Cisco Leitfaden zur Härtung von Cisco IOS-Geräten

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Hintergrundinformationen
Sichere Betriebsabläufe
Überwachung von Cisco Sicherheitsempfehlungen und -antworten
Nutzung von Authentifizierung, Autorisierung und Abrechnung
Zentralisierte Protokollierung und Überwachung
Sichere Protokolle verwenden, wenn möglich
Erhöhte Datenverkehrstransparenz mit NetFlow
Konfigurationsmanagement
Managementebene
Allgemeine Sicherung der Managementebene
Kennwortmanagement
Erweiterte Kennwortsicherheit
Sperrung der Kennwortrückgabe für die Anmeldung
Keine Service-Kennwortwiederherstellung
Nicht verwendete Services deaktivieren
EXEC-Timeout
Keepalives für TCP-Sitzungen
Verwendung der Verwaltungsschnittstelle
Benachrichtigungen zu Speicherschwellenwerten
Benachrichtigung über CPU-Grenzwert
Reservierungsspeicher für Konsolenzugriff
Speicherleckerkenner
Pufferüberlauf: Erkennung und Korrektur von Redzone Corruption
Erweiterte Crashinfo-Dateierfassung
Netzwerkzeitprotokoll
Smart Install deaktivieren
Einschränkung des Netzwerkzugriffs mithilfe von Infrastruktur-ACLs
ICMP-Paketfilterung
IP-Fragmente filtern
ACL-Unterstützung für IP-Filteroptionen
ACL-Unterstützung zum Filtern nach TTL-Wert
Sichere interaktive Verwaltungssitzungen
Schutz der Managementebene
Schutz der Kontrollebene

Verschlüsseln von Management-Sitzungen
SSHv2
SSHv2-Erweiterungen für RSA-Schlüssel
Konsolen- und AUX-Ports
Steuerungs-VTY und TTL-Posten
Steuern des Transports von VTY- und TTL-Posten
Warnbanner
Authentifizierung, Autorisierung und Abrechnung
TACACS+-Authentifizierung
Authentifizierungsfallback
Verwendung von Kennwörtern vom Typ 7
TACACS+-Befehlsautorisierung
TACACS+-Befehlsabrechnung
Redundante AAA-Server
Stärkung des Simple Network Management Protocol
SNMP-Community-Strings
SNMP-Community-Strings mit ACLs
Infrastruktur-ACLs
SNMP-Ansichten
SNMP-Version 3
Schutz der Managementebene
Protokollieren von Best Practices
Protokolle an einen zentralen Standort senden
Protokollierungsebene
Melden Sie sich nicht bei Konsolen- oder Überwachungssitzungen an.
Buffered-Protokollierung verwenden
Konfigurieren der Protokollierungsquellenschnittstelle
Konfigurieren von Protokollzeitstempeln
Konfigurationsmanagement für die Cisco IOS Software
Konfigurationsaustausch und Konfigurations-Rollback
Exklusiver Zugriff auf Konfigurationsänderungen
Ausfallsichere Konfiguration der Cisco IOS Software
Digital signierte Cisco Software
Benachrichtigungen und Protokollierung von Konfigurationsänderungen
Kontrollebene
Sicherung der allgemeinen Kontrollebene
IP ICMP-Umleitungen
ICMP nicht erreichbar
Proxy-ARP
Begrenzung der CPU-Auswirkungen des Datenverkehrs auf der Kontrollebene
Verständnis des Kontrollebenen-Datenverkehrs
Infrastruktur-ACLs
Empfangen von ACLs
CoPP
Schutz der Kontrollebene

Hardware-Ratenlimitierungen
Sicheres BGP
TTL-basierter Sicherheitsschutz
BGP-Peer-Authentifizierung mit MD5
Maximale Präfixe konfigurieren
BGP-Präfixe mit Präfixlisten filtern
Filtern von BGP-Präfixen mit autonomen Systempfad-Zugriffslisten
Secure Interior Gateway-Protokolle
Routing-Protokoll-Authentifizierung und -Verifizierung mit Message Digest 5
Passive Schnittstellenbefehle
Routenfilterung
Ressourcennutzung im Routing-Prozess
Sichere Protokolle für die erste Hop-Redundanz
Datenebene
Allgemeine Datenebenensicherung
IP Options Selective Drop
IP Source Routing deaktivieren
ICMP-Umleitungen deaktivieren
IP-Directed Broadcasts deaktivieren oder beschränken
Filtern von Transit-Datenverkehr mit Transit-ACLs
ICMP-Paketfilterung
IP-Fragmente filtern
ACL-Unterstützung für IP-Filteroptionen
Anti-Spoofing-Schutz
Unicast-RPF
IP Source Guard
Port-Sicherheit
Dynamische ARP-Inspektion
Anti-Spoofing-ACLs
Begrenzung der CPU-Auswirkungen des Datenverkehrs auf der Datenebene
Funktionen und Datenverkehrstypen mit Auswirkungen auf die CPU
Auf TTL-Wert filtern
Filtern auf das Vorhandensein von IP-Optionen
Schutz der Kontrollebene
Identifikation und Rückverfolgung des Datenverkehrs
NetFlow
Klassifizierungs-ACLs
Zugriffskontrolle mit VLAN-Zuordnungen und Port-Zugriffskontrolllisten
Zugriffskontrolle mit VLAN-Zuordnungen
Zugriffskontrolle mit PACLs
Zugriffskontrolle mit MAC
Private VLAN-Nutzung
Isolated-VLANs
Community-VLANs
Promiscuous-Ports

Schlussfolgerung
Bestätigungen
Anhang: Checkliste für die Cisco IOS-Gerätesicherung
Managementebene
Kontrollebene
Datenebene

Einführung

In diesem Dokument werden die Informationen beschrieben, die Ihnen beim Schutz Ihrer Cisco IOS®-Systemgeräte helfen, wodurch die Sicherheit Ihres Netzwerks insgesamt erhöht wird. Dieses Dokument ist rund um die drei Ebenen strukturiert, in die die Funktionen eines Netzwerkgeräts kategorisiert werden können. Es bietet eine Übersicht über die einzelnen Funktionen und Referenzen auf die zugehörige Dokumentation.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Die drei funktionalen Ebenen eines Netzwerks, die Management-Ebene, die Kontrollebene und die Datenebene, bieten jeweils unterschiedliche Funktionen, die geschützt werden müssen.

- **Verwaltungsebene** - Die Verwaltungsebene verwaltet den an das Cisco IOS-Gerät gesendeten Datenverkehr und umfasst Anwendungen und Protokolle wie Secure Shell (SSH) und Simple Network Management Protocol (SNMP).

- **Kontrollebene**: Die Steuerungsebene eines Netzwerkgeräts verarbeitet den Datenverkehr, der für die Aufrechterhaltung der Funktionalität der Netzwerkinfrastruktur von größter Bedeutung ist. Die Kontrollebene besteht aus Anwendungen und Protokollen zwischen Netzwerkgeräten, darunter das Border Gateway Protocol (BGP) sowie Interior Gateway Protocols (IGPs) wie das Enhanced Interior Gateway Routing Protocol (EIGRP) und Open Shortest Path First (OSPF).

- **Datenebene**: Die Datenebene leitet Daten über ein Netzwerkgerät weiter. Die Datenebene

enthält keinen Datenverkehr, der an das lokale Cisco IOS-Gerät gesendet wird.

Die Abdeckung der Sicherheitsfunktionen in diesem Dokument bietet häufig genug Details, um die Funktion zu konfigurieren. Wenn dies jedoch nicht der Fall ist, wird die Funktion so erklärt, dass Sie beurteilen können, ob eine zusätzliche Aufmerksamkeit für die Funktion erforderlich ist. Dieses Dokument enthält, soweit möglich und angemessen, Empfehlungen, die bei der Sicherung eines Netzwerks helfen, falls es implementiert wird.

Sichere Betriebsabläufe

Ein wichtiger Punkt ist der sichere Netzwerkbetrieb. Obwohl der Großteil dieses Dokuments der sicheren Konfiguration eines Cisco IOS-Geräts gewidmet ist, wird ein Netzwerk durch Konfigurationen allein nicht vollständig gesichert. Die im Netzwerk verwendeten Betriebsverfahren tragen ebenso zur Sicherheit bei wie die Konfiguration der zugrunde liegenden Geräte.

Diese Themen enthalten betriebliche Empfehlungen, die Sie implementieren sollten. Diese Themen stellen bestimmte kritische Bereiche des Netzwerkbetriebs heraus und sind nicht umfassend.

Überwachung von Cisco Sicherheitsempfehlungen und -antworten

Das Cisco Product Security Incident Response Team (PSIRT) erstellt und pflegt Veröffentlichungen, die allgemein als PSIRT Advisories bezeichnet werden, für sicherheitsrelevante Probleme von Cisco Produkten. Die für die Kommunikation bei weniger schwerwiegenden Problemen verwendete Methode ist Cisco Security Response. Sicherheitsratgeber und Antworten finden Sie unter http://www.cisco.com/go/psirt.

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

Um ein sicheres Netzwerk zu gewährleisten, müssen Sie die veröffentlichten Cisco Sicherheitsratgeber und -reaktionen kennen. Bevor die Bedrohung für ein Netzwerk ausgewertet werden kann, muss eine Sicherheitslücke bekannt sein. Informationen zu diesem Evaluierungsprozess finden Sie in Risk Triage for Security Vulnerability Ankündigungen.

Nutzung von Authentifizierung, Autorisierung und Abrechnung

Das Authentication, Authorization, and Accounting (AAA)-Framework ist für die Sicherung von Netzwerkgeräten unerlässlich. Das AAA-Framework ermöglicht die Authentifizierung von Managementsitzungen und kann die Benutzer auf spezifische, vom Administrator definierte Befehle beschränken und alle von allen Benutzern eingegebenen Befehle protokollieren. Weitere Informationen zur Verwendung von AAA finden Sie im Abschnitt Authentifizierung, Autorisierung und Abrechnung dieses Dokuments.

Zentralisierte Protokollierung und Überwachung

Um Informationen über bestehende, neue und historische Ereignisse im Zusammenhang mit Sicherheitsvorfällen zu erhalten, muss Ihr Unternehmen über eine einheitliche Strategie für die Protokollierung und Korrelation von Ereignissen verfügen. Diese Strategie muss die Protokollierung aller Netzwerkgeräte nutzen und vorkonfigurierte und anpassbare Korrelationsfunktionen verwenden.

Nach der Implementierung der zentralen Protokollierung müssen Sie einen strukturierten Ansatz für die Protokollanalyse und die Incident-Verfolgung entwickeln. Je nach Anforderungen Ihres Unternehmens reicht dieser Ansatz von einer einfachen sorgfältigen Überprüfung der Protokolldaten bis hin zu einer erweiterten regelbasierten Analyse.

Weitere Informationen zur Implementierung der Protokollierung auf Cisco IOS-Netzwerkgeräten finden Sie im Abschnitt "Best Practices für die Protokollierung" dieses Dokuments.

Sichere Protokolle verwenden, wenn möglich

Viele Protokolle werden zum Übertragen vertraulicher Netzwerkmanagementdaten verwendet. Wenn möglich müssen Sie sichere Protokolle verwenden. Eine sichere Protokollauswahl umfasst die Verwendung von SSH anstelle von Telnet, sodass Authentifizierungsdaten und Managementinformationen verschlüsselt werden. Darüber hinaus müssen Sie beim Kopieren von Konfigurationsdaten sichere Dateiübertragungsprotokolle verwenden. Ein Beispiel hierfür ist die Verwendung des Secure Copy Protocol (SCP) anstelle von FTP oder TFTP.

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

Erhöhte Datenverkehrstransparenz mit NetFlow

NetFlow ermöglicht die Überwachung von Datenverkehrsflüssen im Netzwerk. Ursprünglich für den Export von Datenverkehrsinformationen in Netzwerkmanagement-Anwendungen vorgesehen, kann NetFlow auch verwendet werden, um Flow-Informationen auf einem Router anzuzeigen. So können Sie in Echtzeit sehen, welcher Datenverkehr das Netzwerk passiert. Unabhängig davon, ob Flow-Informationen an einen RemotecCollector exportiert werden, wird empfohlen, Netzwerkgeräte für NetFlow zu konfigurieren, damit diese bei Bedarf reaktiv verwendet werden können.

Weitere Informationen zu dieser Funktion finden Sie im Abschnitt Traffic Identification and Traceback dieses Dokuments und unter http://www.cisco.com/go/netflow (nur registrierte Kunden).

Konfigurationsmanagement

Konfigurationsmanagement ist ein Prozess, mit dem Konfigurationsänderungen vorgeschlagen, überprüft, genehmigt und bereitgestellt werden. Im Zusammenhang mit einer Cisco IOS-Gerätekonfiguration sind zwei weitere Aspekte des Konfigurationsmanagements entscheidend: Konfigurationsarchivierung und Sicherheit.

Sie können Konfigurationsarchive verwenden, um Änderungen an Netzwerkgeräten zurückzusetzen. In einem Sicherheitskontext können auch Konfigurationsarchive verwendet werden, um festzustellen, welche Sicherheitsänderungen vorgenommen wurden und wann diese Änderungen eingetreten sind. In Verbindung mit AAA-Protokolldaten können diese Informationen bei der Sicherheitsprüfung von Netzwerkgeräten hilfreich sein.

Die Konfiguration eines Cisco IOS-Geräts enthält viele vertrauliche Details. Benutzernamen, Kennwörter und der Inhalt von Zugriffskontrolllisten sind Beispiele für diese Art von Informationen. Das Repository, das Sie zur Archivierung der Cisco IOS-Gerätekonfigurationen verwenden, muss gesichert werden. Der unsichere Zugriff auf diese Informationen kann die Sicherheit des gesamten Netzwerks beeinträchtigen.

Managementebene

Die Verwaltungsebene besteht aus Funktionen, die die Managementziele des Netzwerks erreichen. Dazu gehören interaktive Verwaltungssitzungen, die SSH verwenden, sowie die Sammlung von Statistiken mit SNMP oder NetFlow. Wenn Sie die Sicherheit eines Netzwerkgeräts in Betracht ziehen, ist es wichtig, dass die Verwaltungsebene geschützt wird. Wenn ein Sicherheitsvorfall die Funktionen der Managementebene untergraben kann, kann es für Sie unmöglich sein, das Netzwerk wiederherzustellen oder zu stabilisieren.

In diesen Abschnitten dieses Dokuments werden die Sicherheitsfunktionen und -konfigurationen der Cisco IOS-Software erläutert, die zur Stärkung der Verwaltungsebene beitragen.

Allgemeine Sicherung der Managementebene

Die Verwaltungsebene dient dem Zugriff, der Konfiguration und dem Management eines Geräts sowie der Überwachung seines Betriebs und des Netzwerks, in dem es bereitgestellt wird. Die Managementebene ist die Ebene, die Datenverkehr für den Betrieb dieser Funktionen empfängt und sendet. Sie müssen sowohl die Management-Ebene als auch die Kontrollebene eines Geräts sichern, da sich der Betrieb der Kontrollebene direkt auf den Betrieb der Verwaltungsebene auswirkt. Diese Protokollliste wird von der Verwaltungsebene verwendet:

- Einfaches Netzwerkmanagement-Protokoll
- Telnet
- Secure Shell-Protokoll
- Dateiübertragungsprotokoll
- HyperText Transfer Protocol/Secure HyperText Transfer Protocol
- Trivial File Transfer Protocol
- Sicheres Kopierprotokoll
- TACACS+
- RADIUS
- NetFlow
- Netzwerkzeitprotokoll
- Syslog

Es müssen Schritte unternommen werden, um sicherzustellen, dass die Verwaltungs- und Kontrollebenen bei Sicherheitsvorfällen erhalten bleiben. Wenn eine dieser Ebenen erfolgreich ausgenutzt wird, können alle Ebenen kompromittiert werden.

Kennwortmanagement

Passwörter steuern den Zugriff auf Ressourcen oder Geräte. Dies wird durch die Definition eines Kennworts oder Geheimtitels erreicht, das zur Authentifizierung von Anforderungen verwendet wird. Wenn eine Anfrage für den Zugriff auf eine Ressource oder ein Gerät eingeht, wird die Anforderung zur Überprüfung des Kennworts und der Identität angefochten, und der Zugriff kann basierend auf dem Ergebnis gewährt, verweigert oder eingeschränkt werden. Als Best Practice für die Sicherheit müssen Kennwörter mit einem TACACS+- oder RADIUS-Authentifizierungsserver verwaltet werden. Beachten Sie jedoch, dass bei einem Ausfall der TACACS+- oder RADIUS-Dienste weiterhin ein lokal konfiguriertes Kennwort für den privilegierten Zugriff erforderlich ist. Ein Gerät kann auch andere Kennwortinformationen in seiner Konfiguration enthalten, z. B. einen NTP-Schlüssel, einen SNMP Community String oder einen Routing Protocol-Schlüssel.

Der Befehl **enable secret** wird verwendet, um das Kennwort festzulegen, das privilegierten Administratorzugriff auf das Cisco IOS-System gewährt. Der Befehl **enable secret** muss statt des Befehls **enable password** verwendet werden. Der Befehl **enable password** verwendet einen schwachen Verschlüsselungsalgorithmus.

Wenn kein enable secret festgelegt ist und ein Kennwort für die Konsolentty-Leitung konfiguriert ist, kann das Konsolenkennwort verwendet werden, um selbst über eine Remote Virtual tty (vty)-Sitzung privilegierten Zugriff zu erhalten. Diese Aktion ist mit Sicherheit unerwünscht und ein weiterer Grund, die Konfiguration eines "enable secret" zu gewährleisten.

Der globale Konfigurationsbefehl **für die Service-Passwortverschlüsselung** leitet die Cisco IOS-Software an die Verschlüsselung der Passwörter, der CHAP-Geheimnisse (Challenge Handshake Authentication Protocol) und ähnlicher Daten, die in der Konfigurationsdatei gespeichert sind. Eine solche Verschlüsselung ist nützlich, um zu verhindern, dass gelegentliche Beobachter Passwörter lesen, z. B. wenn sie den Bildschirm über der Sicherheitslage eines Administrators betrachten. Der vom Befehl **zur Dienstkennwortverschlüsselung** verwendete Algorithmus ist jedoch eine einfache Vigen re-Verschlüsselung. Der Algorithmus ist nicht dafür konzipiert, Konfigurationsdateien vor ernsthaften Analysen selbst geringfügig komplexer Angreifer zu schützen, und darf nicht für diesen Zweck verwendet werden. Jede Cisco IOS-Konfigurationsdatei, die verschlüsselte Kennwörter enthält, muss mit der gleichen Sorgfalt behandelt werden, die auch für eine Klartextliste dieser Kennwörter verwendet wird.

Dieser schwache Verschlüsselungsalgorithmus wird vom Befehl **enable secret** nicht verwendet, wird jedoch vom globalen Konfigurationsbefehl **enable password** sowie vom Befehl **password** line configuration verwendet. Kennwörter dieses Typs müssen entfernt und der Befehl **enable secret** oder die Funktion Enhanced Password Security verwendet werden.

Der Befehl **enable secret** und die Funktion Enhanced Password Security (Erweiterte Kennwortsicherheit) verwenden Message Digest 5 (MD5) für das Kennwort-Hashing. Dieser Algorithmus wurde von der Öffentlichkeit eingehend geprüft und ist nicht als umkehrbar bekannt. Der Algorithmus ist jedoch auch Wörterbuchangriffen ausgesetzt. Bei einem Wörterbuchangriff versucht ein Angreifer jedes Wort in einem Wörterbuch oder einer anderen Liste potenzieller Passwörter, um eine Übereinstimmung zu finden. Aus diesem Grund müssen Konfigurationsdateien sicher gespeichert und nur für vertrauenswürdige Personen freigegeben werden.

Erweiterte Kennwortsicherheit

Die in der Cisco IOS Software, Version 12.2(8)T, vorgestellte Funktion Enhanced Password Security (Erweiterte Kennwortsicherheit) ermöglicht es einem Administrator, das MD5-Hashing von Kennwörtern für den Befehl **username** zu konfigurieren. Vor dieser Funktion gab es zwei

Arten von Kennwörtern: Geben Sie 0 ein, ein Klartext-Kennwort, und Type 7, der den Algorithmus der Vigen-re-Verschlüsselung verwendet. Die Funktion für erweiterte Kennwortsicherheit kann nicht mit Protokollen verwendet werden, die das Abrufen des Klartext-Kennworts erfordern, z. B. CHAP.

Um ein Benutzerkennwort mit MD5-Hashing zu verschlüsseln, geben Sie den globalen Konfigurationsbefehl **username secret** ein.

```
!

username <name> secret <password>

!
```

Weitere Informationen zu dieser Funktion *finden Sie unter* Erweiterte Kennwortsicherheit.

Sperrung der Kennwortrückgabe für die Anmeldung

Mit der in der Cisco IOS Software, Version 12.3(14)T, hinzugefügten Funktion zur erneuten Eingabe von Kennwörtern können Sie ein lokales Benutzerkonto sperren, nachdem eine konfigurierte Anzahl erfolgloser Anmeldeversuche ausgeführt wurde. Wenn ein Benutzer gesperrt ist, wird sein Konto gesperrt, bis Sie es entsperren. Ein autorisierter Benutzer, der mit der Berechtigungsstufe 15 konfiguriert ist, kann mit dieser Funktion nicht ausgeschlossen werden. Die Anzahl der Benutzer mit der Berechtigungsstufe 15 muss auf ein Minimum beschränkt sein.

Beachten Sie, dass autorisierte Benutzer sich von einem Gerät absperren können, wenn die Anzahl der fehlgeschlagenen Anmeldeversuche erreicht ist. Außerdem kann ein böswilliger Benutzer eine DoS-Bedingung (Denial of Service) erstellen, bei der wiederholt versucht wird, sich mit einem gültigen Benutzernamen zu authentifizieren.

In diesem Beispiel wird veranschaulicht, wie die Sperrfunktion für die Kennwortrückgabe bei der Anmeldung aktiviert wird:

```
!

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

!

username <name> secret <password>

!
```

Diese Funktion gilt auch für Authentifizierungsmethoden wie CHAP und Password Authentication Protocol (PAP).

Keine Service-Kennwortwiederherstellung

In der Cisco IOS Softwareversion 12.3(14)T und höher ermöglicht die Funktion "No Service Password-Recovery" niemandem mit Konsolenzugriff den unsicheren Zugriff auf die Gerätekonfiguration und das Löschen des Kennworts. Darüber hinaus können böswillige Benutzer den Konfigurationsregisterwert nicht ändern und nicht auf den NVRAM zugreifen.

```
!

no service password-recovery

!
```

Die Cisco IOS-Software stellt ein Verfahren zur Kennwortwiederherstellung bereit, das beim Systemstart mithilfe der Break-Taste auf den ROM Monitor Mode (ROMMON) zugreift. In ROMMON kann die Gerätesoftware neu geladen werden, um eine neue Systemkonfiguration mit einem neuen Kennwort anzufordern.

Das aktuelle Verfahren zur Kennwortwiederherstellung ermöglicht jedem Benutzer mit Konsolenzugriff den Zugriff auf das Gerät und das Netzwerk. Die Funktion "No Service Password - Recovery" (Keine Dienstkennwortwiederherstellung) verhindert, dass die Break-Schlüsselsequenz abgeschlossen und während des Systemstarts ROMMON eingegeben wird.

Wenn **keine Wiederherstellung des Dienstkennworts** auf einem Gerät aktiviert ist, wird empfohlen, eine Offline-Kopie der Gerätekonfiguration zu speichern und eine Konfigurationsarchivierungslösung zu implementieren. Wenn das Kennwort eines Cisco IOS-Geräts nach Aktivierung dieser Funktion wiederhergestellt werden muss, wird die gesamte Konfiguration gelöscht.

Weitere Informationen zu dieser Funktion *finden Sie* im Konfigurationsbeispiel für sichere ROMMON.

Nicht verwendete Services deaktivieren

Als Best Practice für die Sicherheit müssen alle unnötigen Dienste deaktiviert werden. Diese nicht benötigten Services, insbesondere solche, die das User Datagram Protocol (UDP) verwenden, werden selten für legitime Zwecke verwendet, können aber zum Starten von DoS und anderen Angriffen verwendet werden, die sonst durch die Paketfilterung verhindert werden.

Die kleinen TCP- und UDP-Dienste müssen deaktiviert werden. Diese Services umfassen:

- echo (Portnummer 7)
- verwerfen (Portnummer 9)
- Tageszeit (Portnummer 13)
- Chargen (Portnummer 19)

Obwohl der Missbrauch kleiner Dienste durch Anti-Spoofing-Zugriffslisten vermieden oder die Gefahr verringert werden kann, müssen die Dienste auf allen Geräten deaktiviert werden, auf die im Netzwerk zugegriffen werden kann. Die kleinen Services sind in Cisco IOS Software Releases 12.0 und höher standardmäßig deaktiviert. In früheren Softwareprogrammen können **keine Service-TCP-Small-Servers** und **keine Service-UDP-Small-Servers** globale Konfigurationsbefehle ausgegeben werden, um diese zu deaktivieren.

Dies ist eine Liste zusätzlicher Dienste, die deaktiviert werden müssen, wenn sie nicht verwendet werden:

- Geben Sie den globalen Konfigurationsbefehl **no ip finger** ein, um den Fingerdienst zu

deaktivieren. In Cisco IOS-Softwareversionen nach 12.1(5) und 12.1(5)T wird dieser Dienst standardmäßig deaktiviert.

- Geben Sie den globalen Konfigurationsbefehl **no ip bootp server** aus, um das Bootstrap Protocol (BOOTP) zu deaktivieren.

- Führen Sie in der Cisco IOS Software Version 12.2(8)T und höher den Befehl **ip dhcp bootp ignore** im globalen Konfigurationsmodus aus, um BOOTP zu deaktivieren. Damit bleiben DHCP-Dienste (Dynamic Host Configuration Protocol) aktiviert.

- DHCP-Dienste können deaktiviert werden, wenn keine DHCP-Relay-Services erforderlich sind. Geben Sie den Befehl **no service dhcp** im globalen Konfigurationsmodus ein.

- Geben Sie im Schnittstellenkonfigurationsmodus den Befehl **no mop enabled** aus, um den Wartungsprotokolldienst (Maintenance Operation Protocol, MOP) zu deaktivieren.

- Geben Sie den globalen Konfigurationsbefehl **no ip domain-lookup** aus, um DNS-Auflösungsdienste zu deaktivieren.

- Geben Sie den Befehl **no service pad** im globalen Konfigurationsmodus ein, um den für X.25-Netzwerke verwendeten Dienst Packet Assembler/Disassembler (PAD) zu deaktivieren.

- Der HTTP-Server kann im globalen Konfigurationsmodus mit dem Befehl **no ip http server** deaktiviert werden, und der Secure HTTP (HTTPS)-Server kann mit dem globalen Konfigurationsbefehl **no ip http secure-server** deaktiviert werden.

- Der globale Konfigurationsbefehl **no service config** muss verwendet werden, es sei denn, Cisco IOS-Geräte rufen während des Starts Konfigurationen aus dem Netzwerk ab. Dadurch wird verhindert, dass das Cisco IOS-Gerät versucht, eine Konfigurationsdatei im Netzwerk mit TFTP zu suchen.

- Cisco Discovery Protocol (CDP) ist ein Netzwerkprotokoll, das zur Erkennung anderer CDP-fähiger Geräte für Nachbarnähe und Netzwerktopologie verwendet wird. CDP kann von Netzwerkmanagementsystemen (NMS) oder bei der Fehlerbehebung verwendet werden. CDP muss auf allen Schnittstellen deaktiviert werden, die mit nicht vertrauenswürdigen Netzwerken verbunden sind. Dies wird mit dem Befehl **no cdp enable** interface erreicht. Alternativ kann CDP mithilfe des globalen Konfigurationsbefehls **no cdp run** global deaktiviert werden. Beachten Sie, dass CDP von einem böswilligen Benutzer für die Aufklärung und Netzwerkzuordnung verwendet werden kann.

- Link Layer Discovery Protocol (LLDP) ist ein IEEE-Protokoll, das in 802.1AB definiert ist. LLDP ähnelt CDP. Dieses Protokoll ermöglicht jedoch die Interoperabilität zwischen anderen Geräten, die CDP nicht unterstützen. LLDP muss auf dieselbe Weise wie CDP behandelt und auf allen Schnittstellen deaktiviert werden, die mit nicht vertrauenswürdigen Netzwerken verbunden sind. Geben Sie dazu die Schnittstellenkonfigurationsbefehle **no lldp send** und **no lldp Receive** an. Geben Sie den globalen Konfigurationsbefehl **no lldp run** aus, um LLDP global zu deaktivieren. LLDP kann auch von böswilligen Benutzern für die Aufklärung und Netzwerkzuordnung verwendet werden.

- Bei Switches, die das Booten von sdflash unterstützen, kann die Sicherheit durch Booten vom Flash-Speicher und Deaktivieren von sdflash mit dem Konfigurationsbefehl "no sdflash" erhöht werden.

EXEC-Timeout

Um das Intervall festzulegen, in dem der EXEC-Befehlsinterpreter auf Benutzereingaben wartet, bevor er eine Sitzung beendet, führen Sie den Konfigurationsbefehl **exec-timeout-**Zeile aus. Der Befehl **exec-timeout** muss verwendet werden, um Sitzungen auf VTY- oder tty-Zeilen abzumelden, die nicht aktiv sind. Standardmäßig werden Sitzungen nach zehn Minuten Inaktivität getrennt.

```
!

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

Keepalives für TCP-Sitzungen

Die **Service-Tcp-Keepalive-in-** und **Service-TCP-Keepalive-out-**globalen Konfigurationsbefehle ermöglichen einem Gerät das Senden von TCP-Keepalives für TCP-Sitzungen. Diese Konfiguration muss verwendet werden, um TCP-Keepalives für eingehende Verbindungen zum Gerät und für ausgehende Verbindungen vom Gerät zu aktivieren. Dadurch wird sichergestellt, dass auf das Gerät am Remote-Ende der Verbindung weiterhin zugegriffen werden kann und dass halb offene oder verwaiste Verbindungen vom lokalen Cisco IOS-Gerät entfernt werden.

```
!

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

Verwendung der Verwaltungsschnittstelle

Der Zugriff auf die Verwaltungsebene eines Geräts erfolgt in-band oder Out-of-Band über eine physische oder logische Verwaltungsschnittstelle. Im Idealfall besteht für jedes Netzwerkgerät sowohl In-Band- als auch Out-of-Band-Managementzugriff, sodass bei Netzwerkausfällen auf die Verwaltungsebene zugegriffen werden kann.

Eine der gebräuchlichsten Schnittstellen für den In-Band-Zugriff auf ein Gerät ist die logische Loopback-Schnittstelle. Loopback-Schnittstellen sind immer aktiv, während physische Schnittstellen den Zustand ändern können und die Schnittstelle möglicherweise nicht zugänglich ist. Es wird empfohlen, jedem Gerät eine Loopback-Schnittstelle als Management-Schnittstelle hinzuzufügen und diese Schnittstelle ausschließlich für die Management-Ebene zu verwenden. So kann der Administrator im gesamten Netzwerk Richtlinien für die Verwaltungsebene anwenden. Nachdem die Loopback-Schnittstelle auf einem Gerät konfiguriert wurde, kann sie von Protokollen der Verwaltungsebene wie SSH, SNMP und Syslog verwendet werden, um Datenverkehr zu senden und zu empfangen.

```
!
```

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

Benachrichtigungen zu Speicherschwellenwerten

Die Funktion Memory Threshold Notification, die in der Cisco IOS Software, Version 12.3(4)T, hinzugefügt wird, ermöglicht Ihnen, die Bedingungen für niedrige Speicherkapazität auf einem Gerät zu mindern. Diese Funktion verwendet zwei Methoden, um dies zu erreichen: Benachrichtigung über Speicherschwellenwerte und Speicherreservierung.

Eine Meldung über Speicherschwellenwerte generiert eine Protokollmeldung, die angibt, dass der freie Speicher auf einem Gerät unter den konfigurierten Grenzwert gefallen ist. In diesem Konfigurationsbeispiel wird veranschaulicht, wie diese Funktion mit dem globalen Konfigurationsbefehl **Low-Watermark-Speicher** aktiviert wird. Dadurch kann ein Gerät eine Benachrichtigung generieren, wenn der verfügbare freie Speicher unter den festgelegten Grenzwert fällt und der verfügbare freie Speicher erneut auf fünf Prozent über dem angegebenen Grenzwert ansteigt.

```
!

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

Die Speicherreservierung wird verwendet, damit genügend Speicher für kritische Benachrichtigungen verfügbar ist. In diesem Konfigurationsbeispiel wird veranschaulicht, wie diese Funktion aktiviert wird. Dadurch wird sichergestellt, dass Verwaltungsprozesse auch bei erschöpftem Gerätemarkt weiter funktionieren.

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

Weitere Informationen zu dieser Funktion *finden Sie unter* Benachrichtigungen zu Speicherschwellenwerten.

Benachrichtigung über CPU-Grenzwert

Die in der Cisco IOS Software, Version 12.3(4)T, eingeführte Funktion für die Benachrichtigung bei CPU-Grenzwertüberschreitung ermöglicht Ihnen die Erkennung und Benachrichtigung, wenn die CPU-Last eines Geräts einen konfigurierten Grenzwert überschreitet. Wenn der Grenzwert überschritten wird, generiert das Gerät eine SNMP-Trap-Meldung und sendet diese. Zwei CPU-Auslastungs-Grenzwertverfahren werden von der Cisco IOS-Software unterstützt: Steigende Schwellenwerte und sinkende Schwellenwerte.

In dieser Beispielkonfiguration wird veranschaulicht, wie die Schwellenwerte für steigende und sinkende Werte aktiviert werden, die eine Meldung über einen CPU-Grenzwert auslösen:

```
!

snmp-server enable traps cpu threshold
!
```

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

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

Weitere Informationen zu dieser Funktion *finden Sie unter* Benachrichtigung über CPU-Schwellwerte.

Reservierungsspeicher für Konsolenzugriff

In der Cisco IOS Software, Version 12.4(15)T und höher, kann die Funktion "Reserve Memory for Console Access" (Reservierungsspeicher für Konsolenzugriff) verwendet werden, um genügend Arbeitsspeicher zu reservieren, um den Konsolenzugriff auf ein Cisco IOS-Gerät für administrative und Fehlerbehebungszwecke sicherzustellen. Diese Funktion ist besonders nützlich, wenn das Gerät wenig Arbeitsspeicher hat. Sie können den globalen Konfigurationsbefehl **Memory Reserve Console** ausführen, um diese Funktion zu aktivieren. In diesem Beispiel wird ein Cisco IOS-Gerät so konfiguriert, dass 4096 Kilobyte für diesen Zweck reserviert werden.

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

Weitere Informationen zu dieser Funktion *finden Sie unter* Reservierungsspeicher für Konsolenzugriff.

Speicherleckerkenner

Die in der Cisco IOS-Softwareversion 12.3(8)T1 vorgestellte Funktion zur Erkennung von Speicherlecks auf einem Gerät ermöglicht die Erkennung von Datenlecks. Memory Leak Detector kann Lecks in allen Speicherpools, Paketpuffern und Chunks finden. Speicherlecks sind statische oder dynamische Speicherzuweisungen, die keinem sinnvollen Zweck dienen. Diese Funktion konzentriert sich auf dynamische Speicherzuweisungen. Sie können den EXEC-Befehl **show memory debug lecks** verwenden, um festzustellen, ob ein Speicherleck vorhanden ist.

Pufferüberlauf: Erkennung und Korrektur von Redzone Corruption

In der Cisco IOS Software, Version 12.3(7)T und höher, bietet der Buffer Overflow folgende Vorteile: Die Funktion zur Erkennung und Korrektur von Redzone Corruption kann von einem Gerät aktiviert werden, um einen Speicherblocküberlauf zu erkennen und zu korrigieren und um den Betrieb fortzusetzen.

Diese globalen Konfigurationsbefehle können verwendet werden, um diese Funktion zu aktivieren. Nach der Konfiguration kann der Befehl **show memory overflow** verwendet werden, um die Erkennungs- und Korrekturstatistiken für Pufferüberläufe anzuzeigen.

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

Erweiterte Crashinfo-Dateierfassung

Die Funktion Enhanced Crashinfo File Collection löscht automatisch alte Crashinfo-Dateien. Mit dieser Funktion, die in der Cisco IOS Software, Version 12.3(11)T, hinzugefügt wird, kann ein Gerät Speicherplatz zurückgewinnen, um beim Absturz des Geräts neue Crashinfo-Dateien zu erstellen. Mit dieser Funktion kann auch die Anzahl der Crashinfo-Dateien konfiguriert werden, die gespeichert werden sollen.

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

Netzwerkzeitprotokoll

Das Network Time Protocol (NTP) ist kein besonders gefährlicher Dienst, aber alle nicht benötigten Services können einen Angriffsvektor darstellen. Wenn NTP verwendet wird, ist es wichtig, eine vertrauenswürdige Zeitquelle explizit zu konfigurieren und die korrekte Authentifizierung zu verwenden. Für Syslog-Zwecke, z. B. bei forensischen Untersuchungen potenzieller Angriffe, sowie für eine erfolgreiche VPN-Verbindung ist eine genaue und zuverlässige Zeit erforderlich, wenn Zertifikate für Phase-1-Authentifizierung benötigt werden.

- **NTP-Zeitzone** - Wenn Sie NTP konfigurieren, muss die Zeitzone so konfiguriert werden, dass Zeitstempel korrekt korreliert werden können. In der Regel gibt es zwei Ansätze, um die Zeitzone für Geräte in einem Netzwerk mit globaler Präsenz zu konfigurieren. Eine Möglichkeit besteht darin, alle Netzwerkgeräte mit der koordinierten universellen Zeit (UTC) (früher Greenwich Mean Time (GMT)) zu konfigurieren. Der andere Ansatz besteht darin, Netzwerkgeräte mit der lokalen Zeitzone zu konfigurieren. Weitere Informationen zu dieser Funktion finden Sie in der "clock timezone" in der Cisco Produktdokumentation.

- **NTP-Authentifizierung**: Wenn Sie die NTP-Authentifizierung konfigurieren, wird sichergestellt, dass NTP-Nachrichten zwischen vertrauenswürdigen NTP-Peers ausgetauscht werden.

Beispielkonfiguration mit NTP-Authentifizierung:

Kunde:

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

Server:

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

Smart Install deaktivieren

Die Best Practices für die Sicherheit der Cisco Smart Install-Funktion (SMI) hängen davon ab, wie die Funktion in einer bestimmten Kundenumgebung verwendet wird. Cisco differenziert diese Anwendungsfälle:

- Kunden, die die Smart Install-Funktion nicht verwenden.
- Kunden, die die Smart Install-Funktion nur für die Bereitstellung ohne Benutzereingriff nutzen.

- Kunden, die die Smart Install-Funktion für eine Bereitstellung ohne Benutzereingriff (Konfiguration und Image-Management) nutzen.

In diesen Abschnitten werden die einzelnen Szenarien im Detail beschrieben:

- Kunden, die die Smart Install-Funktion nicht verwenden.
- Kunden, die die Cisco Smart Install-Funktion nicht verwenden und eine Version der Cisco IOS- und Cisco IOS XE-Software ausführen, wenn der Befehl verfügbar ist, sollten die Smart Install-Funktion mit dem Befehl **no vstack** deaktivieren.

  Hinweis: Der Befehl **vstack** wurde in Cisco IOS Release 12.2(55)SE03 eingeführt.

Dies ist die Beispielausgabe des Befehls **show vstack** auf einem Cisco Catalyst Switch mit deaktivierter Smart Install-Client-Funktion:

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

Kunden, die Smart Install-Funktion nur für Bereitstellungen ohne Benutzereingriffe nutzen

Deaktivieren Sie die Smart Install-Clientfunktion, nachdem die Installation ohne Benutzereingriff abgeschlossen ist, oder verwenden Sie den Befehl **no vstack**.

Verwenden Sie eine der folgenden Methoden, um den Befehl **no vstack** in das Netzwerk zu propagieren:

- Geben Sie den Befehl **no vstack** auf allen Client-Switches entweder manuell oder mit einem Skript ein.
- Fügen Sie den Befehl **no vstack** als Teil der Cisco IOS-Konfiguration hinzu, der im Rahmen der Zero-Touch-Installation in jeden Smart Install-Client übertragen wird.
- In Versionen, die den **vstack-**Befehl nicht unterstützen (Cisco IOS Release 12.2(55)SE02 und frühere Versionen), wenden Sie eine Zugriffskontrollliste (ACL) auf Client-Switches an, um den Datenverkehr auf TCP-Port 4786 zu blockieren.

Um die Smart Install-Clientfunktion später zu aktivieren, geben Sie den Befehl **vstack** auf allen Client-Switches entweder manuell oder mit einem Skript ein.

Kunden, die die Smart Install-Funktion für eine Bereitstellung ohne Benutzereingriffe nutzen

Beim Design einer Smart Install-Architektur sollte darauf geachtet werden, dass der IP-Adressbereich der Infrastruktur für nicht vertrauenswürdige Parteien nicht zugänglich ist. Bei Versionen, die den Befehl **vstack** nicht unterstützen, stellen Sie sicher, dass nur der Smart Install Director über TCP-Verbindungen zu allen Smart Install-Clients auf Port 4786 verfügt.

Administratoren können diese Best Practices für die Sicherheit von Cisco Smart Install-Bereitstellungen auf betroffenen Geräten nutzen:

- Schnittstellen-ACLs
- Control Plane Policing (CoPP) Diese Funktion ist nicht in allen Cisco IOS-Softwareversionen verfügbar.

Dieses Beispiel zeigt eine Schnittstelle-ACL mit der Smart Install Director-IP-Adresse 10.10.10.1

und der Smart Install-Client-IP-Adresse 10.10.10.200:

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

Diese ACL muss auf allen IP-Schnittstellen auf allen Clients bereitgestellt werden. Sie kann auch beim ersten Einsatz von Switches über den Director Switch übertragen werden.

Um den Zugriff auf alle Clients innerhalb der Infrastruktur weiter zu beschränken, können Administratoren diese Best Practices für die Sicherheit auf anderen Geräten im Netzwerk anwenden:

- Infrastruktur-Zugriffskontrolllisten (iACLs)
- VLAN-Zugriffskontrolllisten (VACLs)

Einschränkung des Netzwerkzugriffs mithilfe von Infrastruktur-ACLs

Infrastrukturzugriffskontrolllisten (iACLs) sind eine der wichtigsten Sicherheitskontrollen, die in Netzwerken implementiert werden können, und sollen die unbefugte direkte Kommunikation mit Netzwerkgeräten verhindern. Infrastruktur-ACLs basieren auf der Idee, dass fast der gesamte Netzwerkverkehr das Netzwerk durchläuft und nicht auf das Netzwerk selbst ausgerichtet ist.

Eine iACL wird erstellt und angewendet, um Verbindungen von Hosts oder Netzwerken anzugeben, die für Netzwerkgeräte zulässig sein müssen. Beispiele für diese Verbindungstypen sind eBGP, SSH und SNMP. Nachdem die erforderlichen Verbindungen zugelassen wurden, wird der gesamte andere Datenverkehr zur Infrastruktur explizit abgelehnt. Sämtlicher Transitverkehr, der das Netzwerk durchquert und nicht an Infrastrukturgeräte gerichtet ist, ist dann explizit zulässig.

Die von iACLs bereitgestellten Schutzmaßnahmen sind sowohl für die Verwaltungs- als auch die Kontrollebene relevant. Die Implementierung von iACLs kann durch die Verwendung einer separaten Adressierung für Geräte in der Netzwerkinfrastruktur vereinfacht werden. *Weitere Informationen* zu den Sicherheitsauswirkungen der IP-Adressierung finden Sie unter Ein sicherheitsorientierter Ansatz für die IP-Adressierung.

In diesem Beispiel wird die iACL-Konfiguration veranschaulicht, welche Struktur als Ausgangspunkt für den Beginn des iACL-Implementierungsprozesses verwendet werden muss:

```
!

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

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

```
!

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

permit ip any any
!
```

Nach der Erstellung muss die iACL auf alle Schnittstellen angewendet werden, die nicht infrastrukturbezogenen Geräten zugeordnet sind. Dazu gehören Schnittstellen, die Verbindungen zu anderen Organisationen, Remote-Zugriffssegmenten, Benutzersegmenten und Segmenten in Rechenzentren herstellen.

Weitere Informationen finden Sie unter Schutz Ihres Kerns: Zugriffskontrolllisten für den Infrastrukturschutz für weitere Informationen zu Infrastruktur-ACLs.

ICMP-Paketfilterung

Das Internet Control Message Protocol (ICMP) ist als IP-Steuerungsprotokoll konzipiert. Daher können die von ihm vermittelten Nachrichten weit reichende Auswirkungen auf die TCP- und IP-Protokolle im Allgemeinen haben. Während die Tools zur Behebung von Netzwerkfehlern **ping** und **traceroute** ICMP verwenden, werden externe ICMP-Verbindungen selten für den ordnungsgemäßen Betrieb eines Netzwerks benötigt.

Die Cisco IOS-Software bietet Funktionen zum gezielten Filtern von ICMP-Nachrichten nach Name, Typ und Code. Diese Beispiel-ACL, die zusammen mit den Zugriffskontrolleinträgen (ACEs) früherer Beispiele verwendet werden muss, ermöglicht Pings von vertrauenswürdigen Managementstationen und NMS-Servern und blockiert alle anderen ICMP-Pakete:

```
!

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

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

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

permit ip any any
!
```

IP-Fragmente filtern

Der Filterprozess für fragmentierte IP-Pakete kann Sicherheitsgeräte vor Herausforderungen stellen. Dies liegt daran, dass die Informationen auf Layer 4, die zum Filtern von TCP- und UDP-Paketen verwendet werden, nur im ursprünglichen Fragment vorhanden sind. Die Cisco IOS-

Software verwendet eine bestimmte Methode, um nicht initiale Fragmente auf konfigurierte Zugriffslisten zu überprüfen. Die Cisco IOS-Software bewertet diese nicht initialen Fragmente mit der ACL und ignoriert alle Filterinformationen für Layer 4. Dadurch werden nicht initiale Fragmente nur auf dem Layer-3-Teil eines konfigurierten ACE ausgewertet.

Wenn ein für **192.168.1.1** bestimmtes TCP-Paket auf **Port 22** bei der Übertragung fragmentiert wird, wird das ursprüngliche Fragment wie erwartet vom zweiten ACE verworfen, basierend auf den Layer-4-Informationen im Paket. Alle verbleibenden (nicht initialen) Fragmente werden jedoch vom ersten ACE zugelassen, der vollständig auf den Layer-3-Informationen im Paket und ACE basiert. Dieses Szenario wird in dieser Konfiguration gezeigt:

```
!

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

Aufgrund der intuitiven Art der Fragment-Verarbeitung sind IP-Fragmente von ACLs häufig versehentlich zugelassen. Fragmentierung wird häufig auch bei Versuchen verwendet, die Erkennung von Angriffserkennungssystemen zu umgehen. Aus diesen Gründen werden IP-Fragmente häufig bei Angriffen verwendet, und daher müssen sie explizit oben auf konfigurierten iACLs gefiltert werden. In diesem Beispiel umfasst die ACL eine umfassende Filterung von IP-Fragmenten. Die Funktionalität dieses Beispiels muss zusammen mit der Funktionalität der vorherigen Beispiele verwendet werden.

```
!

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

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

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

permit ip any any
!
```

Weitere Informationen zum Umgang *mit* fragmentierten IP-Paketen *finden Sie unter* Zugriffskontrolllisten und IP-Fragmente.

ACL-Unterstützung für IP-Filteroptionen

Die Cisco IOS Software, Version 12.3(4)T, bietet nun Unterstützung für die Verwendung von ACLs zum Filtern von IP-Paketen basierend auf den im Paket enthaltenen IP-Optionen. IP-Optionen

stellen für Netzwerkgeräte ein Sicherheitsproblem dar, da diese Optionen als Ausnahmepakete verarbeitet werden müssen. Dies erfordert einen gewissen CPU-Aufwand, der für typische Pakete, die das Netzwerk durchlaufen, nicht erforderlich ist. Das Vorhandensein von IP-Optionen in einem Paket kann auch auf den Versuch hinweisen, Sicherheitskontrollen im Netzwerk zu untergraben oder die Übertragungsmerkmale eines Pakets anderweitig zu ändern. Aus diesen Gründen müssen Pakete mit IP-Optionen am Netzwerk-Edge gefiltert werden.

Dieses Beispiel muss zusammen mit den ACEs früherer Beispiele verwendet werden, um das vollständige Filtern von IP-Paketen mit IP-Optionen zu ermöglichen:

```
!

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

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

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

permit ip any any
!
```

ACL-Unterstützung zum Filtern nach TTL-Wert

Die Cisco IOS Software, Version 12.4(2)T, bietet ACL-Unterstützung zum Filtern von IP-Paketen basierend auf dem TTL-Wert (Time to Live). Der TTL-Wert eines IP-Datagramms wird von jedem Netzwerkgerät herabgesetzt, wenn ein Paket von der Quelle zum Ziel fließt. Obwohl die Anfangswerte je nach Betriebssystem unterschiedlich sind, muss das Paket verworfen werden, wenn die TTL eines Pakets null erreicht. Das Gerät, das die TTL auf Null reduziert und somit das Paket verwirft, ist erforderlich, um eine ICMP Time Overceeded-Nachricht zu generieren und an die Quelle des Pakets zu senden.

Die Generierung und Übertragung dieser Nachrichten ist ein Ausnahmeprozess. Router können diese Funktion ausführen, wenn die Anzahl der auslaufenden IP-Pakete gering ist, die Anzahl der Pakete jedoch aufgrund des Auslaufens hoch ist, kann das Generieren und Übertragen dieser Nachrichten alle verfügbaren CPU-Ressourcen beanspruchen. Dies stellt einen DoS-Angriffsvektor dar. Aus diesem Grund müssen Geräte vor DoS-Angriffen geschützt werden, die eine hohe Anzahl an auslaufenden IP-Paketen nutzen.

Es wird empfohlen, IP-Pakete mit niedrigen TTL-Werten am Netzwerk-Edge zu filtern. Durch das vollständige Filtern von Paketen mit TTL-Werten, die nicht ausreichen, um das Netzwerk zu durchqueren, wird die Bedrohung durch TTL-basierte Angriffe verringert.

In diesem Beispiel filtert die ACL Pakete mit TTL-Werten unter sechs. Dies bietet Schutz vor TTL-Ablaufangriffen für Netzwerke mit bis zu fünf Hops in der Breite.

```
!
```

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

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

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

permit ip any any
!
```

> **Hinweis**: Einige Protokolle verwenden Pakete mit niedrigen TTL-Werten legitim. eBGP ist ein solches Protokoll. Unter TTL-Identifizierung und -Minimierung von Angriffen nach Ablauf von TTL-Angriffen finden Sie weitere Informationen zur Abwehr von zeitlich begrenzten Angriffen.

Weitere Informationen zu dieser Funktion *finden Sie unter* ACL-Unterstützung für Filterung auf TTL-Wert.

Sichere interaktive Verwaltungssitzungen

Verwaltungssitzungen für Geräte ermöglichen Ihnen, Informationen über ein Gerät und dessen Betrieb anzuzeigen und zu sammeln. Wenn diese Informationen an einen böswilligen Benutzer weitergegeben werden, kann das Gerät Ziel eines Angriffs sein, kompromittiert sein und zur Durchführung weiterer Angriffe verwendet werden. Jeder mit privilegiertem Zugriff auf ein Gerät hat die Möglichkeit, dieses Gerät vollständig zu verwalten. Es ist unbedingt erforderlich, Managementsitzungen zu sichern, um die Offenlegung von Informationen und den unbefugten Zugriff zu verhindern.

Schutz der Managementebene

In der Cisco IOS Software, Version 12.4(6)T und höher, ermöglicht die Funktion "Management Plane Protection (MPP)" einem Administrator, zu begrenzen, welche Schnittstellen Verwaltungsdatenverkehr von einem Gerät empfangen werden darf. Dadurch hat der Administrator zusätzliche Kontrolle über ein Gerät und darüber, wie auf das Gerät zugegriffen wird.

In diesem Beispiel wird veranschaulicht, wie der MPP aktiviert wird, um nur SSH und HTTPS auf der GigabitEthernet0/1-Schnittstelle zuzulassen:

```
!

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

Weitere Informationen zu MPP *finden Sie unter* Schutz der Managementebene.

Schutz der Kontrollebene

Control Plane Protection (CPPr) baut auf der Funktionalität von Control Plane Policing auf, um den Datenverkehr auf Kontrollebene, der für den Routingprozessor des IOS-Geräts bestimmt ist, zu beschränken und zu überwachen. CPPr wurde in Cisco IOS Software, Version 12.4(4)T, hinzugefügt und unterteilt die Kontrollebene in separate Kontrollebenenkategorien, die als Subschnittstellen bezeichnet werden. Es gibt drei Kontrollebenen-Subschnittstellen: Host, Transit und CEF-Exception. Darüber hinaus bietet CPPr folgende zusätzliche Schutzfunktionen auf Kontrollebene:

- **Port-Filterfunktion** - Diese Funktion ermöglicht das Policing oder Verwerfen von Paketen, die an geschlossene oder nicht überwachende TCP- und UDP-Ports gehen.

- **Richtlinienfunktion für Warteschlangenschwellenwerte** - Diese Funktion beschränkt die Anzahl der Pakete für ein angegebenes Protokoll, die in der IP-Eingabewarteschlange der Kontrollebene zulässig sind.

Mit CPPr kann ein Administrator den Datenverkehr, der zu Verwaltungszwecken über die Host-Subschnittstelle an ein Gerät gesendet wird, klassifizieren, überwachen und beschränken. Beispiele für Pakete, die für die Host-Subschnittstellen-Kategorie klassifiziert sind, sind Verwaltungs-Datenverkehr wie SSH oder Telnet und Routing-Protokolle.

> **Hinweis**: CPPr unterstützt IPv6 nicht und ist auf den IPv4-Eingangspfad beschränkt.

Weitere Informationen zur Cisco CPPr-Funktion *finden Sie im* Funktionsleitfaden 12.4T und Understanding Control Plane Protection (Leitfaden zum Schutz der Kontrollebene).

Verschlüsseln von Management-Sitzungen

Da Informationen in einer interaktiven Managementsitzung offen gelegt werden können, muss dieser Datenverkehr verschlüsselt werden, damit ein böswilliger Benutzer keinen Zugriff auf die übertragenen Daten erhält. Die Datenverkehrsverschlüsselung ermöglicht eine sichere Remote-Verbindung zum Gerät. Wenn der Datenverkehr für eine Managementsitzung in Klartext über das Netzwerk gesendet wird, kann ein Angreifer vertrauliche Informationen über das Gerät und das Netzwerk abrufen.

Administratoren können mit SSH- oder HTTPS-Funktionen (Secure Hypertext Transfer Protocol) eine verschlüsselte und sichere Remote-Zugriffsverwaltungsverbindung zu einem Gerät herstellen. Die Cisco IOS-Software unterstützt SSH Version 1.0 (SSHv1), SSH Version 2.0 (SSHv2) und HTTPS, die Secure Sockets Layer (SSL) und Transport Layer Security (TLS) für Authentifizierung und Datenverschlüsselung verwenden. SSHv1 und SSHv2 sind nicht kompatibel. SSHv1 ist unsicher und nicht standardisiert, daher wird es nicht empfohlen, wenn SSHv2 eine Option ist.

Die Cisco IOS-Software unterstützt außerdem das Secure Copy Protocol (SCP), das eine verschlüsselte und sichere Verbindung zum Kopieren von Gerätekonfigurationen oder Software-Images ermöglicht. SCP nutzt SSH. Diese Beispielkonfiguration aktiviert SSH auf einem Cisco IOS-Gerät:

```
!
```

```
ip domain-name example.com
!

crypto key generate rsa modulus 2048
!

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

line vty 0 4
transport input ssh
!
```

In diesem Konfigurationsbeispiel werden SCP-Dienste aktiviert:

```
!

ip scp server enable
!
```

Dies ist ein Konfigurationsbeispiel für HTTPS-Dienste:

```
!

crypto key generate rsa modulus 2048
!

ip http secure-server
!
```

Häufig gestellte Fragen *zur* Cisco IOS-Software-SSH-Funktion *finden Sie* unter Konfigurieren von Secure Shell auf Routern und Switches mit Cisco IOS und Secure Shell (SSH).

SSHv2

Die in der Cisco IOS Software, Version 12.3(4)T, eingeführte SSHv2-Unterstützungsfunktion ermöglicht es Benutzern, SSHv2 zu konfigurieren. (Die SSHv1-Unterstützung wurde in einer früheren Version der Cisco IOS-Software implementiert.) SSH wird auf einer zuverlässigen Transportschicht ausgeführt und bietet leistungsstarke Authentifizierungs- und Verschlüsselungsfunktionen. Der einzige zuverlässige Transport, der für SSH definiert ist, ist TCP. SSH bietet die Möglichkeit, sicher auf Befehle eines anderen Computers oder Geräts über ein Netzwerk zuzugreifen und diese sicher auszuführen. Die SCP-Funktion (Secure Copy Protocol), die über SSH getunnelt wird, ermöglicht die sichere Übertragung von Dateien.

Wenn der Befehl **ip ssh Version 2** nicht explizit konfiguriert ist, aktiviert Cisco IOS SSH Version 1.99. SSH Version 1.99 ermöglicht sowohl SSHv1- als auch SSHv2-Verbindungen. SSHv1 gilt als unsicher und kann sich nachteilig auf das System auswirken. Wenn SSH aktiviert ist, wird empfohlen, SSHv1 mithilfe des Befehls **ip ssh Version 2** zu deaktivieren.

Diese Beispielkonfiguration aktiviert SSHv2 (bei deaktiviertem SSHv1) auf einem Cisco IOS-Gerät:

```
!
```

```
hostname router

!

ip domain-name example.com

!

crypto key generate rsa modulus 2048

!

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

!

ip ssh version 2

!

line vty 0 4
transport input ssh

!
```

Weitere Informationen zur Verwendung von SSHv2 finden Sie unter Secure Shell Version 2 Support.

SSHv2-Erweiterungen für RSA-Schlüssel

Cisco IOS SSHv2 unterstützt tastateinteraktive und kennwortbasierte Authentifizierungsmethoden. Die Funktion SSHv2-Erweiterungen für RSA-Schlüssel unterstützt auch die RSA-basierte Authentifizierung von öffentlichen Schlüsseln für Client und Server.

Für die Benutzerauthentifizierung wird bei der RSA-basierten Benutzerauthentifizierung ein Private/Public-Key-Paar verwendet, das jedem Benutzer zur Authentifizierung zugeordnet ist. Der Benutzer muss auf dem Client ein privates/öffentliches Schlüsselpaar generieren und auf dem Cisco IOS SSH-Server einen öffentlichen Schlüssel konfigurieren, um die Authentifizierung abzuschließen.

Ein SSH-Benutzer, der versucht, die Anmeldeinformationen festzulegen, stellt eine verschlüsselte Signatur mit dem privaten Schlüssel bereit. Die Signatur und der öffentliche Schlüssel des Benutzers werden zur Authentifizierung an den SSH-Server gesendet. Der SSH-Server berechnet einen Hash über den vom Benutzer bereitgestellten öffentlichen Schlüssel. Der Hash wird verwendet, um zu bestimmen, ob der Server einen Eintrag hat, der übereinstimmt. Wenn eine Übereinstimmung gefunden wird, wird die RSA-basierte Nachrichtenüberprüfung mit dem öffentlichen Schlüssel durchgeführt. Daher wird dem Benutzer aufgrund der verschlüsselten Signatur der Zugriff authentifiziert oder verweigert.

Für die Serverauthentifizierung muss der Cisco IOS SSH-Client jedem Server einen Hostschlüssel zuweisen. Wenn der Client versucht, eine SSH-Sitzung mit einem Server einzurichten, erhält er die Signatur des Servers als Teil der Schlüsselaustauschmeldung. Wenn das Flag für die Überprüfung des Hostschlüssels auf dem Client aktiviert ist, prüft der Client, ob der Hostschlüsseleintrag dem vorkonfigurierten Server entspricht. Wenn eine Übereinstimmung gefunden wird, versucht der Client, die Signatur mit dem Serverhost-Schlüssel zu validieren.

Wenn der Server erfolgreich authentifiziert wurde, wird die Sitzungseinrichtung fortgesetzt. Andernfalls wird er beendet und eine Meldung **über fehlgeschlagene Serverauthentifizierung** angezeigt.

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

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

hostname router
!
! Configure a domain name
!

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

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

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

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

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

ip ssh version 2
!
```

Weitere Informationen zur Verwendung von RSA-Schlüsseln mit SSHv2 finden Sie unter Secure Shell Version 2-Erweiterungen für RSA-Schlüssel.

Mit dieser Beispielkonfiguration kann der Cisco IOS SSH-Server eine RSA-basierte Benutzerauthentifizierung durchführen. Die Benutzerauthentifizierung ist erfolgreich, wenn der auf dem Server gespeicherte öffentliche RSA-Schlüssel mit dem öffentlichen oder dem privaten Schlüsselpaar überprüft wird, das auf dem Client gespeichert ist.

```
!
```

```
! Configure a hostname for the device
!

hostname router
!
! Configure a domain name
!

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

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

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

username ssh-user
!
! Specify the RSA public key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash command (followed by the SSH key type and version.)
!
```

Weitere Informationen zur Verwendung von RSA-Schlüsseln mit SSHv2 finden Sie unter Konfigurieren des Cisco IOS SSH-Servers für die RSA-basierte Benutzerauthentifizierung.

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

```
!
!

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

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

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

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
```

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

ip ssh stricthostkeycheck
!
```

Weitere Informationen zur Verwendung von RSA-Schlüsseln mit SSHv2 finden Sie unter Konfigurieren des Cisco IOS SSH-Clients für die RSA-basierte Serverauthentifizierung.

Konsolen- und AUX-Ports

Bei Cisco IOS-Geräten sind Konsolen- und AUX-Ports asynchrone Leitungen, die für den lokalen und Remote-Zugriff auf ein Gerät verwendet werden können. Beachten Sie, dass Konsolenports auf Cisco IOS-Geräten über besondere Berechtigungen verfügen. Insbesondere ermöglichen diese Berechtigungen einem Administrator, das Kennwortwiederherstellungsverfahren auszuführen. Um eine Kennwortwiederherstellung durchzuführen, muss ein nicht authentifizierter Angreifer Zugriff auf den Konsolenport haben und die Möglichkeit haben, die Stromversorgung des Geräts zu unterbrechen oder den Absturz des Geräts zu verursachen.

Jede Methode, die für den Zugriff auf den Konsolenport eines Geräts verwendet wird, muss in einer Weise gesichert werden, die der für den privilegierten Zugriff auf ein Gerät erzwungenen Sicherheit entspricht. Die zur Sicherung des Zugriffs verwendeten Methoden müssen die Verwendung von AAA-, Exec-Timeout- und Modem-Passwörtern umfassen, wenn ein Modem an die Konsole angeschlossen ist.

Wenn die Kennwortwiederherstellung nicht erforderlich ist, kann ein Administrator mithilfe des globalen Konfigurationsbefehls **no service password-restore die** Möglichkeit zur Kennwortwiederherstellung entfernen. Wenn der Befehl **no service password-restore** aktiviert wurde, kann ein Administrator die Kennwortwiederherstellung auf einem Gerät jedoch nicht mehr durchführen.

In den meisten Fällen muss der AUX-Port eines Geräts deaktiviert werden, um nicht autorisierten Zugriff zu verhindern. Ein AUX-Port kann mit den folgenden Befehlen deaktiviert werden:

```
!

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

Steuerungs-VTY und TTL-Posten

Interaktive Management-Sitzungen in der Cisco IOS-Software verwenden eine tty oder Virtual tty (vty). Eine tty ist eine lokale asynchrone Leitung, an die ein Terminal für den lokalen Zugriff auf das Gerät oder ein Modem für den DFÜ-Zugriff auf ein Gerät angeschlossen werden kann. Beachten Sie, dass Tys für Verbindungen mit Konsolenports anderer Geräte verwendet werden

können. Diese Funktion ermöglicht es einem Gerät mit mehreren Leitungen, als Konsolenserver zu fungieren, auf dem Verbindungen über das Netzwerk zu den Konsolenports von Geräten hergestellt werden können, die mit den Ziffernlinien verbunden sind. Die tty-Leitungen für diese umgekehrten Verbindungen über das Netzwerk müssen ebenfalls gesteuert werden.

Eine VTY-Leitung wird für alle anderen Remote-Netzwerkverbindungen verwendet, die vom Gerät unterstützt werden, unabhängig vom Protokoll (Beispiele sind SSH, SCP oder Telnet). Um sicherzustellen, dass auf ein Gerät über eine lokale oder Remote-Management-Sitzung zugegriffen werden kann, müssen entsprechende Kontrollen sowohl für vty- als auch für tty-Leitungen durchgesetzt werden. Cisco IOS-Geräte verfügen über eine begrenzte Anzahl von VTY-Leitungen. Die Anzahl der verfügbaren Leitungen kann mit dem Befehl show line EXEC ermittelt werden. Wenn alle VTY-Leitungen belegt sind, können keine neuen Management-Sitzungen eingerichtet werden, wodurch eine DoS-Bedingung für den Zugriff auf das Gerät entsteht.

Die einfachste Form der Zugriffskontrolle für eine Einheit oder einen Typ eines Geräts ist die Authentifizierung auf allen Leitungen, unabhängig vom Standort des Geräts im Netzwerk. Dies ist für VTY-Leitungen wichtig, da sie über das Netzwerk zugänglich sind. Eine schöne Leitung, die an ein Modem angeschlossen ist, das für den Remote-Zugriff auf das Gerät verwendet wird, oder eine schöne Leitung, die mit dem Konsolenport anderer Geräte verbunden ist, ist auch über das Netzwerk zugänglich. Andere Formen der Zugriffskontrolle für vty und tty können mithilfe der **Transporteingaben** oder **Zugriffsklassen-**Konfigurationsbefehle erzwungen werden, unter Verwendung der CoPP- und CPPr-Features oder wenn Sie Zugriffslisten auf Schnittstellen auf dem Gerät anwenden.

Die Authentifizierung kann mithilfe von AAA (der empfohlenen Methode für den authentifizierten Zugriff auf ein Gerät, unter Verwendung der lokalen Benutzerdatenbank oder durch eine einfache Kennwortauthentifizierung, die direkt auf der vty- oder tty-Leitung konfiguriert ist, erzwungen werden.

Der Befehl **exec-timeout** muss verwendet werden, um Sitzungen auf VTY- oder tty-Zeilen abzumelden, die nicht aktiv sind. Der Befehl **service tcp-keepalives-in** muss ebenfalls verwendet werden, um TCP-Keepalives für eingehende Verbindungen zum Gerät zu aktivieren. Dadurch wird sichergestellt, dass auf das Gerät am Remote-Ende der Verbindung weiterhin zugegriffen werden kann und dass halb offene oder verwaiste Verbindungen vom lokalen IOS-Gerät entfernt werden.

Steuern des Transports von VTY- und TTL-Posten

Ein vty und tty sollten konfiguriert werden, um nur verschlüsselte und sichere Remote-Zugriffsverwaltungsverbindungen zum Gerät oder über das Gerät zu akzeptieren, wenn sie als Konsolenserver verwendet werden. Dieser Abschnitt behandelt Tys, da solche Leitungen mit Konsolenports an anderen Geräten verbunden werden können, auf die der Zugriff über das Netzwerk möglich ist. Um die Offenlegung von Informationen oder den unbefugten Zugriff auf die Daten, die zwischen dem Administrator und dem Gerät übertragen werden, zu verhindern, sollte **Transport Input SSH** anstelle von Klartext-Protokollen wie Telnet und rlogin verwendet werden. Die **Transporteingabe none**-Konfiguration kann auf einer tty aktiviert werden, wodurch die Verwendung der tty-Leitung für Verbindungen in der Rückkonsole deaktiviert wird.

Sowohl VTY- als auch YTY-Zeilen ermöglichen es einem Administrator, eine Verbindung zu anderen Geräten herzustellen. Um die Transportart zu begrenzen, die ein Administrator für ausgehende Verbindungen verwenden kann, verwenden Sie den Befehl **transport output** line configuration (Konfiguration der **Transportausgabelinie**). Wenn keine ausgehenden Verbindungen erforderlich sind, sollte die **Transportausgabe nicht** verwendet werden. Wenn jedoch ausgehende

Verbindungen zulässig sind, sollte mithilfe von **Transport Output ssh** eine verschlüsselte und sichere Remote-Zugriffsmethode für die Verbindung durchgesetzt werden.

> **Hinweis**: IPSec kann für verschlüsselte und sichere Remote-Zugriffsverbindungen zu einem Gerät verwendet werden, sofern diese unterstützt werden. Wenn Sie IPSec verwenden, wird dem Gerät auch zusätzlicher CPU-Overhead hinzugefügt. SSH muss jedoch auch bei Verwendung von IPSec als Transport durchgesetzt werden.

Warnbanner

In einigen Rechtsgebieten kann es unmöglich sein, böswillige Benutzer zu verfolgen und zu überwachen, es sei denn, sie wurden darüber informiert, dass sie das System nicht nutzen dürfen. Eine Möglichkeit, diese Benachrichtigung zu senden, besteht darin, diese Informationen in eine Bannernachricht einzufügen, die mit dem Anmeldenamen des Cisco IOS-Software-Banners konfiguriert wird.

Die rechtlichen Mitteilungsanforderungen sind komplex, variieren je nach Gerichtsbarkeit und Situation und sollten mit einem Rechtsbeistand besprochen werden. Selbst innerhalb von Gerichtsbarkeiten können Rechtsgutachten abweichen. In Zusammenarbeit mit einem Berater kann ein Banner einige oder alle dieser Informationen bereitstellen:

- Beachten Sie, dass das System nur von speziell autorisierten Mitarbeitern angemeldet oder verwendet werden darf und möglicherweise Informationen darüber, wer die Nutzung autorisieren kann.
- Beachten Sie, dass jede unbefugte Nutzung des Systems rechtswidrig ist und zivil- und strafrechtlich geahndet werden kann.
- Beachten Sie, dass jegliche Nutzung des Systems ohne weitere Ankündigung protokolliert oder überwacht werden kann und dass die daraus resultierenden Protokolle vor Gericht als Beweismittel verwendet werden können.
- Spezifische Mitteilungen, die durch örtliche Gesetze vorgeschrieben sind.

Aus sicherheitstechnischer Sicht sollte ein Anmeldebanner keine spezifischen Informationen über den Router-Namen, das Modell, die Software oder den Eigentümer enthalten. Diese Informationen können von böswilligen Benutzern missbraucht werden.

Authentifizierung, Autorisierung und Abrechnung

Das Authentication, Authorization, and Accounting (AAA)-Framework ist für die Sicherung des interaktiven Zugriffs auf Netzwerkgeräte von entscheidender Bedeutung. Das AAA-Framework bietet eine hochgradig konfigurierbare Umgebung, die auf die Netzwerkanforderungen zugeschnitten werden kann.

TACACS+-Authentifizierung

TACACS+ ist ein Authentifizierungsprotokoll, das Cisco IOS-Geräte zur Authentifizierung von Managementbenutzern für einen Remote-AAA-Server verwenden können. Diese Managementbenutzer können über SSH, HTTPS, Telnet oder HTTP auf das IOS-Gerät zugreifen.

Die TACACS+-Authentifizierung oder generell die AAA-Authentifizierung bietet die Möglichkeit, für jeden Netzwerkadministrator individuelle Benutzerkonten zu verwenden. Wenn Sie sich nicht auf ein einziges gemeinsam genutztes Kennwort verlassen, wird die Sicherheit des Netzwerks erhöht und Ihre Rechenschaftspflicht erhöht.

RADIUS ist ein Protokoll, das mit TACACS+ vergleichbar ist. Sie verschlüsselt jedoch nur das Passwort, das über das Netzwerk gesendet wird. Im Gegensatz dazu verschlüsselt TACACS+ die gesamte TCP-Nutzlast, die sowohl Benutzername als auch Kennwort enthält. Aus diesem Grund sollte TACACS+ anstelle von RADIUS verwendet werden, wenn TACACS+ vom AAA-Server unterstützt wird. Im TACACS+- und RADIUS-Vergleich finden Sie einen ausführlicheren Vergleich dieser beiden Protokolle.

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

```
!

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

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

Die vorherige Konfiguration kann als Ausgangspunkt für eine unternehmensspezifische AAA-Authentifizierungsvorlage verwendet werden. Weitere Informationen zur Konfiguration von AAA finden Sie unter Authentifizierung, Autorisierung und Abrechnung.

Eine Methodenliste ist eine sequenzielle Liste, die die Authentifizierungsmethoden beschreibt, die zur Authentifizierung eines Benutzers abgefragt werden müssen. Methodenlisten ermöglichen Ihnen, ein oder mehrere Sicherheitsprotokolle für die Authentifizierung festzulegen und so ein Backup-System für die Authentifizierung sicherzustellen, falls die ursprüngliche Methode fehlschlägt. Die Cisco IOS-Software verwendet die erste aufgelistete Methode, die einen Benutzer erfolgreich akzeptiert oder ablehnt. Nachfolgende Methoden werden nur dann versucht, wenn frühere Methoden aufgrund von Serverausfällen oder fehlerhafter Konfiguration fehlschlagen.

Weitere Informationen zur Konfiguration von Named Method Lists finden Sie unter Named Method Lists for Authentication.

Authentifizierungsfallback

Wenn nicht alle konfigurierten TACACS+-Server verfügbar sind, kann sich ein Cisco IOS-Gerät auf sekundäre Authentifizierungsprotokolle verlassen. Typische Konfigurationen beinhalten die Verwendung von lokaler Konfiguration oder die Aktivierung der Authentifizierung, wenn nicht alle konfigurierten TACACS+-Server verfügbar sind.

Die vollständige Liste der Optionen für die On-Device-Authentifizierung umfasst enable, local und line. Jede dieser Optionen hat Vorteile. Die Verwendung des enable secret-geheims wird bevorzugt, da der geheime Schlüssel mit einem unidirektionalen Algorithmus gehasht wird, der von Natur aus sicherer ist als der Verschlüsselungsalgorithmus, der mit den Type 7-Kennwörtern für die Line-Authentifizierung oder die lokale Authentifizierung verwendet wird.

Bei Cisco IOS-Softwareversionen, die die Verwendung geheimer Kennwörter für lokal definierte

Benutzer unterstützen, kann ein Fallback auf die lokale Authentifizierung jedoch wünschenswert sein. Dadurch kann ein lokal definierter Benutzer für einen oder mehrere Netzwerkadministratoren erstellt werden. Wenn TACACS+ nicht mehr verfügbar sein sollte, kann jeder Administrator seinen lokalen Benutzernamen und sein lokales Kennwort verwenden. Diese Aktion erhöht zwar die Verantwortlichkeit von Netzwerkadministratoren bei TACACS+-Ausfällen, erhöht jedoch den Verwaltungsaufwand erheblich, da lokale Benutzerkonten auf allen Netzwerkgeräten verwaltet werden müssen.

Dieses Konfigurationsbeispiel baut auf dem vorherigen TACACS+-Authentifizierungsbeispiel auf, um die Fallbackauthentifizierung in das Kennwort aufzunehmen, das lokal mit dem **Befehl enable secret** konfiguriert wurde:

```
!

enable secret <password>
!

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

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

Weitere Informationen zur Verwendung der Fallback-Authentifizierung mit AAA finden Sie unter Konfigurieren der Authentifizierung.

Verwendung von Kennwörtern vom Typ 7

Ursprünglich entwickelt, um die schnelle Entschlüsselung gespeicherter Passwörter zu ermöglichen, sind Type 7-Passwörter keine sichere Form des Kennwortspeichers. Es stehen viele Tools zur Verfügung, mit denen diese Kennwörter leicht entschlüsselt werden können. Die Verwendung von Typ-7-Kennwörtern sollte vermieden werden, es sei denn, dies ist aufgrund einer auf dem Cisco IOS-Gerät verwendeten Funktion erforderlich.

Nach Möglichkeit sollte Typ 9 (Scrypt) verwendet werden:

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

Die Entfernung von Kennwörtern dieses Typs kann durch die AAA-Authentifizierung und die Verwendung der Funktion Enhanced Password Security (Erweiterte Kennwortsicherheit) erleichtert werden, die die Verwendung geheimer Kennwörter für Benutzer ermöglicht, die lokal über den globalen Konfigurationsbefehl **username** definiert sind. Wenn Sie die Verwendung von Typ-7-Passwörtern nicht vollständig verhindern können, halten Sie diese Kennwörter für verdeckt und nicht verschlüsselt.

Weitere Informationen zum Entfernen von Typ-7-Passwörtern finden Sie im Abschnitt Allgemeine Sicherung der Managementebene dieses Dokuments.

TACACS+-Befehlsautorisierung

Die Befehlsautorisierung mit TACACS+ und AAA bietet einen Mechanismus, der jeden Befehl zulässt oder verweigert, der von einem Administrator-Benutzer eingegeben wird. Wenn der

Benutzer EXEC-Befehle eingibt, sendet Cisco IOS jeden Befehl an den konfigurierten AAA-Server. Der AAA-Server verwendet dann seine konfigurierten Richtlinien, um den Befehl für diesen bestimmten Benutzer zuzulassen oder abzulehnen.

Diese Konfiguration kann dem vorherigen AAA-Authentifizierungsbeispiel hinzugefügt werden, um die Befehlsautorisierung zu implementieren:

```
!

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

Weitere Informationen zur Befehlsautorisierung *finden Sie unter* Konfigurieren der Autorisierung.

TACACS+-Befehlsabrechnung

Bei der Konfiguration sendet die AAA-Befehlskontoverwaltung Informationen zu jedem eingegebenen EXEC-Befehl an die konfigurierten TACACS+-Server. Die an den TACACS+-Server gesendeten Informationen umfassen den ausgeführten Befehl, das Ausführungsdatum und den Benutzernamen des Benutzers, der den Befehl eingibt. Die Befehlsabrechnung wird mit RADIUS nicht unterstützt.

Diese Beispielkonfiguration aktiviert die AAA-Befehlsabrechnung für EXEC-Befehle, die auf den Berechtigungsebenen 0, 1 und 15 eingegeben wurden. Diese Konfiguration baut auf vorherigen Beispielen auf, die die Konfiguration der TACACS-Server beinhalten.

```
!

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

Weitere Informationen zur Konfiguration der AAA-Abrechnung *finden Sie unter* Configuring Accounting (Konfiguration der AAA-Abrechnung).

Redundante AAA-Server

Die in einer Umgebung eingesetzten AAA-Server sollten redundant und fehlertolerant bereitgestellt werden. Dadurch wird sichergestellt, dass interaktiver Managementzugriff, wie z. B. SSH, möglich ist, wenn ein AAA-Server nicht verfügbar ist.

Wenn Sie eine redundante AAA-Serverlösung entwerfen oder implementieren, sollten Sie folgende Überlegungen berücksichtigen:

- Verfügbarkeit von AAA-Servern bei potenziellen Netzwerkausfällen
- Geografisch verteilte Platzierung von AAA-Servern

- Laden einzelner AAA-Server im Steady-State und bei Ausfällen
- Netzwerklatenz zwischen Netzwerkzugriffsservern und AAA-Servern
- Synchronisierung der AAA-Serverdatenbanken

Weitere Informationen finden Sie unter Bereitstellen der Zugriffssteuerungsserver.

Stärkung des Simple Network Management Protocol

In diesem Abschnitt werden verschiedene Methoden beschrieben, mit denen die Bereitstellung von SNMP auf IOS-Geräten gesichert werden kann. Es ist wichtig, dass SNMP ordnungsgemäß gesichert wird, um die Vertraulichkeit, Integrität und Verfügbarkeit der Netzwerkdaten und der Netzwerkgeräte zu schützen, über die diese Daten übertragen werden. SNMP stellt Ihnen eine Fülle von Informationen zum Zustand von Netzwerkgeräten zur Verfügung. Diese Informationen sollten vor böswilligen Benutzern geschützt werden, die diese Daten nutzen möchten, um Angriffe auf das Netzwerk durchzuführen.

SNMP-Community-Strings

Community-Strings sind Kennwörter, die auf ein IOS-Gerät angewendet werden, um den Zugriff auf die SNMP-Daten auf dem Gerät sowohl auf Lese- als auch auf Lese- und Schreibzugriff zu beschränken. Diese Community-Strings sollten wie bei allen Passwörtern sorgfältig ausgewählt werden, um sicherzustellen, dass sie nicht trivial sind. Community-Strings sollten in regelmäßigen Abständen und in Übereinstimmung mit Netzwerksicherheitsrichtlinien geändert werden. Beispielsweise sollten die Zeichenfolgen geändert werden, wenn ein Netzwerkadministrator Rollen ändert oder das Unternehmen verlässt.

Diese Konfigurationslinien konfigurieren einen schreibgeschützten Community-String READONLY und einen Community-String mit Lese- und Schreibberechtigung für READWRITE:

```
!

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

> **Hinweis**: Die vorherigen Community-String-Beispiele wurden ausgewählt, um die Verwendung dieser Zeichenfolgen deutlich zu erklären. In Produktionsumgebungen sollten Community-Strings mit Vorsicht ausgewählt werden und aus einer Reihe alphabetischer, numerischer und nicht-alphanumerischer Symbole bestehen. Weitere Informationen zur Auswahl nicht-trivialer Passwörter finden Sie unter Empfehlungen zum Erstellen sicherer Passwörter.

Weitere Informationen zu dieser Funktion *finden Sie unter* IOS SNMP-Befehlsreferenz.

SNMP-Community-Strings mit ACLs

Zusätzlich zum Community String sollte eine ACL angewendet werden, die den SNMP-Zugriff auf eine ausgewählte Gruppe von Quell-IP-Adressen weiter einschränkt. Diese Konfiguration schränkt den schreibgeschützten SNMP-Zugriff auf Endgeräte des Hosts ein, die sich im Adressbereich

192.168.100.0/24 befinden, und beschränkt den SNMP-Schreibzugriff auf das Endhost-Gerät unter 192.168.100.1.

> **Hinweis**: Die Geräte, die von diesen ACLs zugelassen werden, benötigen den richtigen Community String, 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-Befehlsreferenz für das Netzwerkmanagement.

Infrastruktur-ACLs

Infrastruktur-ACLs (iACLs) können bereitgestellt werden, um sicherzustellen, dass nur End-Hosts mit vertrauenswürdigen IP-Adressen SNMP-Datenverkehr an ein IOS-Gerät senden können. Eine iACL sollte eine Richtlinie enthalten, die nicht autorisierte SNMP-Pakete auf dem UDP-Port 161 verweigert.

Weitere Informationen zur Verwendung von iACLs finden Sie im Abschnitt Limiting Access to the Network with Infrastructure ACLs (Eingeschränkter Zugriff auf das Netzwerk mit Infrastruktur-ACLs).

SNMP-Ansichten

SNMP-Ansichten sind eine Sicherheitsfunktion, die den Zugriff auf bestimmte SNMP-MIBs zulassen oder verweigern kann. Nachdem eine Ansicht erstellt und auf einen Community-String mit den globalen Konfigurationsbefehlen der **SNMP-Server-Community** Community-String-Ansicht angewendet wurde, sind Sie beim Zugriff auf MIB-Daten auf die in der Ansicht definierten Berechtigungen beschränkt. Es wird empfohlen, bei Bedarf Ansichten zu verwenden, um SNMP-Benutzer auf die erforderlichen Daten zu beschränken.

In diesem Konfigurationsbeispiel wird der SNMP-Zugriff mit der Community-Zeichenfolge LIMITED auf die MIB-Daten beschränkt, die sich in der Systemgruppe befinden:

```
!

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

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

Weitere Informationen finden Sie unter Konfigurieren des SNMP-Supports.

SNMP-Version 3

SNMP Version 3 (SNMPv3) ist definiert durch RFC3410, RFC3411, RFC3412, RFC3413, RFC3414 und RFC3415. ein interoperables, standardbasiertes Protokoll für die Netzwerkverwaltung. SNMPv3 bietet sicheren Zugriff auf Geräte, da es Pakete über das Netzwerk authentifiziert und optional verschlüsselt. Sofern unterstützt, kann SNMPv3 verwendet werden, um bei der Bereitstellung von SNMP eine weitere Sicherheitsebene hinzuzufügen. SNMPv3 besteht aus drei primären Konfigurationsoptionen:

- **no auth** - Dieser Modus erfordert weder eine Authentifizierung noch eine Verschlüsselung von SNMP-Paketen.
- **auth** - Dieser Modus erfordert die Authentifizierung des SNMP-Pakets ohne Verschlüsselung.
- **priv** - Dieser Modus erfordert für jedes SNMP-Paket sowohl Authentifizierung als auch Verschlüsselung (Datenschutz).

Es muss eine autoritative Engine-ID vorhanden sein, um SNMPv3-Sicherheitsmechanismen - Authentifizierung oder Authentifizierung und Verschlüsselung - für die Verarbeitung von SNMP-Paketen zu verwenden. Standardmäßig wird die Engine-ID lokal generiert. Die Engine-ID kann mit dem Befehl **show snmp engineID** angezeigt werden, wie in diesem Beispiel gezeigt:

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

> **Hinweis**: Wenn die EngineID geändert wird, müssen alle SNMP-Benutzerkonten neu konfiguriert werden.

Im nächsten Schritt wird eine SNMPv3-Gruppe konfiguriert. Dieser Befehl konfiguriert ein Cisco IOS-Gerät für SNMPv3 mit einer SNMP-Servergruppe AUTHGROUP und aktiviert nur die Authentifizierung für diese Gruppe mit dem **auth-**Schlüsselwort:

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

Dieser Befehl konfiguriert ein Cisco IOS-Gerät für SNMPv3 mit einer SNMP-Servergruppe PRIVGROUP und aktiviert sowohl Authentifizierung als auch Verschlüsselung für diese Gruppe mit dem **priv-**Schlüsselwort:

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

Dieser Befehl konfiguriert einen SNMPv3-Benutzer snmpv3user mit einem MD5-Authentifizierungskennwort **authpassword** und einem 3DES-Verschlüsselungskennwort **privpassword**:

```
!

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

Beachten Sie, dass in der Konfigurationsausgabe des Geräts keine **SNMP-Server-**

Benutzerkonfigurationsbefehle angezeigt werden, wie es gemäß RFC 3414 erforderlich ist. Daher kann das Benutzerkennwort in der Konfiguration nicht angezeigt werden. Um die konfigurierten Benutzer anzuzeigen, geben Sie den Befehl **show snmp user** ein, wie in diesem Beispiel gezeigt:

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

Weitere Informationen zu dieser Funktion *finden Sie unter* Konfigurieren des SNMP-Supports.

Schutz der Managementebene

Die MPP-Funktion (Management Plane Protection) der Cisco IOS-Software kann zur Sicherung von SNMP verwendet werden, da sie die Schnittstellen beschränkt, über die SNMP-Datenverkehr auf dem Gerät terminieren kann. Mit der MPP-Funktion kann ein Administrator eine oder mehrere Schnittstellen als Verwaltungsschnittstellen festlegen. Verwaltungsdatenverkehr darf nur über diese Verwaltungsschnittstellen auf ein Gerät zugreifen. Nach Aktivierung von MPP akzeptieren keine Schnittstellen außer designierten Management-Schnittstellen Netzwerkmanagementdatenverkehr, der für das Gerät bestimmt ist.

Beachten Sie, dass das MPP eine Teilmenge der CPPr-Funktion ist und eine Version von IOS erfordert, die CPPr unterstützt. Weitere Informationen zu CPPr finden Sie unter Understanding Control Plane Protection.

In diesem Beispiel wird MPP verwendet, um den SNMP- und SSH-Zugriff auf die FastEthernet 0/0-Schnittstelle zu beschränken:

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

Weitere Informationen finden Sie im Funktionsleitfaden für den Schutz der Managementebene.

Protokollieren von Best Practices

Die Ereignisprotokollierung bietet Ihnen Einblick in den Betrieb eines Cisco IOS-Geräts und das Netzwerk, in dem es bereitgestellt wird. Die Cisco IOS-Software bietet eine Reihe flexibler Protokollierungsoptionen, mit denen die Ziele hinsichtlich Netzwerkmanagement und -transparenz erreicht werden können.

In diesen Abschnitten finden Sie einige grundlegende Best Practices für die Protokollierung, mit denen Administratoren die Protokollierung erfolgreich nutzen und die Auswirkungen der Protokollierung auf ein Cisco IOS-Gerät minimieren können.

Protokolle an einen zentralen Standort senden

Wir empfehlen Ihnen, Protokollierungsinformationen an einen Remote-Syslog-Server zu senden. Auf diese Weise können Netzwerk- und Sicherheitsereignisse auf Netzwerkgeräten besser

korreliert und überprüft werden. Beachten Sie, dass Syslog-Meldungen unzuverlässig über UDP und im Klartext übertragen werden. Aus diesem Grund sollten alle Schutzmechanismen, die ein Netzwerk für den Verwaltungsdatenverkehr bietet (z. B. Verschlüsselung oder Out-of-Band-Zugriff), erweitert werden, um Syslog-Datenverkehr einzubeziehen.

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

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

Weitere Informationen zur Protokollkorrelation *finden Sie unter* Identifizieren von Vorfällen, die Syslog-Ereignisse von Firewall- und IOS-Routern verwenden.

Die in 12.4(15)T integrierte und ursprünglich in 12.0(26)S eingeführte Funktion zur Protokollierung von Nachrichten auf einem ATA-Flash-Datenträger (Advanced Technology Attachment) ermöglicht die Speicherung von Nachrichten zur Systemprotokollierung. Nachrichten, die auf einem ATA-Laufwerk gespeichert wurden, bleiben auch nach dem Neustart des Routers erhalten.

Diese Konfigurationsleitungen konfigurieren 134.217.728 Byte (128 MB) der Protokollierung von Nachrichten im Syslog-Verzeichnis des ATA Flash (disk0) und geben eine Dateigröße von 16.384 Byte an:

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

Bevor Protokollmeldungen in eine Datei auf der ATA-Festplatte geschrieben werden, prüft die Cisco IOS Software, ob genügend Speicherplatz vorhanden ist. Ist dies nicht der Fall, wird die älteste Datei mit Protokollnachrichten (nach Timestamp) gelöscht, und die aktuelle Datei wird gespeichert. Das Format des Dateinamens lautet **log_month:day:year::time**.

> **Hinweis**: Ein ATA-Flash-Laufwerk verfügt nur über einen begrenzten Speicherplatz und muss daher beibehalten werden, um das Überschreiben gespeicherter Daten zu vermeiden.

Dieses Beispiel zeigt, wie Sie Protokollmeldungen vom ATA-Flash-Laufwerk des Routers auf eine externe Festplatte auf dem FTP-Server 192.168.1.129 als Teil der Wartungsmaßnahmen kopieren:

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

Weitere Informationen zu dieser Funktion *finden Sie unter* Anmelden bei lokalem nichtflüchtigen Speicher (ATA-Datenträger).

Protokollierungsebene

Jeder Protokollmeldung, die von einem Cisco IOS-Gerät generiert wird, wird einer von acht Schweregraden zugewiesen, die von Stufe 0, Notfälle, bis zu Stufe 7, Debuggen reichen. Sofern nicht ausdrücklich erforderlich, sollten Sie die Protokollierung auf Stufe 7 vermeiden. Die Protokollierung auf Stufe 7 führt zu einer erhöhten CPU-Last für das Gerät, die zu Geräte- und Netzwerkinstabilität führen kann.

Die **Protokollierungsebene für** globale Konfigurationsbefehle dient dazu, anzugeben, welche Protokollierungsmeldungen an Remote-Syslog-Server gesendet werden. Die angegebene Stufe gibt den niedrigsten Schweregrad an, der gesendet wird. Für die gepufferte Protokollierung wird der Befehl **gepufferte Protokollierungsebene** verwendet.

In diesem Konfigurationsbeispiel werden Protokollmeldungen an Remote-Syslog-Server und der lokale Protokollpuffer auf die Schweregrade 6 (informativ) bis 0 (Notfälle) begrenzt:

```
!

logging trap 6
logging buffered 6
!
```

Weitere Informationen finden Sie unter Fehlerbehebung, Fehlermanagement und Protokollierung.

Melden Sie sich nicht bei Konsolen- oder Überwachungssitzungen an.

Mit der Cisco IOS-Software können Protokollmeldungen zur Überwachung von Sitzungen gesendet werden - Überwachungssitzungen sind interaktive Verwaltungssitzungen, in denen der EXEC-Befehl **Terminalmonitor** ausgegeben wurde - und an die Konsole. Dies kann jedoch die CPU-Last eines IOS-Geräts erhöhen. Daher wird nicht empfohlen. Stattdessen wird empfohlen, Protokollierungsinformationen an den lokalen Protokollpuffer zu senden, der mit dem Befehl **show logging** angezeigt werden kann.

Verwenden Sie die globalen Konfigurationsbefehle **keine Protokollierungskonsole** und **kein Protokollierungsmonitor**, um die Protokollierung für die Konsolen- und Überwachungssitzungen zu deaktivieren. In diesem Konfigurationsbeispiel wird die Verwendung der folgenden Befehle veranschaulicht:

```
!

no logging console
no logging monitor
!
```

Weitere Informationen zu globalen Konfigurationsbefehlen *finden Sie unter* Cisco IOS-Befehlsreferenz für die Netzwerkverwaltung.

Buffered-Protokollierung verwenden

Die Cisco IOS-Software unterstützt die Verwendung eines lokalen Protokollpuffers, sodass ein Administrator lokal generierte Protokollmeldungen anzeigen kann. Es wird dringend empfohlen, eine gepufferte Protokollierung zu verwenden, statt sich entweder an der Konsole oder an den Überwachungssitzungen anzumelden.

Es gibt zwei Konfigurationsoptionen, die für die Konfiguration der gepufferten Protokollierung relevant sind: die Größe des Protokollierungspuffers und die Schweregrade der Nachrichten, die im Puffer gespeichert werden. Die Größe des **Protokollierungspuffers** wird mit der **gepufferten** Größe des globalen Konfigurationsbefehls konfiguriert. Der niedrigste im Puffer enthaltene Schweregrad wird mit dem Befehl logging buffered Severity konfiguriert. Administratoren können den Inhalt des Protokollierungspuffers über den Befehl **show logging** EXEC anzeigen.

Dieses Konfigurationsbeispiel umfasst die Konfiguration eines Protokollierungspuffers von 16384 Byte sowie eines Schweregrads von 6, informativ, der angibt, dass Meldungen der Ebenen 0 (Notfälle) bis 6 (informativ) gespeichert werden:

```
!

logging buffered 16384 6
!
```

Weitere Informationen zur gepufferten Protokollierung finden Sie unter Cisco IOS-Befehlsreferenz für die Netzwerkverwaltung.

Konfigurieren der Protokollierungsquellenschnittstelle

Um eine höhere Konsistenz beim Erfassen und Überprüfen von Protokollmeldungen zu gewährleisten, wird empfohlen, eine Quellschnittstelle für die Protokollierung statisch zu konfigurieren. Durch die statische Konfiguration einer Protokollierungsquellenschnittstelle über den Befehl **source-interface** wird sichergestellt, dass in allen Protokollnachrichten, die von einem einzelnen Cisco IOS-Gerät gesendet werden, dieselbe IP-Adresse angezeigt wird. Um die Stabilität zu erhöhen, wird empfohlen, eine Loopback-Schnittstelle als Protokollierungsquelle zu verwenden.

In diesem Konfigurationsbeispiel wird die Verwendung des globalen Konfigurationsbefehls für die **Protokollierung der Quell-**Schnittstelle veranschaulicht, um anzugeben, dass die IP-Adresse der Loopback 0-Schnittstelle für alle Protokollmeldungen verwendet wird:

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

Weitere Informationen finden Sie in der Cisco IOS-Befehlsreferenz.

Konfigurieren von Protokollzeitstempeln

Die Konfiguration von Protokollierungs-Zeitstempeln ermöglicht die Korrelation von Ereignissen zwischen Netzwerkgeräten. Es ist wichtig, eine korrekte und konsistente Protokollierungs-Zeitstempelkonfiguration zu implementieren, um sicherzustellen, dass Sie Protokollierungsdaten korrelieren können. Protokollierungs-Zeitstempel sollten so konfiguriert werden, dass Datum und Uhrzeit mit Millisekunde-Genauigkeit sowie die auf dem Gerät verwendete Zeitzone enthalten sind.

Dieses Beispiel umfasst die Konfiguration von Protokollierungszeitstempeln mit einer Genauigkeit von Millisekunden innerhalb der UTC-Zone (Coordinated Universal Time):

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

Wenn Sie die Protokollierungszeiten nicht relativ zur UTC-Adresse festlegen möchten, können Sie eine bestimmte lokale Zeitzone konfigurieren und diese Informationen so konfigurieren, dass sie in generierten Protokollmeldungen enthalten sind. Dieses Beispiel zeigt eine Gerätekonfiguration für die PST-Zone (Pacific Standard Time):

```
!

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

Konfigurationsmanagement für die Cisco IOS Software

Die Cisco IOS-Software umfasst mehrere Funktionen, die eine Form des Konfigurationsmanagements auf einem Cisco IOS-Gerät ermöglichen. Zu diesen Funktionen gehören Funktionen zum Archivieren von Konfigurationen und zum Zurücksetzen der Konfiguration auf eine frühere Version sowie zum Erstellen eines detaillierten Konfigurationsänderungsprotokolls.

Konfigurationsaustausch und Konfigurations-Rollback

In der Cisco IOS-Softwareversion 12.3(7)T und höher ermöglichen die Funktionen Configuration Replace and Configuration Rollback (Ersatz und Konfigurations-Rollback) die Archivierung der Cisco IOS-Gerätekonfiguration auf dem Gerät. Die Konfigurationen in diesem Archiv werden manuell oder automatisch gespeichert und können verwendet werden, um die aktuelle Konfiguration durch den Befehl **configure Replace file** (Dateiname **ersetzen)** zu ersetzen. Dies steht im Gegensatz zum Befehl **copy** filename **running-config**. Der Befehl **configure Replace** filename ersetzt die aktuelle Konfiguration anstelle der Zusammenführung durch den Befehl **copy**.

Wir empfehlen Ihnen, diese Funktion auf allen Cisco IOS-Geräten im Netzwerk zu aktivieren. Nach der Aktivierung kann ein Administrator mithilfe des Befehls **archiv config** privilegierter EXEC die aktuelle Konfiguration zum Archiv hinzufügen. Die archivierten Konfigurationen können mit dem Befehl **show archive** EXEC angezeigt werden.

Dieses Beispiel veranschaulicht die Konfiguration der automatischen Konfigurationsarchivierung. In diesem Beispiel wird das Cisco IOS-Gerät angewiesen, archivierte Konfigurationen als Dateien mit dem Namen archived-config-N auf dem Datenträger0 zu speichern: -Dateisystem, um maximal 14 Sicherungen zu verwalten und einmal pro Tag (1440 Minuten) zu archivieren, und wenn ein Administrator den Befehl **write memory** EXEC ausgibt.

```
!

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

Obwohl die Konfigurationsarchivfunktion bis zu 14 Sicherungskonfigurationen speichern kann, sollten Sie die Speicherplatzanforderungen berücksichtigen, bevor Sie den **maximalen** Befehl verwenden.

Exklusiver Zugriff auf Konfigurationsänderungen

Zusätzlich zur Cisco IOS Software, Version 12.3(14)T, stellt die Funktion "Exklusiver Konfigurationsänderungszugriff" sicher, dass nur ein Administrator Konfigurationsänderungen an einem Cisco IOS-Gerät gleichzeitig vornimmt. Diese Funktion trägt dazu bei, die unerwünschten

Auswirkungen gleichzeitiger Änderungen an zugehörigen Konfigurationskomponenten zu vermeiden. Diese Funktion wird im **exklusiven** Konfigurationsmodus des globalen Konfigurationsbefehls konfiguriert und in einem der beiden Modi ausgeführt: automatisch und manuell. Im automatischen Modus wird die Konfiguration automatisch gesperrt, wenn ein Administrator den Befehl **configure terminal** EXEC ausgibt. Im manuellen Modus verwendet der Administrator den Befehl **configure terminal lock** (Terminalsperre konfigurieren), um die Konfiguration zu sperren, wenn sie in den Konfigurationsmodus wechselt.

In diesem Beispiel wird die Konfiguration dieses Features für die automatische Konfigurationssperrung veranschaulicht:

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

Ausfallsichere Konfiguration der Cisco IOS Software

Die in der Cisco IOS Software, Version 12.3(8)T, hinzugefügte Funktion für ausfallsichere Konfiguration ermöglicht das sichere Speichern einer Kopie des Cisco IOS Software-Image und der Gerätekonfiguration, die aktuell von einem Cisco IOS-Gerät verwendet wird. Wenn diese Funktion aktiviert ist, können diese Sicherungsdateien nicht geändert oder entfernt werden. Wir empfehlen Ihnen, diese Funktion zu aktivieren, um sowohl unbeabsichtigte als auch böswillige Versuche zum Löschen dieser Dateien zu verhindern.

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

Wenn diese Funktion aktiviert ist, kann eine gelöschte Konfiguration oder ein Cisco IOS Software-Image wiederhergestellt werden. Der aktuelle Ausführungsstatus dieser Funktion kann mit dem Befehl **show secure boot** EXEC angezeigt werden.

Digital signierte Cisco Software

Die in der Cisco IOS Software-Version 15.0(1)M für die Cisco Router der Serien 1900, 2900 und 3900 integrierte Cisco Software-Funktion vereinfacht die Verwendung der digital signierten Cisco IOS Software, die digital signiert und somit vertrauenswürdig ist. Hierzu wird eine sichere asymmetrische (Public-Key-)Kryptografie verwendet.

Ein digital signiertes Bild enthält einen verschlüsselten (mit einem privaten Schlüssel) Hash von sich selbst. Bei der Überprüfung entschlüsselt das Gerät den Hash mit dem entsprechenden öffentlichen Schlüssel aus den Schlüsseln, die es im Schlüsselspeicher hat, und berechnet auch seinen eigenen Hash des Bildes. Wenn der entschlüsselte Hash mit dem berechneten Image-Hash übereinstimmt, wurde das Bild nicht manipuliert und kann als vertrauenswürdig angesehen werden.

Die digital signierten Cisco Softwareschlüssel werden durch den Typ und die Version des Schlüssels identifiziert. Ein Schlüssel kann ein spezieller, Produktions- oder Rollover-Schlüsseltyp sein. Produktions- und spezielle Schlüsseltypen verfügen über eine zugeordnete Schlüsselversion, die alphabetisch erhöht wird, wenn der Schlüssel widerrufen und ersetzt wird. ROMMON- und reguläre Cisco IOS-Images werden mit einem speziellen oder einem Produktionsschlüssel signiert, wenn Sie die Funktion "Digital Signed Cisco Software" verwenden. Das ROMMON-Image ist erweiterbar und muss mit dem gleichen Schlüssel signiert werden wie

das geladene Spezial- oder Produktionsbild.

Mit diesem Befehl wird die Integrität des Image c3900-universalk9-mz.SSA im Flash-Speicher mit den Tasten im Gerätelager überprüft:

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

Die Cisco Software-Funktion mit digitaler Signatur wurde auch in Cisco IOS XE Version 3.1.0.SG für die Cisco Catalyst Switches der Serie 4500-E integriert.

Weitere Informationen zu dieser Funktion *finden Sie* unter Cisco Software mit digitaler Signatur.

In der Cisco IOS Software-Version 15.1(1)T und höher wurde der Schlüsselaustausch für die digital signierte Cisco Software eingeführt. Der Schlüsselaustausch und -widerruf ersetzt und entfernt einen Schlüssel, der für eine digital signierte Cisco Software-Prüfung verwendet wird, aus dem Schlüsselspeicher einer Plattform. Im Falle einer wichtigen Kompromittierung können nur besondere Tasten und Produktionsschlüssel widerrufen werden.

Ein neuer (Spezial- oder Produktionsschlüssel) Schlüssel für ein (Spezial- oder Produktions-) Bild wird in einem (Produktions- oder Widerruf-) Bild angezeigt, das verwendet wird, um den vorherigen Spezial- oder Produktionsschlüssel zu widerrufen. Die Integrität des Widerrufsbilds wird mithilfe eines Rollover-Schlüssels überprüft, der auf der Plattform vorab gespeichert wird. Ein Rollover-Schlüssel ändert sich nicht. Wenn Sie einen Produktionsschlüssel widerrufen, wird nach dem Laden des Widerrufsbilds der neue Schlüssel zum Schlüsselspeicher hinzugefügt, und der zugehörige alte Schlüssel kann widerrufen werden, solange das ROMMON-Image aktualisiert und das neue Produktionsbild gestartet wird. Wenn Sie einen speziellen Schlüssel aufheben, wird ein Produktionsbild geladen. Dieses Bild fügt den neuen speziellen Schlüssel hinzu und kann den alten speziellen Schlüssel widerrufen. Nach dem Upgrade von ROMMON kann das neue spezielle Image gestartet werden.

In diesem Beispiel wird der Widerruf eines speziellen Schlüssels beschrieben. Diese Befehle fügen dem Schlüsselspeicher den neuen speziellen Schlüssel aus dem aktuellen Produktions-Image hinzu, kopieren ein neues ROMMON-Image (C3900_rom-monitor.srec.SSB) in den Speicherbereich (usbflash0:), aktualisieren die ROMMON-Datei und widerrufen den alten Sonderschlüssel:

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

Ein neues Sonderbild (c3900-universalk9-mz.SSB) kann dann in den zu ladenden Flash kopiert werden, und die Signatur des Bildes wird mit dem neu hinzugefügten Sonderschlüssel (SSB) überprüft:

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

Für Catalyst Switches der Serie 4500-E, auf denen die Cisco IOS XE Software ausgeführt wird, werden keine wichtigen Widerrufs- und Austauschfunktionen unterstützt. Diese Switches unterstützen jedoch die Funktion der digital signierten Cisco Software.

Weitere Informationen zu dieser Funktion *finden Sie* im Abschnitt Digital Signed Cisco Software Key Revocation and Replacement (digital signierte Cisco Softkey-Widerrufung und -Ersatz) im Digital Signed Cisco Software Guide.

Benachrichtigungen und Protokollierung von Konfigurationsänderungen

Die in Cisco IOS Software Release 12.3(4)T hinzugefügte Funktion zur Benachrichtigung und Protokollierung von Konfigurationsänderungen ermöglicht die Protokollierung der Konfigurationsänderungen, die an einem Cisco IOS-Gerät vorgenommen wurden. Das Protokoll wird auf dem Cisco IOS-Gerät verwaltet und enthält die Benutzerinformationen der Person, die die Änderung vorgenommen hat, den eingegebenen Konfigurationsbefehl und den Zeitpunkt, zu dem die Änderung vorgenommen wurde. Diese Funktion wird mit dem Befehl **logging enable** configuration logger configuration mode aktiviert. Die optionalen Befehle **hidekeys** und **Protokollierungsgrößeneinträge** werden verwendet, um die Standardkonfiguration zu verbessern, da sie die Protokollierung von Passwortdaten verhindern und die Länge des Änderungsprotokolls erhöhen.

Es wird empfohlen, diese Funktion zu aktivieren, damit der Konfigurationsänderungsverlauf eines Cisco IOS-Geräts einfacher verständlich ist. Außerdem wird empfohlen, den Befehl **notify syslog** configuration zu verwenden, um die Generierung von Syslog-Meldungen zu ermöglichen, wenn eine Konfigurationsänderung vorgenommen wird.

```
!

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

Nachdem die Funktion für Benachrichtigungen und Protokollierung bei Konfigurationsänderungen aktiviert wurde, kann der privilegierte EXEC-Befehl **show archive log config all** zum Anzeigen des Konfigurationsprotokolls verwendet werden.

Kontrollebene

Funktionen der Steuerungsebene bestehen aus den Protokollen und Prozessen, die zwischen Netzwerkgeräten kommunizieren, um Daten von der Quelle zum Ziel zu übertragen. Dazu gehören Routing-Protokolle wie das Border Gateway Protocol sowie Protokolle wie ICMP und das Resource Reservation Protocol (RSVP).

Es ist wichtig, dass Ereignisse in der Verwaltungs- und Datenebene die Kontrollebene nicht beeinträchtigen. Wenn sich ein Ereignis der Datenebene wie ein DoS-Angriff auf die Kontrollebene auswirkt, kann das gesamte Netzwerk instabil werden. Diese Informationen zu den Funktionen und Konfigurationen der Cisco IOS-Software können die Ausfallsicherheit der Kontrollebene sicherstellen.

Sicherung der allgemeinen Kontrollebene

Der Schutz der Kontrollebene eines Netzwerkgeräts ist von entscheidender Bedeutung, da die Kontrollebene sicherstellt, dass die Verwaltungs- und Datenebenen aufrechterhalten und betriebsbereit sind. Wenn die Kontrollebene während eines Sicherheitsvorfalls instabil wird, kann es für Sie unmöglich sein, die Stabilität des Netzwerks wiederherzustellen.

In vielen Fällen können Sie den Empfang und die Übertragung bestimmter Arten von Nachrichten an einer Schnittstelle deaktivieren, um die CPU-Last zu minimieren, die für die Verarbeitung nicht benötigter Pakete erforderlich ist.

IP ICMP-Umleitungen

Eine ICMP-Umleitungsmeldung kann von einem Router generiert werden, wenn ein Paket auf derselben Schnittstelle empfangen und übertragen wird. In dieser Situation leitet der Router das Paket weiter und sendet eine ICMP-Umleitungsmeldung zurück an den Absender des ursprünglichen Pakets. Dieses Verhalten ermöglicht es dem Absender, den Router zu umgehen und zukünftige Pakete direkt an das Ziel (oder an einen Router näher am Ziel) weiterzuleiten. In einem ordnungsgemäß funktionierenden IP-Netzwerk sendet ein Router nur Umleitungen an Hosts in seinen eigenen lokalen Subnetzen. Anders ausgedrückt: ICMP-Umleitungen sollten niemals über eine Layer-3-Grenze hinausgehen.

Es gibt zwei Arten von ICMP-Umleitungsnachrichten: für eine Hostadresse umleiten und für ein gesamtes Subnetz umleiten. Ein böswilliger Benutzer kann die Fähigkeit des Routers ausnutzen, ICMP-Umleitungen zu senden, indem er Pakete kontinuierlich an den Router sendet. Dadurch wird der Router gezwungen, mit ICMP-Umleitungsnachrichten zu reagieren, was negative Auswirkungen auf die CPU und die Leistung des Routers hat. Um zu verhindern, dass der Router ICMP-Umleitungen sendet, verwenden Sie den Befehl **no ip redirects** interface configuration.

ICMP nicht erreichbar

Beim Filtern mit einer Schnittstellenzugriffsliste wird die Übertragung von nicht erreichbaren ICMP-Nachrichten zurück an die Quelle des gefilterten Datenverkehrs ausgelöst. Die Generierung dieser Nachrichten kann die CPU-Auslastung auf dem Gerät erhöhen. In der Cisco IOS-Software ist die standardmäßig alle 500 Millisekunden erreichbare ICMP-Generierung auf ein Paket beschränkt. Die Generierung nicht erreichbarer ICMP-Nachrichten kann mit dem Schnittstellenkonfigurationsbefehl **no ip unreachables** deaktiviert werden. Die ICMP-Ratenbegrenzung ohne Erreichbarkeit kann mit dem globalen Konfigurationsbefehl **ip icmp rate-limit unreachable** interval-in-ms von der Standardeinstellung geändert werden.

Proxy-ARP

Proxy-ARP ist die Technik, bei der ein Gerät, in der Regel ein Router, ARP-Anfragen beantwortet, die für ein anderes Gerät bestimmt sind. Durch "Fälschen" seiner Identität übernimmt der Router die Verantwortung für das Routing von Paketen zum eigentlichen Ziel. Proxy-ARP kann Geräten in Subnetzen helfen, Remote-Subnetze zu erreichen, ohne Routing oder ein Standard-Gateway zu konfigurieren. Proxy-ARP ist in RFC 1027 definiert.

Die Proxy-ARP-Nutzung hat mehrere Nachteile. Dies kann zu einem Anstieg des ARP-Datenverkehrs im Netzwerksegment sowie zu Ressourcenauslastung und Man-in-the-Middle-Angriffen führen. Der Proxy-ARP stellt einen Angriffsvektor für Ressourcen dar, da jede erweiterte ARP-Anforderung einen geringen Arbeitsspeicher beansprucht. Ein Angreifer kann alle verfügbaren Speicher ausschöpfen, wenn er eine große Anzahl von ARP-Anfragen sendet.

Man-in-the-Middle-Angriffe ermöglichen es einem Host im Netzwerk, die MAC-Adresse des Routers zu verfälschen, was dazu führt, dass ahnungslose Hosts Datenverkehr an den Angreifer senden. Proxy-ARP kann mit dem Schnittstellenkonfigurationsbefehl **no ip proxy-arp** deaktiviert werden.

Weitere Informationen zu dieser Funktion *finden Sie unter* Aktivieren von Proxy-ARP.

Begrenzung der CPU-Auswirkungen des Datenverkehrs auf der Kontrollebene

Der Schutz der Kontrollebene ist von entscheidender Bedeutung. Da die Anwendungsleistung und das Anwendererlebnis ohne Daten- und Verwaltungsdatenverkehr beeinträchtigt werden können, wird durch die Ausfallsicherheit der Kontrollebene sichergestellt, dass die beiden anderen Ebenen erhalten und betriebsbereit sind.

Verständnis des Kontrollebenen-Datenverkehrs

Um die Kontrollebene des Cisco IOS-Geräts angemessen zu schützen, müssen Sie wissen, welche Arten von Datenverkehr von der CPU weitergeleitet werden. Prozessgesteuerter Datenverkehr besteht in der Regel aus zwei verschiedenen Arten von Datenverkehr. Der erste Datenverkehr wird an das Cisco IOS-Gerät weitergeleitet und muss direkt von der Cisco IOS-Geräte-CPU verarbeitet werden. Dieser Datenverkehr besteht aus der Kategorie *Empfangs-Adjacency-Datenverkehr*. Dieser Datenverkehr enthält einen Eintrag in der CEF-Tabelle (Cisco Express Forwarding), wobei der nächste Router-Hop das Gerät selbst ist. Dieser Eintrag wird durch den Begriff "Receive" (Empfangen) in der **show ip cef** CLI-Ausgabe angegeben. Diese Angabe gilt für alle IP-Adressen, die die direkte Verarbeitung durch die Cisco IOS-Geräte-CPU erfordern. Dazu gehören IP-Schnittstellenadressen, Multicast-Adressräume und Broadcast-Adressräume.

Die zweite Art von Datenverkehr, der von der CPU verarbeitet wird, ist Datenverkehr auf der Datenebene - Datenverkehr mit einem Ziel, der über das Cisco IOS-Gerät selbst hinausgeht -, der eine spezielle Verarbeitung durch die CPU erfordert. Obwohl keine vollständige Liste der CPU-Auswirkungen auf den Datenverkehr auf der Datenebene vorliegt, werden diese Datenverkehrstypen prozessgesteuert und können daher den Betrieb der Steuerungsebene beeinflussen:

- **Protokollierung der Zugriffskontrollliste** - Der ACL-Protokolldatenverkehr besteht aus Paketen, die aufgrund einer Übereinstimmung (Zulassen oder Verweigern) eines ACEs generiert werden, auf dem das log-Schlüsselwort verwendet wird.
- **Unicast Reverse Path Forwarding (Unicast Reverse Path Forwarding, Unicast-RPF)** - In Verbindung mit einer ACL kann das Switching bestimmter Pakete durch Unicast RPF erfolgen.
- **IP-Optionen**: Alle IP-Pakete mit enthaltenen Optionen müssen von der CPU verarbeitet werden.
- **Fragmentierung** - Jedes IP-Paket, das fragmentiert werden muss, muss zur Verarbeitung an die CPU übergeben werden.
- **Time-to-Live (TTL) Expiry** - Für Pakete mit einem TTL-Wert von weniger als oder gleich einem müssen Nachrichten über das Internet Control Message Protocol Time Exceeded (ICMP-Typ 11, Code 0) gesendet werden, was zur CPU-Verarbeitung führt.
- **ICMP Unreachables**: Pakete, die aufgrund von Routing, MTU oder Filterung zu nicht erreichbaren ICMP-Nachrichten führen, werden von der CPU verarbeitet.

- **Datenverkehr, für den eine ARP-Anforderung erforderlich ist** - Ziele, für die kein ARP-Eintrag vorhanden ist, müssen von der CPU verarbeitet werden.

- **Nicht-IP-Datenverkehr** - Der gesamte Nicht-IP-Datenverkehr wird von der CPU verarbeitet.

In dieser Liste sind verschiedene Methoden aufgeführt, um zu bestimmen, welche Arten von Datenverkehr von der Cisco IOS-Geräte-CPU verarbeitet werden:

- Der Befehl **show ip cef** stellt die Next-Hop-Informationen für jedes in der CEF-Tabelle enthaltene IP-Präfix bereit. Wie bereits erwähnt, werden Einträge, die als "Nächster Hop" empfangen werden, als Adjacencies angesehen und weisen darauf hin, dass Datenverkehr direkt an die CPU gesendet werden muss.

- Der Befehl **show interface switching** enthält Informationen zur Anzahl der Pakete, die von einem Gerät verlegt werden.

- Der Befehl **show ip traffic** liefert Informationen zur Anzahl der IP-Pakete:

  mit einem lokalen Ziel (d. h. Empfangen von Adjacency-Datenverkehr)mit Optionendie Fragmentierung erforderndie an den Broadcast-Adressbereich gesendet werdendie an den Multicast-Adressbereich gesendet werden

- Der Empfangs-Adjacency-Datenverkehr kann mithilfe des Befehls **show ip cache flow** identifiziert werden. Alle Datenflüsse, die für das Cisco IOS-Gerät bestimmt sind, verfügen über eine Zielschnittstelle (DstIf) des lokalen Datenverkehrs.

- **Control Plane Policing** kann verwendet werden, um die Art und Rate des Datenverkehrs zu identifizieren, der die Kontrollebene des Cisco IOS-Geräts erreicht. Die Control-Plane-Policing kann mithilfe von präzisen Klassifizierungs-ACLs, Protokollierung und dem Befehl **show policy-map control-plane** erfolgen.

Infrastruktur-ACLs

Infrastruktur-ACLs (iACLs) beschränken die externe Kommunikation mit den Geräten im Netzwerk. Infrastruktur-ACLs werden ausführlich im Abschnitt "Limit Access to the Network with Infrastructure ACLs" dieses Dokuments behandelt.

Es wird empfohlen, iACLs zu implementieren, um die Steuerungsebene aller Netzwerkgeräte zu schützen.

Empfangen von ACLs

Für verteilte Plattformen können Receive ACLs (rACLs) eine Option für die Cisco IOS Software Releases 12.0(21)S2 für 12000 (GSR), 12.0(24)S für 7500 und 12.0(31)S für 1072 sein. 0. Die rACL schützt das Gerät vor schädlichem Datenverkehr, bevor sich der Datenverkehr auf den Routingprozessor auswirkt. Empfangs-ACLs dienen nur zum Schutz des Geräts, auf dem sie konfiguriert sind, und der Transitverkehr wird nicht von einer rACL beeinflusst. Daher bezieht sich die Ziel-IP-Adresse, die in den unten aufgeführten Beispieleinträgen für die Zugriffskontrollliste verwendet wird, nur auf die physischen oder virtuellen IP-Adressen des Routers.

Empfangszugriffskontrolllisten gelten ebenfalls als Best Practice für die Netzwerksicherheit und sollten als langfristige Ergänzung einer guten Netzwerksicherheit betrachtet werden.

Dies ist die Empfangs-Pfad-ACL, die geschrieben wird, um SSH-Datenverkehr (TCP-Port 22) von vertrauenswürdigen Hosts im Netzwerk 192.168.100.0/24 zuzulassen:

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

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

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

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

ip receive access-list 151
!
```

Weitere Informationen finden Sie in der GSR: Empfangen von Zugriffskontrolllisten, um legitimen Datenverkehr zu einem Gerät zu identifizieren und zuzulassen und alle unerwünschten Pakete zu verweigern.

CoPP

Die CoPP-Funktion kann auch verwendet werden, um IP-Pakete zu beschränken, die für das Infrastrukturgerät bestimmt sind. In diesem Beispiel darf nur SSH-Datenverkehr von vertrauenswürdigen Hosts die Cisco IOS-Geräte-CPU erreichen.

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

```
!

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

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

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

```
!

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

Im vorherigen CoPP-Beispiel führen die ACL-Einträge, die die nicht autorisierten Pakete mit der Genehmigungsaktion abgleichen, dazu, dass diese Pakete von der Policy-Map-Dropdown-Funktion verworfen werden, während Pakete, die mit der deny-Aktion übereinstimmen, nicht von der Policy-Map-Dropdown-Funktion betroffen sind.

CoPP ist in den Cisco IOS Software Release-Zügen 12.0S, 12.2SX, 12.2S, 12.3T, 12.4 und 12.4T verfügbar.

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

Schutz der Kontrollebene

Control Plane Protection (CPPr), eingeführt in Cisco IOS Software, Version 12.4(4)T, kann verwendet werden, um den Datenverkehr auf Kontrollebene, der zur CPU des Cisco IOS-Geräts bestimmt ist, zu beschränken oder zu überwachen. CPPr ist CoPP ähnlich, kann jedoch den Datenverkehr feinstufiger beschränken. CPPr teilt die aggregierte Kontrollebene in drei separate Kontrollebenen-Kategorien ein, die als Subschnittstellen bezeichnet werden. Unterschnittstellen existieren für die Verkehrskategorien Host, Transit und CEF-Exception. CPPr bietet darüber hinaus folgende Schutzfunktionen auf Kontrollebene:

- **Port-Filterfunktion** - Diese Funktion ermöglicht das Festlegen und Verwerfen von Paketen, die an geschlossene oder nicht überwachende TCP- oder UDP-Ports gesendet werden.

- **Warteschlangen-Grenzwertfunktion** - Diese Funktion beschränkt die Anzahl der Pakete für ein bestimmtes Protokoll, die in der IP-Eingabewarteschlange der Kontrollebene zulässig sind.

Weitere Informationen zur Konfiguration und Verwendung der CPPr-Funktion *finden Sie unter* Schutz und Verständnis von Kontrollebenenschutz (CPPr).

Hardware-Ratenlimitierungen

Die Cisco Catalyst Supervisor Engine 32 der Serie 6500 und die Supervisor Engine 720 unterstützen plattformspezifische, hardwarebasierte Durchsatzratenlimitierungen (HWRLs) für spezielle Netzwerkszenarien. Diese Hardware-Ratenlimitierungen werden als Durchsatzbegrenzer für Sonderfälle bezeichnet, da sie einen bestimmten vordefinierten Satz von IPv4-, IPv6-, Unicast- und Multicast-DoS-Szenarien abdecken. HWRLs können das Cisco IOS-Gerät vor einer Vielzahl von Angriffen schützen, bei denen Pakete von der CPU verarbeitet werden müssen.

Es gibt mehrere standardmäßig aktivierte HWRLs. Weitere Informationen finden Sie unter PFC3 Hardware-basierte Ratenlimitierungs-Standardeinstellungen.

Weitere Informationen zu HWRLs *finden Sie unter* Hardware-basierte Ratenlimitierungen auf dem PFC3.

Sicheres BGP

Das Border Gateway Protocol (BGP) ist die Routing-Grundlage des Internets. Daher verwendet jedes Unternehmen mit mehr als bescheidenen Verbindungsanforderungen häufig BGP. BGP wird häufig von Angreifern angegriffen, da es allgegenwärtig ist und in kleineren Unternehmen *festgelegt ist und* BGP-Konfigurationen *vergessen werden*. Es gibt jedoch viele BGP-spezifische Sicherheitsfunktionen, die zur Erhöhung der Sicherheit einer BGP-Konfiguration eingesetzt werden können.

Diese bietet eine Übersicht über die wichtigsten BGP-Sicherheitsfunktionen. Gegebenenfalls werden Konfigurationsempfehlungen gegeben.

TTL-basierter Sicherheitsschutz

Jedes IP-Paket enthält ein 1-Byte-Feld, das als Time to Live (TTL) bezeichnet wird. Jedes Gerät, das ein IP-Paket durchläuft, verringert diesen Wert um eins. Der Startwert variiert je nach Betriebssystem und liegt in der Regel zwischen 64 und 255. Ein Paket wird verworfen, wenn sein TTL-Wert 0 erreicht.

Ein TTL-basierter Sicherheitsschutz, der sowohl als Generalized TTL-basierter Sicherheitsmechanismus (GTSM) als auch als BGP TTL Security Hack (BTSH) bezeichnet wird, nutzt den TTL-Wert von IP-Paketen, um sicherzustellen, dass die empfangenen BGP-Pakete von einem direkt verbundenen Peer stammen. Diese Funktion erfordert häufig die Koordination durch Peering-Router. Sobald diese Funktion aktiviert ist, kann sie jedoch viele TCP-basierte Angriffe auf das BGP vollständig abwehren.

GTSM für BGP wird mit der **ttl-security-**Option für den Konfigurationsbefehl **Nachbarn**-BGP-Router aktiviert. In diesem Beispiel wird die Konfiguration dieser Funktion veranschaulicht:

```
!

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

Beim Empfang von BGP-Paketen wird der TTL-Wert überprüft und muss größer/gleich 255 minus der angegebenen Hop-Anzahl sein.

BGP-Peer-Authentifizierung mit MD5

Bei der Peer-Authentifizierung mit MD5 wird für jedes im Rahmen einer BGP-Sitzung gesendete Paket ein MD5-Digest erstellt. Insbesondere werden Teile der IP- und TCP-Header, TCP-Payload und ein geheimer Schlüssel zum Generieren des Digest verwendet.

Der erstellte Digest wird dann in der TCP-Option Kind 19 gespeichert, die speziell zu diesem Zweck von RFC 2385 erstellt wurde. Der empfangende BGP-Sprecher verwendet den gleichen Algorithmus und den gleichen geheimen Schlüssel, um den Message Digest neu zu generieren. Wenn der empfangene und der berechnete Datenverkehr nicht identisch sind, wird das Paket verworfen.

Die Peer-Authentifizierung mit MD5 wird mit der **Kennwort-**Option für den Konfigurationsbefehl **Nachbarrouter** konfiguriert. Die Verwendung dieses Befehls wird wie folgt veranschaulicht:

```
!

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

Weitere Informationen zur BGP-Peer-Authentifizierung mit MD5 *finden Sie unter* Nachbarrouterauthentifizierung.

Maximale Präfixe konfigurieren

BGP-Präfixe werden von einem Router im Speicher gespeichert. Je mehr Präfixe ein Router enthalten muss, desto mehr Arbeitsspeicher muss das BGP beanspruchen. In einigen Konfigurationen kann eine Teilmenge aller Internet-Präfixe gespeichert werden, z. B. in Konfigurationen, die nur eine oder mehrere Standardrouten für Kundennetzwerke eines Anbieters nutzen.

Um eine Speichererschöpfung zu vermeiden, ist es wichtig, die maximale Anzahl an Präfixen pro Peer zu konfigurieren. Es wird empfohlen, für jeden BGP-Peer einen Grenzwert zu konfigurieren.

Wenn Sie diese Funktion mit dem BGP-Router-Konfigurationsbefehl **mit dem maximalen Präfix des Nachbarn** konfigurieren, ist ein Argument erforderlich: die maximale Anzahl von Präfixen, die akzeptiert werden, bevor ein Peer heruntergefahren wird. Optional kann auch eine Zahl zwischen 1 und 100 eingegeben werden. Diese Zahl stellt den Prozentsatz der maximalen Präfixe dar, zu dem eine Protokollmeldung gesendet wird.

```
!

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

Weitere Informationen zu den maximalen Präfixen pro Peer *finden Sie unter* Konfigurieren der BGP-Funktion für maximale Präfixe.

BGP-Präfixe mit Präfixlisten filtern

Mit Präfixlisten kann ein Netzwerkadministrator bestimmte Präfixe zulassen oder ablehnen, die über das BGP gesendet oder empfangen werden. Präfixlisten sollten möglichst verwendet werden, um sicherzustellen, dass Netzwerkverkehr über die vorgesehenen Pfade gesendet wird. Präfixlisten sollten auf jeden eBGP-Peer sowohl in der ein- als auch in der ausgehenden Richtung angewendet werden.

Konfigurierte Präfixlisten beschränken die Präfixe, die an die Präfixe gesendet oder empfangen werden, die speziell durch die Routing-Richtlinie eines Netzwerks zulässig sind. Wenn dies aufgrund der großen Anzahl der empfangenen Präfixe nicht möglich ist, sollte eine Präfixliste so konfiguriert werden, dass bekannte schädliche Präfixe ausdrücklich blockiert werden. Zu diesen bekannten schädlichen Präfixen gehören nicht zugewiesener IP-Adressraum und Netzwerke, die RFC 330 für interne oder Testzwecke reserviert. Ausgehende Präfixlisten sollten so konfiguriert werden, dass nur die Präfixe zulässig sind, die eine Organisation anzukündigen beabsichtigt.

In diesem Konfigurationsbeispiel werden Präfixlisten verwendet, um die Routings zu beschränken, die gelernt und angekündigt werden. Insbesondere ist nur ein Standard-Routing durch die

Präfixliste BGP-PL-INBOUND eingehend zulässig, und das Präfix 192.168.2.0/24 ist die einzige Route, die von BGP-PL-OUTBOUND angekündigt werden darf.

```
!

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

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

Informationen zur vollständigen Abdeckung der BGP-Präfixfilterung finden Sie unter Verbindung mit einem Dienstanbieter über externes BGP.

Filtern von BGP-Präfixen mit autonomen Systempfad-Zugriffslisten

Mithilfe von Zugriffslisten für den AS-Pfad (Autonomous System) des BGP kann der Benutzer empfangene und angegebene Präfixe auf der Grundlage des AS-Path-Attributs eines Präfix filtern. Dies kann in Verbindung mit Präfixlisten verwendet werden, um einen robusten Satz von Filtern zu erstellen.

In diesem Konfigurationsbeispiel werden AS-Pfadzugriffslisten verwendet, um eingehende Präfixe auf die Präfixe zu beschränken, die vom Remote-AS generiert werden, und ausgehende Präfixe auf Präfixe, die vom lokalen autonomen System stammen. Präfixe, die von allen anderen autonomen Systemen stammen, werden gefiltert und nicht in der Routing-Tabelle installiert.

```
!

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

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

Secure Interior Gateway-Protokolle

Die Fähigkeit eines Netzwerks, Datenverkehr ordnungsgemäß weiterzuleiten und nach Topologieänderungen oder -fehlern wiederherzustellen, hängt von einer genauen Ansicht der Topologie ab. Sie können häufig ein Interior Gateway Protocol (IGP) ausführen, um diese Ansicht bereitzustellen. IGPs sind standardmäßig dynamisch und erkennen zusätzliche Router, die mit dem jeweils verwendeten IGP kommunizieren. IGPs erkennen auch Routen, die bei einem Netzwerkverbindungsausfall verwendet werden können.

Diese Unterabschnitte bieten einen Überblick über die wichtigsten IGP-Sicherheitsfunktionen. Gegebenenfalls werden Empfehlungen und Beispiele für Routing Information Protocol Version 2 (RIPv2), Enhanced Interior Gateway Routing Protocol (EIGRP) und Open Shortest Path First (OSPF) bereitgestellt.

Routing-Protokoll-Authentifizierung und -Verifizierung mit Message Digest 5

Wenn der Austausch von Routing-Informationen nicht gesichert wird, können Angreifer falsche Routing-Informationen in das Netzwerk einführen. Durch die Passwortauthentifizierung mit Routing-Protokollen zwischen Routern können Sie die Sicherheit des Netzwerks erhöhen. Da diese Authentifizierung jedoch als Klartext gesendet wird, kann es für einen Angreifer einfach sein, diese Sicherheitskontrolle zu untergraben.

Durch das Hinzufügen von MD5-Hash-Funktionen zum Authentifizierungsprozess enthalten Routing-Updates keine Klartext-Passwörter mehr, und der gesamte Inhalt des Routing-Updates ist widerstandsfähiger gegen Manipulationen. Die MD5-Authentifizierung ist jedoch weiterhin anfällig für Brute-Force- und Wörterbuchangriffe, wenn schwache Passwörter gewählt werden. Es wird empfohlen, Kennwörter mit ausreichender Randomisierung zu verwenden. Da die MD5-Authentifizierung im Vergleich zur Kennwortauthentifizierung viel sicherer ist, sind diese Beispiele auf die MD5-Authentifizierung ausgerichtet. IPSec kann auch für die Validierung und Sicherung von Routing-Protokollen verwendet werden. In diesen Beispielen wird jedoch nicht näher auf die Verwendung eingegangen.

EIGRP und RIPv2 verwenden Schlüsselketten als Teil der Konfiguration. *Weitere Informationen* zur Konfiguration und Verwendung von Key-Chains *finden Sie* unter Key.

Dies ist eine Beispielkonfiguration für die EIGRP-Routerauthentifizierung mit MD5:

```
!

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

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

Dies ist ein Beispiel für eine MD5-Router-Authentifizierungskonfiguration für RIPv2. RIPv1 unterstützt keine Authentifizierung.

```
!

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

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

Dies ist eine Beispielkonfiguration für die OSPF-Router-Authentifizierung mit MD5. OSPF verwendet keine Key-Chains.

```
!

interface <interface>
```

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

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

Weitere Informationen finden Sie unter Konfigurieren von OSPF.

Passive Schnittstellenbefehle

Informationslecks oder die Einführung falscher Informationen in ein IGP können mithilfe des Befehls **passive-interface** reduziert werden, der die Steuerung der Meldung von Routing-Informationen unterstützt. Es wird empfohlen, keine Informationen an Netzwerke weiterzuleiten, die sich außerhalb Ihrer administrativen Kontrolle befinden.

In diesem Beispiel wird die Verwendung dieses Features veranschaulicht:

```
!

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

Routenfilterung

Um die Möglichkeit einzuschränken, falsche Routing-Informationen im Netzwerk einzugeben, müssen Sie die Routenfilterung verwenden. Im Gegensatz zum Befehl zur **passiven Schnittstellenkonfiguration** erfolgt das Routing auf Schnittstellen, sobald die Routenfilterung aktiviert ist. Die angegebenen oder verarbeiteten Informationen sind jedoch begrenzt.

Für EIGRP und RIP beschränkt die Verwendung des Befehls **distribute-** mit dem **out**-Schlüsselwort, welche Informationen angekündigt werden, während die Verwendung des **in-**Schlüsselworts die Verarbeitung von Aktualisierungen beschränkt. Der Befehl **distribute-list** ist für OSPF verfügbar, verhindert jedoch nicht, dass ein Router gefilterte Routen weitergibt. Stattdessen kann der Befehl **Bereichsfilter-Liste** verwendet werden.

In diesem EIGRP-Beispiel werden ausgehende Meldungen mithilfe des Befehls **distribute-** und einer Präfixliste gefiltert:

```
!

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

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

In diesem EIGRP-Beispiel werden eingehende Updates mithilfe einer Präfixliste gefiltert:

```
!
```

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

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

Weitere Informationen zur Kontrolle der Werbung und Verarbeitung von Routing-Updates finden Sie unter Konfiguration von IP Routing Protocol-Independent Features.

In diesem OSPF-Beispiel wird eine Präfixliste mit dem OSPF-spezifischen Befehl **Area Filter List** verwendet:

```
!

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

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

Ressourcennutzung im Routing-Prozess

Routingprotokollpräfixe werden von einem Router im Arbeitsspeicher gespeichert, und der Ressourcenverbrauch steigt mit zusätzlichen Präfixen, die ein Router enthalten muss. Um eine Ressourcenerschöpfung zu verhindern, muss das Routing-Protokoll so konfiguriert werden, dass die Ressourcenauslastung begrenzt wird. Dies ist mit OSPF möglich, wenn Sie die Funktion zum Überlastungsschutz für Link-State-Datenbanken verwenden.

In diesem Beispiel wird die Konfiguration des OSPF Link State Database Overload Protection-Features veranschaulicht:

```
!

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

Weitere Informationen zum Schutz vor OSPF-Link-Überlastungen finden Sie unter Einschränken der Anzahl selbstgenerierender LSAs für einen OSPF-Prozess.

Sichere Protokolle für die erste Hop-Redundanz

First Hop Redundancy Protocols (FHRPs) bieten Ausfallsicherheit und Redundanz für Geräte, die als Standard-Gateways fungieren. Diese Situation und diese Protokolle sind in Umgebungen üblich, in denen ein Paar von Layer-3-Geräten Standard-Gateway-Funktionen für ein Netzwerksegment oder eine Gruppe von VLANs bereitstellt, die Server oder Workstations enthalten.

Alle FHRPs sind das Gateway Load Balancing Protocol (GLBP), das Hot Standby Router Protocol (HSRP) und das Virtual Router Redundancy Protocol (VRRP). Standardmäßig kommunizieren diese Protokolle mit nicht authentifizierten Kommunikationsvorgängen. Diese Art der

Kommunikation kann es einem Angreifer ermöglichen, sich als FHRP-sprechendes Gerät zu präsentieren und die Standard-Gateway-Rolle im Netzwerk zu übernehmen. Diese Übernahme würde es einem Angreifer ermöglichen, einen Man-in-the-Middle-Angriff durchzuführen und den gesamten Benutzerdatenverkehr abzufangen, der das Netzwerk verlässt.

Um diese Art von Angriffen zu verhindern, verfügen alle von der Cisco IOS-Software unterstützten FHRPs über eine Authentifizierungsfunktion mit MD5- oder Textzeichenfolgen. Aufgrund der Bedrohung durch nicht authentifizierte FHRPs wird empfohlen, dass Instanzen dieser Protokolle MD5-Authentifizierung verwenden. In diesem Konfigurationsbeispiel wird die Verwendung der GLBP-, HSRP- und VRRP MD5-Authentifizierung veranschaulicht:

```
!

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

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

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

Datenebene

Obwohl die Datenebene für das Verschieben von Daten von der Quelle zum Ziel verantwortlich ist, ist die Datenebene im Kontext der Sicherheit die geringste Bedeutung der drei Ebenen. Aus diesem Grund ist es wichtig, die Management- und Steuerungsebenen vor der Datenebene zu schützen, wenn Sie ein Netzwerkgerät sichern.

In der Datenebene selbst gibt es jedoch eine Vielzahl von Funktionen und Konfigurationsoptionen, die zur Sicherung des Datenverkehrs beitragen können. In diesen Abschnitten werden diese Funktionen und Optionen beschrieben, mit denen Sie Ihr Netzwerk einfacher schützen können.

Allgemeine Datenebenensicherung

Der Großteil des Datenverkehrs auf der Datenebene fließt über das Netzwerk, was durch die Routing-Konfiguration des Netzwerks bestimmt wird. Es gibt jedoch eine IP-Netzwerkfunktion, um den Pfad von Paketen im Netzwerk zu verändern. Funktionen wie IP-Optionen, insbesondere die Source-Routing-Option, stellen in modernen Netzwerken eine Herausforderung für die Sicherheit dar.

Die Verwendung von Transit-ACLs ist auch für die Härtung der Datenebene von Bedeutung.

Weitere Informationen finden Sie im Abschnitt Filter Transit Traffic with Transit ACLs (Transit-ACLs filtern) dieses Dokuments.

IP Options Selective Drop

Die IP-Optionen werfen zwei Sicherheitsbedenken auf. Datenverkehr, der IP-Optionen enthält, muss von Cisco IOS-Geräten prozessgesteuert werden, was zu einer erhöhten CPU-Last führen kann. IP-Optionen beinhalten auch die Funktion, den Pfad des Datenverkehrs durch das Netzwerk zu ändern, wodurch Sicherheitskontrollen untergraben werden können.

Aus diesen Gründen wird der globale Konfigurationsbefehl **ip options {drop | ignore}** wurde den Cisco IOS Software-Versionen 12.3(4)T, 12.0(22)S und 12.2(25)S hinzugefügt. In der ersten Form dieses Befehls, **ip options drop**, werden alle IP-Pakete verworfen, die IP-Optionen enthalten, die vom Cisco IOS-Gerät empfangen werden. Dies verhindert sowohl eine erhöhte CPU-Last als auch eine mögliche Subversion von Sicherheitskontrollen, die durch IP-Optionen aktiviert werden können.

Die zweite Form dieses Befehls, **ip options ignore**, konfiguriert das Cisco IOS-Gerät, um IP-Optionen zu ignorieren, die in empfangenen Paketen enthalten sind. Dadurch werden zwar die Bedrohungen im Zusammenhang mit IP-Optionen für das lokale Gerät verringert, es ist jedoch möglich, dass Downstream-Geräte durch das Vorhandensein von IP-Optionen beeinträchtigt werden. Aus diesem Grund wird die **Drop**-Form dieses Befehls dringend empfohlen. Dies wird im Konfigurationsbeispiel veranschaulicht:

```
!
ip options drop
!
```

Beachten Sie, dass einige Protokolle, z. B. der RSVP, IP-Optionen legitim nutzen. Dieser Befehl beeinträchtigt die Funktionalität dieser Protokolle.

Sobald der selektive Drop der IP-Optionen aktiviert ist, kann der Befehl **show ip traffic** EXEC verwendet werden, um die Anzahl der Pakete zu bestimmen, die aufgrund von IP-Optionen verworfen werden. Diese Informationen befinden sich im Drop-Zähler für erzwungene Nachrichten.

Weitere Informationen zu dieser Funktion *finden Sie unter* ACL IP Options Selective Drop.

IP Source Routing deaktivieren

Beim IP-Quellrouting werden die Optionen Loose Source Route und Record Route gemeinsam mit der Option Strict Source Route verwendet, um der Quelle des IP-Datagramms die Angabe des Netzwerkpfads zu ermöglichen, den ein Paket annimmt. Diese Funktion kann bei Versuchen verwendet werden, den Datenverkehr um Sicherheitskontrollen im Netzwerk zu leiten.

Wenn die IP-Optionen mithilfe der Funktion "Selektive Drop" (IP-Optionen) nicht vollständig deaktiviert wurden, ist es wichtig, dass das IP-Quellrouting deaktiviert wird. IP Source Routing, das in allen Cisco IOS Software Releases standardmäßig aktiviert ist, wird über den globalen Konfigurationsbefehl **no ip source-route** deaktiviert. In diesem Konfigurationsbeispiel wird die Verwendung dieses Befehls veranschaulicht:

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

ICMP-Umleitungen deaktivieren

Mithilfe von ICMP-Umleitungen wird ein Netzwerkgerät über einen besseren Pfad zu einem IP-Ziel informiert. Standardmäßig sendet die Cisco IOS-Software eine Umleitung, wenn sie ein Paket empfängt, das über die empfangene Schnittstelle geroutet werden muss.

In einigen Situationen kann es für einen Angreifer möglich sein, dass das Cisco IOS-Gerät viele ICMP-Umleitungsnachrichten sendet, was zu einer erhöhten CPU-Last führt. Aus diesem Grund wird empfohlen, die Übertragung von ICMP-Umleitungen zu deaktivieren. ICMP-Umleitungen sind mit dem Befehl **no ip redirects** (Schnittstellenkonfiguration **no ip redirects**) deaktiviert, wie in der Beispielkonfiguration gezeigt:

```
!

interface FastEthernet 0
no ip redirects
!
```

IP-Directed Broadcasts deaktivieren oder beschränken

IP-Directed Broadcasts ermöglichen das Senden eines IP-Broadcast-Pakets an ein Remote-IP-Subnetz. Sobald das Remote-Netzwerk erreicht ist, sendet das weiterleitende IP-Gerät das Paket als Layer-2-Broadcast an alle Stationen im Subnetz. Diese gezielte Broadcast-Funktion wurde in mehreren Angriffen, einschließlich des SMURF-Angriffs, als Verstärkung und Reflektionshilfe genutzt.

Bei aktuellen Versionen der Cisco IOS-Software ist diese Funktion standardmäßig deaktiviert. Sie kann jedoch über den Schnittstellenkonfigurationsbefehl **ip directed-Broadcast** aktiviert werden. Versionen der Cisco IOS-Software, die älter als 12.0 sind, haben diese Funktionalität standardmäßig aktiviert.

Wenn für ein Netzwerk eine gezielte Broadcast-Funktionalität unbedingt erforderlich ist, sollte dessen Nutzung kontrolliert werden. Dies ist möglich, wenn eine Zugriffskontrollliste als Option für den Befehl **ip directed-broadcast** verwendet wird. In diesem Konfigurationsbeispiel werden gezielte Broadcasts auf UDP-Pakete beschränkt, die von einem vertrauenswürdigen Netzwerk stammen, 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
!
```

Filtern von Transit-Datenverkehr mit Transit-ACLs

Es ist möglich, mithilfe von Transit-ACLs (tACLs) zu steuern, welcher Datenverkehr durch das Netzwerk fließt. Dies steht im Gegensatz zu Infrastruktur-ACLs, die Datenverkehr filtern möchten, der für das Netzwerk selbst bestimmt ist. Die von den tACLs bereitgestellte Filterung ist von Vorteil, wenn der Datenverkehr auf eine bestimmte Gruppe von Geräten oder Datenverkehr, der das Netzwerk durchläuft, gefiltert werden soll.

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

Transit-ACLs sind auch ein geeigneter Ort, um statische Anti-Spoofing-Schutzmaßnahmen zu implementieren.

Weitere Informationen finden Sie im Abschnitt Anti-Spoofing-Schutz dieses Dokuments.

Weitere Informationen finden Sie in den Transit Access Control Lists: Filtern am Edge für weitere Informationen zu tACLs.

ICMP-Paketfilterung

Das Internet Control Message Protocol (ICMP) wurde als Steuerungsprotokoll für IP entwickelt. Daher können die von ihm vermittelten 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 Path MTU Discovery verwendet. Allerdings ist für den ordnungsgemäßen Betrieb eines Netzwerks selten eine externe ICMP-Anbindung erforderlich.

Die Cisco IOS-Software bietet Funktionen zum gezielten Filtern von ICMP-Nachrichten nach Name, Typ und Code. In diesem Beispiel lässt die ACL ICMP von vertrauenswürdigen Netzwerken zu, während sie alle ICMP-Pakete von anderen Quellen blockiert:

```
!

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

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

deny icmp any any
!
```

IP-Fragmente filtern

Wie bereits im Abschnitt "Limit Access to the Network with Infrastructure ACLs" dieses Dokuments beschrieben, kann das Filtern fragmentierter IP-Pakete Sicherheitsgeräte vor Herausforderungen stellen.

Da die Fragment-Verarbeitung nicht intuitiv ist, werden IP-Fragmente häufig versehentlich von ACLs zugelassen. Fragmentierung wird häufig auch bei Versuchen verwendet, die Erkennung von Angriffserkennungssystemen zu umgehen. Aus diesen Gründen werden IP-Fragmente häufig bei Angriffen verwendet und sollten explizit oben auf konfigurierten tACLs gefiltert werden. Die folgende ACL enthält eine umfassende Filterung von IP-Fragmenten. Die in diesem Beispiel veranschaulichte Funktionalität muss zusammen mit der Funktionalität der vorherigen Beispiele verwendet werden:

```
!

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

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

Weitere Informationen zur Verarbeitung fragmentierter IP-Pakete *finden Sie unter* Zugriffskontrolllisten und IP-Fragmente.

ACL-Unterstützung für IP-Filteroptionen

In der Cisco IOS Software, Version 12.3(4)T und höher, unterstützt die Cisco IOS-Software die Verwendung von ACLs zum Filtern von IP-Paketen basierend auf den im Paket enthaltenen IP-Optionen. Das Vorhandensein von IP-Optionen in einem Paket kann auf einen Versuch hinweisen, Sicherheitskontrollen im Netzwerk zu untergraben oder die Übertragungsmerkmale eines Pakets anderweitig zu ändern. Aus diesen Gründen sollten Pakete mit IP-Optionen am Netzwerk-Edge gefiltert werden.

Dieses Beispiel muss zusammen mit dem Inhalt der vorherigen Beispiele verwendet werden, um das vollständige Filtern von IP-Paketen mit IP-Optionen zu ermöglichen:

```
!

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

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

Anti-Spoofing-Schutz

Viele Angriffe nutzen IP-Adressen-Spoofing als Quelle, um effektiv zu sein oder die tatsächliche Quelle eines Angriffs zu verbergen und eine genaue Nachverfolgung zu verhindern. Die Cisco IOS-Software bietet Unicast RPF und IP Source Guard (IPSG), um Angriffe abzuwehren, die auf Quell-IP-Adressen-Spoofing basieren. Darüber hinaus werden ACLs und Null-Routing häufig als manuelles Mittel zur Verhinderung von Spoofing eingesetzt.

IP Source Guard minimiert Spoofing für Netzwerke, die direkt von der Administration kontrolliert werden, indem Switch-Port, MAC-Adresse und Quelladresse überprüft werden. Unicast RPF ermöglicht die Überprüfung des Quellnetzwerks und kann gefälschte Angriffe von Netzwerken reduzieren, die nicht direkt von der Verwaltung kontrolliert werden. Port Security kann zur Validierung von MAC-Adressen auf dem Access Layer verwendet werden. Dynamic Address Resolution Protocol (ARP) Inspection (DAI) verhindert Angriffsvektoren, die auf lokalen Segmenten ARP-Poisoning verwenden.

Unicast-RPF

Mit Unicast RPF kann ein Gerät überprüfen, ob die Quelladresse eines weitergeleiteten Pakets über die Schnittstelle erreicht werden kann, die das Paket empfangen hat. Sie dürfen sich nicht auf Unicast RPF als einzigen Schutz vor Spoofing verlassen. Gefälschte Pakete können über eine Unicast RPF-fähige Schnittstelle in das Netzwerk gelangen, wenn eine entsprechende Rückgaberoute zur Quell-IP-Adresse vorhanden ist. Das Unicast-RPF wird für die Cisco Express Forwarding auf jedem Gerät konfiguriert und auf Schnittstellenbasis konfiguriert.

Unicast RPF kann in einem von zwei Modi konfiguriert werden: locker oder strikt. In Fällen mit asymmetrischem Routing wird der Lose-Modus bevorzugt, da in diesen Situationen der strikte Modus bekanntermaßen Pakete verwirft. Während der Konfiguration des Schnittstellenkonfigurationsbefehls **ip verify** konfiguriert das Schlüsselwort **any** den losen Modus, während das Schlüsselwort **rx** den strikten Modus konfiguriert.

In diesem Beispiel wird die Konfiguration dieses Features veranschaulicht:

```
!

ip cef
!

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

Weitere Informationen zur Konfiguration und Verwendung von Unicast RPF finden Sie unter Understanding Unicast Reverse Path Forwarding.

IP Source Guard

IP Source Guard ist ein effektives Mittel zur Spoofing-Prävention, das verwendet werden kann, wenn Sie die Kontrolle über Layer-2-Schnittstellen haben. IP Source Guard verwendet Informationen aus DHCP-Snooping, um eine Port Access Control List (PACL) auf der Layer-2-Schnittstelle dynamisch zu konfigurieren und jeglichen Datenverkehr von IP-Adressen abzulehnen, die nicht der IP-Quellbindungstabelle zugeordnet sind.

IP Source Guard kann auf Layer-2-Schnittstellen angewendet werden, die zu DHCP-Snooping-fähigen VLANs gehören. Diese Befehle ermöglichen DHCP-Snooping:

```
!

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

Wenn DHCP-Snooping aktiviert ist, aktivieren diese Befehle IPSG:

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

Die Portsicherheit kann mit dem Schnittstellenkonfigurationsbefehl **ip verify source port security** interface aktiviert werden. Hierfür ist die Option zum globalen Konfigurationsbefehl **ip dhcp**

snooping information erforderlich. Zusätzlich muss der DHCP-Server die DHCP-Option 82 unterstützen.

Weitere Informationen zu dieser Funktion *finden Sie unter* Konfigurieren von DHCP-Funktionen und IP Source Guard.

Port-Sicherheit

Port Security wird verwendet, um MAC-Adressen-Spoofing an der Zugriffsschnittstelle zu verhindern. Port Security kann dynamisch erlernte (klebrige) MAC-Adressen verwenden, um die Erstkonfiguration zu vereinfachen. Sobald die Port-Sicherheit eine MAC-Verletzung festgestellt hat, kann sie einen von vier Verletzungsmodi verwenden. Diese Modi sind VLANs zum Schützen, Einschränken, Herunterfahren und Herunterfahren. In Fällen, in denen ein Port nur Zugriff für eine einzelne Workstation bietet, wobei Standardprotokolle verwendet werden, kann eine Höchstzahl von einem ausreichend sein. Protokolle, die virtuelle MAC-Adressen wie HSRP nutzen, funktionieren nicht, wenn die maximale Anzahl auf eine festgelegt ist.

```
!

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

Weitere Informationen zur Sicherheitsüberladung für Ports *finden Sie unter* Konfigurieren der Port-Sicherheit.

Dynamische ARP-Inspektion

Dynamic ARP Inspection (DAI) kann eingesetzt werden, um Angriffe auf lokale Segmente durch ARP-Vergiftung zu verhindern. Ein ARP-Poisoning-Angriff ist eine Methode, bei der ein Angreifer gefälschte ARP-Informationen an ein lokales Segment sendet. Diese Informationen dienen dazu, den ARP-Cache anderer Geräte zu beschädigen. Häufig verwendet ein Angreifer ARP-Poisoning, um einen Man-in-the-Middle-Angriff durchzuführen.

DAI fängt die IP-zu-MAC-Adressbeziehung aller ARP-Pakete an nicht vertrauenswürdigen Ports ab und validiert diese. In DHCP-Umgebungen verwendet DAI die Daten, die durch die DHCP-Snooping-Funktion generiert werden. ARP-Pakete, die auf vertrauenswürdigen Schnittstellen empfangen werden, werden nicht validiert, und ungültige Pakete auf nicht vertrauenswürdigen Schnittstellen werden verworfen. In Nicht-DHCP-Umgebungen ist die Verwendung von ARP-ACLs erforderlich.

Diese Befehle ermöglichen DHCP-Snooping:

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

Sobald DHCP-Snooping aktiviert wurde, aktivieren diese Befehle DAI:

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

In Nicht-DHCP-Umgebungen sind ARP-ACLs erforderlich, um DAI zu aktivieren. Dieses Beispiel veranschaulicht die grundlegende Konfiguration von DAI mit ARP-ACLs:

```
!

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

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

DAi kann auch auf Schnittstellenbasis aktiviert werden, wo immer dies unterstützt wird.

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

Weitere Informationen zum Konfigurieren von DAI finden Sie unter Konfigurieren der dynamischen ARP-Inspektion.

Anti-Spoofing-ACLs

Manuell konfigurierte ACLs bieten statischen Anti-Spoofing-Schutz vor Angriffen, bei denen bekannter nicht verwendeter und nicht vertrauenswürdiger Adressbereich verwendet wird. In der Regel werden diese Anti-Spoofing-ACLs als Komponente einer größeren ACL auf eingehenden Datenverkehr an Netzwerkgrenzen angewendet. Anti-Spoofing-ACLs erfordern eine regelmäßige Überwachung, da sie häufig geändert werden können. Spoofing kann bei Datenverkehr aus dem lokalen Netzwerk minimiert werden, wenn ausgehende ACLs angewendet werden, die den Datenverkehr auf gültige lokale Adressen beschränken.

Dieses Beispiel veranschaulicht, wie ACLs verwendet werden können, um IP-Spoofing einzuschränken. Diese ACL wird eingehend auf die gewünschte Schnittstelle angewendet. Die ACEs, aus denen diese ACL besteht, sind nicht umfassend. Wenn Sie diese Arten von ACLs konfigurieren, suchen Sie nach einer aktuellen Referenz, die aussagekräftig ist.

```
!

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

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

Weitere Informationen zum Konfigurieren von Zugriffskontrolllisten finden Sie unter Konfigurieren häufig verwendeter IP-Zugriffskontrolllisten.

Die offizielle Liste der nicht zugewiesenen Internetadressen wird von Team Cymru geführt. Weitere Informationen zum Filtern nicht verwendeter Adressen finden Sie auf der Bogon-Referenzseite .

Begrenzung der CPU-Auswirkungen des Datenverkehrs auf der Datenebene

Der Hauptzweck von Routern und Switches besteht darin, Pakete und Frames über das Gerät an die endgültigen Ziele weiterzuleiten. Diese Pakete, die die Geräte durchlaufen, die im Netzwerk bereitgestellt werden, können den CPU-Betrieb eines Geräts beeinträchtigen. Die Datenebene, die aus dem Datenverkehr besteht, der das Netzwerkgerät durchläuft, sollte gesichert werden, um den Betrieb der Verwaltungs- und Kontrollebenen sicherzustellen. Wenn der Transitverkehr dazu führen kann, dass ein Gerät Switch-Datenverkehr verarbeitet, kann dies Auswirkungen auf die Kontrollebene eines Geräts haben, was zu einer Betriebsunterbrechung führen kann.

Funktionen und Datenverkehrstypen mit Auswirkungen auf die CPU

Diese Liste ist zwar nicht vollständig, enthält jedoch Datenverkehrsarten, die eine spezielle CPU-Verarbeitung erfordern und von der CPU auf Prozessschaltungen umgestellt werden:

- **ACL-Protokollierung** - Der ACL-Protokolldatenverkehr besteht aus Paketen, die aufgrund einer Übereinstimmung (Zulassen oder Ablehnen) eines ACE generiert werden, auf dem das **log-**Schlüsselwort verwendet wird.
- **Unicast RPF** - In Verbindung mit einer ACL verwendeter Unicast RPF kann das Switching bestimmter Pakete zur Folge haben.
- **IP-Optionen**: Alle IP-Pakete mit enthaltenen Optionen müssen von der CPU verarbeitet werden.
- **Fragmentierung** - Jedes IP-Paket, das fragmentiert werden muss, muss zur Verarbeitung an die CPU übergeben werden.
- **Time-to-Live (TTL) Expiry** - Für Pakete mit einem TTL-Wert kleiner/gleich 1 müssen Nachrichten mit dem Status "Internet Control Message Protocol Time Exceeded" (ICMP-Typ 11, Code 0) gesendet werden, was zur CPU-Verarbeitung führt.
- **ICMP Unreachables** - Pakete, die aufgrund von Routing, MTU oder Filterung zu nicht erreichbaren ICMP-Nachrichten führen, werden von der CPU verarbeitet.
- **Datenverkehr, für den eine ARP-Anforderung erforderlich ist** - Ziele, für die kein ARP-Eintrag vorhanden ist, müssen von der CPU verarbeitet werden.
- **Nicht-IP-Datenverkehr** - Der gesamte Nicht-IP-Datenverkehr wird von der CPU verarbeitet.

Weitere Informationen zur Datenebenensicherung finden Sie im Abschnitt Allgemeine Datenebenensicherung dieses Dokuments.

Auf TTL-Wert filtern

Sie können die Funktion "ACL Support for Filtering on TTL Value" (ACL-Unterstützung für Filterung nach TTL-Wert) verwenden, die in der Cisco IOS Software, Version 12.4(2)T, in einer erweiterten IP-Zugriffsliste eingeführt wurde, um Pakete basierend auf dem TTL-Wert zu filtern. Diese Funktion kann verwendet werden, um ein Gerät zu schützen, das Transitverkehr empfängt, bei dem der TTL-Wert 0 oder 1 ist. Filterpakete, die auf TTL-Werten basieren, können ebenfalls

verwendet werden, um sicherzustellen, dass der TTL-Wert nicht niedriger als der Durchmesser des Netzwerks ist. Auf diese Weise wird die Kontrollebene von Downstream-Infrastrukturgeräten vor TTL-Auslaufangriffen geschützt.

Beachten Sie, dass einige Anwendungen und Tools wie **Traceroute** TTL-Ablaufpaket zu Test- und Diagnosezwecken verwenden. Einige Protokolle wie IGMP verwenden legitim einen TTL-Wert von einem.

In diesem ACL-Beispiel wird eine Richtlinie erstellt, die IP-Pakete filtert, deren TTL-Wert unter 6 liegt.

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

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

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

Weitere Informationen zum Filtern von Paketen basierend auf dem TTL-Wert *finden Sie unter* TTL-Ablaufdatum für die Identifizierung und Beseitigung von Angriffen.

Weitere Informationen zu dieser Funktion *finden Sie unter* ACL-Unterstützung für Filterung auf TTL-Wert.

In der Cisco IOS Softwareversion 12.4(4)T und höher ermöglicht Flexible Packet Matching (FPM) einem Administrator, beliebige Bits eines Pakets abzugleichen. Diese FPM-Richtlinie verwirft Pakete mit einem TTL-Wert unter sechs.

```
!

load protocol flash:ip.phdf
!

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

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

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

Weitere Informationen zu dieser Funktion finden Sie unter Flexible Packet Matching (Flexible Packet Matching) auf der Startseite von Cisco IOS Flexible Packet Matching.

Filtern auf das Vorhandensein von IP-Optionen

In der Cisco IOS-Softwareversion 12.3(4)T und höher können Sie die Funktion ACL-Unterstützung für die IP-Filteroptionen in einer benannten erweiterten IP-Zugriffsliste verwenden, um IP-Pakete mit vorhandenen IP-Optionen zu filtern. Die Filterung von IP-Paketen, die auf dem Vorhandensein von IP-Optionen basieren, kann ebenfalls verwendet werden, um zu verhindern, dass die Kontrollebene von Infrastrukturgeräten diese Pakete auf CPU-Ebene verarbeiten muss.

Beachten Sie, dass die Funktion "ACL Support for Filtering IP Options" (ACL-Unterstützung für IP-Optionen zum Filtern) nur mit benannten erweiterten ACLs verwendet werden kann. RSVP, Multiprotocol Label Switching Traffic Engineering, IGMP Version 2 und 3 sowie andere Protokolle, die IP-Optionspakete verwenden, können möglicherweise nicht ordnungsgemäß funktionieren, wenn Pakete für diese Protokolle verworfen werden. Wenn diese Protokolle im Netzwerk verwendet werden, kann die ACL-Unterstützung für IP-Filteroptionen verwendet werden. Die Funktion "Selective Drop" (Selektiver Drop) der ACL IP-Optionen kann diesen Datenverkehr jedoch verwerfen, und diese Protokolle funktionieren möglicherweise nicht ordnungsgemäß. Wenn keine Protokolle verwendet werden, die IP-Optionen erfordern, ist das selektive Verwerfen der Pakete mithilfe des ACL IP Options die bevorzugte Methode.

In diesem ACL-Beispiel wird eine Richtlinie erstellt, die IP-Pakete filtert, die IP-Optionen enthalten:

```
!

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

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

In diesem Beispiel zeigt die ACL eine Richtlinie, die IP-Pakete mit fünf spezifischen IP-Optionen filtert. Pakete, die diese Optionen enthalten, werden abgelehnt:

- 0 Liste der Optionen am Ende (EoOL)
- 7 Aufzeichnungsroute (Record-Route)
- 68 Zeitstempel (Zeitstempel)
- 131 - Loose Source Route (lsr)
- 137 - Strict Source Route (SSR)

```
!

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

```
!

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

Weitere Informationen über das selektive Verwerfen von ACL-IP-Optionen finden Sie im Abschnitt Allgemeine Datenebenensicherung dieses Dokuments.

Weitere Informationen finden Sie in den Transit Access Control Lists: Filtern am Edge für weitere Informationen zum Filtern von Transit- und Edge-Datenverkehr.

Eine weitere Funktion der Cisco IOS-Software, die zum Filtern von Paketen mit IP-Optionen verwendet werden kann, ist CoPP. In der Cisco IOS Software, Version 12.3(4)T und höher, ermöglicht CoPP einem Administrator, den Datenverkehrsfluss von Kontrollebenenpaketen zu filtern. Ein Gerät, das die CoPP- und ACL-Unterstützung für die Filterung von IP-Optionen unterstützt, die in Version 12.3(4)T der Cisco IOS-Software eingeführt wurde, kann eine Zugriffslistenrichtlinie verwenden, um Pakete mit IP-Optionen zu filtern.

Diese CoPP-Richtlinie verwirft Transitpakete, die von einem Gerät empfangen werden, wenn IP-Optionen vorhanden sind:

```
!

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

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

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

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

Diese CoPP-Richtlinie verwirft Transitpakete, die von einem Gerät empfangen werden, wenn diese IP-Optionen vorhanden sind:

- 0 Liste der Optionen am Ende (EoOL)
- 7 Aufzeichnungsroute (Record-Route)
- 68 Zeitstempel (Zeitstempel)
- 131 Loose Source Route (lsr)
- 137 Strict Source Route (SSR)

```
!
```

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

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

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

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

In den vorherigen CoPP-Richtlinien werden diese Pakete von den Zugriffskontrolllisten-Einträgen (ACEs), die Pakete mit der Genehmigungsaktion abgleichen, durch die Policy-map-Dropdown-Funktion verworfen, während Pakete, die der deny-Aktion entsprechen (nicht abgebildet), nicht von der Policy-Map-Dropdown-Funktion betroffen sind.

Weitere Informationen zur CoPP-Funktion finden Sie unter Bereitstellen von Control Plane Policing.

Schutz der Kontrollebene

In der Cisco IOS Software, Version 12.4(4)T und höher, kann Control Plane Protection (CPPr) verwendet werden, um den Datenverkehr der Steuerungsebene durch die CPU eines Cisco IOS-Geräts zu beschränken oder zu überwachen. CPPr ist CoPP ähnlich, kann jedoch den Datenverkehr mithilfe einer feineren Präzision als CoPP beschränken oder überwachen. CPPr teilt die aggregierte Kontrollebene in drei separate Kontrollebenen-Kategorien ein, die als Subschnittstellen bezeichnet werden: Host-, Transit- und CEF-Exception-Subschnittstellen sind vorhanden.

Diese CPPr-Richtlinie verwirft Transitpakete, die von einem Gerät empfangen werden, dessen TTL-Wert weniger als 6 beträgt, und Transit- oder Nicht-Transit-Pakete, die von einem Gerät empfangen werden, dessen TTL-Wert 0 oder 1 ist. Die CPPr-Richtlinie verwirft außerdem Pakete mit ausgewählten IP-Optionen, die vom Gerät empfangen werden.

```
!

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

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

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

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

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

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

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

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

!

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

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

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

In der vorherigen CPPr-Richtlinie werden die Einträge der Zugriffskontrollliste, die Pakete mit der Genehmigungsaktion abgleichen, von der Funktion Policy-map Drop verworfen, während Pakete, die der deny-Aktion entsprechen (nicht abgebildet), nicht von der Policy-Map-Dropdown-Funktion betroffen sind.

Weitere Informationen zur CPPr-Funktion *finden Sie unter* Understanding and Control Plane Protection.

Identifikation und Rückverfolgung des Datenverkehrs

In manchen Fällen müssen Sie Netzwerkverkehr schnell identifizieren und zurückverfolgen, insbesondere bei Incident Response oder schlechter Netzwerkleistung. NetFlow und Klassifizierungs-ACLs sind die beiden primären Methoden, um dies mit der Cisco IOS-Software zu erreichen. NetFlow bietet Transparenz für den gesamten Datenverkehr im Netzwerk. Darüber hinaus kann NetFlow mit Collectors implementiert werden, die eine langfristige Trendanalyse und automatisierte Analysen ermöglichen. Klassifizierungs-ACLs sind eine Komponente von ACLs und erfordern eine Vorabplanung, um bestimmten Datenverkehr und manuelle Eingriffe während der Analyse zu identifizieren. In diesen Abschnitten finden Sie eine kurze Übersicht über die einzelnen Funktionen.

NetFlow

NetFlow identifiziert ungewöhnliche und sicherheitsrelevante Netzwerkaktivitäten, indem es die Netzwerkflüsse verfolgt. NetFlow-Daten können über die CLI angezeigt und analysiert werden, oder die Daten können zur Aggregation und Analyse an einen kommerziellen oder Freeware NetFlow Collector exportiert werden. NetFlow-Collectors können durch langfristige Trends Netzwerkverhalten und Nutzungsanalysen bereitstellen. NetFlow-Funktionen durch Analyse bestimmter Attribute in IP-Paketen und Erstellung von Datenflüssen. Version 5 ist die am häufigsten verwendete Version von NetFlow, Version 9 ist jedoch erweiterbar. NetFlow-Datenflüsse können in Umgebungen mit hohen Datenvolumen mit Stichproben von Datenverkehrsdaten erstellt werden.

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

In diesem Beispiel wird die grundlegende Konfiguration dieses Features veranschaulicht. In früheren Versionen der Cisco IOS-Software lautet der Befehl zur Aktivierung von NetFlow auf einer Schnittstelle **ip route-cache flow** anstatt **ip flow {ingress | Ausgang**.

```
!

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

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

Dies ist ein Beispiel für die NetFlow-Ausgabe aus der CLI. Das SrcIf-Attribut kann in traceback hilfreich sein.

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

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

IP Flow Switching Cache, 4456704 bytes
55 active, 65481 inactive, 1014683 added
41000680 ager polls, 0 flow alloc failures
Active flows timeout in 2 minutes
Inactive flows timeout in 60 seconds
IP Sub Flow Cache, 336520 bytes
110 active, 16274 inactive, 2029366 added, 1014683 added to flow
0 alloc failures, 0 force free
1 chunk, 15 chunks added
last clearing of statistics never
Protocol Total Flows Packets Bytes Packets Active(Sec) Idle(Sec)
-------- Flows /Sec /Flow /Pkt /Sec /Flow /Flow
TCP-Telnet 11512 0.0 15 42 0.2 33.8 44.8
TCP-FTP 5606 0.0 3 45 0.0 59.5 47.1
TCP-FTPD 1075 0.0 13 52 0.0 1.2 61.1
TCP-WWW 77155 0.0 11 530 1.0 13.9 31.5
TCP-SMTP 8913 0.0 2 43 0.0 74.2 44.4
```

```
TCP-X 351 0.0 2 40 0.0 0.0 60.8
TCP-BGP 114 0.0 1 40 0.0 0.0 62.4
TCP-NNTP 120 0.0 1 42 0.0 0.7 61.4
TCP-other 556070 0.6 8 318 6.0 8.2 38.3
UDP-DNS 130909 0.1 2 55 0.3 24.0 53.1
UDP-NTP 116213 0.1 1 75 0.1 5.0 58.6
UDP-TFTP 169 0.0 3 51 0.0 15.3 64.2
UDP-Frag 1 0.0 1 1405 0.0 0.0 86.8
UDP-other 86247 0.1 226 29 24.0 31.4 54.3
ICMP 19989 0.0 37 33 0.9 26.0 53.9
IP-other 193 0.0 1 22 0.0 3.0 78.2
Total: 1014637 1.2 26 99 32.8 13.8 43.9

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

Weitere Informationen zu NetFlow-Funktionen *finden Sie* unter Cisco IOS NetFlow.

Eine technische Übersicht über NetFlow finden Sie unter Einführung in Cisco IOS NetFlow - Eine technische Übersicht.

Klassifizierungs-ACLs

Klassifizierungs-ACLs bieten Transparenz für Datenverkehr, der eine Schnittstelle durchläuft. Klassifizierungs-ACLs ändern die Sicherheitsrichtlinien eines Netzwerks nicht und werden in der Regel zur Klassifizierung einzelner Protokolle, Quelladressen oder Ziele konzipiert. Beispielsweise kann ein ACE, der den gesamten Datenverkehr zulässt, in bestimmte Protokolle oder Ports aufgeteilt werden. Diese präzisere Klassifizierung des Datenverkehrs in bestimmte ACEs kann ein besseres Verständnis des Netzwerkverkehrs ermöglichen, da jede Datenverkehrskategorie über einen eigenen Trefferzähler verfügt. Ein Administrator kann auch die implizite Verweigerung am Ende einer ACL in granulare ACEs aufteilen, um die Typen von abgelehntem Datenverkehr zu identifizieren.

Administratoren können die Reaktion auf Vorfälle beschleunigen, indem sie Klassifizierungs-ACLs mit den EXEC-Befehlen **show access-list** und **clear ip access-list** verwenden.

In diesem Beispiel wird die Konfiguration einer Klassifizierungs-ACL zur Identifizierung von SMB-Datenverkehr vor einer Standardverweigerung veranschaulicht:

```
!

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

Um den Datenverkehr zu identifizieren, der eine Klassifizierungs-ACL verwendet, verwenden Sie den Befehl **show access-list** acl-name EXEC. Die ACL-Zähler können mithilfe des Befehls **clear ip access-list counter** acl-name EXEC gelöscht werden.

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

Weitere Informationen zum Aktivieren von Protokollfunktionen in ACLs finden Sie unter Protokollierung von Zugriffskontrolllisten.

Zugriffskontrolle mit VLAN-Zuordnungen und Port-Zugriffskontrolllisten

VLAN Access Control Lists (VACLs) oder VLAN Maps und Port ACLs (PACLs) ermöglichen die Durchsetzung von Zugriffskontrollen für nicht gerouteten Datenverkehr, der näher an Endgeräten ist als Zugriffskontrolllisten, die auf geroutete Schnittstellen angewendet werden.

Diese Abschnitte bieten einen Überblick über die Funktionen, Vorteile und potenziellen Verwendungsszenarien von VACLs und PACLs.

Zugriffskontrolle mit VLAN-Zuordnungen

VACLs oder VLAN-Zuordnungen, die für alle Pakete gelten, die in das VLAN eingehen, ermöglichen die Durchsetzung der Zugriffskontrolle für den VLAN-internen Datenverkehr. Dies ist bei ACLs an gerouteten Schnittstellen nicht möglich. Beispielsweise kann eine VLAN-Zuordnung verwendet werden, um zu verhindern, dass Hosts, die im gleichen VLAN enthalten sind, miteinander kommunizieren. Dies verringert die Wahrscheinlichkeit, dass lokale Angreifer oder Würmer einen Host im gleichen Netzwerksegment ausnutzen. Um zu verhindern, dass Pakete eine VLAN-Zuordnung verwenden, können Sie eine Zugriffskontrollliste (ACL) erstellen, die mit dem Datenverkehr übereinstimmt, und in der VLAN-Zuordnung die Aktion auf "Drop" festlegen. Nach der Konfiguration einer VLAN-Zuordnung werden alle im LAN eingehenden Pakete nacheinander anhand der konfigurierten VLAN-Zuordnung ausgewertet. VLAN-Zugriffskarten unterstützen IPv4- und MAC-Zugriffslisten. Sie unterstützen jedoch keine Protokollierung oder IPv6-ACLs.

In diesem Beispiel wird eine erweiterte benannte Zugriffsliste verwendet, die die Konfiguration dieses Features veranschaulicht:

```
!

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

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

In diesem Beispiel wird die Verwendung einer VLAN-Map veranschaulicht, um die TCP-Ports 139 und 445 sowie das vines-ip-Protokoll zu verweigern:

```
!

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

```
!

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

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

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

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

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

vlan filter VACL vlan 100
!
```

Weitere Informationen zur Konfiguration von VLAN-Zuordnungen *finden Sie unter* Konfigurieren von Netzwerksicherheit mit ACLs.

Zugriffskontrolle mit PACLs

PACLs können nur auf die eingehende Richtung an den physischen Layer-2-Schnittstellen eines Switches angewendet werden. Ähnlich wie VLAN-Maps ermöglichen PACLs die Zugriffskontrolle für nicht gerouteten oder Layer-2-Datenverkehr. Die Syntax für die Erstellung von PACLs, die Vorrang vor VLAN-Maps und Router-ACLs hat, entspricht der Syntax der Router-ACLs. Wenn eine ACL auf eine Layer-2-Schnittstelle angewendet wird, wird sie als PACL bezeichnet. Die Konfiguration umfasst die Erstellung einer IPv4-, IPv6- oder MAC-ACL und deren Anwendung auf die Layer-2-Schnittstelle.

In diesem Beispiel wird eine erweiterte benannte Zugriffsliste verwendet, um die Konfiguration dieser Funktion zu veranschaulichen:

```
!

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

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

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

Zugriffskontrolle mit MAC

Mithilfe dieses Befehls im Schnittstellenkonfigurationsmodus können MAC-Zugriffskontrolllisten oder erweiterte Listen im IP-Netzwerk angewendet werden:

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

> **Hinweis**: Layer-3-Pakete werden als Layer-2-Pakete klassifiziert. Der Befehl wird in der Cisco IOS Software Release 12.2(18)SXD (für Sup 720) und in den Cisco IOS Software Releases 12.2(33)SRA oder höher unterstützt.

Dieser Schnittstellenbefehl muss auf die Eingangs-Schnittstelle angewendet werden, und er weist die Weiterleitungs-Engine an, den IP-Header nicht zu überprüfen. Das Ergebnis ist, dass Sie in der IP-Umgebung eine MAC-Zugriffsliste verwenden können.

Private VLAN-Nutzung

Private VLANs (PVLANs) sind eine Layer-2-Sicherheitsfunktion, die die Verbindung zwischen Workstations oder Servern innerhalb eines VLAN einschränkt. Ohne PVLANs können alle Geräte in einem Layer-2-VLAN frei miteinander kommunizieren. Netzwerksituationen, in denen Sicherheit durch die Einschränkung der Kommunikation zwischen Geräten in einem einzelnen VLAN unterstützt werden kann. PVLANs werden beispielsweise häufig verwendet, um die Kommunikation zwischen Servern in einem öffentlich zugänglichen Subnetz zu untersagen. Wenn ein einzelner Server kompromittiert wird, kann die mangelnde Verbindung zu anderen Servern aufgrund der Anwendung von PVLANs dazu beitragen, die Beeinträchtigung auf einen Server zu begrenzen.

Es gibt drei Arten von privaten VLANs: Isolated-VLANs, Community-VLANs und primäre VLANs. Bei der Konfiguration von PVLANs werden primäre und sekundäre VLANs verwendet. Das primäre VLAN enthält alle Promiscuous-Ports, die später beschrieben werden, und umfasst ein oder mehrere sekundäre VLANs, die entweder isoliert oder als Community-VLANs fungieren können.

Isolated-VLANs

Die Konfiguration eines sekundären VLANs als isoliertes VLAN verhindert vollständig die Kommunikation zwischen Geräten im sekundären VLAN. Pro primärem VLAN kann nur ein einzelnes VLAN vorhanden sein, und nur Promiscuous-Ports können mit Ports in einem isolierten VLAN kommunizieren. Isolated-VLANs sollten in nicht vertrauenswürdigen Netzwerken wie Netzwerken verwendet werden, die Gäste unterstützen.

In diesem Konfigurationsbeispiel wird VLAN 11 als isoliertes VLAN konfiguriert und dem primären VLAN VLAN 20 zugeordnet. Im folgenden Beispiel wird Schnittstelle FastEthernet 1/1 auch als isolierter Port in VLAN 11 konfiguriert:

```
!

vlan 11
private-vlan isolated
```

```
!

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

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

Community-VLANs

Ein sekundäres VLAN, das als Community-VLAN konfiguriert ist, ermöglicht die Kommunikation zwischen Mitgliedern des VLANs sowie mit allen Promiscuous-Ports im primären VLAN. Es ist jedoch keine Kommunikation zwischen zwei Community-VLANs oder von einem Community-VLAN zu einem isolierten VLAN möglich. Community-VLANs müssen verwendet werden, um Server zu gruppieren, die miteinander verbunden werden müssen, bei denen jedoch keine Verbindung zu allen anderen Geräten im VLAN erforderlich ist. Dieses Szenario ist in einem öffentlich zugänglichen Netzwerk oder überall dort üblich, wo Server Inhalte für nicht vertrauenswürdige Clients bereitstellen.

In diesem Beispiel wird ein einzelnes Community-VLAN konfiguriert und der Switch-Port FastEthernet 1/2 als Mitglied dieses VLAN konfiguriert. Das Community VLAN, VLAN 12, ist ein sekundäres VLAN zum primären 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
!
```

Promiscuous-Ports

Switch-Ports, die in das primäre VLAN integriert werden, werden als Promiscuous-Ports bezeichnet. Promiscuous-Ports können mit allen anderen Ports in den primären und sekundären VLANs kommunizieren. Router- oder Firewall-Schnittstellen sind die gebräuchlichsten Geräte in diesen VLANs.

In diesem Konfigurationsbeispiel werden die vorherigen Beispiele für isolierte und Community-VLANs kombiniert und die Konfiguration der Schnittstelle FastEthernet 1/12 als Promiscuous-Port hinzugefügt:

```
!

vlan 11
private-vlan isolated
!

vlan 12
private-vlan community
!

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

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

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

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

Wenn Sie PVLANs implementieren, ist es wichtig, sicherzustellen, dass die vorhandene Layer-3-Konfiguration die von PVLANs auferlegten Einschränkungen unterstützt und keine Subversion der PVLAN-Konfiguration zulässt. Die Layer-3-Filterung mit einer Router-ACL oder einer Firewall kann eine Subversion der PVLAN-Konfiguration verhindern.

Unter Private VLANs (PVLANs) - Promiscuous, Isolated, Community auf der Startseite von LAN Security finden Sie weitere Informationen zur Verwendung und Konfiguration privater VLANs.

Schlussfolgerung

Dieses Dokument bietet einen umfassenden Überblick über die Methoden, mit denen ein Cisco IOS-Systemgerät gesichert werden kann. Wenn Sie die Geräte sichern, erhöht dies die Sicherheit der Netzwerke, die Sie verwalten. In dieser Übersicht wird der Schutz der Verwaltungs-, Steuerungs- und Datenebene behandelt, und es werden Konfigurationsempfehlungen gegeben. Wenn möglich, werden für die Konfiguration der jeweiligen Funktion ausreichende Details bereitgestellt. In jedem Fall werden Ihnen jedoch umfassende Referenzen zur Verfügung gestellt, um Ihnen die für die weitere Bewertung erforderlichen Informationen zur Verfügung zu stellen.

Bestätigungen

Einige Funktionsbeschreibungen in diesem Dokument wurden von den Cisco Informationsentwicklungsteams verfasst.

Anhang: Checkliste für die Cisco IOS-Gerätesicherung

Diese Checkliste ist eine Sammlung aller Härtungsschritte, die in diesem Leitfaden vorgestellt werden. Administratoren können diese Funktion als Erinnerung an alle für ein Cisco IOS-Gerät verwendeten und in Betracht gezogenen Härtungsfunktionen verwenden, selbst wenn eine Funktion nicht implementiert wurde, da sie nicht angewendet wurde. Administratoren wird empfohlen, jede Option vor der Implementierung der Option nach ihrem potenziellen Risiko zu bewerten.

Managementebene

- Kennwörter

  MD5-Hashing (geheime Option) für aktivierte und lokale Benutzerkennwörter aktivierenKonfigurieren der Sperrung für KennwortwiederholungKennwortwiederherstellung deaktivieren (Risiko berücksichtigen)

- Nicht verwendete Services deaktivieren

- Konfigurieren von TCP-Keepalives für Managementsitzungen

- Einstellen von Benachrichtigungen zu Arbeitsspeicher- und CPU-Grenzwerten

- Konfigurieren

  Benachrichtigungen zu Arbeitsspeicher- und CPU-GrenzwertenReservieren von Speicher für den KonsolenzugriffSpeicherleckdetektorBuffer-Overflow-ErkennungErweiterte Crashinfo-Sammlung

- iACLs verwenden, um den Managementzugriff zu beschränken

- Filtern (Risiko berücksichtigen)

  ICMP-PaketeIP-FragmenteIP-OptionenTTL-Wert in Paketen

- Schutz der Kontrollebene

  Port-Filterung konfigurierenKonfigurieren von Warteschlangenschwellen

- Management-Zugriff

  Management Plane Protection verwenden, um Management-Schnittstellen einzuschränkenExec-Timeout festlegenVerwendung eines verschlüsselten Transportprotokolls (z. B. SSH) für den CLI-ZugriffSteuerung des Transports für VTY- und TTL-Leitungen (Option für Zugriffsklasse)Banner verwenden

- AAA

AAA für Authentifizierung und Fallback verwendenVerwenden von AAA (TACACS+) für die BefehlsautorisierungAAA für die Rechnungslegung verwendenVerwendung redundanter AAA-Server

- SNMP

  SNMPv2-Communitys konfigurieren und Zugriffskontrolllisten anwendenSNMPv3 konfigurieren

- Protokollierung

  Zentrale Protokollierung konfigurierenEinrichten von Protokollierungsstufen für alle relevanten KomponentenFestlegen der Quellschnittstelle für die ProtokollierungKonfiguration der Protokollierung mit Zeitstempelgranularität

- Konfigurationsmanagement

  Ersatz und RollbackExklusiver Zugriff auf KonfigurationsänderungenKonfiguration der SoftwareausfallsicherheitBenachrichtigungen zu Konfigurationsänderungen

Kontrollebene

- Deaktivieren (Risiko berücksichtigen)

  ICMP-UmleitungenICMP nicht erreichbarProxy-ARP

- NTP-Authentifizierung konfigurieren, wenn NTP verwendet wird

- Konfigurieren von Control Plane Policing/Protection (Port-Filterung, Warteschlangenschwellen)

- Sichere Routing-Protokolle

  BGP (TTL, MD5, maximale Präfixe, Präfixlisten, Systempfad-ACLs)IGP (MD5, passive Schnittstelle, Routenfilterung, Ressourcenverbrauch)

- Hardware-Ratenlimitierungen konfigurieren

- Sichere First-Hop-Redundanzprotokolle (GLBP, HSRP, VRRP)

Datenebene

- IP-Optionen selektives Drop konfigurieren

- Deaktivieren (Risiko berücksichtigen)

  IP Source RoutingIP-Directed BroadcastsICMP-Umleitungen

- Beschränkung von IP-Directed Broadcasts
- Konfigurieren von tACLs (Risiko berücksichtigen)

  ICMP filternIP-Fragmente filternIP-FilteroptionenTTL-Werte filtern
- Konfigurieren der erforderlichen Anti-Spoofing-Schutzmaßnahmen

  ACLsIP Source GuardDynamische ARP-InspektionUnicast-RPFPort-Sicherheit
- Schutz der Kontrollebene (cef-exception)
- Konfiguration von NetFlow und Klassifizierungs-ACLs für die Identifizierung des Datenverkehrs
- Konfigurieren der erforderlichen Zugriffskontrolllisten (VLAN-Maps, PACLs, MAC)
- Konfigurieren privater VLANs