.
6. ICMP Unreachables - Pakete, die nicht-erreichbare Meldungen ICMP ergeben, die zur Verlegung passend sind, MTU oder die Entstörung wird durch die CPU verarbeitet.
7. Verkehr, der benötigt eine ARP-Anfrage - Zieleinheiten, für die ein ARP-Eintrag nicht existiert, benötigen die Verarbeitung durch die CPU.
8. Verkehr Nicht-IP - Aller Verkehr NichtiP wird durch die CPU verarbeitet.

   In dieser Liste werden verschiedene Methoden zur Bestimmung der von der CPU des Cisco IOS XE-Geräts verarbeiteten Datenverkehrstypen aufgeführt:
9. Der Show-IP-cef Befehl stellt die Folgendhopfeninformationen für jedes IP-Vorzeichen zur Verfügung, das in der CEF-Tabelle enthalten wird. Wie bereits erwähnt, werden Einträge, die "Receive" als "Next Hop" enthalten, als Empfangs-Adjacencies betrachtet und weisen darauf hin, dass der Datenverkehr direkt an die CPU gesendet werden muss.
10. Der Showschnittstellenschaltbefehl stellt Informationen auf der Anzahl von Paketen zur Verfügung, die der Prozess sind, der durch ein Gerät geschaltet wird.
11. Der Befehl show ip traffic liefert Informationen zur Anzahl der IP-Pakete: mit einem lokalen Ziel (d. h. Empfangs-Adjacency-Datenverkehr). Dabei stehen Optionen zur Verfügung, die eine Fragmentierung erfordern, die an Broadcast-Adressräume gesendet werden, die an Multicast-Adressräume gesendet werden.
12. Empfangen Sie Umgebungsverkehr kann durch den Gebrauch von dem Show-IP-Cacheflussbefehl identifiziert werden. Alle Datenflüsse, die an das Cisco IOS XE-Gerät gerichtet sind, verfügen über eine lokale Zielschnittstelle (Destination Interface, DstIf).

13. Control Plane Policing kann verwendet werden, um den Typ und die Rate des Datenverkehrs zu identifizieren, der die Kontrollebene des Cisco IOS XE-Geräts erreicht. Das Steuerflächenpolizeilich überwachen kann durch den Gebrauch von granulierter Klassifikation ACLs, Protokollieren und der Gebrauch durchgeführt werden vom Showpolitikkarten-Steuerungflächenbefehl.

Infrastruktur ACLs

Grenzmitteilung nach außen Infrastruktur ACLs (iACLs) zu den Geräten des Netzes.

Infrastruktur ACLs werden weitgehend im Grenzzugriff zum Netz mit Infrastruktur ACLs-Kapitel dieses Dokuments umfasst.

Sie werden geraten, iACLs einzuführen, um die Steuerfläche aller Netzgeräte zu schützen.

Empfangen Sie ACLs

Das rACL schützt das Gerät vor schädlichem Verkehr vor dem Verkehr auswirkt den Wegprozessor. Empfangen Sie ACLs sind konzipiert, das Gerät nur zu schützen, auf dem es konfiguriert wird und Durchgangsverkehr nicht durch ein rACL beeinflußt wird. Daher bezieht sich die Ziel-IP-Adresse, die in den Beispieleinträgen der ACL verwendet wird, nur auf die physischen oder virtuellen IP-Adressen des Routers. Empfangszugriffskontrolllisten werden ebenfalls als Best Practice für die Netzwerksicherheit betrachtet und können als langfristige Ergänzung für eine gute Netzwerksicherheit betrachtet werden.

Dieses ist der Empfangsweg ACL, der geschrieben wird, um Verkehr SSHs (TCP-Kanal 22) von verlässlichen Hauptrechnern im Netz 192.168.100.0/24 zu ermöglichen:

— SSH von vertrauenswürdigen Hosts zulassen, die für das Gerät zugelassen sind.

access-list 151 permit tcp 192.168.100.0 0.0.0.255 any eq 22

- Verweigern Sie SSH von allen anderen Quellen an den RP.

access-list 151 deny tcp any any eq 22

- Zulassen des gesamten anderen Datenverkehrs zum Gerät

- gemäß Sicherheitsrichtlinien und -konfigurationen

access-list 151 permit ip any

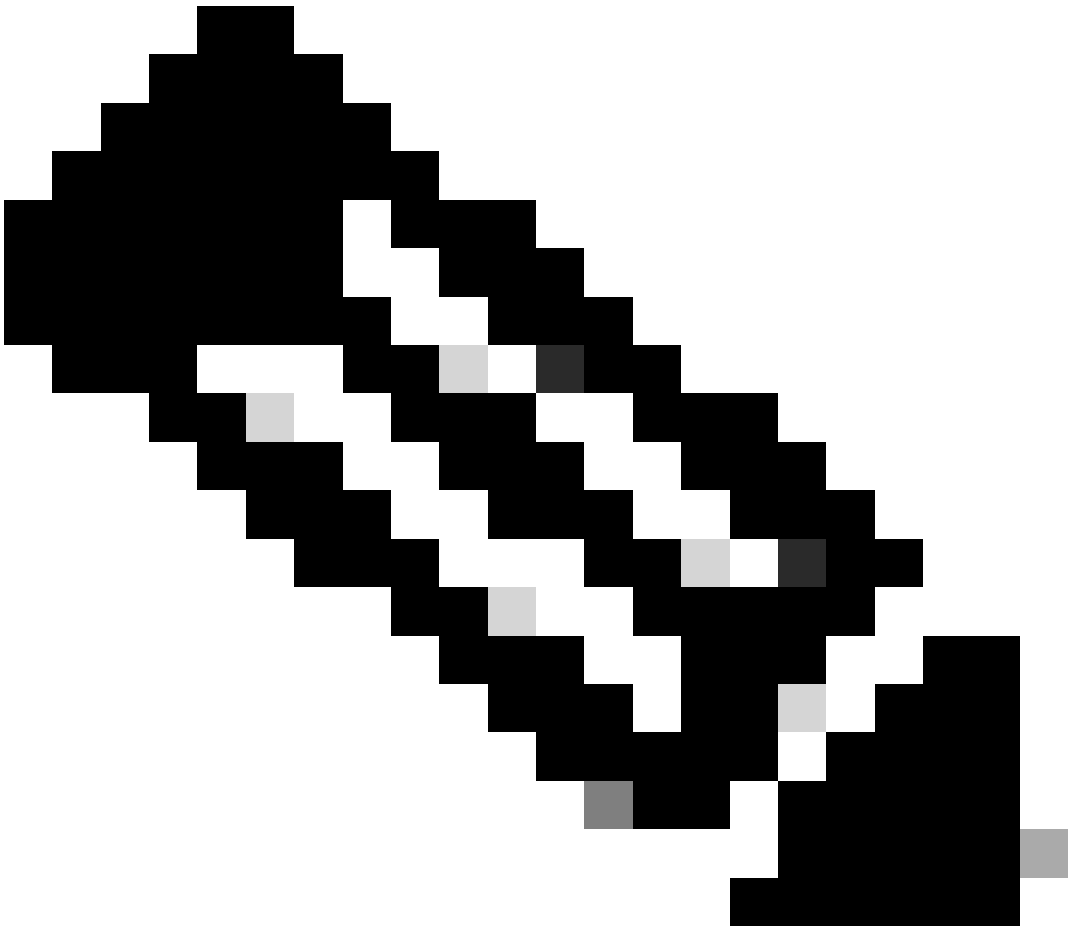
— Diese Zugriffsliste auf den Empfangspfad anwenden.

ip receive access-list 151

Unter Zugriffskontrolllisten finden Sie Informationen zur Identifizierung und Zulässigkeit von legitimem Datenverkehr für ein Gerät sowie zur Ablehnung aller unerwünschten Pakete.

CoPP

Die CoPP-Funktion kann auch benutzt werden, um IP-Pakete einzuschränken, die zum Infrastrukturgerät vorgesehen werden. In diesem Beispiel darf nur SSH-Datenverkehr von vertrauenswürdigen Hosts die CPU des Cisco IOS XE-Geräts erreichen.



> Hinweis: Das Verwerfen von Datenverkehr von unbekannten oder nicht vertrauenswürdigen IP-Adressen kann Hosts mit dynamisch zugewiesenen IP-Adressen daran hindern, eine Verbindung mit dem Cisco IOS XE-Gerät herzustellen.

---

access-list 152 deny tcp <vertrauenswürdige Adressen> <Maske> any eq 22

access-list 152 permit tcp any any eq 22

access-list 152 deny ip any

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

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

CoPP-INPUT-POLICY auf Kontrollebene

Im vorhergehenden CoPP-Beispiel lassen die ACL-Einträge, die abgleichen, die nicht autorisierten Pakete mit dem Erlaubnisaktionsergebnis in einem Ausschuss dieser Pakete durch die Politikkarte Funktion fallen, während Pakete, die die Leugnungsaktion abgleichen, nicht durch die Politikkartenrückgangsfunktion beeinflußt werden.

CoPP ist in der Cisco IOS XE Software-Version verfügbar.

Weitere Informationen zur Konfiguration und Verwendung der CoPP-Funktion finden Sie unter Control Plane Policing.

Steuern Sie flachen Schutz

Control Plane Protection (CPPr), eingeführt in Version 16.6.4 der Cisco IOS XE-Software, kann verwendet werden, um den Datenverkehr auf der Kontrollebene, der für die CPU des Cisco IOS XE-Geräts bestimmt ist, einzuschränken oder zu regeln. Wenn ähnlich CoPP, hat CPPr die Fähigkeit, Verkehr mit feinerer Körnigkeit einzuschränken. CPPr teilt die gesamte Steuerfläche in drei verschiedene Steuerflächenkategorien unter, die als Subinterfaces bekannt sind. Subinterfaces existieren für Hauptrechner-, Durchfahrt- und CEF-Ausnahmeverkehr Kategorien. Darüber hinaus enthält CPPr diese Steuerflache Schutzmerkmale:

1. Kanal-Entstörungsmerkmal - Dieses Merkmal stellt für das Polizeilich überwachen und das Fallen von Paketen zur Verfügung, die zu geschlossenen oder nicht-hörenden TCP- oder UDP-Kanälen geschickt werden.
2. Warteschlange-Thresholdingmerkmal - Dieses Merkmal begrenzt die Anzahl von Paketen für ein spezifiziertes Protokoll, die in der Steuerungfläche IP-Eingabewarteschlange erlaubt werden.

   Siehe das Steuerflachen Schutz und -verständnis des Steuerflachen Schutzes (CPPr) zu mehr Information über die Konfiguration und den Gebrauch von dem CPPr-Merkmal.

Hardware Rate Limiters

Der Cisco-Katalysator 6500 Serien-Überwachungsprogramm-Maschine 32 und Support der Überwachungsprogramm-Maschine 720 Plattform-spezifisch, Kinetikbegrenzer Hardware gestützt (HWRLs) für spezielle Vernetzungsszenario. Diese Hardware-Kinetikbegrenzer gekennzeichnet als Speziellfallkinetikbegrenzer, weil sie ein Besondere vorbestimmtes Set IPv4, IPv6, unicast und multicast DOS-Szenario umfassen. HWRLs können das Cisco IOS XE-Gerät vor einer Vielzahl von Angriffen schützen, bei denen Pakete von der CPU verarbeitet werden müssen.

Sichern Sie BGP

Das Border Gateway Protocol (BGP) ist die Wegewahlgrundlage des Internets. Als solches verwendet jede mögliche Organisation mit mehr als bescheidenen

Anschlussfähigkeitsanforderungen häufig BGP. BGP wird häufig durch Angreifer wegen seiner Allgegenwart und des Sets anvisiert und Art von BGP-Konfigurationen in den kleineren Organisationen vergisst. Jedoch gibt es viele BGP-spezifischen Sicherheitsmerkmale, die wirksam eingesetzt werden können, um die Sicherheit einer BGP-Konfiguration zu erhöhen.

Dieses liefert einen Überblick über die wichtigsten BGP-Sicherheitsmerkmale. Gegebenenfalls werden Konfigurationsempfehlungen gemacht.

TTL-basierte Sicherheits-Schutze

Jedes IP-Paket enthält ein Feld 1-byte, das als das Time to Live (TTL) bekannt ist. Jedes Gerät, dass ein IP-Paket Dekrement dieser Wert durch einen überquert. Der Anfangswert schwankt durch Betriebssystem und reicht gewöhnlich von 64 bis 255. Ein Paket wird fallen gelassen, wenn sein TTL-Wert null erreicht.

Bekannt als beide generalisierte TTL-basierte Kerbe des Sicherheits-Mechanismus-(GTSM) und Sicherheit BGP TTL (BTSH), setzt ein TTL-basierter Sicherheitsschutz den TTL-Wert von IP-Paketen wirksam ein, um zu garantieren, dass die BGP-Pakete, die empfangen werden, von einem direkt verbundenen Gleichen sind. Diese Funktion erfordert häufig die Koordination von Peering-Routern, kann jedoch nach der Aktivierung viele TCP-basierte Angriffe gegen BGP abwehren.

GTSM für BGP wird mit der TTLsicherheitsoption für den Nachbar BGP-Routerkonfigurationsbefehl aktiviert. Dieses Beispiel veranschaulicht die Konfiguration dieses Merkmals:

router bgp <asn>

neighbor <IP-Adresse> remote-as <Remote-SAN>

neighbor <IP-Adresse> ttl-security-Hops <Hop-Count>

Während BGP-Pakete empfangen werden, wird der TTL-Wert überprüft und muss als oder Gleichgestelltes bis 255 minus der spezifizierten Hopfenzählung größer sein.

BGP Peer Authentication mit MD5

Gleichauthentisierung mit MD5 stellt eine Auswahl MD5 jedes Pakets her, das als Teil einer BGP-Sitzung gesendet wird. Speziell werden Teile der IP- und TCP-Vorsätze, DER TCP-Nutzlast und der geheimen Taste benutzt, um die Auswahl festzulegen.

Die hergestellte Auswahl wird dann in TCP-Option Art 19 gespeichert, die speziell zu diesem Zweck durch RFC 2385 erstellt wurde. Der empfangende BGP-Sprecher verwendet die gleiche Algorithmus- und Geheimnistaste, um die Meldungsauswahl zu regenerieren. Wenn die empfangenen und Berechnungs- Auswahl nicht identisch sind, wird das Paket verworfen

Gleichauthentisierung mit MD5 wird mit der Passwortoption zum Nachbar BGP-Routerkonfigurationsbefehl konfiguriert. Der Gebrauch von diesem Befehl wird veranschaulicht,

wie folgt:

router bgp <asn> neighbor <IP-Adresse> remote-as <remote-asn>

neighbor <IP-Adresse> password <geheim>

Sprechen Sie Nachbarrouter-Authentisierung zu mehr Information über BGP-Gleichauthentisierung mit MD5 an.

Konfigurieren Sie maximale Vorzeichen

BGP-Vorzeichen werden durch einen Router im Speicher gespeichert. Je mehr Vorzeichen ein Router anhalten muss, desto mehr Speicher BGP verbrauchen muss. In einigen Konfigurationen kann eine Teilmenge aller Internet-Präfixe gespeichert werden, z. B. in Konfigurationen, die nur eine Standardroute oder Standardrouten für die Benutzernetzwerke eines Anbieters nutzen.

Zwecks Speicherabführung zu verhindern, ist es wichtig die Höchstzahl von Vorzeichen zu konfigurieren die auf einer Progleichbasis angenommen wird. Es wird empfohlen, dass eine Grenze für jeden BGP-Gleichen konfiguriert wird.

Wenn Sie diese Funktion mit dem Konfigurationsbefehl für den Nachbar-BGP-Router mit maximalem Präfix konfigurieren, ist ein Argument erforderlich: die maximale Anzahl von Präfixen, die akzeptiert werden, bevor ein Peer heruntergefahren wird. Beliebig kann eine Zahl von 1 bis 100 auch eingegeben werden. Diese Zahl stellt den Prozentsatz des maximalen Vorzeichenwertes an dar, welchem Punkt eine Logmeldung gesendet wird.

router bgp <asn> neighbor <IP-Adresse> remote-as <remote-asn>

neighbor <IP-Adresse> maximum-prefix <Shutdown-threshold> <Protokoll-Prozent>

Siehe das Konfigurieren des BGP-Maximum-Vorzeichen-Merkmals zu mehr Information über Progleichmaximumvorzeichen.

Filtern Sie BGP-Vorzeichen mit Vorzeichen-Listen

Vorzeichenlisten erlauben einem Netzwerkadministrator, spezifische Vorzeichen zu ermöglichen oder zu verweigern, die über BGP gesendet oder empfangen werden. Präfixlisten können nach Möglichkeit verwendet werden, um sicherzustellen, dass der Netzwerkverkehr über die beabsichtigten Pfade gesendet wird. Präfixlisten können auf jeden eBGP-Peer angewendet werden, sowohl in eingehender als auch in ausgehender Richtung.

Konfiguriertes Vorzeichen druckt Grenze die Vorzeichen aus, die zu denen geschickt oder empfangen werden, die speziell durch die Wegewahlpolitik eines Netzes die Erlaubnis gehabt werden. Wenn dies aufgrund der großen Anzahl empfangener Präfixe nicht möglich ist, kann eine Präfixliste so konfiguriert werden, dass bekannte fehlerhafte Präfixe gezielt blockiert werden. Diese bekannten falschen Vorzeichen umfassen nicht zugewiesenen IP- addressplatz und -netze, die zu den internen oder Prüfungszwecken durch RFC 3330 reserviert sind. Ausgehende Präfixlisten können so konfiguriert werden, dass nur die Präfixe zulässig sind, die eine

Organisation bekanntzugeben beabsichtigt.

Dieses Konfigurationsbeispiel benutzt Vorzeichenlisten, um die Wege zu begrenzen, die gelehrt sind und machte bekannt. Speziell nur ein default route wird Inlands durch Vorzeichenliste BGP-PL-INBOUND erlaubt, und das Vorzeichen 192.168.2.0/24 ist der einzige Weg, der durch BGP-PL-OUTBOUND bekannt gemacht werden lassen wird.

ip prefix-list BGP-PL-INBOUND seq 5 permit 0.0.0.0/0

ip prefix-list BGP-PL-OUTBOUND seq 5 permit 192.168.2.0/24

router bgp <asn>

neighbor <IP-Adresse> prefix-list BGP-PL-INBOUND in

neighbor <IP-Adresse> prefix-list BGP-PL-OUTBOUND out

Die vollständige Abdeckung der BGP-Präfixfilterung finden Sie unter Präfix-Based Outbound Route Filtering (Präfix-basierte ausgehende Routenfilterung).

Filtern Sie BGP-Vorzeichen mit Autonomouss- Systempfad-Zugriffs-Listen

Pfad-Zugriffslisten BGP-Autonomous System (WIE) erlaubt dem Benutzer, die empfangenen und bekannt gemachten Vorzeichen zu filtern, die auf dem Wie-Pfadattribut eines Vorzeichens basieren. Dieses kann in Verbindung mit Vorzeichenlisten verwendet werden, um ein robustes Set Filter herzustellen.

Gebrauch dieses Konfigurationsbeispiels ALS Pfadzugriffslisten, zwecks Inlandsvorzeichen auf die einzuschränken entstand durch die entfernte Station, WIE und Auslandsvorzeichen zu denen durch das lokale Autonomous System entstanden. Vorzeichen, die von allen weiteren Autonomous System Ursprungs sind, sind gefiltert und installiert nicht in die Leitwegtabelle.

ip as-path access-list 1 permit

ip as-path access-list 2 permit

router bgp <asn>

neighbor <IP-Adresse> remote-as 65501

neighbor <IP-Adresse> filter-list 1 in

neighbor <IP-Adresse> filter-list 2 out

Sichern Sie Innenkommunikationsrechner-Protokolle

Die Fähigkeit eines Netzes schicken richtig Verkehr nach und erholen sich von Topologieänderungen, oder Störungen ist von einer genauen Ansicht der Topologie abhängig. Sie können ein Interior Gateway Protocol (IGP) in der Ordnung häufig ausführen zur Verfügung stellen

diese Ansicht. Standardmäßig sind IGP dynamisch und entdecken zusätzliche Router, die das bestimmte gebräuchliche IGP sind. IGP entdecken auch Wege, die während einer Netzwerk-Link-Störung benutzt werden können.

Diese Unterabschnitte liefern einen Überblick über die wichtigsten IGP-Sicherheitsmerkmale.

Empfehlungen und Beispiele, die Routing- Information Protocolversion 2 (RIPv2) umfassen, erhöhtes Innenkommunikationsrechner-Wegewahl-Protokoll (EIGRP) und offenes Shortest-Path zuerst (OSPF) werden zur Verfügung gestellt, wenn passend.

Verlegung von von Protokoll-Authentisierung und Überprüfung mit Meldungs-Auswahl 5

Störung, den Austausch der Leitinformation zu sichern erlaubt einem Angreifer, falsche Leitinformation in das Netz vorzustellen. Durch die Verwendung von Passwortauthentifizierung mit Routing-Protokollen zwischen Routern können Sie die Sicherheit des Netzwerks erhöhen. Jedoch weil diese Authentisierung als Klartext gesendet wird, kann es einfach sein, damit ein Angreifer diese Sicherheitskontrolle umstürzt.

Wenn Sie dem Authentifizierungsprozess MD5-Hash-Funktionen hinzufügen, enthalten Routing-Updates keine Klartext-Kennwörter mehr, und der gesamte Inhalt der Routing-Aktualisierung ist manipulationssicherer. Jedoch ist Authentisierung MD5 gegen Angriffe der Gewalt und des Wörterbuches noch anfällig, wenn schwache Passwörter gewählt werden. Sie werden geraten, Passwörter mit genügender Zufallszuteilung zu verwenden. Da Authentisierung MD5, wenn sie mit Passwortauthentisierung verglichen wird, diese Beispiele, sind spezifisch zur Authentisierung MD5 viel sicherer ist. IPSec kann auch verwendet werden, um Wegewahlprotokolle zu validieren und zu sichern, aber diese Beispiele führen nicht seinen Gebrauch einzeln auf.

EIGRP und RIPv2 verwenden Schlüsselanhänger als Teil der Konfiguration. Siehe Taste zu mehr Information über die Konfiguration und den Gebrauch der Schlüsselanhänger.

Hier eine Beispielkonfiguration für die EIGRP-Router-Authentifizierung mit MD5:

key chain <Schlüsselname>

key <Schlüsselkennung>

key-string <Kennwort>

interface <Schnittstelle> ip authentication mode eigrp <AS-Nummer> md5

ip authentication key-chain eigrp <as-number> <Schlüsselname>

Dieses ist eine Router-Authentisierungskonfiguration des Beispiels MD5 für RIPv2. RIPv1 unterstützt nicht Authentisierung.

key chain <Schlüsselname>

key <Schlüsselkennung>

key-string <Kennwort>

interface <Schnittstelle> ip rip authentication mode md5

ip rip authentication key-chain <Schlüsselname>

Dies ist eine Beispielkonfiguration für die OSPF-Router-Authentifizierung, die MD5 verwendet. OSPF verwendet nicht Schlüsselanhänger.

interface <interface> ip ospf message-digest-key <Schlüssel-ID> md5 <Kennwort>

router ospf <Prozess-ID>

network 10.0.0.0 0.255.255.255 area 0 area 0 authentication message-digest

Sprechen Sie konfigurierendes OSPF zu mehr Information an.

Passiv-Schnittstellen-Befehle

Informationslecks oder das Einschleusen falscher Informationen in ein IGP können durch den Befehl passive-interface behoben werden, der die Steuerung der Meldung von Routing-Informationen unterstützt. Sie werden, geraten keine Informationen zu den Netzen bekanntzumachen, die außerhalb Ihrer Verwaltungskontrolle sind.

Dieses Beispiel zeigt Verwendung dieses Merkmals:

router eigrp <as-number> passive-interface default

no passive-interface <Schnittstelle>

Weg-Entstörung

Zwecks die Möglichkeit zu verringern dass Sie falsche Leitinformation im Netz vorstellen, müssen Sie die Weg-Entstörung verwenden. Anders als den Passivschnittstellenrouter-Konfigurationsbefehl tritt die Verlegung auf der Wegentstörung der Schnittstellen einmal wird aktiviert auf, aber die Informationen, die bekannt gemacht oder verarbeitet wird, sind begrenzt.

Für EIGRP und RISS Verwendung des Verteilenlistenbefehls mit den Herausschlüsselwortgrenzen, welche Informationen bekannt gemacht werden, während Verwendung von im Schlüsselwort begrenzt, welche Aktualisierungen verarbeitet werden. Der Verteilenlistenbefehl ist für OSPF verfügbar, aber er verhindert, ein dass Router nicht gefilterte Wege fortpflanzt. Stattdessen kann der Bereichsfilterlistenbefehl verwendet werden.

Dieses EIGRP-Beispiel filtert Auslandsanzeigen mit dem Verteilenlistenbefehl und einer Vorzeichenliste:

ip prefix-list <Listenname>

10 seq permit <Präfix>

router eigrp <AS-Nummer>

Standard für passive Schnittstelle

no passive-interface <Schnittstelle>

distribute-list prefix <Listenname> out <Schnittstelle>

Dieses EIGRP-Beispiel filtert Inlandsaktualisierungen mit einer Vorzeichenliste:

ip prefix-list <Listenname> seq 10 permit <Präfix>

router eigrp <AS-Nummer>

Standard für passive Schnittstelle

no passive-interface <Schnittstelle>

distribute-list prefix <Listenname> in <Schnittstelle>

Weitere Informationen zur Steuerung der Meldung und Verarbeitung von Routing-Updates finden Sie unter EIGRP-Routenfilterung.

Dieses OSPF-Beispiel benutzt eine Vorzeichenliste mit dem OSPF-spezifischen Bereichsfilterlistenbefehl:

ip prefix-list <Listenname> seq 10 permit <Präfix>

router ospf <Prozess-ID>

<Bereich-ID> Filterlistenpräfix <Listenname> in

Wegewahl-Prozess-Ressourcen-Verbrauch

Protokollvorzeichen verlegend, werden durch einen Router im Speicher und Ressourcenverbrauchszunahmen mit zusätzlichen Vorzeichen gespeichert, die ein Router anhalten muss. Zwecks Ressourcenabführung zu verhindern, ist es wichtig das Wegewahlprotokoll zu konfigurieren um Ressourcenverbrauch zu begrenzen. Dieses ist mit OSPF möglich, wenn Sie die Link-Zustands-Datenbank-Überlastschutzfunktion benutzen.

Dieses Beispiel zeigt Konfiguration des OSPF-Link-Zustands-Datenbank-Überlastschutzmerkmals:

router ospf <Prozess-ID> max-lsa <Maximalanzahl>

Siehe die Begrenzung der Zahl von Selbst-Generierungslsas für einen OSPF-Prozess zu mehr Information über OSPF-Link-Zustands-Datenbank-Überlastschutz.

Sichern Sie erste Hopfenredundanz-Protokolle

Erste Hopfenredundanz-Protokolle (FHRPs) stellen Elastizität und Redundanz für Geräte zur Verfügung, die als Nichterfüllungskommunikationsrechner auftreten. Diese Situation und diese Protokolle sind in den Umgebungen alltäglich, in denen ein Paar Geräte der Schicht 3 Nichterfüllungskommunikationsrechnerfunktionalität für ein Netzsegment oder Set von VLANs zur Verfügung stellt, die Servers oder Arbeitsplätze enthalten.

Das Kommunikationsrechner-Eingabe-balancierende Protokoll (GLBP), das Hot-standbyrouter-Protokoll (HSRP) und das virtuelle Router-Redundanz-Protokoll (VRRP) sind alles FHRPs. Standardmäßig sind diese Protokolle unauthenticated Kommunikationen verbunden. Diese Art der Kommunikation kann einem Angreifer erlauben, als FHRP-sprechendes Gerät aufzuwerfen, um die Nichterfüllungskommunikationsrechnerrolle im Netz anzunehmen. Diese Übernahme würde einem Angreifer erlauben, einen Mann-in-d-mittleren Angriff durchzuführen und allen Benutzerverkehr abzufangen, der das Netz beendet.

Um diesen Angriffstyp zu verhindern, enthalten alle von der Cisco IOS XE Software unterstützten FHRPs eine Authentifizierungsfunktion mit MD5- oder Text-Strings. Wegen der Drohung, die durch unauthenticated FHRPs aufgeworfen wird, wird es empfohlen, dass Fälle dieser Protokolle Authentisierung MD5 verwenden. Dieses Konfigurationsbeispiel zeigt den Gebrauch von GLBP-, HSRP- und VRRP-MD5 Authentisierung:

interface FastEthernet 1

description *** GLBP-Authentifizierung ***

glbp1 authentication md5 key-string <glbp-secret>

glbp 1 ip 10.1.1.1

interface FastEthernet 2

description *** HSRP-Authentifizierung ***

Standby 1 Authentifizierung MD5-Schlüsselzeichenfolge <hsrp-secret>

Standby 1 IP 10.2.2.1

interface FastEthernet 3

description *** VRRP-Authentifizierung ***

vrrp 1 authentication md5 key-string <vrrp-secret>

vrrp 1 ip 10.3.3.1

Daten-Fläche

Obgleich die Datenfläche für das Verschieben von Daten von Quelle zu Zieleinheit, im

Zusammenhang mit Sicherheit, die Datenfläche ist das wenige wichtige der drei Flächen verantwortlich ist. Aus diesem Grunde ist es wichtig, das Management zu schützen und Flächen in der Präferenz über der Datenfläche zu steuern, wenn Sie ein Netzgerät sichern.

Jedoch innerhalb der Datenfläche selbst, gibt es viele Merkmale und Konfigurationsoptionen, die sicherem Verkehr helfen können. Diese Kapitel führen diese Merkmale und Optionen so einzeln auf, dass Sie leicht sicher Ihr Netz können.

Allgemeine Daten-flache Verhärtung

Die überwiegende Mehrheit von Daten planieren Verkehrsströme über das Netz, wie durch die Wegewahlkonfiguration des Netzes bestimmt. Jedoch existiert IP-Netzfunktionalität, um den Pfad von Paketen über dem Netz zu ändern. Merkmale wie IP-Optionen, speziell die Quellwegewahloption, bilden eine Sicherheitsherausforderung in den heutigen Netzen.

Der Gebrauch von Durchfahrt ACLs ist auch zur Verhärtung der Datenfläche relevant.

Sehen Sie den Filter-Durchgangsverkehr mit Durchfahrt ACLs-Kapitel dieses Dokuments zu mehr Information.

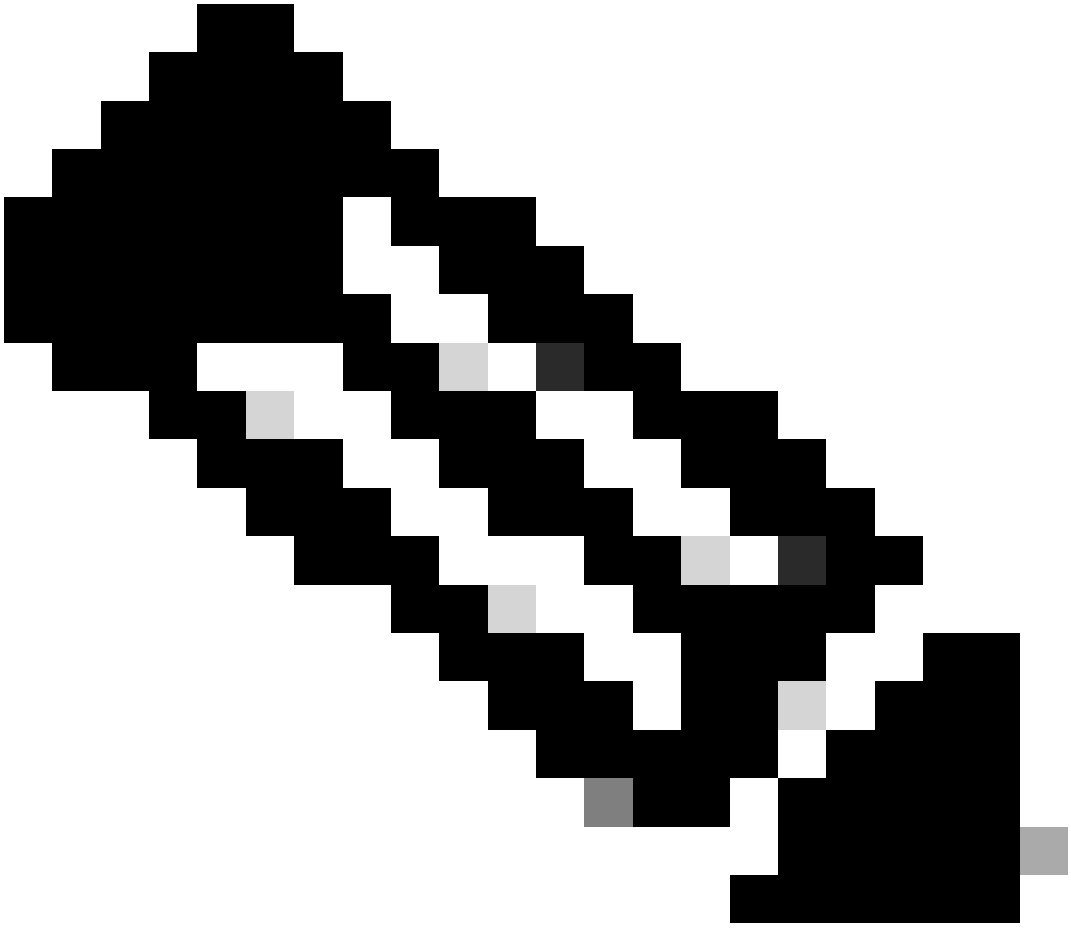
IP-Options-selektiver Tropfen

Es gibt zwei Sicherheitsprobleme, die durch IP-Optionen dargestellt werden. Datenverkehr, der IP-Optionen enthält, muss von Cisco IOS XE-Geräten prozessgesteuert werden, was zu einer erhöhten CPU-Auslastung führen kann. IP-Optionen umfassen auch die Funktionalität, um den Pfad zu ändern, den Verkehr durch das Netz nimmt, das ihn möglicherweise Sicherheitskontrollen umstürzen lässt.

Wegen dieser Interessen, die globalen Konfigurationsbefehls-IP-Optionen {Tropfen | ignore} wurde der Cisco IOS XE Software Version 16.6.4 und höher hinzugefügt. In der ersten Form dieses Befehls, ip options drop, werden alle IP-Pakete mit IP-Optionen, die vom Cisco IOS XE-Gerät empfangen werden, verworfen. Dieses verhindert die erhöhte CPU-Eingabe und mögliche Subversion von Sicherheitskontrollen, die IP-Optionen aktivieren können.

Die zweite Form dieses Befehls, ip options ignore, konfiguriert das Cisco IOS XE-Gerät so, dass in empfangenen Paketen enthaltene IP-Optionen ignoriert werden. Während dieses die Drohungen abschwächt, die auf IP-Optionen für die lokale Einheit in Verbindung gestanden werden, ist es möglich, dass abwärts gerichtete Geräte durch das Vorhandensein von IP-Optionen beeinflußt werden konnten. Aus diesem Grunde wird das Tropfenformular dieses Befehls in hohem Grade empfohlen. Dieses wird im Konfigurationsbeispiel demonstriert:

ip options drop



Hinweis: Einige Protokolle, z. B. RSVP, verwenden legitime IP-Optionen. Die Funktionalität dieser Protokolle wird durch diesen Befehl ausgewirkt.

Sobald IP-Options-selektiver Tropfen aktiviert worden ist, kann der Show-IP-Verkehr Bedienungsaufruf an den Ablaufteil verwendet werden, um die Anzahl von Paketen zu bestimmen, die am Vorhandensein von IP-Optionen fallengelassenes liegen. Diese Informationen sind im vorverlegten Rückgangszähler anwesend.

Sprechen Sie ACL-IP-Options-selektiven Tropfen zu mehr Information über dieses Merkmal an.

Sperrung IP-Quellwegewahl

IP-Quellwegewahl setzt die losen Quellweg- und Satz-Wegoptionen im Tandem oder im strengen Quellweg zusammen mit der Rekordwegoption wirksam ein, um die Quelle des IP datagram zu aktivieren, den Netzpfad zu spezifizieren Nehmen eines Pakets. Diese Funktionalität kann in den Versuchen verwendet werden, Verkehr um Sicherheitskontrollen im Netz zu verlegen.

Wenn IP-Optionen nicht vollständig über das IP-Options-selektive Tropfenmerkmal deaktiviert worden sind, ist es wichtig, dass IP-Quellwegewahl behindert ist-. Das IP-Source-Routing, das in allen Cisco IOS XE Software-Versionen standardmäßig aktiviert ist, wird über den globalen Konfigurationsbefehl no ip source-route deaktiviert.

Dieses Konfigurationsbeispiel veranschaulicht den Gebrauch von diesem Befehl:

Keine IP-Quellroute

Sperrung ICMP adressiert um

ICMP adressiert werden verwendet, um ein Netzgerät über einen besseren Pfad zu einer IP-Zieleinheit zu informieren um. Standardmäßig sendet die Cisco IOS XE Software eine Umleitung, wenn ein Paket empfangen wird, das über die empfangene Schnittstelle geroutet werden muss.

In einigen Situationen kann es für einen Angreifer möglich sein, das Senden vieler ICMP-Umleitungsnachrichten durch das Cisco IOS XE-Gerät zu verursachen, was zu einer erhöhten CPU-Last führt. Aus diesem Grund wird es empfohlen, dass die Übertragung von ICMP ist behindert umadressiert. ICMP adressiert werden deaktiviert mit der Schnittstellenkonfiguration, die kein IP Befehl umadressiert, wie in der Beispielkonfiguration gezeigt um:

interface FastEthernet 0

no ip redirects

Sperrungs-oder Grenz-IP verwiesene Sendungen

IP verwiesene Sendungen machen es möglich, ein IP-Sendungspaket zu einem Fern-IP-Teilnetze zu schicken. Sobald es das Netz mit größerer geographischer Ausdehnung erreicht, schickt das nachschickende IP-Gerät das Paket als Sendung der Schicht 2 zu allen Stationen auf dem Teilnetze. Diese gezielte Broadcast-Funktionalität wurde als Verstärkungs- und Reflexionshilfe bei verschiedenen Angriffen eingesetzt, zu denen auch der Schlumpf-Angriff gehört.

Bei aktuellen Versionen der Cisco IOS XE Software ist diese Funktion standardmäßig deaktiviert. Sie kann jedoch über den Konfigurationsbefehl ip directed-broadcast interface aktiviert werden. Für Versionen der Cisco IOS XE Software vor 12.0 ist diese Funktion standardmäßig aktiviert.

Wenn ein Netzwerk eine gezielte Broadcast-Funktionalität unbedingt benötigt, kann seine Verwendung kontrolliert werden. Dieses ist mit dem Gebrauch eines Access Control List als Option zum IP-verweisensendungsbefehl möglich. Grenzen dieses Konfigurationsbeispiels verwiesen Sendungen auf jene UDP-Pakete, die an einem verlässlichen Netz entstehen, 192.168.1.0/24:

access-list 100 permit udp 192.168.1.0 0.0.0.255 any

interface FastEthernet 0

ip directed-broadcast 100

Filter-Durchgangsverkehr mit Durchfahrt ACLs

Es ist möglich, zu steuern, welcher Verkehr das Netz mit dem Gebrauch von Durchfahrt ACLs (tACLs) durchfährt. Dieses ist im Gegensatz zu Infrastruktur ACLs, das suchen, Verkehr zu filtern, der zum Netz selbst vorgesehen wird. Die Entstörung, die von den tACLs bereitgestellt wird, ist nützlich, wenn zu handeln ist wünschenswert, Verkehr zu einer bestimmten Gruppe Geräten zu filtern oder dass das Netz durchfährt.

Dieser Typ der Entstörung wird traditionsgemäß durch Firewalls durchgeführt. Es gibt jedoch Fälle, in denen es von Vorteil sein kann, diese Filterung auf einem Cisco IOS XE-Gerät im Netzwerk durchzuführen, z. B. wenn eine Filterung durchgeführt werden muss, aber keine Firewall vorhanden ist.

Durchfahrt ACLs sind auch ein passender Platz, in dem statische anti-spoofing Schutze einführen.

Sehen Sie das Anti-Spoofing Schutzkapitel dieses Dokuments zu mehr Information.

Weitere Informationen zu tACLs finden Sie bei den Hinweisen zu Transit-Zugriffskontrolllisten: Filtern am Edge.

ICMP-Paket-Entstörung

Das Internet Control Message Protocol (ICMP) war als Steuerprotokoll für IP konzipiert. Daher können die von ihm übermittelten Nachrichten weit reichende Auswirkungen auf die TCP- und IP-Protokolle im Allgemeinen haben. ICMP wird von den Tools zur Behebung von Netzwerkfehlern, Ping und Traceroute sowie von der MTU-Pfaderkennung verwendet. Für den ordnungsgemäßen Betrieb eines Netzwerks ist jedoch eine externe ICMP-Verbindung selten erforderlich.

Die Cisco IOS XE Software bietet Funktionen zum gezielten Filtern von ICMP-Nachrichten nach Name, Typ und Code. Dieses Beispiel ACL erlaubt ICMP von verlässlichen Netzen, während es alle ICMP-Pakete von anderen Quellen blockt:

ip access-list extended ACL-TRANSIT-IN

— ICMP-Pakete nur von vertrauenswürdigen Netzwerken zulassen

icmp host <vertrauenswürdige-netzwerke> any

- Anderen IP-Datenverkehr an jedes Netzwerkgerät ablehnen

icmp any

Filter IP-Fragmente

Wie im Grenzzugriff zum Netz mit Infrastruktur ACLs-Kapitel dieses Dokuments vorher einzeln aufgeführt, kann die Entstörung von zersplitterten IP-Paketen eine Herausforderung zu den Arten der Sicherheitsleistung darstellen.

Wegen der nonintuitive Art des Fragments handhabend, werden IP-Fragmente häufig unbeabsichtigt durch ACLs die Erlaubnis gehabt. Fragmentierung ist auch in den Versuchen, Entdeckung durch EindringenErfassungssysteme auszuweichen häufig benutzt. Aus diesen Gründen werden IP-Fragmente häufig für Angriffe verwendet und können explizit am Anfang konfigurierter tACLs gefiltert werden.

Die ACL umfasst eine umfassende Filterung von IP-Fragmenten. Die Funktionalität, die in diesem Beispiel veranschaulicht wird, muss in Verbindung mit der Funktionalität der vorhergehenden Beispiele verwendet werden:

ip access-list extended ACL-TRANSIT-IN

- Verweigern von IP-Fragmenten, die protokollspezifische ACEs verwenden, um

— Klassifizierung des Angriffsverkehrs

tcp alle Fragmente verweigern

udp alle Fragmente verweigern

icmp alle Fragmente verweigern

ip alle Fragmente verweigern

Weitere Informationen zur ACL-Behandlung fragmentierter IP-Pakete finden Sie unter Access List Processing of Fragments (Verarbeitung von Fragmenten in Zugriffslisten).

Acl-Support für die Entstörung von IP-Optionen

In Version 16.6.4 der Cisco IOS XE Software unterstützt die Cisco IOS XE Software die Verwendung von ACLs zum Filtern von IP-Paketen basierend auf den im Paket enthaltenen IP-Optionen. Das Vorhandensein von IP-Optionen innerhalb eines Pakets kann auf einen Versuch hinweisen, Sicherheitskontrollen im Netzwerk zu untergraben oder anderweitig die Übertragungseigenschaften eines Pakets zu ändern. Aus diesen Gründen können Pakete mit IP-Optionen am Netzwerk-Edge gefiltert werden.

Dieses Beispiel muss mit dem Inhalt von den vorhergehenden Beispielen verwendet werden, um die komplette Entstörung von IP-Paketen einzuschließen, die IP-Optionen enthalten:

ip access-list extended ACL-TRANSIT-IN

- IP-Pakete mit IP-Optionen verweigern

deny ip any option any option any options

Anti-Spoofing Schutze

Gebrauchsquellip address vieler Angriffe, das, um effektiv zu sein- spoofing ist oder die wahre Quelle eines Angriffs zu verbergen und genauen Traceback zu hindern. Die Cisco IOS XE

Software bietet Unicast RPF und IP Source Guard (IPSG), um Angriffe abzuwehren, die auf Quell-IP-Adressen-Spoofing basieren. Darüber hinaus wird ACLs und ungültige Wegewahl häufig als manuelle Durchschnitte von spoofing Verhinderung eingesetzt.

IP-Quellschutz arbeitet, um spoofing für Netze herabzusetzen, die unter direkter Verwaltungskontrolle durch Ausführungsschalterkanal, MAC address und Quelladreßüberprüfung sind. Unicast RPF liefert Quellnetzüberprüfung und kann spoofed Angriffe von den Netzen verringern, die nicht unter direkter Verwaltungskontrolle sind. Kanal-Sicherheit kann verwendet werden, um MAC-Adressen an der Zugriffsschicht zu validieren. Dynamische Inspektion des Address- Resolution Protocol(ARP) (DAI) schwächt Angriffsvektoren ab, die ARP-Vergiftung auf lokalen Segmenten verwenden.

Unicast RPF

Unicast RPF aktiviert ein Gerät, zu überprüfen, dass die Quelladresse eines nachgeschickten Pakets durch die Schnittstelle erreicht werden kann, die das Paket empfing. Sie dürfen nicht auf Unicast RPF als der einzige Schutz gegen spoofing bauen. Gefälschte Pakete könnten über eine Unicast RPF-fähige Schnittstelle in das Netzwerk gelangen, wenn eine geeignete Rückgaberoute zur Quell-IP-Adresse vorhanden ist. Unicast RPF beruht auf Ihnen, um Eilbeförderung Ciscos auf jedem Gerät zu aktivieren und wird auf einer Proschnittstellenbasis konfiguriert.

Unicast RPF kann in einem von zwei Modi konfiguriert werden: „Loose“ (locker) oder „Strict“ (streng). In den Fällen wo es asymetrische Wegewahl gibt, wird loser Modus bevorzugt, weil strenger Modus bekannt, um Pakete in diesen Situationen fallenzulassen. Während der Konfiguration des IP überprüfen Sie Schnittstellenkonfigurationsbefehl, das Schlüsselwort konfiguriert irgendwie losen Modus, während das Schlüsselwort rx strengen Modus konfiguriert.

Dieses Beispiel veranschaulicht Konfiguration dieses Merkmals:

ip cef

interface <Schnittstelle>

ip verify unicast source reachable-via <mode>

Siehe Verständnis des Rückpfad-Versendens Unicast zu mehr Information über die Konfiguration und den Gebrauch Unicast RPF.

IP-Quellschutz

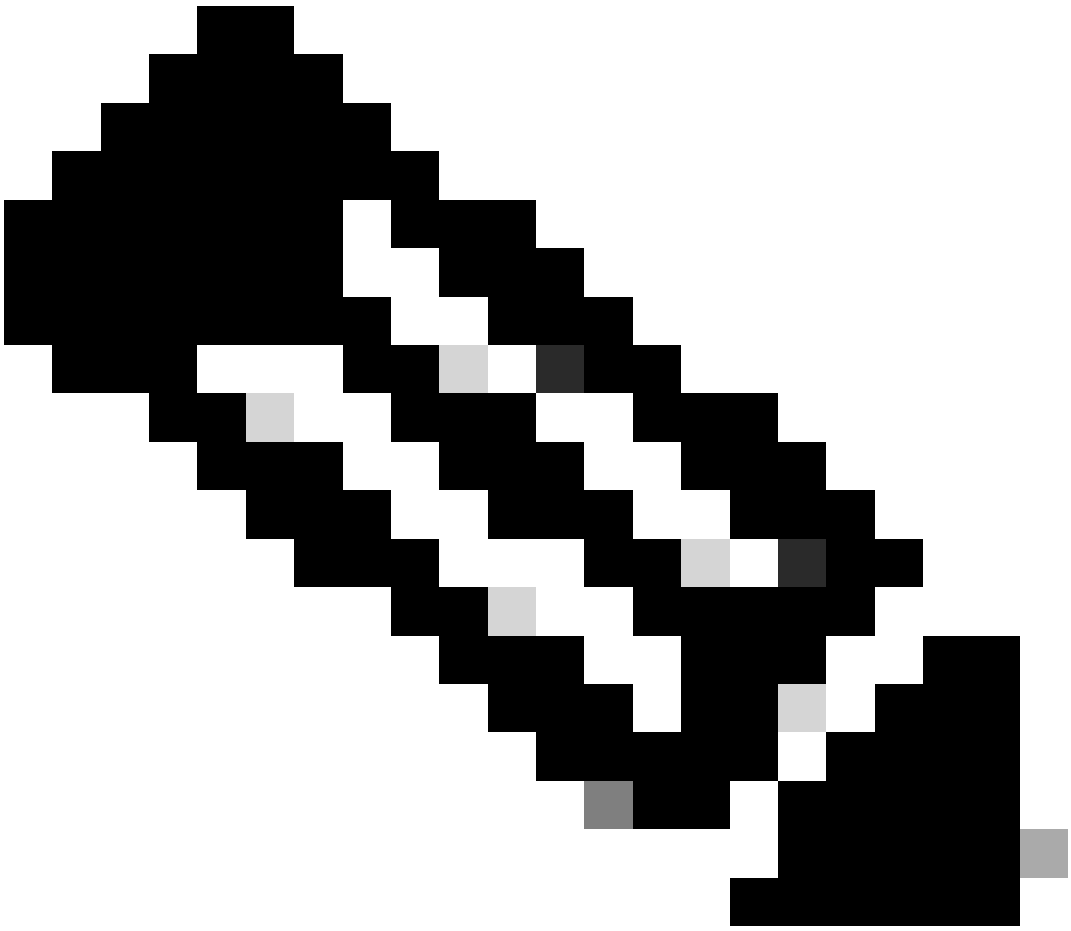
IP-Quellschutz ist- effektive Durchschnitte von spoofing Verhinderung, die verwendet werden kann, wenn Sie Steuerung über Schnittstellen der Schicht 2 haben. IP-Quellschutzgebrauchsinformationen von DHCP, das herumschnüffelt, um ein Kanalaccess control list (PACL) auf der Schnittstelle der Schicht 2 dynamisch zu konfigurieren, irgendeinen Verkehr von den IP address verweigernd, die nicht in der IP-Quellverbindlichen Tabelle sind.

IP-Quellschutz kann angewendet werden, um 2 Schnittstellen zu überlagern, die DHCP herumgeschnüffelte-aktiviertem VLANs gehören. Diese Befehle aktivieren DHCP-

Herumschnüffeln:

ip dhcp snooping

ip dhcp snooping vlan <VLAN-Bereich>



> Hinweis: Zur Unterstützung von IP Source Guard benötigt das Chassis/der Router ein Layer-2-Switching-Modul.

Kanalsicherheit kann mit dem IP aktiviert werden überprüfen Quellkanalsicherheits-Schnittstellen-Konfigurationsbefehl. Dazu ist der globale Konfigurationsbefehl ip dhcp snooping information option erforderlich. Zusätzlich muss der DHCP-Server die DHCP-Option 82 unterstützen.

Weitere Informationen zu dieser Funktion finden Sie unter IP Source Guard.

Kanal-Sicherheit

Kanal-Sicherheit wird verwendet, um das MAC address abzuschwächen, das an der

Zugriffsschnittstelle spoofing ist. Kanal-Sicherheit kann dynamisch gelehrte (klebrige) MAC-Adressen verwenden, um in der Erstkonfiguration nachzulassen. Sobald Kanalsicherheit eine MAC-Verletzung bestimmt hat, kann sie einen von vier Verletzungsmodi verwenden. Diese Modi sind sich schützen, einschränken, Abschaltung und Abschaltung VLAN. In den Fällen, in denen ein Port nur Zugriff für eine einzelne Workstation unter Verwendung von Standardprotokollen bietet, kann eine maximale Anzahl von 1 ausreichen. Protokolle, die wirksam einsetzen, virtuelles MAC wendet sich wie HSRP arbeiten nicht, wenn die Höchstzahl bis eine eingestellt wird.

interface <Schnittstelle> switchport

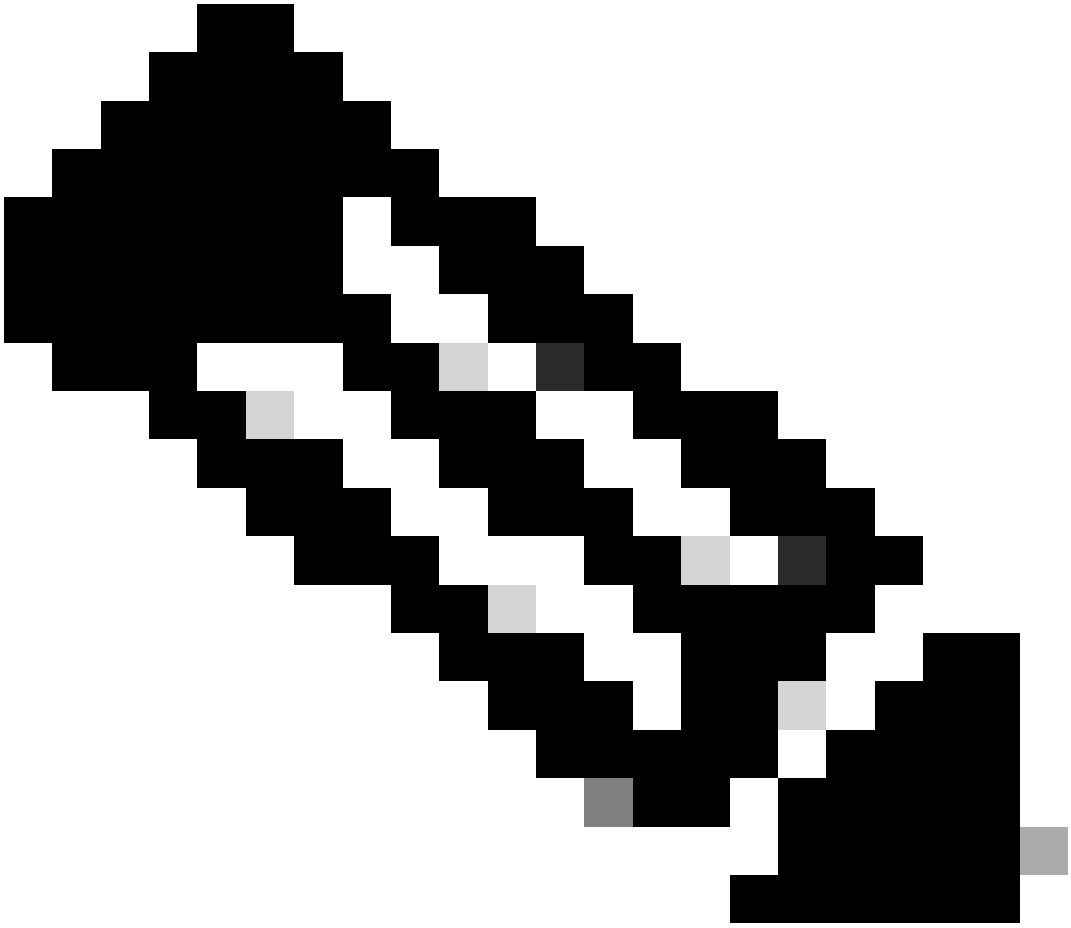
switchport mode access

switchport port-security

switchport-security mac-address haftend

switchport-security maximum <Nummer>

switchport port-security violment <Verletzungsmodus>



Hinweis: Zur Unterstützung von "port-security" benötigt das Chassis/der Router ein Layer-2-Switching-Modul.

Weitere Informationen zur Port-Sicherheitskonfiguration finden Sie unter Konfigurieren der Port-Sicherheit.

Anti-Spoofing ACLs

Manuell konfiguriertes ACLs kann statischen anti-spoofing Schutz gegen Angriffe bieten, die bekannten unbenutzten und untrusted Adressbereich benutzen. Geläufig werden diese, die ACLs anti-spoofing sind, am Eintrittverkehr an den Netzgrenzen als Komponente eines größeren ACL angewendet. Anti-spoofing ACLs benötigen Sie regelmäßige Überwachung, weil sie häufig ändern können. Spoofing kann im Verkehr herabgesetzt werden, der vom lokalen Netzwerk (LAN) entsteht, wenn Sie Auslands-ACLs anwenden, das den Verkehr auf gültige lokale Adressen begrenzen.

Dieses Beispiel zeigt, wie ACLs verwendet werden kann, um IP spoofing zu begrenzen. Dieser

ACL ist auf der gewünschten Schnittstelle angewandtes Inlands. Die Asse, die diesen ACL bilden, sind nicht umfassend. Wenn Sie diese Typen von ACLs konfigurieren, suchen Sie eine aktuelle Referenz, die entscheidend ist.

ip access-list extended ACL-ANTISPOOF-IN

ip 10.0.0.0 0.255.255.255 any

ip 192.168.0.0 0.0.255.255 any

interface <Schnittstelle>

ip access-group ACL-ANTISPOOF-IN in

Weitere Informationen zum Konfigurieren von Zugriffskontrolllisten finden Sie unter Konfigurieren von IPv4-Zugriffskontrolllisten.

Grenze-CPU-Auswirkung des Daten-Flächen-Verkehrs

Der Hauptzweck von Routern und von Schaltern ist, Pakete und Felder durch das Gerät zu den endgültigen Bestimmungsorts vorwärts nachzuschicken. Diese Pakete, die die Geräte durchfahren, setzten während des Netzes, können CPU-Operationen eines Gerätes auswirken ein. Die Datenebene, die aus Datenverkehr besteht, der durch das Netzwerkgerät fließt, kann gesichert werden, um den Betrieb der Management- und Kontrollebenen sicherzustellen. Wenn Transitverkehr dazu führen kann, dass ein Gerät Switch-Datenverkehr verarbeitet, kann dies Auswirkungen auf die Steuerungsebene eines Geräts haben, was zu Betriebsunterbrechungen führen kann.

Merkmale und Verkehrs-Typen, die die CPU auswirken

Obgleich nicht vollständig, umfasst diese Liste Typen von Daten planieren Verkehr, die spezielle CPU benötigen, die verarbeitet und sind der Prozess, der durch die CPU geschaltet wird:

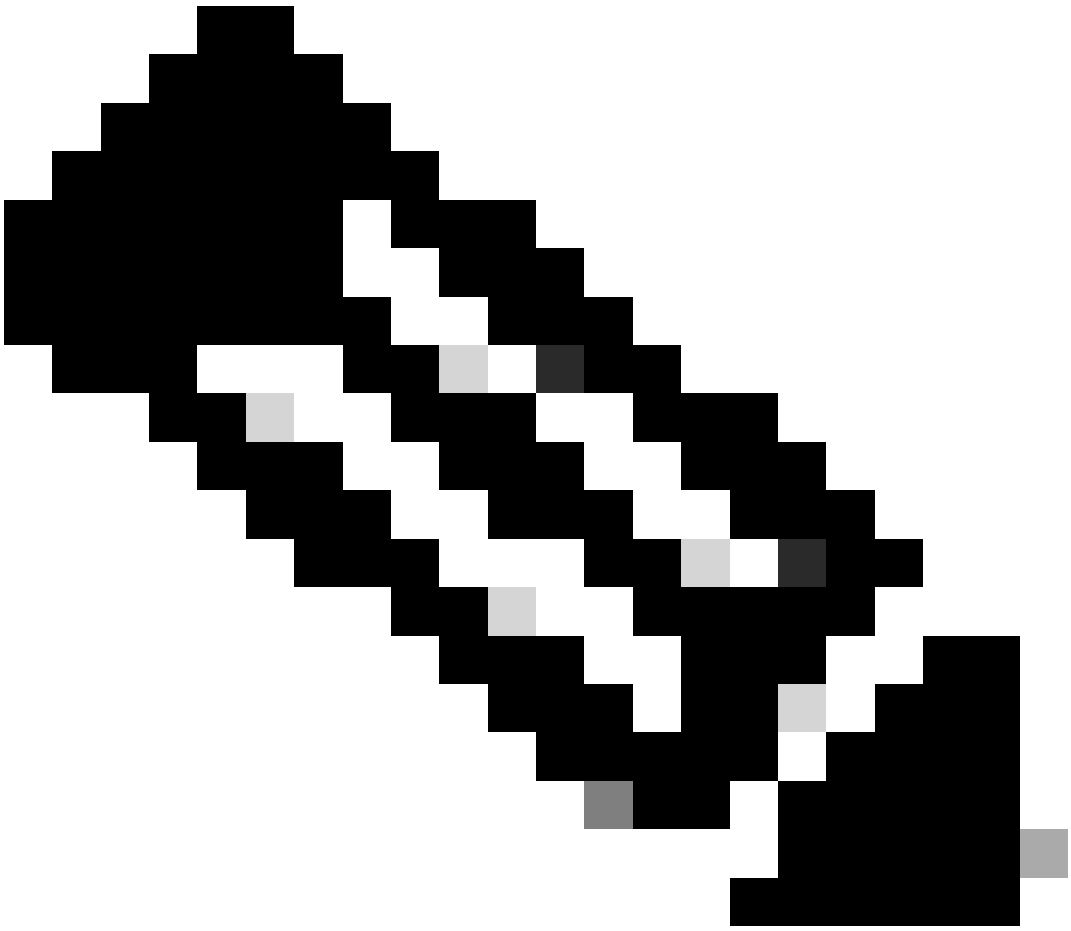
1. ACL protokollieren - Protokollierender Verkehr ACL besteht aus allen möglichen Paketen, die an einer Abgleichung (Erlaubnis oder verweigert) von ACE festgelegtes liegen, auf denen das Logschlüsselwort verwendet wird.
2. Unicast-RPF: Wenn Unicast-RPF in Verbindung mit einer ACL verwendet wird, kann der Prozess zum Switching bestimmter Pakete führen.
3. IP-Optionen - Alle mögliche IP-Pakete mit den eingeschlossenen Optionen müssen durch die CPU verarbeitet werden.
4. Fragmentierung - Jedes mögliches IP-Paket, das Fragmentierung benötigt, muss zur CPU für die Verarbeitung geführt werden.
5. Ende des Time- to Live(TTL) - Pakete, die einen TTL-Wert weniger als oder Gleichgestelltes bis 1 Internet- Control Message Protocolzeit fordern lassen, überstiegen (ICMP-Typ 11, Code 0) die gesendet zu werden Meldungen, das CPUverarbeitung ergibt.
6. ICMP Unreachables - Pakete, die nicht-erreichbare Meldungen ICMP ergeben, die zur Verlegung, zu MTU oder zur Entstörung passend sind, werden durch die CPU verarbeitet.

7. Verkehr, der benötigt eine ARP-Anfrage - Zieleinheiten, für die ein ARP-Eintrag nicht existiert, benötigen die Verarbeitung durch die CPU.
8. Verkehr Nicht-IP - Aller Verkehr NichtiP wird durch die CPU verarbeitet.

   Sehen Sie das flache Verhärtungskapitel der allgemeinen Daten dieses Dokuments zu mehr Information über die Daten-flache Verhärtung.

Filter auf TTL-Wert

Sie können die Funktion "ACL Support for Filtering on TTL Value" (ACL-Unterstützung für Filterung nach TTL-Wert), die in Version 16.6.4 der Cisco IOS XE-Software eingeführt wurde, in einer erweiterten IP-Zugriffsliste verwenden, um Pakete basierend auf dem TTL-Wert zu filtern. Diese Funktion kann benutzt werden, um ein Gerät zu schützen, das Durchgangsverkehr empfängt, in dem der TTL-Wert null oder das ist. Filterpakete, die auf TTL-Werten basieren, können ebenfalls verwendet werden, um sicherzustellen, dass der TTL-Wert nicht kleiner als der Durchmesser des Netzwerks ist. Auf diese Weise wird die Kontrollebene nachgeschalteter Infrastrukturgeräte vor TTL-Ablaufangriffen geschützt.



Hinweis: Einige Anwendungen und Tools, z. B. Traceroute, verwenden TTL-Ablaufpakete zu Test- und Diagnosezwecken. Einige Protokolle, wie IGMP, verwenden legitim einen TTL-Wert von einem.

Dieses ACL-Beispiel erstellt eine Politik dieses Filter IP-Pakete, wo der TTL-Wert kleiner als 6. ist.

— Erstellen Sie eine ACL-Richtlinie, die IP-Pakete mit einem TTL-Wert filtert.

— weniger als 6

ip access-list extended ACL-TRANSIT-IN

ip any ttl lt 6 verweigern

permit ip any any

- Wenden Sie die Zugriffsliste in Eingangsrichtung auf die Schnittstelle an.

interface GigabitEthernet 0/0

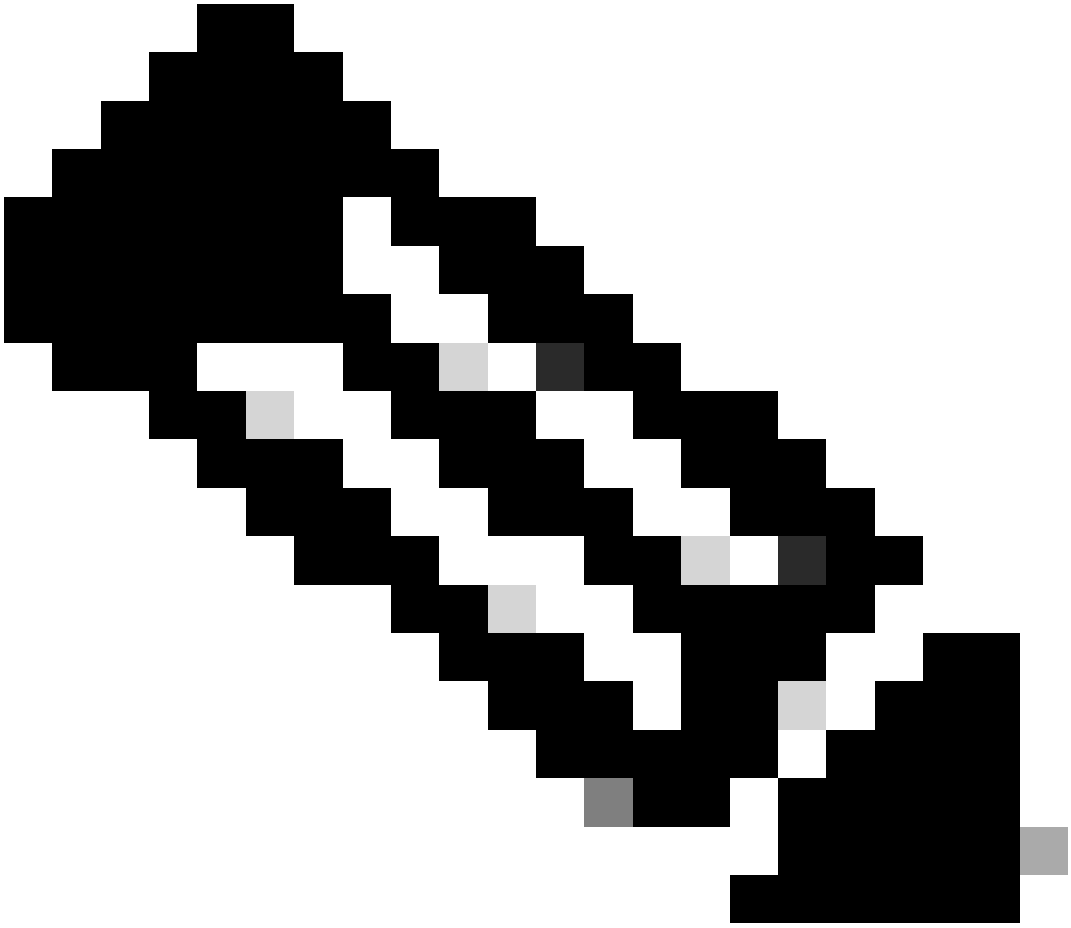
ip access-group ACL-TRANSIT-IN eingehend

Siehe TTL-Endangriffs-Kennzeichen und Abschwächung zu mehr Information über die Entstörungspakete, die auf TTL-Wert basieren.

Siehe ACL-Support für die Entstörung auf TTL-Wert zu mehr Information über dieses Merkmal.

Filter auf dem Vorhandensein von IP-Optionen

In Cisco IOS XE Software, Version 16.6.4 und höher, können Sie die Funktion ACL Support for the Filtering IP Options in einer benannten, erweiterten IP-Zugriffsliste verwenden, um IP-Pakete mit vorhandenen IP-Optionen zu filtern. Darüber hinaus können IP-Pakete gefiltert werden, die auf vorhandenen IP-Optionen basieren, um zu verhindern, dass die Kontrollebene von Infrastrukturgeräten diese Pakete auf CPU-Ebene verarbeiten muss.



Hinweis: Die ACL-Unterstützung für das Filtern von IP-Optionen kann nur mit benannten erweiterten ACLs verwendet werden.

Außerdem ist zu beachten, dass Pakete mit RSVP, Multi Protocol Label Switching Traffic Engineering, IGMP Version 2 und 3 sowie andere Protokolle, die IP-Optionen verwenden, nicht ordnungsgemäß funktionieren können, wenn Pakete für diese Protokolle verworfen werden. Wenn diese Protokolle im Netzwerk verwendet werden, kann die ACL-Unterstützung für das Filtern von IP-Optionen verwendet werden. Die ACL-Funktion zum selektiven Löschen von IP-Optionen kann diesen Datenverkehr jedoch verwerfen, und diese Protokolle können nicht ordnungsgemäß funktionieren. Wenn es keine gebräuchlichen Protokolle gibt, die IP-Optionen benötigen, ist ACL-IP-Options-selektiver Rückgang die bevorzugte Methode, zum dieser Pakete fallenzulassen.

Dieses ACL-Beispiel erstellt eine Politik dieses Filter IP-Pakete, die alle mögliche IP-Optionen enthalten:

ip access-list extended ACL-TRANSIT-IN

deny ip any option any option any options

permit ip any any

interface GigabitEthernet 0/0

ip access-group ACL-TRANSIT-IN eingehend

Dieses Beispiel ACL zeigt eine Politik dieses Filter IP-Pakete mit fünf spezifischen IP-Optionen. Pakete, die diese Optionen enthalten, werden verweigert:

1. 0 Ende Options-Liste (eool)
2. Rekordweg 7 (Satzweg)
3. Stempel der Zeit-68 (Zeitstempel)
4. 131 - Loser Quellweg (lsr)
5. 137 - Strenger Quellweg (ssr)

ip access-list extended ACL-TRANSIT-IN

ip any option eool verweigern

deny ip any option record-route

deny ip any option timestamp

deny ip any option lsr

deny ip any option ssr

permit ip any any

interface GigabitEthernet 0/0

ip access-group ACL-TRANSIT-IN eingehend

Sehen Sie das flache Verhärtungskapitel der allgemeinen Daten dieses Dokuments zu mehr Information über ACL-IP-Options-selektiven Tropfen.

Eine weitere Funktion der Cisco IOS XE Software, die zum Filtern von Paketen mit IP-Optionen verwendet werden kann, ist CoPP. In Cisco IOS XE Software, Version 16.6.4 und höher, ermöglicht CoPP einem Administrator, den Datenverkehrsfluss von Paketen der Steuerungsebene zu filtern. Ein Gerät, das CoPP und ACL-Unterstützung für das Filtern von IP-Optionen unterstützt, wurde in Version 16.6.4 der Cisco IOS XE-Software eingeführt und kann mithilfe einer Zugriffslistenrichtlinie Pakete filtern, die IP-Optionen enthalten.

Diese CoPP-Politik lässt Durchfahrtpakete fallen, die durch ein Gerät empfangen werden, wenn alle mögliche IP-Optionen anwesend sind:

ip access-list extended ACL-IP-OPTIONEN-ANY

permit ip any any option any options

class-map ACL-IP-OPTIONS-CLASS

Zuordnungsname ACL-IP-OPTIONS-ANY

policy-map COPP-POLICY

class ACL-IP-OPTIONS-CLASS

Polizei 80000 konform Senden überschreiten Tropfen

Kontrollebene

service-policy input COPP-POLICY !

Diese CoPP-Politik lässt die Durchfahrtpakete fallen, die durch ein Gerät empfangen werden, wenn diese IP-Optionen anwesend sind:

1. 0 Ende Options-Liste (eool)
2. Rekordweg 7 (Satzweg)
3. Stempel der Zeit-68 (Zeitstempel)
4. Loser Weg des Quell131 (lsr)
5. Strenger Weg des Quell137 (ssr)

ip access-list erweiterte ACL-IP-OPTIONEN

permit ip any option eool

permit ip any any option record-route

permit ip any any option timestamp

permit ip any any option lsr

permit ip any option ssr

class-map ACL-IP-OPTIONS-CLASS

Zuordnungsname ACL-IP-OPTIONS

policy-map COPP-POLICY

class ACL-IP-OPTIONS-CLASS

Polizei 80000 konform Senden überschreiten Tropfen

Kontrollebene

service-policy input COPP-POLICY

In den vorherigen CoPP-Richtlinien führen die Zugriffskontrolllisteneinträge (ACEs), die Pakete mit der Genehmigungsaktion abgleichen, dazu, dass diese Pakete von der Policy-Map-Dropfunktion verworfen werden, während Pakete, die der Ablehnungsaktion entsprechen (nicht dargestellt), von der Policy-Map-Dropfunktion nicht betroffen sind.

Sprechen Sie die einsetzende Steuerfläche an, die zu mehr Information über das CoPP-Merkmal polizeilich überwacht.

Steuern Sie flachen Schutz

In Cisco IOS XE Software, Version 16.6.4 und höher, kann Control Plane Protection (CPPr) verwendet werden, um den Datenverkehr auf der Kontrollebene durch die CPU eines Cisco IOS XE-Geräts zu beschränken oder zu steuern. CPPr ist CoPP ähnlich, kann jedoch Datenverkehr, der eine höhere Genauigkeit als CoPP benötigt, einschränken oder regeln. Bei CPPr wird die aggregierte Kontrollebene in drei getrennte Kontrollebenenkategorien aufgeteilt, die als Unterschnittstellen bezeichnet werden: Host, Transit und CEF-Exception.

Diese CPPr-Politik lässt die Durchfahrtpakete fallen, die durch ein Gerät empfangen werden, in dem der TTL-Wert kleiner als 6 und die Durchfahrt- oder Nichtdurchfahrtpakete, die durch ein Gerät empfangen werden ist, in dem der TTL-Wert null oder eins ist. Die CPPr-Politik lässt auch Pakete mit ausgewählten IP-Optionen fallen, die durch das Gerät empfangen werden.

ip access-list extended ACL-IP-TTL-0/1

permit ip any ttl eq 0 1

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

Zuordnungsname ACL-IP-TTL-0/1

ip access-list extended ACL-IP-TTL-LOW

permit ip any ttl lt 6

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

match access-group name ACL-IP-TTL-LOW

ip access-list erweiterte ACL-IP-OPTIONEN

permit ip any option eool

permit ip any any option record-route

permit ip any any option timestamp

permit ip any any option lsr

permit ip any option ssr

class-map ACL-IP-OPTIONS-CLASS

Zuordnungsname ACL-IP-OPTIONS

policy-map CPPR-CEF-EXCEPTION-POLICY

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

police 80000 conform action drop

class ACL-IP-OPTIONS-CLASS

Police 8000 conform-action drop

policy-map CPPR-TRANSIT-POLICY

class ACL-IP-TTL-LOW-CLASS

Police 8000 conform-action drop

Transit auf der Kontrollebene

service-policy input CPPR-TRANSIT-POLICY

In der vorhergehenden CPPr-Politik die Access- Control Listeinträge, die Pakete mit dem Erlaubnisaktionsergebnis in diesen Paketen abgleichen, die durch die Politikkartenrückgangsfunktion verworfen werden, während Pakete, die die Leugnungsaktion abgleichen (nicht gezeigt) nicht durch die Politikkartenrückgangsfunktion beeinflußt werden.

Weitere Informationen zur CPPr-Funktion finden Sie unter Control Plane Policing.

Handeln Sie Kennzeichen und Traceback

In manchen Fällen ist eine schnelle Identifizierung und Nachverfolgung des Netzwerkverkehrs erforderlich, insbesondere bei Zwischenfällen oder einer Beeinträchtigung der Netzwerkleistung. NetFlow und Classification ACLs sind die beiden primären Methoden, um dies mit der Cisco IOS XE Software zu erreichen. NetFlow kann Sicht in allen Verkehr auf dem Netz zur Verfügung stellen. Darüber hinaus kann NetFlow mit Collectors implementiert werden, die langfristige Trends und automatische Analysen bereitstellen können. Klassifikation ACLs sind eine Komponente von ACLs und benötigen das Im Voraus planen, zum des spezifischen Verkehrs und der manuellen

Intervention während der Analyse zu identifizieren. Diese Kapitel liefern einen kurzen Überblick über jedes Merkmal.

NetFlow

NetFlow identifiziert unregelmäßige und sicherheitsbezogene Netzaktivität durch Gleichlaufnetzflüsse. NetFlow-Daten können über das CLI angesehen werden und analysiert werden, oder die Daten können in einen Werbung oder Freeware NetFlow-Kollektor für Anhäufung und Analyse exportiert werden. NetFlow-Kollektoren, durch das langfristige Neigen, können Netzverhalten und Verwendungsanalyse zur Verfügung stellen. NetFlow arbeitet, indem er Analyse auf spezifischen Attributen innerhalb IP-Pakete durchführt und das Erstellen fließt. Version 5 ist die allgemein verwendetste Version von NetFlow, jedoch ist Version 9 dehnbarer. NetFlow-Flüsse können mit geprüften Verkehrsdaten in den Großserienumgebungen erstellt werden.

CEF oder Distributed CEF ist eine Voraussetzung für die Aktivierung von NetFlow. NetFlow kann auf Routern und Schaltern konfiguriert werden.

Dieses Beispiel veranschaulicht die Grundkonfiguration dieses Merkmals. In früheren Versionen der Cisco IOS XE Software lautet der Befehl zum Aktivieren von NetFlow auf einer Schnittstelle ip route-cache flow anstelle von ip flow {ingress | Ausgang}.

ip flow-export destination <IP-Adresse> <udp-port>

ip flow-export version <Version>

interface <Schnittstelle>

ip flow <Eingang|Ausgang>

Dieses ist ein Beispiel von NetFlow ausgab vom CLI. Das SrcIf-Attribut kann im Traceback helfen.

router#show ip cache flow IP-Paketgrößenverteilung (insgesamt 26662860 Pakete):

+1-32 64 96 128 160 192 224 256 288 320 352 384 416 448 480

.741 .124 .047 .006 .005 .005 .002 .008 .000 .000 .003 .000 .001 .000 .000

512 544 576 1024 1536 2048 2560 3072 3584 4096 4608

.000 .000 .001 .007 .039 .000 .000 .000 .000 .000 .000

IP-Fluss-Switching-Cache, 4456704 Bytes

55 aktiv, 65481 inaktiv, 1014683 hinzugefügt

41000680 Polling-Anfragen, 0 Fehler bei der Flusszuweisung

Timeout für aktive Datenflüsse in 2 Minuten

Timeout für inaktive Flüsse in 60 Sekunden

IP-Unterfluss-Cache, 336520 Bytes

110 aktiv, 16274 inaktiv, 2029366 hinzugefügt, 1014683 hinzugefügt

0 Zuordnungsfehler, 0 erzwingen frei 1 Stück, 15 Stück hinzugefügt letzte Bereinigung von Statistiken nie

Protokoll - Gesamtanzahl an Datenflüssen Pakete Byte Aktive Pakete (Sek.) Inaktivität (Sek.)

-------- Flows /Sec /Flow /Pkt /Sec /Flow /Flow

TCP-Telnet 11512 0,0 15 42 0,2 33,8 44,8

TCP-FTP 5606 0,0 3 45 0,0 59,5 47,1

TCP-FTPD 1075 0,0 13 52 0,0 1,2 61,1

TCP-WWW 77155 0,0 11 530 1,0 13,9 31,5

TCP-SMTP 8913 0,0 2 43 0,0 74,2 44,4

TCP-X 351 0,0 2 40 0,0 0,0 60,8

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

TCP-NNTP 120 0,0 1 42 0,0 0,7 61,4

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

UDP-DNS 130909 0,1 2 55 0,3 24,0 53,1

UDP-NTP 116213 0,1 1 75 0,1 5,0 58,6

UDP-TFTP 169 0,0 3 51 0,0 15,3 64,2

UDP-Frag 1 0,0 1 1405 0,0 0,0 86,8

UDP-Sonstige 86247 0,1 226 29 24,0 31,4 54,3

ICMP 19989 0,0 37 33 0,9 26,0 53,9

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

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

SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkte

Gi0/1 192.168.128.21 Lokal 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 Lokal 192.168.206.20 01 000 0303 11

Gi0/0 10,89,17,146 Gi0/1 192,168,150,60 06 07F1 0016 1

Weitere Informationen zu den NetFlow-Funktionen finden Sie unter Flexible NetFlow.

Klassifikation ACLs

Klassifikation ACLs stellen Sicht in Verkehr zur Verfügung, der eine Schnittstelle überquert. Klassifikation ACLs ändern nicht die Sicherheitspolitik eines Netzes und werden gewöhnlich konstruiert, um einzelne Protokolle, Quelladressen oder Zieleinheiten zu klassifizieren. Zum Beispiel könnte ACE, der allen Verkehr ermöglicht, in spezifische Protokolle oder in Kanäle getrennt werden. Diese granuliertere Klassifikation des Verkehrs in spezifische Asse kann helfen, ein Verständnis des Netzwerkverkehrs zur Verfügung zu stellen, weil jede Verkehrskategorie seinen eigenen Trefferzähler hat. Ein Administrator kann auch die implizite Ablehnung am Ende einer ACL in detaillierte ACEs aufteilen, um die Typen von abgelehntem Datenverkehr zu identifizieren.

Ein Administrator kann eine Reaktion auf einen Vorfall beschleunigen, indem er Klassifizierungs-ACLs mit den EXEC-Befehlen show access-list und clear ip access-list counters verwendet.

Dieses Beispiel veranschaulicht die Konfiguration einer Klassifikation ACL, um SMB-Verkehr vor einer Nichterfüllung zu identifizieren verweigern:

ip access-list extended ACL-SMB-CLASSIFY

Hinweis Vorhandener Inhalt von ACL

Hinweis Klassifizierung von SMB-spezifischem TCP-Datenverkehr

tcp any eq 139

deny tcp any eq 445

ip any

Um den Datenverkehr zu identifizieren, der eine Klassifizierungs-ACL verwendet, verwenden Sie show access-list acl-name

EXEC-Befehl. Die ACL-Zähler können mit dem Befehl clear ip access-list counters aclname EXEC gelöscht werden.

router#show access-list ACL-SMB-CLASSIFY Erweiterte IP-Zugriffsliste ACL-SMB-CLASSIFY

10 deny tcp any any eq 139 (10 Treffer)

20 deny tcp any any eq 445 (9 Treffer)

30 deny ip any any (184 Treffer)

Siehe Verständnis des Access Control List, das zu mehr Information protokolliert über, wie man protokollierende Fähigkeiten innerhalb ACLs aktiviert.

Zugriffssteuerung mit PACLs

PACLs kann an der Inlandsrichtung auf körperliche Schnittstellen der Schicht 2 eines Schalters nur angewendet werden. Ähnlich VLAN-Karten, stellen PACLs Zugriffssteuerung auf nicht-verlegt zur Verfügung oder überlagern Verkehr 2. Die Syntax für PACLs-Schaffung, die Vorrang vor VLAN-Karten und Router ACLs hat, ist die selbe wie Router ACLs. Wenn ein ACL an einer Schnittstelle der Schicht 2 angewendet wird, dann gekennzeichnet es als ein PACL.

Konfiguration bezieht die Schaffung eines IPv4, des IPv6 oder des MAC ACL und der Anwendung von ihr zur Schnittstelle der Schicht 2 mit ein.

Dieses Beispiel benutzt eine ausgedehnte benannte Zugriffsliste, um die Konfiguration dieses Merkmals zu veranschaulichen:

ip access-list extended <acl-name> permit <Protokoll> <Quelladresse> <Quellport> <Zieladresse> <Zielport> !

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

Weitere Informationen zur Konfiguration von PACLs finden Sie im Abschnitt Konfigurieren der Netzwerksicherheit mit Port-ACLs.

Lokalisiertes VLANs

Die Konfiguration von Sekundär-VLAN als lokalisierten VLAN verhindert vollständig Kommunikation zwischen Geräten in Sekundär-VLAN. Pro primärem VLAN kann nur ein isoliertes VLAN vorhanden sein, und nur Promiscuous Ports können mit Ports in einem isolierten VLAN kommunizieren. Isolierte VLANs können in nicht vertrauenswürdigen Netzwerken verwendet werden, beispielsweise in Netzwerken mit Unterstützung für Gastzugriff.

Dieses Konfigurationsbeispiel konfiguriert VLAN 11 als lokalisiertes VLAN und verbindet es zu Primär-VLAN, VLAN 20. In diesem Beispiel wird die FastEthernet 1/1-Schnittstelle auch als isolierter Port in VLAN 11 konfiguriert:

VLAN 11, privates VLAN, isoliert

VLAN 20 Private-VLAN Primary Private-VLAN Association 11

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

Gemeinschaft VLANs

Sekundär-VLAN, die als Gemeinschaft VLAN konfiguriert wird, erlaubt Kommunikation unter Bauteilen VLANs sowie mit allen gemischten Kanälen in Primär-VLAN. Jedoch ist keine Kommunikation zwischen jeder möglicher zwei Gemeinschaft VLANs oder von einer Gemeinschaft VLAN zu lokalisierten VLAN möglich. Gemeinschaft VLANs muss sein, um zu gruppieren Servers, die Anschlussfähigkeit miteinander benötigen, aber wo Anschlussfähigkeit zu allen weiteren Geräten in VLAN nicht benötigt wird. Dieses Szenario ist in einem öffentlich zugänglichen Netz geläufig, oder überall das Servers stellen Inhalt zu den untrusted Kunden zur Verfügung.

Dieses Beispiel konfiguriert eine einzelne Gemeinschaft VLAN und konfiguriert Schalterkanal FastEthernet 1/2 als Bauteil von diesem VLAN. Die Gemeinschaft VLAN, VLAN 12, ist Sekundär-VLAN zu Primär-VLAN 20.

VLAN 12 Private-VLAN-Community

VLAN 20 Private-VLAN Primary Private-VLAN Association 12

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

Schlussfolgerung

Dieses Dokument gibt Ihnen einen umfassenden Überblick über die Methoden, die zum Sichern eines Cisco IOS XE-Systemgeräts verwendet werden können. Wenn Sie die Geräte sichern, erhöht es die Gesamtsicherheit der Netze, die Sie handhaben. In diesem Überblick werden Schutz des Managements, Steuerung, und Datenflächen wird behandelt, und Empfehlungen für Konfiguration geliefert. Wo möglich wird genügendes Detail für die Konfiguration jedes verbundenen Merkmals bereitgestellt. Jedoch in allen Fällen, werden umfassende Referenzen zur Verfügung gestellt, um Sie mit den Informationen zur Verfügung zu stellen, die für weitere Bewertung benötigt werden.

Quittungen

Einige Merkmalsbeschreibungen in diesem Dokument wurden von den Cisco-Informationsentwicklerteams geschrieben.

Anhang: Checkliste zur Gerätesicherung für Cisco IOS XE

Diese Checkliste ist eine Sammlung aller Verhärtungsschritte, die in dieser Anleitung dargestellt werden.

Administratoren können damit an alle Härtungsfunktionen erinnern, die für ein Cisco IOS XE-Gerät verwendet und berücksichtigt werden, auch wenn eine Funktion nicht implementiert wurde, weil sie nicht anwendbar war. Verwalter werden geraten, jede Option für sein potenzielles Risiko auszuwerten, bevor sie die Option einführen.

Management-Fläche

1. Passwörter
   MD5-Hashing aktivieren (geheime Option) für Kennwörter für lokale und aktivierte BenutzerKennwort konfigurieren, Passwortsperre wiederholenKennwortwiederherstellung deaktivieren (Risiko berücksichtigen)
2. Deaktivieren Sie unbenutzte Dienstleistungen
3. Konfigurieren Sie TCP-Keepalives für Managementsitzungen
4. Stellen Sie Speicher- und CPU-Schwellwertmitteilungen ein
5. Konfigurieren
   Speicher- und CPU-Schwellenwertbenachrichtigungen Reservespeicher für Konsolenzugriff Speicherleckdetektor Buffer-Overflow-Erkennung Erweiterte Absturzinformationen
6. Benutzen Sie iACLs, um Managementzugriff einzuschränken
7. Filtern Sie (betrachten Sie Risiko)
   ICMP-PaketeIP-FragmenteIP-OptionenTTL-Wert in Paketen
8. Steuern Sie flachen Schutz
   Konfigurieren der PortfilterungKonfigurieren von Warteschlangenschwellenwerten
9. Managementzugriff
   Verwenden Sie den Schutz der Verwaltungsebene, um die Verwaltungsschnittstellen einzuschränkenFestlegen des exec-TimeoutsVerwenden Sie ein verschlüsseltes Transportprotokoll (z. B. SSH) für den CLI-ZugriffSteuern Sie den Transport für VTY- und TTY-Leitungen (Option für die Zugriffsklasse)Warnen Sie, dass Banner verwendet werden.
10. AAA
    AAA für Authentifizierung und Fallback verwendenAAA (TACACS+) für Befehlsautorisierung verwendenAAA für Abrechnung verwendenRedundante AAA-Server verwenden
11. SNMP
    SNMPv2-Communitys konfigurieren und ACLs anwendenSNMPv3 konfigurieren
12. Protokollieren
    Zentrale Protokollierung konfigurierenFestlegen von Protokollierungsebenen für alle relevanten KomponentenFestlegen der ProtokollierungsquelleSchnittstelleKonfigurieren der Protokollierung Zeitstempel-Granularität
13. Konfigurationsverwaltung
    Ersetzen und RollbackExklusiver KonfigurationsänderungszugriffKonfiguration der Software-AusfallsicherheitBenachrichtigungen zu Konfigurationsänderungen.

Steuern Sie Fläche

1. Deaktivieren Sie (betrachten Sie Risiko)
   ICMP-UmleitungenICMP nicht erreichbarProxy-ARP
2. Konfigurieren der NTP-Authentifizierung bei Verwendung von NTP
3. Konfigurieren Sie das Steuerflächen-Polizeilich überwachen/Schutz (Kanalentstörung, Warteschlangenschwellwerte)
4. Sichern Sie Wegewahlprotokolle
   BGP (TTL, MD5, maximale Präfixe, Präfixlisten, Systempfad-ACLs)IGP (MD5, passive Schnittstelle, Routenfilterung, Ressourcenauslastung)

5. Konfigurieren Sie Hardware-Kinetikbegrenzer
6. Sichern Sie erste Hopfenredundanz-Protokolle (GLBP, HSRP, VRRP)

Daten-Fläche

1. Konfigurieren Sie IP-Options-selektiven Tropfen
2. Deaktivieren Sie (betrachten Sie Risiko)
   IP-Source-RoutingIP-Directed BroadcastsICMP-Umleitungen
3. Grenz-IP verwiesene Sendungen
4. Konfigurieren Sie tACLs (betrachten Sie Risiko)
   Filtern ICMPFilter IP-FragmenteFilter IP-OptionenFilter TTL-Werte
5. Configure benötigte anti-spoofing Schutze
   ACLsIP Source GuardDynamic ARP InspectionUnicast RPFPort Security
6. Steuern Sie flachen Schutz (Steuerungflächencefausnahme)
7. Konfigurieren Sie NetFlow und Klassifikation ACLs für Verkehrskennzeichen
8. Configure benötigte Zugriffssteuerung ACLs (VLAN-Karten, PACLs, MAC)
9. Konfigurieren Sie privates VLANs

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.