Guida Cisco per fortificare i dispositivi Cisco IOS

Sommario

Miglioramenti SSHv2 per le chiavi RSA
Porte console e AUX
Controllo righe vty e tty
Controllo del trasporto per le linee vty e tty
Banner avviso
Autenticazione, autorizzazione e accounting
Autenticazione TACACS+
Fallback autenticazione
Utilizzo di password di tipo 7
Autorizzazione comando TACACS+
Accounting comando TACACS+
Server AAA ridondanti
Rafforzamento del protocollo SNMP (Simple Network Management Protocol)
Stringhe della community SNMP
Stringhe della community SNMP con ACL
ACL di infrastruttura
Viste SNMP
SNMP versione 3
Protezione del piano di gestione
Registrazione delle procedure ottimali
Invia log a una posizione centrale
Livello di registrazione
Non accedere alle sessioni di console o di monitoraggio
Usa registrazione nel buffer
Configura interfaccia origine di registrazione
Configura timestamp di registrazione
Gestione configurazione software Cisco IOS
Sostituzione della configurazione e rollback della configurazione
Accesso esclusivo alle modifiche alla configurazione
Configurazione resiliente del software Cisco IOS
Software Cisco con firma digitale
Notifica e registrazione delle modifiche alla configurazione
Piano di controllo
Protezione avanzata piano di controllo generale
Reindirizzamenti IP ICMP
Impossibile raggiungere ICMP
Proxy ARP
Limitazione dell'impatto della CPU sul traffico del Control Plane
Informazioni sul traffico del Control Plane
ACL di infrastruttura
Receive ACL
CoPP
Control Plane Protection
Limitatori di velocità hardware
Secure BGP

Introduzione

In questo documento viene spiegato come proteggere i dispositivi di sistema Cisco IOS® e aumentare la sicurezza complessiva della rete. Strutturato attorno ai tre piani in cui è possibile categorizzare le funzioni di un dispositivo di rete, questo documento fornisce una panoramica di ogni funzionalità inclusa e riferimenti alla documentazione correlata.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

I tre piani funzionali di una rete, il piano di gestione, il piano di controllo e il piano dati, ciascuno forniscono funzionalità diverse che devono essere protette.

- **Management Plane**: il management plane gestisce il traffico inviato al dispositivo Cisco IOS ed è costituito da applicazioni e protocolli quali Secure Shell (SSH) e Simple Network Management Protocol (SNMP).

- **Control Plane**: il control plane di un dispositivo di rete elabora il traffico che è fondamentale per mantenere la funzionalità dell'infrastruttura di rete. Il control plane è costituito da applicazioni e protocolli tra dispositivi di rete, che include il Border Gateway Protocol (BGP), nonché i protocolli IGP (Interior Gateway Protocol), ad esempio EIGRP (Enhanced Interior Gateway Routing Protocol) e OSPF (Open Shortest Path First).

- **Piano dati** - Il piano dati inoltra i dati attraverso un dispositivo di rete. Il data plane non include il traffico inviato al dispositivo Cisco IOS locale.

La descrizione delle funzionalità di sicurezza in questo documento spesso fornisce informazioni sufficienti per configurare la funzionalità. Tuttavia, in caso contrario, la feature viene spiegata in modo che sia possibile valutare se è necessaria una maggiore attenzione alla feature. Ove

possibile e opportuno, questo documento contiene raccomandazioni che, se implementate, contribuiscono a proteggere una rete.

Operazioni sicure

La sicurezza delle operazioni di rete è un argomento fondamentale. Sebbene la maggior parte di questo documento sia dedicata alla configurazione sicura di un dispositivo Cisco IOS, le sole configurazioni non proteggono completamente una rete. Le procedure operative in uso sulla rete contribuiscono alla sicurezza tanto quanto la configurazione dei dispositivi sottostanti.

Questi argomenti contengono suggerimenti operativi che è consigliabile implementare. Questi argomenti evidenziano aree critiche specifiche delle operazioni di rete e non sono completi.

Monitoraggio dei consigli e delle risposte in materia di sicurezza di Cisco

Il Cisco Product Security Incident Response Team (PSIRT) crea e gestisce pubblicazioni, comunemente note come consigli PSIRT, per problemi relativi alla sicurezza dei prodotti Cisco. Il metodo utilizzato per la comunicazione di problemi meno gravi è Cisco Security Response. Gli avvisi e le risposte sulla sicurezza sono disponibili all'indirizzo http://www.cisco.com/go/psirt.

Ulteriori informazioni su questi veicoli di comunicazione sono disponibili in Cisco Security Vulnerability Policy.

Per mantenere una rete sicura, è necessario conoscere le avvertenze e le risposte sulla sicurezza Cisco rilasciate. È necessario essere a conoscenza di una vulnerabilità prima di poter valutare la minaccia che può rappresentare per una rete. Per informazioni sul processo di valutazione, fare riferimento a Valutazione dei rischi per la vulnerabilità della sicurezza.

Utilizzo di autenticazione, autorizzazione e accounting

Il framework AAA (Authentication, Authorization, and Accounting) è essenziale per proteggere i dispositivi di rete. La struttura AAA fornisce l'autenticazione delle sessioni di gestione e può inoltre limitare gli utenti a comandi specifici definiti dall'amministratore e registrare tutti i comandi immessi da tutti gli utenti. Per ulteriori informazioni su come usare il protocollo AAA, vedere la sezione Autenticazione, autorizzazione e accounting di questo documento.

Raccolta e monitoraggio centralizzati dei log

Per conoscere gli eventi esistenti, emergenti e storici relativi agli incidenti di sicurezza, l'organizzazione deve disporre di una strategia unificata per la registrazione e la correlazione degli eventi. Questa strategia deve sfruttare la registrazione da tutti i dispositivi di rete e utilizzare funzionalità di correlazione preconfigurate e personalizzabili.

Dopo l'implementazione della registrazione centralizzata, è necessario sviluppare un approccio strutturato per l'analisi dei registri e il monitoraggio degli incidenti. In base alle esigenze dell'organizzazione, questo approccio può variare da una semplice analisi diligente dei dati di registro ad un'analisi avanzata basata su regole.

Per ulteriori informazioni su come implementare la registrazione sui dispositivi di rete Cisco IOS, *vedere* la sezione Best Practices di registrazione in questo documento.

Usa protocolli sicuri quando possibile

Molti protocolli vengono utilizzati per trasportare dati sensibili relativi alla gestione della rete. Ove possibile, è necessario utilizzare protocolli sicuri. Un protocollo sicuro include l'uso del protocollo SSH anziché Telnet, in modo che i dati di autenticazione e le informazioni di gestione vengano crittografati. Quando si copiano i dati di configurazione, è inoltre necessario utilizzare protocolli di trasferimento file protetti. Un esempio è l'uso del protocollo SCP (Secure Copy Protocol) al posto di FTP o TFTP.

Per ulteriori informazioni sulla gestione sicura dei dispositivi Cisco IOS, *vedere* la sezione Sessioni di gestione interattiva protette di questo documento.

Maggiore visibilità del traffico con NetFlow

NetFlow consente di monitorare i flussi di traffico nella rete. Originariamente progettato per esportare informazioni sul traffico in applicazioni di gestione di rete, NetFlow può essere usato anche per mostrare le informazioni sul flusso su un router. Questa funzionalità consente di visualizzare in tempo reale il traffico che attraversa la rete. Indipendentemente dal fatto che le informazioni di flusso vengano esportate in un raccoglitore remoto, è consigliabile configurare i dispositivi di rete per NetFlow in modo che possano essere utilizzati in modo reattivo, se necessario.

Per ulteriori informazioni su questa funzione, consultare la sezione Identificazione e tracciamento del traffico in questo documento e visitare il sito http://www.cisco.com/go/netflow (solo utenti registrati).

Gestione della configurazione

La gestione della configurazione è un processo mediante il quale vengono proposte, esaminate, approvate e distribuite le modifiche alla configurazione. Nel contesto di una configurazione di dispositivo Cisco IOS, due aspetti aggiuntivi della gestione della configurazione sono critici: archiviazione e protezione della configurazione.

Èpossibile utilizzare gli archivi di configurazione per eseguire il rollback delle modifiche apportate ai dispositivi di rete. In un contesto di protezione, è possibile utilizzare gli archivi di configurazione anche per determinare quali modifiche alla protezione sono state apportate e quando sono state apportate. Insieme ai dati di registro AAA, queste informazioni possono essere utili per il controllo della sicurezza dei dispositivi di rete.

La configurazione di un dispositivo Cisco IOS contiene molti dettagli riservati. Nomi utente, password e contenuto degli elenchi di controllo di accesso sono esempi di questo tipo di informazioni. Il repository utilizzato per archiviare le configurazioni dei dispositivi Cisco IOS deve essere protetto. Un accesso non sicuro a queste informazioni può compromettere la sicurezza dell'intera rete.

Piano di gestione

Il piano di gestione è costituito da funzioni che consentono di raggiungere gli obiettivi di gestione della rete. Ciò include sessioni di gestione interattive che usano SSH, nonché la raccolta di statistiche con SNMP o NetFlow. Se si considera la sicurezza di un dispositivo di rete, è

fondamentale proteggere il piano di gestione. Se un problema di sicurezza può compromettere le funzioni del piano di gestione, potrebbe essere impossibile ripristinare o stabilizzare la rete.

Nelle sezioni seguenti di questo documento vengono descritte in dettaglio le funzionalità e le configurazioni di sicurezza disponibili nel software Cisco IOS per fortificare il piano di gestione.

Protezione avanzata piano di gestione generale

Il piano di gestione viene utilizzato per accedere, configurare e gestire un dispositivo, nonché per monitorarne le operazioni e la rete in cui viene distribuito. Il piano di gestione è il piano che riceve e invia traffico per le operazioni di queste funzioni. È necessario fissare sia il piano di gestione che il piano di controllo di un dispositivo, in quanto le operazioni del piano di controllo influiscono direttamente sulle operazioni del piano di gestione. Questo elenco di protocolli viene utilizzato dal management plane:

- Protocollo SCEP (Simple Network Management Protocol)
- Telnet
- Protocollo Secure Shell
- Protocollo di trasferimento file
- Protocollo HyperText Transfer / Protocollo Secure HyperText Transfer
- Protocollo Trivial File Transfer
- Secure Copy Protocol
- TACACS+
- RAGGIO
- NetFlow
- Protocollo orario di rete
- Syslog

Devono essere prese misure per garantire la sopravvivenza dei piani di gestione e di controllo durante gli incidenti di sicurezza. Se uno di questi aerei viene sfruttato con successo, tutti gli aerei possono essere compromessi.

Gestione password

Le password controllano l'accesso a risorse o dispositivi. A tale scopo, è necessario definire una password o un segreto utilizzato per autenticare le richieste. Quando si riceve una richiesta di accesso a una risorsa o a un dispositivo, la richiesta viene contestata per la verifica della password e dell'identità e l'accesso può essere concesso, negato o limitato in base al risultato. Come buona norma per la sicurezza, le password devono essere gestite con un server di

autenticazione TACACS+ o RADIUS. Tuttavia, si noti che, in caso di errore dei servizi TACACS+ o RADIUS, è ancora necessaria una password configurata localmente per l'accesso privilegiato. Un dispositivo può inoltre includere altre informazioni sulla password nella propria configurazione, ad esempio una chiave NTP, una stringa della community SNMP o una chiave del protocollo di routing.

Il comando **enable secret** viene usato per impostare la password che concede l'accesso amministrativo privilegiato al sistema Cisco IOS. È necessario utilizzare il comando **enable secret** anziché il precedente comando **enable password**. Il comando **enable password** usa un algoritmo di crittografia debole.

Se non viene impostato alcun segreto enable e viene configurata una password per la riga di tty della console, è possibile utilizzare la password della console per ricevere l'accesso con privilegi, anche da una sessione remote virtual tty (vty). Questa azione è quasi certamente indesiderata ed è un altro motivo per garantire la configurazione di un segreto abilitante.

Il comando di configurazione globale **service password-encryption** indica al software Cisco IOS di crittografare le password, i segreti del protocollo CHAP (Challenge Handshake Authentication Protocol) e dati simili salvati nel file di configurazione. Tale cifratura è utile per impedire agli osservatori occasionali di leggere le password, ad esempio quando guardano lo schermo sopra il banco di un amministratore. Tuttavia, l'algoritmo utilizzato dal comando **service password-encryption** è un semplice cifrario Vigen re. L'algoritmo non è progettato per proteggere i file di configurazione da analisi gravi da parte di utenti malintenzionati anche leggermente sofisticati e non deve essere utilizzato a questo scopo. I file di configurazione Cisco IOS che contengono password crittografate devono essere gestiti con la stessa attenzione usata per un elenco non crittografato delle stesse password.

Sebbene questo algoritmo di crittografia debole non venga utilizzato dal comando **enable secret**, viene utilizzato dal comando **enable password** in modalità di configurazione globale e dal comando di configurazione da riga di **password**. È necessario eliminare le password di questo tipo e utilizzare il comando **enable secret** o la funzionalità Enhanced Password Security.

Il comando **enable secret** e la funzione Enhanced Password Security utilizzano Message Digest 5 (MD5) per l'hashing della password. Questo algoritmo ha avuto una notevole revisione pubblica e non è noto per essere reversibile. Tuttavia, l'algoritmo è soggetto ad attacchi di dizionario. In un attacco di dizionario, un utente malintenzionato prova ogni parola in un dizionario o in un altro elenco di password candidate per trovare una corrispondenza. Pertanto, i file di configurazione devono essere archiviati in modo sicuro e condivisi solo con utenti attendibili.

Sicurezza potenziata delle password

La funzione di sicurezza potenziata delle password, introdotta nel software Cisco IOS versione 12.2(8)T, consente agli amministratori di configurare l'hashing MD5 delle password per il comando **username**. Prima di questa funzione, esistevano due tipi di password: Digitare 0, che è una password non crittografata, e Digitare 7, che utilizza l'algoritmo della cifratura Vigen re. La funzione Sicurezza avanzata password non può essere utilizzata con protocolli che richiedono il recupero della password non crittografata, ad esempio CHAP.

Per crittografare una password utente con hashing MD5, eseguire il comando di configurazione globale **username secret**.

!

```
username <name> secret <password>

!
```

Per ulteriori informazioni su questa funzione, fare riferimento a Sicurezza potenziata delle password.

Blocco tentativi password di accesso

La funzione Login Password Retry Lockout, aggiunta nel software Cisco IOS versione 12.3(14)T, consente di bloccare un account utente locale dopo un numero configurato di tentativi di accesso non riusciti. Dopo che un utente è stato bloccato, il suo account viene bloccato fino a quando non viene sbloccato. Impossibile bloccare con questa funzionalità un utente autorizzato configurato con il livello di privilegio 15. È necessario ridurre al minimo il numero di utenti con livello di privilegio 15.

Si noti che gli utenti autorizzati possono bloccarsi da un dispositivo se viene raggiunto il numero di tentativi di accesso non riusciti. Un utente malintenzionato può inoltre creare una condizione DoS (Denial of Service) con ripetuti tentativi di autenticazione tramite un nome utente valido.

Nell'esempio viene mostrato come abilitare la funzione di blocco dei tentativi di accesso con password:

```
!

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

!

username <name> secret <password>

!
```

Questa funzionalità si applica anche a metodi di autenticazione quali CHAP e PAP (Password Authentication Protocol).

Nessun recupero della password del servizio

Nel software Cisco IOS versione 12.3(14)T e successive, la funzione No Service Password-Recovery non consente a nessuno con accesso alla console di accedere in modo sicuro alla configurazione del dispositivo e di cancellare la password. Inoltre, non consente a utenti malintenzionati di modificare il valore del registro di configurazione e accedere alla NVRAM.

```
!

no service password-recovery

!
```

Il software Cisco IOS fornisce una procedura di recupero della password che si basa sull'accesso a ROM Monitor Mode (ROMMON) utilizzando il tasto Break durante l'avvio del sistema. In ROMMON, il software del dispositivo può essere ricaricato per richiedere una nuova configurazione del sistema che includa una nuova password.

La procedura di recupero della password corrente consente a chiunque disponga dell'accesso alla console di accedere al dispositivo e alla relativa rete. La funzione No Service Password-Recovery impedisce il completamento della sequenza di tasti di interruzione e l'immissione di ROMMON durante l'avvio del sistema.

Se in un dispositivo non è abilitato il **recupero della password del servizio**, è consigliabile salvare una copia offline della configurazione del dispositivo e implementare una soluzione di archiviazione della configurazione. Se è necessario recuperare la password di un dispositivo Cisco IOS dopo aver abilitato questa funzione, l'intera configurazione viene eliminata.

Per ulteriori informazioni su questa funzione, fare riferimento a Esempio di configurazione Secure ROMMON.

Disabilita servizi inutilizzati

Come buona norma per la sicurezza, qualsiasi servizio non necessario deve essere disabilitato. Questi servizi non necessari, in particolare quelli che utilizzano il protocollo UDP (User Datagram Protocol), vengono raramente utilizzati per scopi legittimi, ma possono essere utilizzati per avviare DoS e altri attacchi che vengono altrimenti impediti dal filtro pacchetti.

I servizi di piccole dimensioni TCP e UDP devono essere disabilitati. Questi servizi includono:

- echo (numero porta 7)
- scarta (numero porta 9)
- diurno (numero porta 13)
- chargen (numero porta 19)

Sebbene l'utilizzo abusivo dei piccoli servizi possa essere evitato o reso meno pericoloso da elenchi di accesso anti-spoofing, i servizi devono essere disabilitati su qualsiasi dispositivo accessibile in rete. Per impostazione predefinita, i servizi di piccole dimensioni sono disabilitati nel software Cisco IOS versione 12.0 e successive. Nel software precedente, è possibile usare i comandi di configurazione globale **no service tcp-small-servers** e **no service udp-small-servers** per disabilitarli.

Di seguito sono elencati i servizi aggiuntivi da disabilitare se non vengono utilizzati:

- Usare il comando di configurazione globale **no ip finger** per disabilitare il servizio Finger. Per impostazione predefinita, il software Cisco IOS versioni successive alla 12.1(5) e alla 12.1(5)T disabilita questo servizio.
- Usare il comando di configurazione globale **no ip bootp server** per disabilitare il protocollo BOOTP (Bootstrap Protocol).
- Nel software Cisco IOS versione 12.2(8)T e successive, usare il comando **ip dhcp bootp ignore** in modalità di configurazione globale per disabilitare il comando BOOTP. In questo modo i servizi DHCP (Dynamic Host Configuration Protocol) rimangono abilitati.
- Se i servizi di inoltro DHCP non sono necessari, è possibile disattivare i servizi DHCP.

Eseguire il comando **no service dhcp** in modalità di configurazione globale.

- Per disabilitare il servizio MOP (Maintenance Operation Protocol), eseguire il comando **no mop enabled** in modalità di configurazione interfaccia.
- Utilizzare il comando di configurazione globale **no ip domain-lookup** per disabilitare i servizi di risoluzione DNS (Domain Name System).
- Utilizzare il comando **no service pad** in modalità di configurazione globale per disabilitare il servizio Packet Assembler/Disassembler (PAD), utilizzato per le reti X.25.
- Il server HTTP può essere disabilitato con il comando **no ip http server** in modalità di configurazione globale e il server HTTP protetto (HTTPS) può essere disabilitato con il comando di configurazione globale **no ip http secure-server**.
- A meno che i dispositivi Cisco IOS non recuperino le configurazioni dalla rete durante l'avvio, è necessario utilizzare il comando di configurazione globale **no service config**. In questo modo si impedisce al dispositivo Cisco IOS di tentare di individuare un file di configurazione sulla rete con TFTP.
- Il protocollo CDP (Cisco Discovery Protocol) è un protocollo di rete usato per individuare altri dispositivi CDP abilitati alle adiacenze e alla topologia di rete. Il CDP può essere utilizzato dai sistemi NMS (Network Management Systems) o durante la risoluzione dei problemi. Il CDP deve essere disabilitato su tutte le interfacce connesse a reti non attendibili. a tal fine, usare il comando **no cdp enable** interface. In alternativa, il CDP può essere disabilitato globalmente con il comando di configurazione globale **no cdp run**. Notare che il CDP può essere utilizzato da un utente malintenzionato per la ricognizione e la mappatura della rete.
- LLDP (Link Layer Discovery Protocol) è un protocollo IEEE definito in 802.1AB. LLDP è simile a CDP. Tuttavia, questo protocollo consente l'interoperabilità tra altri dispositivi che non supportano CDP. LLDP deve essere trattato allo stesso modo di CDP e disabilitato su tutte le interfacce che si connettono a reti non attendibili. A tal fine, usare i comandi di configurazione dell'interfaccia **no lldp transmission** e **no lldp receive**. Utilizzare il comando di configurazione globale **no lldp run** per disabilitare LLDP a livello globale. LLDP può anche essere utilizzato da un utente malintenzionato per la ricognizione e la mappatura della rete.
- Per gli switch che supportano l'avvio da sdflash, la sicurezza può essere migliorata avviando da flash e disabilitando sdflash con il comando di configurazione "no sdflash".

Timeout esecuzione

Per impostare l'intervallo di attesa dell'input utente da parte dell'interprete dei comandi EXEC prima di terminare una sessione, eseguire il comando di configurazione della riga **exec-timeout**. il comando **exec-timeout** deve essere usato per disconnettere le sessioni sulle righe vty o tty lasciate inattive. Per impostazione predefinita, le sessioni vengono disconnesse dopo dieci minuti di inattività.

```
!

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

Mantenimento attività per sessioni TCP

I comandi di configurazione globale **service tcp-keepalives-in** e **service tcp-keepalives-out** consentono a un dispositivo di inviare pacchetti TCP keepalive per le sessioni TCP. Questa configurazione deve essere usata per abilitare i pacchetti TCP keepalive sulle connessioni in entrata al dispositivo e sulle connessioni in uscita dal dispositivo. In questo modo, il dispositivo sull'estremità remota della connessione è ancora accessibile e le connessioni half-open o orfane vengono rimosse dal dispositivo Cisco IOS locale.

```
!

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

Uso dell'interfaccia di gestione

Èpossibile accedere al piano di gestione di un dispositivo in banda o fuori banda tramite un'interfaccia di gestione fisica o logica. Idealmente, l'accesso alla gestione sia in banda che fuori banda esiste per ciascun dispositivo di rete, in modo che sia possibile accedere al piano di gestione durante le interruzioni della rete.

Una delle interfacce più comuni utilizzate per l'accesso in banda a un dispositivo è l'interfaccia di loopback logico. Le interfacce di loopback sono sempre attive, mentre le interfacce fisiche possono cambiare stato e l'interfaccia potrebbe non essere accessibile. Si consiglia di aggiungere un'interfaccia di loopback a ciascun dispositivo come interfaccia di gestione e di utilizzarla esclusivamente per il piano di gestione. In questo modo l'amministratore può applicare le regole a tutta la rete per il piano di gestione. Una volta configurata su un dispositivo, l'interfaccia di loopback può essere utilizzata dai protocolli del piano di gestione, ad esempio SSH, SNMP e syslog, per inviare e ricevere il traffico.

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

Notifiche di soglia della memoria

La funzione Memory Threshold Notification, aggiunta nel software Cisco IOS versione 12.3(4)T, consente di ridurre il numero di condizioni di memoria insufficiente su un dispositivo. A tal fine, questa funzione utilizza due metodi: Notifica soglia memoria e prenotazione memoria.

Notifica soglia memoria genera un messaggio di registro per indicare che la memoria disponibile su un dispositivo è scesa al di sotto della soglia configurata. Nell'esempio di configurazione viene mostrato come abilitare questa funzione con il comando di configurazione globale **memory free low-watermark**. In questo modo, un dispositivo può generare una notifica quando la memoria disponibile scende al di sotto della soglia specificata e di nuovo quando la memoria disponibile

supera del 5% la soglia specificata.

```
!

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

La prenotazione della memoria viene utilizzata in modo che sia disponibile memoria sufficiente per le notifiche critiche. Nell'esempio di configurazione viene mostrato come abilitare questa funzione. In questo modo i processi di gestione continuano a funzionare anche quando la memoria del dispositivo è esaurita.

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

Per ulteriori informazioni su questa funzione, fare riferimento a Notifiche di soglia della memoria.

Notifica soglia CPU

Introdotta nel software Cisco IOS versione 12.3(4)T, la funzione di notifica dei valori di soglia della CPU consente di rilevare e ricevere una notifica quando il carico della CPU su un dispositivo supera una soglia configurata. Quando la soglia viene superata, il dispositivo genera e invia un messaggio trap SNMP. Sul software Cisco IOS sono supportati due metodi di soglia per l'utilizzo della CPU: Soglia crescente e Soglia decrescente.

In questa configurazione di esempio viene mostrato come abilitare le soglie di aumento e di diminuzione che attivano un messaggio di notifica di soglia della CPU:

```
!

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>]
!
```

Per ulteriori informazioni su questa funzione, fare riferimento a Notifica soglia CPU.

Riserva memoria per accesso da console

Nel software Cisco IOS versione 12.4(15)T e successive, è possibile usare la funzione Reserve Memory for Console Access per riservare memoria sufficiente a garantire l'accesso da console a un dispositivo Cisco IOS a scopo di amministrazione e risoluzione dei problemi. Questa funzione è particolarmente utile quando la memoria del dispositivo è insufficiente. Per abilitare questa funzione, è possibile usare il comando di configurazione globale della **console di riserva di memoria**. Nell'esempio, viene usato un dispositivo Cisco IOS con una configurazione che riserva 4096 kilobyte.

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

Per ulteriori informazioni su questa funzione, fare riferimento a Riserva memoria per accesso da console.

Rilevatore perdite di memoria

Introdotta nel software Cisco IOS versione 12.3(8)T1, la funzione di rilevamento delle perdite di memoria consente di rilevare le perdite di memoria su un dispositivo. Rilevamento perdite di memoria è in grado di trovare le perdite in tutti i pool di memoria, i buffer dei pacchetti e i blocchi. Le perdite di memoria sono allocazioni statiche o dinamiche di memoria che non servono a nessuno scopo utile. Questa funzionalità è incentrata sulle allocazioni di memoria dinamiche. È possibile usare il comando **show memory debug leaks** in modalità di esecuzione per rilevare eventuali perdite di memoria.

Overflow del buffer: Rilevamento e correzione della corruzione di Redzone

Nel software Cisco IOS versione 12.3(7)T e successive, il comando Buffer Overflow: La funzione di rilevamento e correzione della corruzione di Redzone può essere abilitata da su un dispositivo per rilevare e correggere un overflow del blocco di memoria e continuare le operazioni.

Questi comandi di configurazione globale possono essere usati per abilitare questa funzione. Una volta configurato, il comando **show memory overflow** può essere usato per visualizzare le statistiche di rilevamento e correzione dell'overflow del buffer.

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

Raccolta avanzata file Crashinfo

La funzione avanzata Crashinfo File Collection elimina automaticamente i vecchi file crashinfo. Questa funzione, aggiunta nel software Cisco IOS versione 12.3(11)T, consente a un dispositivo di recuperare spazio per creare nuovi file crashinfo quando il dispositivo si blocca. Questa funzione consente inoltre di configurare il numero di file crashinfo da salvare.

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

Protocollo orario di rete

Il Network Time Protocol (NTP) non è un servizio particolarmente pericoloso, ma qualsiasi servizio non necessario può rappresentare un vettore di attacco. Se si utilizza NTP, è importante configurare in modo esplicito un'origine ora attendibile e utilizzare l'autenticazione corretta. Per gli scopi del syslog, ad esempio durante le indagini forensi su potenziali attacchi, nonché per una connettività VPN efficace quando si dipende dai certificati per l'autenticazione di fase 1, è necessario disporre di tempo accurato e affidabile.

- **Fuso orario NTP** - Quando si configura NTP, il fuso orario deve essere configurato in modo che i timestamp possano essere accuratamente correlati. Di solito ci sono due approcci per configurare il fuso orario per i dispositivi in una rete con una presenza globale. Un metodo consiste nel configurare tutti i dispositivi di rete con l'ora UTC (Coordinated Universal Time), in precedenza GMT (Greenwich Mean Time). L'altro approccio consiste nel configurare i dispositivi di rete con il fuso orario locale. Per ulteriori informazioni su questa funzione, consultare la sezione "clock timezone" nella documentazione del prodotto Cisco.

- **Autenticazione NTP** - Se si configura l'autenticazione NTP, questa assicura che i messaggi NTP vengano scambiati tra peer NTP attendibili.

Esempio di configurazione con autenticazione NTP:

Cliente:

```
(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
```

Disabilita Smart Install

Le best practice in materia di sicurezza relative alla funzionalità Cisco Smart Install (SMI) dipendono dal modo in cui tale funzionalità viene utilizzata in uno specifico ambiente del cliente. Cisco distingue questi casi di utilizzo:

- Clienti che non utilizzano la funzionalità Smart Install.
- Clienti che utilizzano la funzionalità Smart Install solo per l'installazione zero-touch.
- Clienti che sfruttano la funzionalità Smart Install per un'installazione più che zero-touch (configurazione e gestione delle immagini).

Le sezioni seguenti descrivono in dettaglio ogni scenario:

- Clienti che non utilizzano la funzionalità Smart Install.
- I clienti che non usano la funzione Cisco Smart Install e usano una versione del software Cisco IOS e Cisco IOS XE dove il comando è disponibile, devono disabilitare la funzione Cisco Smart Install con il comando **no vstack**.

  Nota: Il comando **vstack** è stato introdotto in Cisco IOS versione 12.2(55)SE03.

Di seguito viene riportato un esempio di output del comando **show vstack** su uno switch Cisco Catalyst con la funzione client di Smart Install disabilitata:

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

Clienti che utilizzano la funzionalità Smart Install solo per l'installazione zero-touch

Disabilitare la funzionalità client di Smart Install al termine dell'installazione zero-touch o usare il comando **no vstack**.

Per propagare il comando **no vstack** nella rete, utilizzare uno dei seguenti metodi:

- Immettere il comando **no vstack** su tutti gli switch client manualmente o con uno script.
- Aggiungere il comando **no vstack** come parte della configurazione di Cisco IOS da inserire in ciascun client Smart Install come parte dell'installazione zero-touch.
- Nelle versioni che non supportano il comando **vstack** (Cisco IOS versione 12.2(55)SE02 e precedenti), applicare un elenco di controllo di accesso (ACL) sugli switch client per bloccare il traffico sulla porta TCP 4786.

Per abilitare in seguito la funzionalità client di Smart Install, immettere il comando **vstack** su tutti gli switch client manualmente o con uno script.

Clienti che utilizzano la funzionalità di installazione intelligente per un'installazione senza interruzioni

Nella progettazione di un'architettura Smart Install, è necessario prestare attenzione affinché lo spazio di indirizzi IP dell'infrastruttura non sia accessibile a parti non attendibili. Nelle versioni che non supportano il comando **vstack**, verificare che solo la directory di Smart Install abbia la connettività TCP per tutti i client Smart Install sulla porta 4786.

Gli amministratori possono utilizzare le seguenti best practice sulla sicurezza per le distribuzioni Cisco Smart Install sui dispositivi interessati:

- ACL di interfaccia
- Control Plane Policing (CoPP). Questa funzione non è disponibile su tutte le versioni del software Cisco IOS.

Nell'esempio viene mostrato un ACL di interfaccia con l'indirizzo IP della directory di Smart Install come 10.10.10.1 e l'indirizzo IP del client di Smart Install come 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
```

Questo ACL deve essere distribuito su tutte le interfacce IP su tutti i client. La pressione del tasto può avvenire direttamente dal director al momento dell'installazione degli switch.

Per limitare ulteriormente l'accesso a tutti i client all'interno dell'infrastruttura, gli amministratori possono utilizzare queste procedure ottimali di sicurezza su altri dispositivi della rete:

- iACL (Infrastructure Access Control List)
- VACL (VLAN Access Control List)

Limitazione dell'accesso alla rete con ACL di infrastruttura

Progettati per prevenire la comunicazione diretta non autorizzata ai dispositivi di rete, gli iACL (Access Control List) dell'infrastruttura sono uno dei controlli di sicurezza più critici che possono essere implementati nelle reti. Gli ACL dell'infrastruttura sfruttano l'idea che quasi tutto il traffico di

rete attraversa la rete e non è destinato alla rete stessa.

Un iACL viene costruito e applicato per specificare le connessioni dagli host o dalle reti che devono essere autorizzate ai dispositivi di rete. Esempi comuni di questi tipi di connessioni sono eBGP, SSH e SNMP. Dopo aver autorizzato le connessioni richieste, tutto il resto del traffico verso l'infrastruttura viene esplicitamente rifiutato. Tutto il traffico di transito che attraversa la rete e non è destinato a dispositivi dell'infrastruttura è quindi esplicitamente autorizzato.

Le protezioni fornite dagli iACL sono significative sia per i piani di gestione che per quelli di controllo. L'implementazione degli iACL può essere semplificata dall'uso di indirizzi distinti per i dispositivi dell'infrastruttura di rete. Per ulteriori informazioni sulle implicazioni dell'indirizzamento IP per la sicurezza, fare riferimento a A Security Oriented Approach to IP Addressing *(Un approccio orientato alla sicurezza all'indirizzamento IP).*

Nell'esempio, la configurazione degli ACL mostra la struttura da usare come punto di partenza quando si inizia il processo di implementazione degli ACL:

```
!

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
!
```

Dopo la creazione, l'iACL deve essere applicato a tutte le interfacce con dispositivi non di infrastruttura. Ciò include le interfacce che si connettono ad altre organizzazioni, segmenti di accesso remoto, segmenti di utenti e segmenti nei centri dati.

Per ulteriori informazioni, fare riferimento al documento sulla protezione del core: Access Control List di protezione dell'infrastruttura.

Filtro pacchetti ICMP

Il protocollo ICMP (Internet Control Message Protocol) è progettato come protocollo di controllo IP. Pertanto, i messaggi trasmessi possono avere ramificazioni di vasta portata per i protocolli TCP e IP in generale. Mentre gli strumenti di risoluzione dei problemi di rete **ping** e **traceroute** usano ICMP, la connettività ICMP esterna raramente è necessaria per il corretto funzionamento di una rete.

Il software Cisco IOS fornisce una funzionalità che consente di filtrare specificamente i messaggi ICMP per nome, tipo e codice. Questo ACL di esempio, che deve essere usato con le voci di controllo di accesso (ACE) degli esempi precedenti, consente i ping da stazioni di gestione attendibili e server NMS e blocca tutti gli altri pacchetti ICMP:

```
!

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
!
```

Filtra frammenti IP

Il processo di filtro dei pacchetti IP frammentati può rappresentare una sfida per i dispositivi di sicurezza. Infatti, le informazioni di layer 4 usate per filtrare i pacchetti TCP e UDP sono presenti solo nel frammento iniziale. Il software Cisco IOS utilizza un metodo specifico per verificare i frammenti non iniziali rispetto agli elenchi degli accessi configurati. Il software Cisco IOS valuta questi frammenti non iniziali rispetto all'ACL e ignora qualsiasi informazione di filtro di layer 4. In questo modo, i frammenti non iniziali vengono valutati solo sulla parte di layer 3 di qualsiasi ACE configurata.

In questa configurazione di esempio, se un pacchetto TCP destinato a **192.168.1.1** sulla **porta 22** viene frammentato in transito, il frammento iniziale viene scartato, come previsto, dal secondo ACE in base alle informazioni di layer 4 contenute nel pacchetto. Tuttavia, tutti i frammenti rimanenti (non iniziali) sono autorizzati dalla prima voce ACE in base alle informazioni di layer 3 contenute nel pacchetto e nella voce ACE. Questo scenario viene mostrato nella configurazione seguente:

```
!

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
!
```

A causa della natura non intuitiva della gestione dei frammenti, i frammenti IP sono spesso autorizzati inavvertitamente dagli ACL. La frammentazione è spesso utilizzata anche per tentare di eludere il rilevamento con sistemi di rilevamento delle intrusioni. Per questi motivi, i frammenti IP sono spesso utilizzati negli attacchi e devono essere filtrati esplicitamente nella parte superiore di qualsiasi ACL configurato. Questo ACL di esempio include un filtro completo dei frammenti IP. Le funzionalità di questo esempio devono essere utilizzate insieme a quelle degli esempi precedenti.

```
!

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
!
```

Per ulteriori informazioni sulla gestione dei pacchetti IP frammentati da parte degli ACL, consultare il documento Access Control Lists and IP Fragments.

Supporto ACL per filtro opzioni IP

Dal software Cisco IOS versione 12.3(4)T, è supportato l'uso degli ACL per filtrare i pacchetti IP in base alle opzioni IP contenute nel pacchetto. Le opzioni IP rappresentano una sfida per la sicurezza dei dispositivi di rete in quanto devono essere elaborate come pacchetti di eccezione. Ciò richiede un livello di sforzo della CPU che non è richiesto dai pacchetti tipici che attraversano la rete. La presenza di opzioni IP all'interno di un pacchetto può anche indicare un tentativo di sovvertire i controlli di sicurezza nella rete o di alterare in altro modo le caratteristiche di transito di un pacchetto. Per questi motivi, i pacchetti con opzioni IP devono essere filtrati al margine della rete.

Questo esempio deve essere usato con le voci ACE degli esempi precedenti per includere il filtro completo dei pacchetti IP che contengono le opzioni IP:

```
!

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
!
```

Supporto ACL per filtrare in base al valore TTL

Dal software Cisco IOS versione 12.4(2)T, è stato aggiunto il supporto ACL per filtrare i pacchetti IP in base al valore TTL (Time to Live). Il valore TTL di un datagramma IP viene ridotto da ciascun dispositivo di rete man mano che il pacchetto passa dall'origine alla destinazione. Anche se i valori iniziali variano a seconda del sistema operativo, quando il valore TTL di un pacchetto raggiunge zero, il pacchetto deve essere scartato. Il dispositivo che riduce il valore TTL a zero, e quindi scarta il pacchetto, è richiesto per generare e inviare un messaggio ICMP "Time Exceeded" (Tempo scaduto) all'origine del pacchetto.

La generazione e la trasmissione di questi messaggi costituisce un processo di eccezione. I router possono eseguire questa funzione quando il numero di pacchetti IP in scadenza è basso, ma se il numero di pacchetti in scadenza è alto, la generazione e la trasmissione di questi messaggi possono utilizzare tutte le risorse CPU disponibili. Questo presenta un vettore di attacco DoS. Per questo motivo, i dispositivi devono essere protetti dagli attacchi DoS che utilizzano una frequenza elevata di pacchetti IP con scadenza.

Si consiglia alle organizzazioni di filtrare i pacchetti IP con valori TTL bassi al bordo della rete. Il filtraggio completo dei pacchetti con valori TTL insufficienti per attraversare la rete riduce la minaccia di attacchi basati su TTL.

In questo esempio, un ACL filtra i pacchetti con valori TTL inferiori a sei. Ciò fornisce la protezione dagli attacchi TTL in scadenza per le reti fino a cinque hop di larghezza.

```
!

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
!
```

> **Nota:** Alcuni protocolli fanno un uso legittimo di pacchetti con valori TTL bassi. eBGP è uno di questi protocolli. Per ulteriori informazioni sull'attenuazione degli attacchi TTL basati sulla scadenza, fare riferimento a TTL Expiry Attack Identification and Mitigation (Identificazione e mitigazione degli attacchi TTL in scadenza).

Per ulteriori informazioni su questa funzionalità, fare riferimento al supporto ACL per il filtro sul valore TTL.

Sessioni di gestione interattiva protette

Le sessioni di gestione dei dispositivi consentono di visualizzare e raccogliere informazioni su un dispositivo e sulle relative operazioni. Se queste informazioni vengono divulgate a un utente malintenzionato, il dispositivo può diventare oggetto di un attacco, essere compromesso e utilizzato per eseguire ulteriori attacchi. Chiunque disponga di accesso privilegiato a un dispositivo ha la capacità di esercitare il controllo amministrativo completo su tale dispositivo. È fondamentale proteggere le sessioni di gestione per impedire la divulgazione delle informazioni e l'accesso non autorizzato.

Protezione del piano di gestione

Nel software Cisco IOS versione 12.4(6)T e successive, la funzionalità Management Plane Protection (MPP) consente a un amministratore di limitare le interfacce che possono essere ricevute da un dispositivo per il traffico di gestione. In questo modo l'amministratore può esercitare un ulteriore controllo su un dispositivo e sulla modalità di accesso al dispositivo.

Nell'esempio viene mostrato come abilitare il protocollo MPP in modo da consentire solo SSH e HTTPS sull'interfaccia Gigabit Ethernet 0/1:

```
!

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

Per ulteriori informazioni sul protocollo MPP, fare riferimento a Management Plane Protection.

Control Plane Protection

Control Plane Protection (CPPr) si basa sulla funzionalità Control Plane Policing per limitare e controllare il traffico aereo destinato al processore di routing del dispositivo IOS. La funzionalità CPPr, aggiunta nel software Cisco IOS versione 12.4(4)T, suddivide il control plane in categorie di control plane distinte, note come sottointerfacce. Esistono tre sottointerfacce del piano di controllo: Host, transito e CEF-Exception. Inoltre, CPPr include le seguenti funzioni aggiuntive di protezione del control plane:

- **Funzione di filtro delle porte**: questa funzione consente di controllare o eliminare i pacchetti diretti alle porte TCP e UDP chiuse o non in ascolto.

- **Caratteristica dei criteri di soglia della coda**: questa funzionalità limita il numero di pacchetti per un protocollo specificato consentiti nella coda di input IP del control plane.

CPPr consente agli amministratori di classificare, controllare e limitare il traffico inviato a un dispositivo a scopo di gestione tramite la sottointerfaccia host. Esempi di pacchetti classificati per la categoria della sottointerfaccia host includono il traffico di gestione, ad esempio SSH o Telnet, e i protocolli di routing.

> **Nota:** CPPr non supporta IPv6 ed è limitato al percorso di input IPv4.

Per ulteriori informazioni sulla funzione Cisco CPPr, consultare il documento Control Plane

Protection Feature Guide - 12.4T *and* Understanding Control Plane Protection.

Sessioni di gestione crittografia

Poiché le informazioni possono essere divulgate in una sessione di gestione interattiva, questo traffico deve essere crittografato in modo che un utente malintenzionato non possa accedere ai dati trasmessi. La crittografia del traffico consente una connessione di accesso remoto sicura al dispositivo. Se il traffico di una sessione di gestione viene inviato in rete in formato non crittografato, un utente non autorizzato può ottenere informazioni riservate sul dispositivo e sulla rete.

Un amministratore può stabilire una connessione crittografata e sicura per la gestione dell'accesso remoto a un dispositivo con le funzionalità SSH o HTTPS (Secure Hypertext Transfer Protocol). Il software Cisco IOS supporta SSH versione 1.0 (SSHv1), SSH versione 2.0 (SSHv2) e HTTPS che utilizza Secure Sockets Layer (SSL) e Transport Layer Security (TLS) per l'autenticazione e la crittografia dei dati. SSHv1 e SSHv2 non sono compatibili. SSHv1 non è sicuro e non è standardizzato, quindi non è consigliato se SSHv2 è un'opzione.

Il software Cisco IOS supporta anche il protocollo SCP (Secure Copy Protocol), che consente una connessione crittografata e sicura per copiare le configurazioni dei dispositivi o le immagini software. SCP si basa sul protocollo SSH. Nell'esempio, la configurazione abilita SSH su un dispositivo Cisco IOS:

```
!

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
!
```

Questo esempio di configurazione abilita i servizi SCP:

```
!

ip scp server enable
!
```

Questo è un esempio di configurazione per i servizi HTTPS:

```
!

crypto key generate rsa modulus 2048
!

ip http secure-server
!
```

Per ulteriori informazioni sulla funzionalità SSH del software Cisco IOS, consultare le domande frequenti sulla configurazione di Secure Shell sui router e gli switch con Cisco IOS e Secure Shell (SSH).

SSHv2

La funzione di supporto SSHv2 introdotta nel software Cisco IOS versione 12.3(4)T consente all'utente di configurare SSHv2. Il supporto SSHv1 è stato implementato in una versione precedente del software Cisco IOS. SSH viene eseguito su un livello di trasporto affidabile e fornisce funzionalità avanzate di autenticazione e crittografia. L'unico trasporto affidabile definito per SSH è TCP. SSH consente di accedere ed eseguire in modo sicuro i comandi su un altro computer o dispositivo tramite una rete. La funzionalità SCP (Secure Copy Protocol) tunneling su SSH consente il trasferimento sicuro dei file.

Se il comando **ip ssh versione 2** non è configurato in modo esplicito, Cisco IOS abilita SSH versione 1.9. SSH versione 1.99 consente entrambe le connessioni SSHv1 e SSHv2. SSHv1 è considerato non sicuro e può avere effetti negativi sul sistema. Se il protocollo SSH è abilitato, si consiglia di disabilitare SSHv1 usando il comando **ip ssh versione 2**.

Questa configurazione di esempio abilita SSHv2 (con SSHv1 disabilitato) su un dispositivo Cisco IOS:

```
!

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

!
```

per ulteriori informazioni sull'uso del protocollo SSHv2, fare riferimento al supporto Secure Shell versione 2.

Miglioramenti SSHv2 per le chiavi RSA

Cisco IOS SSHv2 supporta metodi di autenticazione interattivi da tastiera e basati su password. La funzionalità SSHv2 Enhancements for RSA Keys supporta anche l'autenticazione con chiave pubblica basata su RSA per client e server.

Per l'autenticazione degli utenti, l'autenticazione RSA utilizza una coppia di chiavi privata/pubblica associata a ciascun utente per l'autenticazione. Per completare l'autenticazione, l'utente deve generare una coppia di chiavi privata/pubblica sul client e configurare una chiave pubblica sul server SSH Cisco IOS.

Un utente SSH che tenta di stabilire le credenziali fornisce una firma crittografata con la chiave privata. La firma e la chiave pubblica dell'utente vengono inviate al server SSH per l'autenticazione. Il server SSH calcola un hash sulla chiave pubblica fornita dall'utente. L'hash viene utilizzato per determinare se nel server è presente una voce corrispondente. Se viene trovata una corrispondenza, la verifica del messaggio basata su RSA viene eseguita con la chiave pubblica. L'utente viene quindi autenticato o non autorizzato in base alla firma crittografata.

Per l'autenticazione del server, il client SSH Cisco IOS deve assegnare una chiave host per ciascun server. Quando il client tenta di stabilire una sessione SSH con un server, riceve la firma del server come parte del messaggio di scambio chiave. Se sul client è attivato il flag di controllo rigoroso della chiave host, il client verifica se dispone della voce della chiave host corrispondente al server preconfigurato. Se viene trovata una corrispondenza, il client tenta di convalidare la firma con la chiave host del server. Se l'autenticazione del server ha esito positivo, la creazione della sessione continua; in caso contrario viene interrotta e viene visualizzato un messaggio di **errore Autenticazione server**.

Questa configurazione di esempio consente di usare le chiavi RSA con SSHv2 su un dispositivo Cisco IOS:

```
!
! 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
!
```

per ulteriori informazioni sull'uso delle chiavi RSA con SSHv2, fare riferimento a Secure Shell versione 2 Enhancements for RSA Keys.

Questa configurazione di esempio consente al server SSH Cisco IOS di eseguire l'autenticazione RSA. L'autenticazione dell'utente ha esito positivo se la chiave pubblica RSA memorizzata sul server viene verificata con la coppia di chiavi pubblica o privata memorizzata sul client.

```
!
! 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.)
!
```

Per ulteriori informazioni sull'uso delle chiavi RSA con SSHv2, consultare il documento sulla configurazione del server SSH Cisco IOS per eseguire l'autenticazione RSA.

Questa configurazione di esempio consente al client SSH Cisco IOS di eseguire l'autenticazione del server basata su RSA.

```
!
!

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
!
```

Per ulteriori informazioni sull'uso delle chiavi RSA con SSHv2, consultare il documento sulla configurazione del client SSH Cisco IOS per eseguire l'autenticazione server basata su RSA.

Porte console e AUX

Nei dispositivi Cisco IOS, le porte console e le porte ausiliarie (AUX) sono linee asincrone che possono essere utilizzate per l'accesso locale e remoto a un dispositivo. Occorre tenere presente che le porte console sui dispositivi Cisco IOS dispongono di privilegi speciali. In particolare, questi privilegi consentono a un amministratore di eseguire la procedura di recupero della password. Per eseguire il recupero della password, un utente non autenticato dovrebbe avere accesso alla porta della console e la possibilità di interrompere l'alimentazione del dispositivo o di causare il blocco del dispositivo.

Qualsiasi metodo utilizzato per accedere alla porta console di un dispositivo deve essere protetto in modo equivalente alla protezione applicata per l'accesso privilegiato a un dispositivo. I metodi utilizzati per proteggere l'accesso devono includere l'uso di password AAA, exec-timeout e modem se il modem è collegato alla console.

Se il recupero della password non è richiesto, un amministratore può rimuovere la possibilità di eseguire la procedura di recupero della password utilizzando il comando di configurazione globale **no service password-recovery**; tuttavia, se il comando **no service password-recovery** è stato abilitato, un amministratore non può più eseguire il recupero della password su un dispositivo.

Nella maggior parte dei casi, la porta AUX di un dispositivo deve essere disabilitata per impedire accessi non autorizzati. Una porta AUX può essere disabilitata con questi comandi:

```
!

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

Controllo righe vty e tty

Le sessioni di gestione interattive nel software Cisco IOS utilizzano un tty o virtual tty (vty). Un tty è una linea asincrona locale alla quale un terminale può essere collegato per l'accesso locale al dispositivo o a un modem per l'accesso remoto a un dispositivo. Si noti che i tty possono essere utilizzati per le connessioni alle porte console di altri dispositivi. Questa funzione consente a un dispositivo con linee tty di fungere da console server dove è possibile stabilire connessioni attraverso la rete alle porte console dei dispositivi connessi alle linee tty. È necessario controllare anche le linee tty per queste connessioni inverse sulla rete.

Una linea vty viene utilizzata per tutte le altre connessioni di rete remote supportate dal dispositivo, indipendentemente dal protocollo (SSH, SCP o Telnet sono esempi). Per garantire che un dispositivo sia accessibile tramite una sessione di gestione locale o remota, è necessario applicare controlli appropriati sulle linee vty e tty. i dispositivi Cisco IOS hanno un numero limitato di linee vty; il numero di righe disponibili può essere determinato con il comando show line EXEC. Quando tutte le linee vty sono in uso, non è possibile stabilire nuove sessioni di gestione, il che crea una condizione DoS per l'accesso al dispositivo.

La forma più semplice di controllo dell'accesso a un vty o tty di un dispositivo è l'utilizzo dell'autenticazione su tutte le righe, indipendentemente dalla posizione del dispositivo all'interno della rete. Ciò è fondamentale per le linee vty, in quanto sono accessibili attraverso la rete. Tramite la rete è possibile accedere anche a una linea tty collegata a un modem utilizzato per l'accesso remoto alla periferica o a una linea tty collegata alla porta console di altre periferiche. Altre forme di controllo degli accessi vty e tty possono essere applicate con i comandi di **input transport** o di configurazione **access-class**, con le funzionalità CoPP e CPPr o se si applicano elenchi degli accessi alle interfacce sul dispositivo.

L'autenticazione può essere imposta tramite l'uso del server AAA, il metodo consigliato per l'accesso autenticato a un dispositivo, con l'uso del database utenti locale, o tramite una semplice autenticazione tramite password configurata direttamente sulla riga vty o tty.

il comando **exec-timeout** deve essere usato per disconnettere le sessioni sulle righe vty o tty lasciate inattive. Anche il comando **service tcp-keepalives-in** deve essere usato per abilitare i pacchetti TCP keepalive sulle connessioni in arrivo al dispositivo. In questo modo il dispositivo sull'estremità remota della connessione è ancora accessibile e le connessioni half-open o orfane vengono rimosse dal dispositivo IOS locale.

Controllo del trasporto per le linee vty e tty

Configurare vty e tty in modo da accettare solo connessioni di gestione dell'accesso remoto

crittografate e sicure al dispositivo o tramite il dispositivo, se usato come console server. In questa sezione vengono illustrati i tipi di chiamata perché è possibile connettere tali linee alle porte console di altri dispositivi, in modo da rendere il tty accessibile in rete. Per impedire la divulgazione delle informazioni o l'accesso non autorizzato ai dati trasmessi tra l'amministratore e il dispositivo, è consigliabile utilizzare il protocollo **transport input ssh** anziché i protocolli non crittografati, ad esempio Telnet e rlogin. La configurazione **transport input none** può essere abilitata su un tty, il che in effetti disabilita l'uso della linea tty per le connessioni alla console inversa.

Le linee vty e tty consentono all'amministratore di connettersi ad altre periferiche. Per limitare il tipo di trasporto che un amministratore può utilizzare per le connessioni in uscita, utilizzare il comando di configurazione della riga di **output del trasporto**. Se le connessioni in uscita non sono necessarie, è consigliabile utilizzare **l'output di trasporto none**. Tuttavia, se le connessioni in uscita sono consentite, un metodo di accesso remoto crittografato e sicuro per la connessione deve essere imposto tramite l'utilizzo dell'**output di trasporto ssh**.

> **Nota:** Se supportato, IPSec può essere utilizzato per connessioni di accesso remoto crittografate e protette a un dispositivo. Se si utilizza IPSec, viene aggiunto un ulteriore sovraccarico della CPU al dispositivo. Tuttavia, il protocollo SSH deve essere ancora applicato come trasporto anche quando si usa IPSec.

Banner avviso

In alcune giurisdizioni legali, può essere impossibile perseguire e illegale monitorare utenti malintenzionati a meno che non siano stati informati che non è loro consentito utilizzare il sistema. Un metodo per inviare questa notifica è inserire le informazioni in un messaggio banner configurato con il comando Cisco IOS software banner login.

Gli obblighi di notifica legale sono complessi, variano in base alla giurisdizione e alla situazione e devono essere discussi con il consulente legale. Anche all'interno delle giurisdizioni, le opinioni legali possono differire. In collaborazione con il consulente legale, uno striscione può fornire alcune o tutte queste informazioni:

- Notare che il sistema deve essere connesso o utilizzato solo da personale specificamente autorizzato e forse anche informazioni su chi può autorizzare l'uso.
- Si noti che qualsiasi utilizzo non autorizzato del sistema è illegale e può essere soggetto a sanzioni civili e penali.
- Si noti che qualsiasi utilizzo del sistema può essere registrato o monitorato senza ulteriori avvisi e che i registri risultanti possono essere utilizzati come prova in tribunale.
- Avvisi specifici richiesti dalle leggi locali.

Da un punto di vista della sicurezza, piuttosto che da un punto di vista legale, un banner di accesso non deve contenere informazioni specifiche sul nome, il modello, il software o la proprietà del router. Tali informazioni possono essere utilizzate in modo non corretto da utenti malintenzionati.

Autenticazione, autorizzazione e accounting

Il framework AAA (Authentication, Authorization, and Accounting) è fondamentale per proteggere l'accesso interattivo ai dispositivi di rete. La struttura AAA fornisce un ambiente altamente configurabile che può essere personalizzato in base alle esigenze della rete.

Autenticazione TACACS+

TACACS+ è un protocollo di autenticazione che i dispositivi Cisco IOS possono utilizzare per autenticare gli utenti di gestione su un server AAA remoto. Questi utenti di gestione possono accedere al dispositivo IOS tramite SSH, HTTPS, telnet o HTTP.

L'autenticazione TACACS+, o più in generale l'autenticazione AAA, consente di usare i singoli account utente per ciascun amministratore di rete. Quando non si dipende da una singola password condivisa, la sicurezza della rete è migliorata e la responsabilità è rafforzata.

RADIUS è un protocollo simile a TACACS+; tuttavia, viene crittografata solo la password inviata attraverso la rete. Al contrario, TACACS+ cripta l'intero payload TCP, che include sia il nome utente che la password. Per questo motivo, TACACS+ deve essere usato al posto di RADIUS quando TACACS+ è supportato dal server AAA. Per un confronto più dettagliato dei due protocolli, fare riferimento a TACACS+ e RADIUS Comparison.

L'autenticazione TACACS+ può essere abilitata su un dispositivo Cisco IOS con una configurazione simile a quella dell'esempio seguente:

```
!

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

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

La configurazione precedente può essere utilizzata come punto di partenza per un modello di autenticazione AAA specifico dell'organizzazione. Per ulteriori informazioni sulla configurazione del server AAA, fare riferimento a Autenticazione, autorizzazione e accounting.

Un elenco di metodi è un elenco sequenziale che descrive i metodi di autenticazione da interrogare per autenticare un utente. Gli elenchi di metodi consentono di designare uno o più protocolli di protezione da utilizzare per l'autenticazione e quindi di garantire un sistema di backup per l'autenticazione in caso di errore del metodo iniziale. Il software Cisco IOS utilizza il primo metodo elencato che accetta o rifiuta correttamente un utente. I metodi successivi vengono tentati solo nei casi in cui i metodi precedenti hanno esito negativo a causa della mancata disponibilità del server o di una configurazione errata.

Per ulteriori informazioni sulla configurazione degli elenchi di metodi denominati, fare riferimento a Elenchi di metodi denominati per l'autenticazione.

Fallback autenticazione

Se tutti i server TACACS+ configurati non sono disponibili, un dispositivo Cisco IOS può fare affidamento sui protocolli di autenticazione secondari. Le configurazioni tipiche includono l'uso dell'autenticazione locale o attiva se tutti i server TACACS+ configurati non sono disponibili.

L'elenco completo delle opzioni per l'autenticazione su dispositivo include enable, local e line. Ognuna di queste opzioni ha dei vantaggi. L'utilizzo del segreto enable è preferibile perché il segreto viene sottoposto a hash con un algoritmo unidirezionale che è intrinsecamente più sicuro dell'algoritmo di crittografia utilizzato con le password di tipo 7 per l'autenticazione di linea o locale.

Tuttavia, nelle versioni software Cisco IOS che supportano l'utilizzo di password segrete per gli utenti definiti localmente, può essere opportuno eseguire il fallback all'autenticazione locale. Ciò consente di creare un utente definito localmente per uno o più amministratori di rete. Se TACACS+ dovesse diventare completamente non disponibile, ciascun amministratore può utilizzare il proprio nome utente e password locali. Sebbene questa azione accresca la responsabilità degli amministratori di rete nelle interruzioni TACACS+, aumenta in modo significativo il carico amministrativo in quanto è necessario mantenere gli account utente locali su tutti i dispositivi di rete.

Questo esempio di configurazione si basa sull'esempio di autenticazione TACACS+ precedente per includere l'autenticazione di fallback alla password configurata localmente con il comando **enable secret**:

```
!

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>
!
```

Per ulteriori informazioni sull'uso dell'autenticazione fallback con AAA, consultare il documento sulla configurazione dell'autenticazione.

Utilizzo di password di tipo 7

Originariamente concepite per consentire una rapida decrittografia delle password archiviate, le password Type 7 non rappresentano una forma sicura di memorizzazione delle password. Sono disponibili numerosi strumenti che consentono di decrittografare facilmente queste password. È consigliabile evitare di utilizzare password di tipo 7, a meno che non sia richiesto da una funzionalità in uso sul dispositivo Cisco IOS.

Utilizzare il tipo 9 (scrypt) quando possibile:

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

La rimozione di password di questo tipo può essere facilitata tramite l'autenticazione AAA e l'uso della funzione di sicurezza potenziata delle password, che consente di utilizzare password segrete con utenti definiti localmente tramite il comando di configurazione globale **username**. Se non è possibile impedire completamente l'utilizzo di password di tipo 7, considerare queste password offuscate, non crittografate.

Per ulteriori informazioni sulla rimozione delle password di tipo 7, *vedere* la sezione Protezione

avanzata piano di gestione generale di questo documento.

Autorizzazione comando TACACS+

L'autorizzazione dei comandi con TACACS+ e AAA fornisce un meccanismo che consente o nega ciascun comando immesso da un utente amministrativo. Quando l'utente immette i comandi EXEC, Cisco IOS invia ciascun comando al server AAA configurato. Il server AAA utilizza quindi i criteri configurati per autorizzare o negare il comando per quel particolare utente.

Questa configurazione può essere aggiunta al precedente esempio di autenticazione AAA per implementare l'autorizzazione del comando:

```
!

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
!
```

Per ulteriori informazioni sull'autorizzazione dei comandi, consultare il documento sulla configurazione dell'autorizzazione.

Accounting comando TACACS+

Una volta configurato, l'accounting dei comandi AAA invia informazioni su ciascun comando EXEC immesso ai server TACACS+ configurati. Le informazioni inviate al server TACACS+ includono il comando eseguito, la data di esecuzione e il nome utente dell'utente che immette il comando. L'accounting dei comandi non è supportato con RADIUS.

Questa configurazione di esempio abilita l'accounting dei comandi AAA per i comandi EXEC immessi ai livelli di privilegio zero, uno e 15. Questa configurazione si basa su esempi precedenti che includono la configurazione dei server TACACS.

```
!

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
!
```

Per ulteriori informazioni sulla configurazione dell'accounting AAA, consultare il documento sulla configurazione dell'accounting.

Server AAA ridondanti

I server AAA utilizzati in un ambiente devono essere ridondanti e installati in modo fault-tolerant. In questo modo, è possibile garantire l'accesso interattivo alla gestione, ad esempio SSH, nel caso in cui un server AAA non sia disponibile.

Quando si progetta o si implementa una soluzione server AAA ridondante, tenere presenti le seguenti considerazioni:

- Disponibilità dei server AAA durante potenziali errori di rete
- Posizionamento geograficamente distribuito dei server AAA
- Caricamento su singoli server AAA in condizioni di stato stazionario e di errore
- Latenza di rete tra server di accesso alla rete e server AAA
- Sincronizzazione database server AAA

Per ulteriori informazioni, fare riferimento a Distribuire i server di controllo di accesso.

Rafforzamento del protocollo SNMP (Simple Network Management Protocol)

In questa sezione vengono evidenziati diversi metodi che è possibile utilizzare per proteggere la distribuzione di SNMP nei dispositivi IOS. È fondamentale proteggere correttamente il protocollo SNMP per proteggere la riservatezza, l'integrità e la disponibilità sia dei dati di rete che dei dispositivi di rete attraverso cui transitano tali dati. L'SNMP fornisce una vasta gamma di informazioni sullo stato dei dispositivi di rete. È consigliabile proteggere queste informazioni da utenti malintenzionati che desiderano utilizzare questi dati per eseguire attacchi alla rete.

Stringhe della community SNMP

Le stringhe della community sono password che vengono applicate a un dispositivo IOS per limitare l'accesso, sia di sola lettura che di lettura/scrittura, ai dati SNMP sul dispositivo. Queste stringhe della community, come tutte le password, devono essere scelte attentamente per evitare che siano insignificanti. Le stringhe comunitarie dovrebbero essere modificate periodicamente e in conformità delle politiche di sicurezza delle reti. Ad esempio, le stringhe devono essere modificate quando un amministratore di rete cambia ruolo o lascia la società.

Queste righe di configurazione configurano una stringa della community di sola lettura di READONLY e una stringa della community di lettura/scrittura di READWRITE:

```
!

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

> **Nota:** Gli esempi di stringhe della community precedenti sono stati scelti per spiegare chiaramente l'utilizzo di tali stringhe. Per gli ambienti di produzione, le stringhe della community devono essere scelte con cautela e devono essere composte da una serie di simboli alfabetici, numerici e non alfanumerici. Per ulteriori informazioni sulla selezione di password non banali, fare riferimento a Suggerimenti per la creazione di password complesse.

Per ulteriori informazioni su questa funzione, consultare la guida di riferimento dei comandi SNMP di IOS.

Stringhe della community SNMP con ACL

Oltre alla stringa della community, occorre applicare un ACL che limiti ulteriormente l'accesso SNMP a un gruppo selezionato di indirizzi IP di origine. Questa configurazione limita l'accesso SNMP in sola lettura ai dispositivi host terminali che risiedono nello spazio di indirizzi 192.168.100.0/24 e limita l'accesso SNMP in lettura/scrittura solo al dispositivo host terminale a 192.168.100.1.

> **Nota:** I dispositivi autorizzati da questi ACL richiedono la stringa della community corretta per accedere alle informazioni SNMP richieste.

```
!

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
!
```

Per ulteriori informazioni su questa funzione, consultare la community snmp-server *nella guida di riferimento dei comandi di Cisco IOS Network Management.*

ACL di infrastruttura

Èpossibile distribuire gli ACL di infrastruttura (iACL) in modo da garantire che solo gli host terminali con indirizzi IP attendibili possano inviare il traffico SNMP a un dispositivo IOS. Un iACL deve contenere una policy che nega i pacchetti SNMP non autorizzati sulla porta UDP 161.

Per ulteriori informazioni sull'uso degli ACL, vedere la sezione Limitazione dell'accesso alla rete con ACL di infrastruttura di questo documento.

Viste SNMP

Le viste SNMP sono una funzione di sicurezza che consente o nega l'accesso a determinati MIB SNMP. Una volta creata e applicata una vista a una stringa della community con i comandi di configurazione globale **snmp-server community**-string view, l'accesso ai dati MIB è limitato alle autorizzazioni definite dalla vista. Se appropriato, si consiglia di utilizzare le visualizzazioni per limitare gli utenti di SNMP ai dati richiesti.

Questo esempio di configurazione limita l'accesso SNMP con la stringa della community LIMITATA ai dati MIB presenti nel gruppo di sistema:

```
!

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

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

Per ulteriori informazioni, fare riferimento a Configurazione del supporto SNMP.

SNMP versione 3

Il protocollo SNMP versione 3 (SNMPv3) è definito dalle specifiche RFC3410, RFC3411, RFC3412, RFC3413, RFC3414 e RFC3415 ed è un protocollo interoperabile basato su standard per la gestione della rete. L'SNMPv3 fornisce un accesso sicuro ai dispositivi perché autentica e facoltativamente cripta i pacchetti sulla rete. Se supportato, SNMPv3 può essere utilizzato per aggiungere un altro livello di sicurezza quando si distribuisce SNMP. SNMPv3 è costituito da tre opzioni di configurazione principali:

- **no auth** - Questa modalità non richiede alcuna autenticazione né crittografia dei pacchetti SNMP
- **auth** - Questa modalità richiede l'autenticazione del pacchetto SNMP senza crittografia
- **priv** - Questa modalità richiede sia l'autenticazione che la crittografia (privacy) di ciascun pacchetto SNMP

Per gestire i pacchetti SNMP, è necessario che esista un ID motore autorevole che consenta di utilizzare i meccanismi di sicurezza SNMPv3 (autenticazione o autenticazione e crittografia); per default, l'ID del motore viene generato localmente. L'ID del motore può essere visualizzato con il comando **show snmp engineID**, come mostrato nell'esempio:

```
router#show snmp engineID
Local SNMP engineID: 800000090300000152BD35496
Remote Engine ID IP-addr Port
```

> **Nota:** Se l'ID del motore viene modificato, tutti gli account utente SNMP devono essere riconfigurati.

Il passaggio successivo è quello di configurare un gruppo SNMPv3. Questo comando configura un dispositivo Cisco IOS per SNMPv3 con un gruppo di server SNMP AUTHGROUP e abilita solo l'autenticazione per questo gruppo con la parola chiave **auth**:

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

Questo comando configura un dispositivo Cisco IOS per SNMPv3 con un gruppo di server SNMP PRIVGROUP e abilita l'autenticazione e la crittografia per questo gruppo con la parola chiave **priv**:

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

Questo comando configura un utente SNMPv3 con una password di autenticazione MD5 di **authpassword** e una password di crittografia 3DES di **privpassword**:

```
!

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

Notare che i comandi di configurazione dell'**utente snmp-server** non vengono visualizzati nell'output di configurazione del dispositivo come richiesto dalla RFC 3414; pertanto, la password utente non è visualizzabile dalla configurazione. Per visualizzare gli utenti configurati, immettere il

comando **show snmp user** come mostrato nell'esempio:

```
router#show snmp user
User name: snmpv3user
Engine ID: 80000090300000152BD35496
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: 3DES
Group-name: PRIVGROUP
```

Per ulteriori informazioni su questa funzione, fare riferimento a Configurazione del supporto SNMP.

Protezione del piano di gestione

La funzione Management Plane Protection (MPP) nel software Cisco IOS può essere utilizzata per proteggere il protocollo SNMP perché limita le interfacce attraverso cui il traffico SNMP può terminare sul dispositivo. La funzione MPP consente agli amministratori di designare una o più interfacce come interfacce di gestione. Il traffico di gestione può entrare in un dispositivo solo attraverso queste interfacce di gestione. Dopo l'abilitazione del protocollo MPP, nessuna interfaccia, ad eccezione di quelle di gestione designate, accetta il traffico di gestione della rete destinato al dispositivo.

Si noti che il protocollo MPP è un sottoinsieme della funzionalità CPPr e richiede una versione di IOS che supporti tale funzionalità. Per ulteriori informazioni su CPPr, fare riferimento a Descrizione di Control Plane Protection.

Nell'esempio, il protocollo MPP viene usato per limitare l'accesso SNMP e SSH solo all'interfaccia Fast Ethernet 0/0:

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

per ulteriori informazioni, consultare la Management Plane Protection Feature Guide.

Registrazione delle procedure ottimali

La registrazione degli eventi consente di visualizzare il funzionamento di un dispositivo Cisco IOS e la rete in cui è distribuito. Il software Cisco IOS offre diverse opzioni di registrazione flessibili che possono contribuire a raggiungere gli obiettivi di gestione della rete e visibilità di un'organizzazione.

In queste sezioni vengono illustrate alcune best practice di base per la registrazione che possono aiutare gli amministratori a utilizzare correttamente la registrazione, riducendo al minimo l'impatto della registrazione su un dispositivo Cisco IOS.

Invia log a una posizione centrale

Si consiglia di inviare le informazioni di registrazione a un server syslog remoto. Ciò rende possibile correlare e controllare gli eventi di rete e di sicurezza tra i dispositivi di rete in modo più efficace. I messaggi syslog vengono trasmessi in modo non affidabile da UDP e in formato non

crittografato. Per questo motivo, tutte le protezioni offerte da una rete per la gestione del traffico (ad esempio, la crittografia o l'accesso fuori banda) devono essere estese in modo da includere il traffico syslog.

Nell'esempio di configurazione che segue viene configurato un dispositivo Cisco IOS per inviare le informazioni di registrazione a un server syslog remoto:

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

Per ulteriori informazioni sulla correlazione dei log, fare riferimento a Identificazione degli incidenti tramite firewall e eventi syslog del router IOS.

Integrata nella versione 12.4(15)T e originariamente introdotta nella versione 12.0(26)S, la funzione Logging to Local Nonvolatile Storage (ATA Disk) consente di salvare i messaggi di registrazione del sistema su un disco flash ATA (Advanced Technology Attachment). I messaggi salvati su un'unità ATA vengono salvati in modo permanente dopo il riavvio di un router.

Questa configurazione prevede la configurazione di 134.217.728 byte (128 MB) di messaggi di logging nella directory syslog della memoria flash ATA (disk0), specificando una dimensione file di 16.384 byte:

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

Prima di registrare i messaggi scritti su un file sul disco ATA, il software Cisco IOS controlla se lo spazio su disco è sufficiente. In caso contrario, viene eliminato il file meno recente dei messaggi di registrazione (mediante timestamp) e viene salvato il file corrente. Il formato del nome file è **log_month:day:year::time**.

> **Nota:** Un'unità flash ATA ha uno spazio su disco limitato e deve quindi essere mantenuta per evitare la sovrascrittura dei dati archiviati.

Nell'esempio viene mostrato come copiare i messaggi di log dal disco flash ATA del router a un disco esterno sul server FTP 192.168.1.129 come parte delle procedure di manutenzione:

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

Per ulteriori informazioni su questa funzione, fare riferimento a Registrazione su disco ATA (Local Nonvolatile Storage).

Livello di registrazione

A ogni messaggio di log generato da un dispositivo Cisco IOS viene assegnata una delle otto priorità, dal livello 0, Emergenze, al livello 7, Debug. Se non espressamente richiesto, si consiglia di evitare la registrazione al livello 7. La registrazione al livello 7 produce un carico elevato della CPU sul dispositivo che può causare instabilità del dispositivo e della rete.

il comando di configurazione globale **logging trap** level viene usato per specificare quali messaggi di logging devono essere inviati ai server syslog remoti. Il livello specificato indica il messaggio con il livello di gravità più basso inviato. Per la registrazione nel buffer, viene utilizzato il comando

logging buffered level.

In questo esempio di configurazione i messaggi di log inviati ai server syslog remoti e al buffer di log locale vengono limitati ai livelli di gravità da 6 (informazioni) a 0 (emergenze):

```
!

logging trap 6
logging buffered 6
!
```

per ulteriori informazioni, fare riferimento a Risoluzione dei problemi, Gestione degli errori e Registrazione.

Non accedere alle sessioni di console o di monitoraggio

Con il software Cisco IOS, è possibile inviare messaggi di log alle sessioni di monitoraggio - le sessioni di monitoraggio sono sessioni di gestione interattive in cui è stato emesso il comando EXEC **terminal monitor** - e alla console. Tuttavia, questa operazione può aumentare il carico della CPU di un dispositivo IOS e pertanto non è consigliata. Si consiglia invece di inviare le informazioni di registrazione al buffer di registro locale, che può essere visualizzato con il comando **show logging**.

Usare i comandi di configurazione globale **no logging console** e **no logging monitor** per disabilitare la registrazione sulla console e monitorare le sessioni. L'esempio di configurazione mostrato di seguito illustra l'utilizzo dei comandi:

```
!

no logging console
no logging monitor
!
```

Per ulteriori informazioni sui comandi di configurazione globale, consultare la guida di riferimento dei comandi di Cisco IOS Network Management.

Usa registrazione nel buffer

Il software Cisco IOS supporta l'uso di un buffer di registro locale in modo che un amministratore possa visualizzare i messaggi di registro generati localmente. Si consiglia di utilizzare la registrazione nel buffer piuttosto che la registrazione su sessioni console o monitor.

Durante la configurazione della registrazione nel buffer, sono disponibili due opzioni di configurazione: le dimensioni del buffer di registrazione e la gravità dei messaggi archiviati nel buffer. La dimensione del **buffer di registrazione** è configurata con il comando di configurazione globale **logging buffered** size. La severità minima inclusa nel buffer è configurata con il comando logging buffered severity. Gli amministratori possono visualizzare il contenuto del buffer di registrazione tramite il comando **show logging** EXEC.

Questo esempio di configurazione include la configurazione di un buffer di registrazione di 16384 byte e un livello di gravità pari a 6, di tipo informativo, che indica che sono memorizzati messaggi di livello da 0 (emergenze) a 6 (di tipo informativo):

```
!

logging buffered 16384 6
!
```

Per ulteriori informazioni sulla registrazione nel buffer, consultare la guida di riferimento dei comandi di Cisco IOS Network Management.

Configura interfaccia origine di registrazione

Per garantire un livello di coerenza maggiore durante la raccolta e l'analisi dei messaggi di log, è consigliabile configurare in modo statico un'interfaccia di origine di log. Eseguita tramite il comando **log source-interface** interface, la configurazione statica di un'interfaccia di origine di registrazione assicura che lo stesso indirizzo IP venga visualizzato in tutti i messaggi di registrazione inviati da un singolo dispositivo Cisco IOS. Per una maggiore stabilità, si consiglia di utilizzare un'interfaccia di loopback come origine di registrazione.

Questo esempio di configurazione illustra l'utilizzo del comando di configurazione globale **log source-interface** per specificare che l'indirizzo IP dell'interfaccia loopback 0 deve essere utilizzato per tutti i messaggi di log:

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

Per ulteriori informazioni, *consultare* la guida di riferimento dei comandi di Cisco IOS.

Configura timestamp di registrazione

La configurazione della registrazione dei timestamp consente di correlare gli eventi tra i dispositivi di rete. È importante implementare una configurazione di timestamp di registrazione corretta e coerente per garantire la correlazione dei dati di registrazione. I timestamp di registrazione devono essere configurati in modo da includere la data e l'ora con una precisione di millisecondi e includere il fuso orario in uso nel dispositivo.

Questo esempio include la configurazione dei timestamp di registrazione con precisione in millisecondi all'interno della zona UTC (Coordinated Universal Time):

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

Se si preferisce non registrare gli orari relativi all'ora UTC, è possibile configurare un fuso orario locale specifico e configurare le informazioni in modo che siano presenti nei messaggi di registro generati. Nell'esempio viene mostrata una configurazione del dispositivo per l'area PST (Pacific Standard Time):

```
!

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

Gestione configurazione software Cisco IOS

Il software Cisco IOS include diverse funzionalità che possono abilitare una forma di gestione della configurazione su un dispositivo Cisco IOS. Tali funzionalità includono la funzionalità per archiviare le configurazioni e per eseguire il rollback della configurazione a una versione precedente, nonché per creare un registro delle modifiche della configurazione dettagliato.

Sostituzione della configurazione e rollback della configurazione

Nel software Cisco IOS versione 12.3(7)T e successive, le funzionalità di sostituzione e ripristino della configurazione consentono di archiviare la configurazione del dispositivo Cisco IOS sul dispositivo. Memorizzate manualmente o automaticamente, le configurazioni in questo archivio possono essere usate per sostituire la configurazione corrente in esecuzione con il comando **configure replace** filename. a differenza del comando **copy** filename **running-config**. Il comando **configure replace** filename sostituisce la configurazione in esecuzione rispetto all'unione eseguita dal comando **copy**.

Si consiglia di abilitare questa funzione su tutti i dispositivi Cisco IOS della rete. Dopo aver abilitato la funzione, l'amministratore può aggiungere la configurazione corrente in esecuzione all'archivio con il comando **archive config** in modalità di esecuzione privilegiata. Per visualizzare le configurazioni archiviate, usare il comando **show archive** EXEC.

In questo esempio viene illustrata la configurazione dell'archiviazione automatica della configurazione. In questo esempio viene indicato al dispositivo Cisco IOS di archiviare le configurazioni archiviate come file denominati archived-config-N sul disco 0: file system, per mantenere un massimo di 14 backup e per archiviare una volta al giorno (1440 minuti) e quando un amministratore esegue il comando **write memory** EXEC.

```
!

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

Sebbene la funzionalità di archiviazione della configurazione sia in grado di memorizzare fino a 14 configurazioni di backup, si consiglia di considerare i requisiti di spazio prima di utilizzare il comando **maximum**.

Accesso esclusivo alle modifiche alla configurazione

Aggiunta al software Cisco IOS versione 12.3(14)T, la funzione Accesso esclusivo alle modifiche alla configurazione assicura che solo un amministratore apporti modifiche alla configurazione di un dispositivo Cisco IOS alla volta. Questa funzione consente di eliminare l'impatto indesiderato delle modifiche simultanee apportate ai componenti di configurazione correlati. Questa funzione viene configurata con il comando di configurazione globale in **modalità esclusiva** e funziona in una delle due modalità seguenti: automatica e manuale. In modalità automatica, la configurazione si blocca automaticamente quando un amministratore esegue il comando **configure terminal** EXEC. In modalità manuale, l'amministratore utilizza il comando **configure terminal lock** per bloccare la configurazione quando entra in modalità di configurazione.

L'esempio mostra la configurazione di questa funzione per il blocco automatico della configurazione:

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

Configurazione resiliente del software Cisco IOS

Aggiunta nel software Cisco IOS versione 12.3(8)T, la funzionalità di configurazione resiliente permette di archiviare in modo sicuro una copia dell'immagine software e della configurazione del dispositivo Cisco IOS attualmente in uso da un dispositivo Cisco IOS. Quando questa funzionalità è attivata, non è possibile modificare o rimuovere i file di backup. È consigliabile attivare questa caratteristica per impedire tentativi di eliminazione involontari o dannosi dei file.

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

Dopo aver abilitato questa funzione, è possibile ripristinare una configurazione eliminata o un'immagine software Cisco IOS. Per visualizzare lo stato di esecuzione corrente di questa funzione, usare il comando **show secure boot** in modalità di esecuzione.

Software Cisco con firma digitale

Aggiunta nel software Cisco IOS versione 15.0(1)M per i router Cisco serie 1900, 2900 e 3900, la funzionalità software Cisco con firma digitale semplifica l'utilizzo del software Cisco IOS con firma digitale e quindi sicuro, tramite la crittografia asimmetrica protetta (chiave pubblica).

Un'immagine con firma digitale contiene un hash crittografato (con una chiave privata) di se stessa. Una volta effettuato il controllo, il dispositivo decrittografa l'hash con la chiave pubblica corrispondente dalle chiavi che ha nel suo archivio chiavi e calcola anche il proprio hash dell'immagine. Se l'hash decrittografato corrisponde all'hash dell'immagine calcolata, l'immagine non è stata alterata e può essere considerata attendibile.

Le chiavi software Cisco con firma digitale sono identificate dal tipo e dalla versione della chiave. Una chiave può essere di tipo speciale, di produzione o di rollover. Ai tipi di chiave di produzione e speciale è associata una versione di chiave che viene incrementata alfabeticamente ogni volta che la chiave viene revocata e sostituita. Quando si utilizza la funzionalità Software Cisco con firma digitale, le immagini ROMMON e Cisco IOS normali sono entrambe firmate con una chiave speciale o di produzione. L'immagine ROMMON è aggiornabile e deve essere firmata con la stessa chiave dell'immagine speciale o di produzione caricata.

Questo comando verifica l'integrità dell'immagine c3900-universalk9-mz.SSA nella memoria flash con le chiavi nell'archivio chiavi del dispositivo:

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

La funzionalità software Cisco con firma digitale è stata integrata anche in Cisco IOS XE versione 3.1.0.SG per gli switch Cisco Catalyst serie 4500 E.

Per ulteriori informazioni su questa funzione, fare riferimento a Software Cisco con firma digitale.

Nel software Cisco IOS versione 15.1(1)T e successive, è stata introdotta la sostituzione della chiave per il software Cisco con firma digitale. La sostituzione e la revoca della chiave sostituiscono e rimuovono una chiave utilizzata per un controllo del software Cisco con firma

digitale dall'archivio chiavi di una piattaforma. In caso di compromissione della chiave, è possibile revocare solo le chiavi speciali e di produzione.

Una nuova chiave (speciale o di produzione) per un'immagine (speciale o di produzione) viene inserita in un'immagine (di produzione o di revoca) utilizzata per revocare la chiave speciale o di produzione precedente. L'integrità dell'immagine di revoca viene verificata con una chiave di rollover prememorizzata nella piattaforma. La chiave di rollover non cambia. Quando si revoca una chiave di produzione, dopo il caricamento dell'immagine di revoca la nuova chiave viene aggiunta all'archivio chiavi e la chiave precedente corrispondente può essere revocata a condizione che l'immagine ROMMON venga aggiornata e che la nuova immagine di produzione venga avviata. Quando si revoca una chiave speciale, viene caricata un'immagine di produzione. Questa immagine aggiunge la nuova chiave speciale e può revocare la vecchia chiave speciale. Dopo aver aggiornato ROMMON, è possibile avviare la nuova immagine speciale.

In questo esempio viene descritta la revoca di una chiave speciale. Con questi comandi viene aggiunta la nuova chiave speciale all'archivio chiavi dall'immagine di produzione corrente, viene copiata una nuova immagine ROMMON (C3900_rom-monitor.srec.SSB) nell'area di archiviazione (usbflash0:), viene aggiornato il file ROMMON e viene revocata la vecchia chiave speciale:

```
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
```

Una nuova immagine speciale (c3900-universalk9-mz.SSB) può quindi essere copiata sulla memoria flash per essere caricata e la firma dell'immagine viene verificata con la chiave speciale appena aggiunta (SSB):

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

La revoca e la sostituzione delle chiavi non sono supportate sugli switch Catalyst serie 4500 E con software Cisco IOS XE, anche se supportano la funzionalità software Cisco con firma digitale.

Per ulteriori informazioni su questa funzione, *consultare* la sezione Revoca e sostituzione della chiave del software Cisco con firma digitale nella guida al software.

Notifica e registrazione delle modifiche alla configurazione

La funzionalità di notifica e registrazione delle modifiche alla configurazione, aggiunta nel software Cisco IOS versione 12.3(4)T, consente di registrare le modifiche alla configurazione apportate a un dispositivo Cisco IOS. Il registro viene mantenuto sul dispositivo Cisco IOS e contiene le informazioni utente della persona che ha apportato la modifica, il comando di configurazione immesso e l'ora in cui è stata apportata la modifica. Questa funzionalità viene abilitata con il comando **logging enable** configuration logger configuration mode. I comandi opzionali **hidekey** e **logging size** vengono usati per migliorare la configurazione predefinita perché impediscono la registrazione dei dati della password e aumentano la lunghezza del log delle modifiche.

Si consiglia di abilitare questa funzionalità in modo che la cronologia delle modifiche alla configurazione di un dispositivo Cisco IOS possa essere compresa più facilmente. Inoltre, si consiglia di utilizzare il comando **ify syslog** configuration per abilitare la generazione di messaggi syslog quando viene apportata una modifica alla configurazione.

```
!

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

Dopo aver abilitato la funzione Configuration Change Notification and Logging, è possibile usare il comando in modalità di esecuzione privilegiata **show archive log config all** per visualizzare il log di configurazione.

Piano di controllo

Le funzioni del Control Plane sono costituite dai protocolli e dai processi che comunicano tra i dispositivi di rete al fine di spostare i dati dall'origine alla destinazione. Ciò include protocolli di routing come Border Gateway Protocol, nonché protocolli come ICMP e Resource Reservation Protocol (RSVP).

Èimportante che gli eventi nei piani di gestione e di dati non influiscano negativamente sul piano di controllo. Se un evento del piano dati, ad esempio un attacco DoS, influisce sul piano di controllo, l'intera rete può diventare instabile. Queste informazioni sulle funzionalità e sulle configurazioni del software Cisco IOS possono aiutare a garantire la resilienza del control plane.

Protezione avanzata piano di controllo generale

La protezione del control plane di un dispositivo di rete è fondamentale in quanto il control plane garantisce la manutenzione e l'operatività dei piani di gestione e dei dati. Se il control plane dovesse diventare instabile durante un problema di sicurezza, potrebbe essere impossibile ripristinare la stabilità della rete.

In molti casi, è possibile disabilitare la ricezione e la trasmissione di alcuni tipi di messaggi su un'interfaccia per ridurre al minimo la quantità di carico della CPU necessaria per elaborare i pacchetti non necessari.

Reindirizzamenti IP ICMP

Un messaggio di reindirizzamento ICMP può essere generato da un router quando un pacchetto viene ricevuto e trasmesso sulla stessa interfaccia. In questa situazione, il router inoltra il pacchetto e invia un messaggio di reindirizzamento ICMP al mittente del pacchetto originale. Questo comportamento consente al mittente di ignorare il router e inoltrare i pacchetti futuri direttamente alla destinazione (o a un router più vicino alla destinazione). In una rete IP correttamente funzionante, un router invia i reindirizzamenti solo agli host delle proprie subnet locali. In altre parole, i reindirizzamenti ICMP non devono mai oltrepassare un limite di layer 3.

Sono disponibili due tipi di messaggi di reindirizzamento ICMP: reindirizzare un indirizzo host e reindirizzare un'intera subnet. Un utente malintenzionato può sfruttare la capacità del router di inviare reindirizzamenti ICMP inviando continuamente pacchetti al router, che a sua volta è costretto a rispondere con messaggi di reindirizzamento ICMP, con conseguente impatto negativo sulla CPU e sulle prestazioni del router. Per impedire al router di inviare reindirizzamenti ICMP, usare il comando di configurazione dell'interfaccia **no ip redirects**.

Impossibile raggiungere ICMP

L'applicazione di un filtro con un elenco degli accessi all'interfaccia comporta la trasmissione di messaggi ICMP "destinazione irraggiungibile" alla sorgente del traffico filtrato. La generazione di questi messaggi può aumentare l'utilizzo della CPU nel dispositivo. Per impostazione predefinita, nel software Cisco IOS la generazione di pacchetti ICMP "destinazione irraggiungibile" è limitata a un pacchetto ogni 500 millisecondi. La generazione di messaggi ICMP "destinazione irraggiungibile" può essere disabilitata con il comando di configurazione interfaccia **no ip unreachables**. La limitazione della velocità non raggiungibile ICMP può essere modificata dal valore predefinito con il comando di configurazione globale **ip icmp rate-limit unreachable** interval-in-ms.

Proxy ARP

Il proxy ARP è la tecnica con cui un dispositivo, in genere un router, risponde alle richieste ARP destinate a un altro dispositivo. "Falsificando" la propria identità, il router si assume la responsabilità di inoltrare i pacchetti alla destinazione reale. L'ARP proxy consente ai computer di una subnet di raggiungere subnet remote senza configurare il routing o un gateway predefinito. Il proxy ARP è definito nella RFC 1027.

L'utilizzo di ARP proxy presenta diversi svantaggi. Ciò può causare un aumento della quantità di traffico ARP sul segmento di rete, l'esaurimento delle risorse e attacchi man-in-the-middle. ARP proxy presenta un vettore di attacco di esaurimento risorse in quanto ogni richiesta ARP proxy consuma una piccola quantità di memoria. Un utente non autorizzato può esaurire tutta la memoria disponibile se invia un numero elevato di richieste ARP.

Gli attacchi man-in-the-middle consentono a un host sulla rete di eseguire lo spoofing dell'indirizzo MAC del router, con il risultato che gli host non sospettati inviano il traffico all'aggressore. Il proxy ARP può essere disabilitato con il comando di configurazione interfaccia **no ip proxy-arp**.

Per ulteriori informazioni su questa funzione, fare riferimento ad Abilitazione del proxy ARP.

Limitazione dell'impatto della CPU sul traffico del Control Plane

La protezione del control plane è fondamentale. Poiché le prestazioni delle applicazioni e l'esperienza dell'utente finale possono risentire della presenza di traffico di dati e di gestione, la sopravvivenza del control plane garantisce che gli altri due piani siano mantenuti e operativi.

Informazioni sul traffico del Control Plane

Per proteggere correttamente il control plane del dispositivo Cisco IOS, è essenziale comprendere i tipi di traffico a cui viene applicata la commutazione di contesto da parte della CPU. Il traffico di commutazione di processo è in genere composto da due tipi diversi di traffico. Il primo tipo di traffico viene indirizzato al dispositivo Cisco IOS e deve essere gestito direttamente dalla CPU del dispositivo Cisco IOS. Il traffico è costituito dalla categoria *Traffico adiacente alla ricezione*. Questo traffico contiene una voce nella tabella Cisco Express Forwarding (CEF) in cui l'hop del router successivo è il dispositivo stesso, indicato dal termine receive nell'output del comando **show ip cef** CLI. Questa indicazione si riferisce a tutti gli indirizzi IP che richiedono la gestione diretta da parte della CPU del dispositivo Cisco IOS, compresi gli indirizzi IP dell'interfaccia, lo spazio degli indirizzi multicast e lo spazio degli indirizzi di broadcast.

Il secondo tipo di traffico gestito dalla CPU è il traffico del piano dati, ossia il traffico con una destinazione diversa dal dispositivo Cisco IOS stesso, che richiede un'elaborazione speciale da parte della CPU. Sebbene non si tratti di un elenco esaustivo di CPU che hanno un impatto sul traffico del piano dati, questi tipi di traffico sono commutati in base al processo e possono pertanto influire sul funzionamento del piano di controllo:

- **Access Control List logging**: il traffico di registrazione ACL è costituito da qualsiasi pacchetto generato a causa di una corrispondenza (autorizzazione o rifiuto) di una voce ACE su cui viene utilizzata la parola chiave log.

- **Unicast Reverse Path Forwarding (Unicast RPF)** - RPF unicast, utilizzato in combinazione con un ACL, può causare la commutazione di determinati pacchetti.

- **Opzioni IP** - Tutti i pacchetti IP con opzioni incluse devono essere elaborati dalla CPU.

- **Frammentazione**: tutti i pacchetti IP che richiedono la frammentazione devono essere passati alla CPU per essere elaborati.

- **Scadenza TTL (Time-to-Live)**: i pacchetti il cui valore TTL è inferiore o uguale a uno richiedono l'invio di messaggi ICMP (Internet Control Message Protocol Time Exceeded) (ICMP Type 11, Code 0), che determinano l'elaborazione della CPU.

- **ICMP Unreachables**: i pacchetti che generano messaggi ICMP "destinazione irraggiungibile" a causa di routing, MTU o filtro vengono elaborati dalla CPU.

- **Traffico che richiede una richiesta ARP** - Le destinazioni per cui non esiste una voce ARP richiedono l'elaborazione da parte della CPU.

- **Traffico non IP**: tutto il traffico non IP viene elaborato dalla CPU.

In questo elenco vengono illustrati in dettaglio diversi metodi per determinare quali tipi di traffico vengono elaborati dalla CPU del dispositivo Cisco IOS:

- Il comando **show ip cef** restituisce le informazioni dell'hop successivo per ciascun prefisso IP contenuto nella tabella CEF. Come indicato in precedenza, le voci che contengono receive come "hop successivo" vengono considerate adiacenze di ricezione e indicano che il traffico deve essere inviato direttamente alla CPU.

- Il comando **show interface switching** restituisce informazioni sul numero di pacchetti elaborati da un dispositivo.

- Il comando **show ip traffic** fornisce informazioni sul numero di pacchetti IP:

  con una destinazione locale (ovvero, ricevi traffico adiacente)con opzioniche richiedono la frammentazioneinviati allo spazio degli indirizzi di broadcastinviati a uno spazio degli indirizzi multicast

- Il traffico di ricezione adiacente può essere identificato usando il comando **show ip cache flow**. Tutti i flussi destinati al dispositivo Cisco IOS hanno un'interfaccia di destinazione (DstIf)

locale.

- **Control Plane Policing** può essere usato per identificare il tipo e la velocità del traffico che raggiunge il control plane del dispositivo Cisco IOS. Il control plane policing può essere eseguito tramite la classificazione granulare degli ACL, la registrazione e l'uso del comando **show policy-map control-plane**.

ACL di infrastruttura

Gli ACL di infrastruttura (iACL) limitano la comunicazione esterna ai dispositivi della rete. Gli ACL di infrastruttura sono illustrati nella sezione Limitazione dell'accesso alla rete con ACL di infrastruttura di questo documento.

Si consiglia di implementare gli iACL per proteggere il control plane di tutti i dispositivi di rete.

Receive ACL

Per le piattaforme distribuite, l'opzione Receive ACL (ACL ricevuti) può essere usata nel software Cisco IOS versione 12.0(21)S2 per la 12000 (GSR), 12.0(24)S per la 7500 e 12.0(31)S per la 10720. L'ACL riceve il traffico prima che influisca sul processore di routing. I receive ACL sono progettati per proteggere solo il dispositivo su cui sono configurati e il traffico di transito non è influenzato da un rACL. Di conseguenza, l'indirizzo IP di destinazione qualsiasi utilizzato nelle voci ACL di esempio riportate di seguito fa riferimento solo agli indirizzi IP fisici o virtuali del router. I receive ACL sono anche considerati una best practice per la sicurezza della rete e devono essere considerati un'aggiunta a lungo termine alla buona sicurezza della rete.

Questo è l'ACL del percorso di ricezione che è stato scritto per autorizzare il traffico SSH (porta TCP 22) da host attendibili sulla rete 192.168.100.0/24:

```
!
!--- 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
!
```

Per ulteriori informazioni, fare riferimento al documento GSR: receive Access Control List per identificare e autorizzare il traffico legittimo verso un dispositivo e rifiutare tutti i pacchetti indesiderati.

CoPP

La funzione CoPP può essere usata anche per limitare i pacchetti IP destinati al dispositivo dell'infrastruttura. Nell'esempio, solo il traffico SSH proveniente da host attendibili può raggiungere la CPU del dispositivo Cisco IOS.

> **Nota:** Se si elimina il traffico proveniente da indirizzi IP sconosciuti o non attendibili, gli host con indirizzi IP assegnati in modo dinamico non potranno connettersi al dispositivo Cisco IOS.

```
!

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
!
```

Nell'esempio precedente di CoPP, le voci ACL che corrispondono ai pacchetti non autorizzati con l'azione di autorizzazione determinano l'eliminazione di questi pacchetti tramite la funzione di eliminazione della mappa dei criteri, mentre i pacchetti che corrispondono all'azione di negazione non sono interessati dalla funzione di eliminazione della mappa dei criteri.

CoPP è disponibile nei software Cisco IOS versione 12.0S, 12.2SX, 12.2S, 12.3T, 12.4 e 12.4T.

Per ulteriori informazioni sulla configurazione e sull'uso della funzione CoPP, fare riferimento a Distribuzione del Control Plane Policing.

Control Plane Protection

La funzionalità Control Plane Protection (CPPr), introdotta nel software Cisco IOS versione 12.4(4)T, può essere utilizzata per limitare o controllare il traffico aereo destinato alla CPU del dispositivo Cisco IOS. Mentre è simile al CoPP, il CPPr ha la capacità di limitare il traffico con una maggiore granularità. La funzione CPPr divide il piano di controllo aggregato in tre categorie distinte di piani di controllo, note come sottointerfacce. Sono presenti sottointerfacce per le categorie di traffico Host, Transito e CEF-Exception. Inoltre, CPPr include le seguenti funzioni di protezione del control plane:

- **Funzione di filtro delle porte**: questa funzione consente di controllare e rilasciare i pacchetti inviati a porte TCP o UDP chiuse o non in ascolto.
- **Funzione di soglia della coda** - Questa funzione limita il numero di pacchetti per un protocollo

specificato consentiti nella coda di input IP del control plane.

Per ulteriori informazioni sulla configurazione e sull'uso della funzione CPPr, fare riferimento a Control Plane Protection *e* Descrizione di Control Plane Protection (CPPr).

Limitatori di velocità hardware

Cisco Catalyst serie 6500 Supervisor Engine 32 e Supervisor Engine 720 supportano limitatori di velocità basati su hardware specifici per piattaforma, per scenari di rete speciali. Questi limitatori di velocità hardware vengono definiti come limitatori di velocità speciali in quanto coprono un insieme predefinito specifico di scenari IPv4, IPv6, unicast e multicast DoS. I moduli HWRL possono proteggere il dispositivo Cisco IOS da una serie di attacchi che richiedono l'elaborazione dei pacchetti da parte della CPU.

Per impostazione predefinita, sono disponibili diversi HWRL abilitati. Per ulteriori informazioni, fare riferimento a Impostazioni predefinite del limitatore di velocità basato su hardware PFC3.

Per ulteriori informazioni sugli HWRL, fare riferimento a Limitatori di velocità basati su hardware sul PFC3.

Secure BGP

Il Border Gateway Protocol (BGP) è la base di routing di Internet. Di conseguenza, qualsiasi organizzazione con requisiti di connettività più che modesti utilizza spesso BGP. BGP è spesso bersaglio di attacchi da parte di utenti non autorizzati a causa della sua ubiquità e della natura *preconfigurata* delle configurazioni BGP nelle organizzazioni più piccole. Tuttavia, esistono molte funzionalità di sicurezza specifiche di BGP che possono essere utilizzate per aumentare la sicurezza di una configurazione BGP.

Questo documento offre una panoramica delle funzionalità di sicurezza BGP più importanti. Se necessario, vengono forniti suggerimenti per la configurazione.

Protezione basata su TTL

Ogni pacchetto IP contiene un campo da 1 byte noto come TTL (Time to Live). Ogni dispositivo attraversato da un pacchetto IP diminuisce di uno questo valore. Il valore iniziale varia a seconda del sistema operativo e in genere è compreso tra 64 e 255. Un pacchetto viene scartato quando il valore TTL raggiunge zero.

Conosciuto come GTSM (Generalized TTL-based Security Mechanism) e BGP TTL Security Hack (BTSH), un sistema di sicurezza basato su TTL sfrutta il valore TTL dei pacchetti IP per garantire che i pacchetti BGP ricevuti provengano da un peer connesso direttamente. Questa funzionalità richiede spesso il coordinamento da parte dei router peer; tuttavia, una volta abilitato, può completamente sconfiggere molti attacchi basati su TCP contro BGP.

Il protocollo GTSM per BGP è abilitato con l'opzione **ttl-security** per il comando di configurazione del router BGP del **router adiacente**. L'esempio mostra come configurare questa funzione:

```
!

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

```
neighbor <ip-address> ttl-security hops <hop-count>
!
```

Alla ricezione dei pacchetti BGP, il valore TTL viene controllato e deve essere maggiore o uguale a 255 meno il numero di hop specificato.

Autenticazione peer BGP con MD5

L'autenticazione peer con MD5 crea un digest MD5 di ciascun pacchetto inviato come parte di una sessione BGP. In particolare, per generare il digest vengono utilizzate parti delle intestazioni IP e TCP, il payload TCP e una chiave segreta.

Il digest creato viene quindi archiviato nell'opzione TCP Kind 19, creata appositamente a questo scopo dalla RFC 2385 . Il diffusore BGP ricevente usa lo stesso algoritmo e la stessa chiave segreta per rigenerare il digest del messaggio. Se i digest ricevuti e quelli calcolati non sono identici, il pacchetto viene scartato.

L'autenticazione peer con MD5 è configurata con l'opzione **password** per il comando di configurazione del router BGP **adiacente**. L'utilizzo di questo comando è illustrato come segue:

```
!

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

Per ulteriori informazioni sull'autenticazione peer BGP con MD5, fare riferimento a Autenticazione router adiacente.

Configura numero massimo prefissi

I prefissi BGP vengono memorizzati da un router. Maggiore è il numero di prefissi che un router deve contenere, maggiore è la memoria che BGP deve utilizzare. In alcune configurazioni è possibile memorizzare un sottoinsieme di tutti i prefissi Internet, ad esempio in configurazioni che utilizzano solo una route o route predefinite per le reti dei clienti di un provider.

Per evitare l'esaurimento della memoria, è importante configurare il numero massimo di prefissi accettati per peer. È consigliabile configurare un limite per ogni peer BGP.

Quando si configura questa funzionalità con il comando di configurazione del router BGP **maximum-prefix per il router adiacente**, è richiesto un argomento: numero massimo di prefissi accettati prima dell'arresto di un peer. Facoltativamente, è possibile immettere anche un numero compreso tra 1 e 100. Questo numero rappresenta la percentuale del valore massimo dei prefissi in corrispondenza della quale viene inviato un messaggio di log.

```
!

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

Per ulteriori informazioni sui prefissi massimi per peer, fare riferimento a Configurazione della funzione BGP Maximum-Prefix.

Filtra prefissi BGP con elenchi di prefissi

Gli elenchi di prefissi consentono a un amministratore di rete di autorizzare o negare prefissi specifici inviati o ricevuti tramite BGP. Ove possibile, è opportuno utilizzare gli elenchi di prefissi per garantire l'invio del traffico di rete sui percorsi previsti. Gli elenchi di prefissi devono essere applicati a ogni peer eBGP in entrambe le direzioni in entrata e in uscita.

Gli elenchi di prefissi configurati limitano i prefissi inviati o ricevuti a quelli specificamente consentiti dai criteri di routing di una rete. Se ciò non è possibile a causa dell'elevato numero di prefissi ricevuti, è necessario configurare un elenco di prefissi per bloccare in modo specifico i prefissi noti non validi. Questi prefissi noti non validi includono lo spazio degli indirizzi IP non allocato e le reti riservate per scopi interni o di test dalla RFC 3330. Gli elenchi di prefissi in uscita devono essere configurati in modo da consentire specificamente solo i prefissi che un'organizzazione intende annunciare.

In questo esempio di configurazione vengono utilizzati elenchi di prefissi per limitare le route apprese e annunciate. In particolare, solo una route predefinita è consentita in entrata dall'elenco di prefissi BGP-PL-INBOUND e il prefisso 192.168.2.0/24 è l'unica route che può essere annunciata da BGP-PL-OUTBOUND.

```
!

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

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

Per una descrizione completa del filtro dei prefissi BGP, consultare il documento sulla connessione a un provider di servizi tramite BGP esterno.

Filtrare i prefissi BGP con elenchi degli accessi ai percorsi di sistema autonomi

Gli elenchi degli accessi al percorso del sistema autonomo BGP (AS) consentono all'utente di filtrare i prefissi ricevuti e annunciati in base all'attributo AS-path di un prefisso. Questa funzione può essere utilizzata in combinazione con gli elenchi di prefissi per stabilire una serie di filtri solida.

In questo esempio di configurazione vengono utilizzati gli elenchi di accesso ai percorsi AS per limitare i prefissi in ingresso a quelli originati dai prefissi in uscita e AS remoti a quelli originati dal sistema autonomo locale. I prefissi originati da tutti gli altri sistemi autonomi vengono filtrati e non installati nella tabella di routing.

```
!

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
!
```

Protocolli gateway interni sicuri

La capacità di una rete di inoltrare correttamente il traffico e di ripristinare il sistema in seguito a modifiche o errori della topologia dipende da una vista accurata della topologia. Per ottenere questa vista, è spesso possibile eseguire un IGP (Interior Gateway Protocol). Per impostazione predefinita, gli IGP sono dinamici e rilevano router aggiuntivi che comunicano con il particolare IGP in uso. Gli IGP individuano inoltre le route che possono essere utilizzate in caso di errore del collegamento di rete.

Queste sottosezioni forniscono una panoramica delle principali funzioni di sicurezza IGP. Se necessario, vengono forniti suggerimenti ed esempi relativi a Routing Information Protocol versione 2 (RIPv2), Enhanced Interior Gateway Routing Protocol (EIGRP) e Open Shortest Path First (OSPF).

Autenticazione e verifica del protocollo di routing con Message Digest 5

La mancata protezione dello scambio di informazioni di routing consente all'utente malintenzionato di introdurre informazioni di routing false nella rete. L'autenticazione tramite password e i protocolli di routing tra router consentono di migliorare la sicurezza della rete. Tuttavia, poiché l'autenticazione viene inviata come testo non crittografato, per un utente non autorizzato può essere semplice sovvertire questo controllo di sicurezza.

Aggiungendo funzionalità hash MD5 al processo di autenticazione, gli aggiornamenti di routing non contengono più password non crittografate e l'intero contenuto dell'aggiornamento di routing è più resistente alle manomissioni. Tuttavia, l'autenticazione MD5 è ancora soggetta ad attacchi di forza bruta e dizionario se vengono scelte password deboli. Si consiglia di utilizzare password con una casualità sufficiente. Poiché l'autenticazione MD5 è molto più sicura rispetto all'autenticazione tramite password, questi esempi sono specifici dell'autenticazione MD5. IPSec può essere utilizzato anche per convalidare e proteggere i protocolli di routing, ma in questi esempi non viene descritto in dettaglio l'utilizzo di IPSec.

EIGRP e RIPv2 utilizzano le catene di chiavi come parte della configurazione. Per ulteriori informazioni sulla configurazione e sull'uso delle catene di chiavi, consultare il documento key.

Questa è una configurazione di esempio per l'autenticazione del router EIGRP con 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>
!
```

Questo è un esempio di configurazione dell'autenticazione router MD5 per RIPv2. RIPv1 non supporta l'autenticazione.

```
!

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

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

Si tratta di una configurazione di esempio per l'autenticazione del router OSPF con MD5. OSPF non utilizza le catene di chiavi.

```
!

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
!
```

Per ulteriori informazioni, fare riferimento a Configurazione di OSPF.

Comandi dell'interfaccia passiva

Le perdite di informazioni, o l'introduzione di informazioni false in un IGP, possono essere mitigate utilizzando il comando **dell'interfaccia passiva** che aiuta a controllare la pubblicità delle informazioni di routing. Si consiglia di non annunciare alcuna informazione alle reti che non sono soggette al controllo amministrativo.

Nell'esempio viene mostrato come usare questa funzione:

```
!

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

Filtro di indirizzamento

Per ridurre la possibilità di introdurre informazioni di routing false nella rete, è necessario utilizzare il filtro di routing. A differenza del comando di configurazione del router dell'interfaccia **passiva**, il routing si verifica sulle interfacce quando il filtro di routing è abilitato, ma le informazioni annunciate o elaborate sono limitate.

Per EIGRP e RIP, l'uso del comando **distribute-list** con la parola chiave **out** limita le informazioni annunciate, mentre l'uso della parola chiave **in** limita gli aggiornamenti elaborati. Il comando **distribute-list** è disponibile per OSPF, ma non impedisce a un router di propagare le route filtrate. È possibile usare al suo posto il comando **area filter-list**.

Nell'esempio del protocollo EIGRP, gli annunci in uscita vengono filtrati con il comando **distribute-list** e un elenco di prefissi:

```
!

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>
!
```

Nell'esempio seguente il protocollo EIGRP filtra gli aggiornamenti in ingresso con un elenco di prefissi:

```
!

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>
!
```

Per ulteriori informazioni su come controllare la pubblicità e l'elaborazione degli aggiornamenti del routing, consultare il documento sulla configurazione delle funzioni indipendenti dal protocollo di routing IP.

Nell'esempio di OSPF che segue viene utilizzato un elenco di prefissi con il comando **area filter-list** specifico per OSPF:

```
!

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

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

Consumo risorse processo ciclo

I prefissi del protocollo di routing vengono memorizzati da un router e il consumo delle risorse aumenta con l'aggiunta di prefissi che un router deve conservare. Per evitare l'esaurimento delle risorse, è importante configurare il protocollo di routing in modo da limitare l'utilizzo delle risorse. Ciò è possibile con OSPF se si utilizza la funzione di protezione dall'overload del database dello stato del collegamento.

In questo esempio viene illustrata la configurazione della funzione di protezione dall'overload del database dello stato del collegamento OSPF:

```
!
```

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

Per ulteriori informazioni sulla protezione dall'overload del database dello stato del collegamento OSPF, fare riferimento a Limitazione del numero di LSA autogeneranti per un processo OSPF.

Protocolli di ridondanza Secure First Hop

I protocolli di ridondanza First Hop (FHRP) forniscono resilienza e ridondanza per i dispositivi che fungono da gateway predefiniti. Questa situazione e questi protocolli sono comuni in ambienti in cui una coppia di dispositivi di layer 3 fornisce la funzionalità gateway predefinita per un segmento di rete o un set di VLAN che contengono server o workstation.

Il protocollo GLBP (Gateway Load-Balancing Protocol), il protocollo HSRP (Hot Standby Router Protocol) e il protocollo VRRP (Virtual Router Redundancy Protocol) sono tutti protocolli FHRP. Per impostazione predefinita, questi protocolli comunicano con comunicazioni non autenticate. Questo tipo di comunicazione può consentire a un utente non autorizzato di presentarsi come dispositivo che parla FHRP per assumere il ruolo di gateway predefinito nella rete. Questa acquisizione permetterebbe all'aggressore di eseguire un attacco man-in-the-middle e di intercettare tutto il traffico utente che esce dalla rete.

Per prevenire questo tipo di attacchi, tutti gli FHRP supportati dal software Cisco IOS includono una funzionalità di autenticazione con MD5 o stringhe di testo. A causa della minaccia rappresentata da FHRP non autenticati, è consigliabile che le istanze di questi protocolli utilizzino l'autenticazione MD5. In questo esempio di configurazione viene illustrato l'utilizzo dell'autenticazione GLBP, HSRP e VRRP MD5:

```
!

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
!
```

Piano dati

Sebbene il piano dati sia responsabile dello spostamento dei dati dall'origine alla destinazione, nel contesto della sicurezza, il piano dati è il meno importante dei tre piani. È per questo motivo che è importante proteggere i piani di gestione e di controllo di preferenza rispetto al piano dati quando si protegge un dispositivo di rete .

Tuttavia, all'interno dello stesso piano dati, ci sono molte funzionalità e opzioni di configurazione che possono aiutare a proteggere il traffico. Le sezioni seguenti descrivono in dettaglio le funzionalità e le opzioni disponibili, consentendo di proteggere più facilmente la rete.

Protezione avanzata piano dati generale

La grande maggioranza dei flussi di traffico dei data plane attraverso la rete come determinato dalla configurazione di routing della rete. Tuttavia, la funzionalità di rete IP permette di modificare il percorso dei pacchetti sulla rete. Caratteristiche come le opzioni IP, in particolare l'opzione di routing dell'origine, costituiscono una sfida per la sicurezza delle reti moderne.

L'uso degli ACL transit è anche importante per la protezione del piano dati.

Per ulteriori informazioni, *vedere* la sezione Filtro del traffico di transito con ACL transit di questo documento.

Caduta selettiva opzioni IP

Le opzioni IP pongono due problemi di sicurezza. Il traffico che contiene opzioni IP deve essere commutato in base al processo dai dispositivi Cisco IOS, il che può portare a un carico elevato della CPU. Le opzioni IP includono anche la funzionalità di modifica del percorso del traffico sulla rete, che potenzialmente consente di sovvertire i controlli di sicurezza.

Per risolvere queste criticità, usare il comando di configurazione globale **ip options {drop | ignore}** è stato aggiunto al software Cisco IOS versione 12.3(4)T, 12.0(22)S e 12.2(25)S. Nella prima forma di questo comando, **ip options drop**, tutti i pacchetti IP che contengono opzioni IP ricevute dal dispositivo Cisco IOS vengono scartati. In questo modo si evita sia il carico elevato della CPU che la possibile sovversione dei controlli di sicurezza che le opzioni IP possono attivare.

La seconda forma di questo comando, **ip options ignore**, configura il dispositivo Cisco IOS in modo da ignorare le opzioni IP contenute nei pacchetti ricevuti. Anche se in questo modo si riducono le minacce relative alle opzioni IP per il dispositivo locale, è possibile che la presenza di opzioni IP possa influire sui dispositivi downstream. Per questo motivo, si consiglia di **eliminare** la forma di questo comando. Questa condizione viene dimostrata nell'esempio di configurazione:

```
!
ip options drop
!
```

Si noti che alcuni protocolli, ad esempio l'RSVP, utilizzano in modo legittimo le opzioni IP. Questo comando influisce sulle funzionalità di questi protocolli.

Dopo aver abilitato la funzione IP Options Selective Drop, è possibile usare il comando **show ip traffic** EXEC per determinare il numero di pacchetti ignorati a causa della presenza delle opzioni IP. Queste informazioni sono presenti nel contatore di rilascio forzato.

Per ulteriori informazioni su questa funzione, fare riferimento a ACL IP Options Selective Drop.

Disabilita routing origine IP

Il routing dell'origine IP sfrutta le opzioni Loose Source Route e Record Route in tandem o Strict Source Route insieme all'opzione Record Route per consentire all'origine del datagramma IP di

specificare il percorso di rete di un pacchetto. Questa funzionalità può essere utilizzata nei tentativi di indirizzare il traffico attorno ai controlli di sicurezza nella rete.

Se le opzioni IP non sono state disabilitate completamente tramite la funzione di eliminazione selettiva delle opzioni IP, è importante che il routing della sorgente IP sia disabilitato. Il routing della sorgente IP, abilitato per impostazione predefinita in tutte le versioni del software Cisco IOS, è disabilitato con il comando di configurazione globale **no ip source-route**. Nell'esempio di configurazione viene mostrato come usare questo comando:

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

Disabilita reindirizzamenti ICMP

I reindirizzamenti ICMP vengono usati per informare un dispositivo di rete di un percorso migliore verso una destinazione IP. Per impostazione predefinita, il software Cisco IOS invia un reindirizzamento se riceve un pacchetto che deve essere instradato tramite l'interfaccia che ha ricevuto.

In alcune situazioni, è possibile che un utente non autorizzato faccia in modo che il dispositivo Cisco IOS invii molti messaggi di reindirizzamento ICMP, con un conseguente carico della CPU elevato. Per questo motivo, si consiglia di disabilitare la trasmissione dei reindirizzamenti ICMP. I reindirizzamenti ICMP vengono disabilitati con il comando **no ip redirects** della configurazione dell'interfaccia, come mostrato nell'esempio di configurazione:

```
!

interface FastEthernet 0
no ip redirects
!
```

Disabilitare o limitare le trasmissioni dirette IP

Le trasmissioni dirette IP consentono di inviare un pacchetto di trasmissione IP a una subnet IP remota. Una volta raggiunta la rete remota, il dispositivo IP di inoltro invia il pacchetto come trasmissione di layer 2 a tutte le stazioni della subnet. Questa funzionalità di trasmissione diretta è stata utilizzata come un aiuto per l'amplificazione e la riflessione in diversi attacchi, tra cui l'attacco del mirino.

Nelle versioni correnti del software Cisco IOS, questa funzionalità è disabilitata per impostazione predefinita; tuttavia, può essere abilitata con il comando di configurazione **ip direct-broadcast** interface. Nelle versioni precedenti alla 12.0, questa funzionalità è abilitata per impostazione predefinita.

Se una rete richiede assolutamente una funzionalità di trasmissione diretta, il suo utilizzo deve essere controllato. A tal fine, è possibile usare un elenco di controllo degli accessi come opzione del comando **ip direct-broadcast**. Questo esempio di configurazione limita le trasmissioni dirette ai pacchetti UDP provenienti da una rete attendibile, 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
!
```

Filtra il traffico di transito con ACL transit

Èpossibile controllare il traffico che attraversa la rete utilizzando gli ACL di transito (tACL). In questo modo, la differenza con gli ACL dell'infrastruttura che cercano di filtrare il traffico destinato alla rete stessa. Il filtro fornito dagli elenchi ACL è utile quando è opportuno filtrare il traffico diretto a un particolare gruppo di dispositivi o il traffico che attraversa la rete.

Questo tipo di filtraggio viene in genere eseguito dai firewall. Tuttavia, in alcuni casi può essere utile eseguire il filtro su un dispositivo Cisco IOS della rete, ad esempio quando è necessario eseguire il filtro ma non è presente alcun firewall.

Gli ACL transit sono anche una postazione appropriata in cui implementare le protezioni statiche anti-spoofing.

Per ulteriori informazioni, *vedere* la sezione Protezione da spoofing di questo documento.

Per ulteriori informazioni, fare riferimento al documento Access Control List transit: filtraggio sul perimetro della rete.

Filtro pacchetti ICMP

Il protocollo ICMP (Internet Control Message Protocol) è stato progettato come protocollo di controllo per IP. Di conseguenza, i messaggi trasmessi possono avere implicazioni di vasta portata sui protocolli TCP e IP in generale. Il protocollo ICMP viene utilizzato dagli strumenti di risoluzione dei problemi di rete **ping** e **traceroute**, nonché dal rilevamento dell'MTU del percorso; tuttavia, la connettività ICMP esterna è raramente necessaria per il corretto funzionamento di una rete.

Il software Cisco IOS offre la funzionalità per filtrare specificamente i messaggi ICMP per nome o tipo e codice. Nell'esempio, l'ACL permette l'ICMP da reti attendibili e blocca tutti i pacchetti ICMP da altre origini:

```
!

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
!
```

Filtra frammenti IP

Come spiegato in precedenza nella sezione Limitazione dell'accesso alla rete con ACL di infrastruttura in questo documento, il filtro dei pacchetti IP frammentati può rappresentare una sfida per i dispositivi di sicurezza.

A causa della natura non intuitiva della gestione dei frammenti, i frammenti IP sono spesso autorizzati inavvertitamente dagli ACL. La frammentazione è spesso utilizzata anche per tentare di eludere il rilevamento con sistemi di rilevamento delle intrusioni. Per questi motivi, i frammenti IP vengono spesso utilizzati negli attacchi e devono essere filtrati in modo esplicito all'inizio di qualsiasi ACL configurato. L'ACL seguente include un filtro completo dei frammenti IP. Le funzionalità illustrate in questo esempio devono essere utilizzate insieme a quelle degli esempi precedenti:

```
!

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
!
```

Per ulteriori informazioni sulla gestione degli ACL di pacchetti IP frammentati, consultare il documento Access Control Lists and IP Fragments.

Supporto ACL per filtro opzioni IP

Nel software Cisco IOS versione 12.3(4)T e successive, il software Cisco IOS supporta l'uso degli ACL per filtrare i pacchetti IP in base alle opzioni IP contenute nel pacchetto. La presenza di opzioni IP all'interno di un pacchetto può indicare un tentativo di sovvertire i controlli di sicurezza nella rete o alterare in altro modo le caratteristiche di transito di un pacchetto. Per questi motivi, i pacchetti con opzioni IP devono essere filtrati al margine della rete.

Questo esempio deve essere utilizzato con il contenuto degli esempi precedenti per includere il filtro completo dei pacchetti IP che contengono le opzioni IP:

```
!

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

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

Protezione da spoofing

Molti attacchi utilizzano lo spoofing degli indirizzi IP di origine per essere efficaci o per nascondere la vera origine di un attacco e ostacolare un traceback accurato. Il software Cisco IOS fornisce RPF unicast e IP Source Guard (IPSG) per scoraggiare attacchi che si basano sullo spoofing degli

indirizzi IP di origine. Inoltre, gli ACL e il routing nullo sono spesso implementati come mezzo manuale per prevenire lo spoofing.

IP Source Guard opera per ridurre al minimo lo spoofing delle reti sotto controllo amministrativo diretto, eseguendo la verifica della porta dello switch, dell'indirizzo MAC e dell'indirizzo di origine. Unicast RPF fornisce la verifica della rete di origine e consente di ridurre gli attacchi di tipo spoofing da reti non sottoposte a controllo amministrativo diretto. La sicurezza delle porte può essere utilizzata per convalidare gli indirizzi MAC al livello di accesso. L'ispezione DAI (Dynamic Address Resolution Protocol) riduce i vettori di attacco che utilizzano l'avvelenamento ARP sui segmenti locali.

RPF unicast

Unicast RPF consente a un dispositivo di verificare che l'indirizzo di origine di un pacchetto inoltrato possa essere raggiunto tramite l'interfaccia che ha ricevuto il pacchetto. Non è possibile fare affidamento su RPF unicast come unica protezione contro lo spoofing. I pacchetti oggetto di spoofing potrebbero entrare nella rete tramite un'interfaccia Unicast abilitata per RPF se esiste una route di ritorno appropriata all'indirizzo IP di origine. Unicast RPF si basa sull'utente per abilitare Cisco Express Forwarding su ciascun dispositivo ed è configurato per singola interfaccia.

Unicast RPF può essere configurato in una di due modalità: sciolto o rigido. Nei casi in cui è presente il routing asimmetrico, si preferisce la modalità "libero" perché è noto che la modalità rigorosa causa il rifiuto dei pacchetti in queste situazioni. Durante la configurazione del comando di configurazione dell'interfaccia **ip verify**, la parola chiave **any** configura la modalità libero, mentre la parola chiave **rx** configura la modalità rigorosa.

L'esempio mostra come configurare questa funzione:

```
!

ip cef
!

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

Per ulteriori informazioni sulla configurazione e l'utilizzo di RPF unicast, fare riferimento a Descrizione di Unicast Reverse Path Forwarding.

Protezione origine IP

IP Source Guard è un mezzo efficace per prevenire lo spoofing che può essere utilizzato se si ha controllo sulle interfacce di layer 2. IP Source Guard utilizza le informazioni dello snooping DHCP per configurare in modo dinamico un elenco di controllo di accesso (PACL) delle porte sull'interfaccia di layer 2, impedendo qualsiasi traffico proveniente da indirizzi IP non associati nella tabella di binding dell'origine IP.

IP Source Guard può essere applicato alle interfacce di layer 2 che appartengono alle VLAN abilitate per lo snooping DHCP. Questi comandi abilitano lo snooping DHCP:

```
!
```

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

Dopo aver abilitato lo snooping DHCP, questi comandi abilitano IPSG:

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

La sicurezza delle porte può essere abilitata con il comando di configurazione dell'interfaccia di **sicurezza porta di origine ip verify**. A tal fine, è necessario usare il comando di configurazione globale **ip dhcp snooping information option**; inoltre, il server DHCP deve supportare l'opzione DHCP 82.

Per ulteriori informazioni su questa funzione, fare riferimento a Configurazione delle funzionalità DHCP e IP Source Guard.

Sicurezza porta

La funzione di sicurezza delle porte viene usata per ridurre lo spoofing degli indirizzi MAC sull'interfaccia di accesso. La sicurezza delle porte può utilizzare indirizzi MAC appresi in modo dinamico (permanenti) per semplificare la configurazione iniziale. Una volta che la sicurezza delle porte ha determinato una violazione MAC, può utilizzare una delle quattro modalità di violazione. Queste modalità sono la protezione, la limitazione, l'arresto e la disattivazione della VLAN. Nei casi in cui una porta fornisce l'accesso a una sola workstation utilizzando protocolli standard, può essere sufficiente un numero massimo di una porta. I protocolli che utilizzano indirizzi MAC virtuali, ad esempio HSRP, non funzionano quando il numero massimo è impostato su uno.

```
!

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>
!
```

Per ulteriori informazioni sulla configurazione della sicurezza delle porte, consultare il documento sulla configurazione della sicurezza delle porte.

Ispezione ARP dinamica

La DAI (Dynamic ARP Inspection) può essere utilizzata per mitigare gli attacchi di avvelenamento ARP sui segmenti locali. Un attacco avvelenamento ARP è un metodo in cui un attaccante invia informazioni ARP falsificate ad un segmento locale. Queste informazioni sono state progettate per danneggiare la cache ARP di altri dispositivi. Spesso un aggressore usa l'avvelenamento ARP per eseguire un attacco man-in-the-middle.

DAI intercetta e convalida la relazione tra indirizzi IP e MAC di tutti i pacchetti ARP su porte non attendibili. Negli ambienti DHCP, DAI utilizza i dati generati dalla funzionalità di snooping DHCP. I pacchetti ARP ricevuti su interfacce attendibili non vengono convalidati e i pacchetti non validi su

interfacce non attendibili vengono ignorati. In ambienti non DHCP, è necessario usare ACL ARP.

Questi comandi abilitano lo snooping DHCP:

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

Dopo aver abilitato lo snooping DHCP, questi comandi abilitano DAI:

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

Negli ambienti non DHCP, per abilitare DAI sono necessari ACL ARP. Nell'esempio viene mostrata la configurazione di base di DAI con ACL ARP:

```
!

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

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

Èinoltre possibile abilitare DAi per singola interfaccia, se supportato.

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

Per ulteriori informazioni su come configurare DAI, fare riferimento a Configurazione dell'ispezione ARP dinamica.

ACL anti-spoofing

Gli ACL configurati manualmente possono fornire una protezione anti-spoofing statica contro gli attacchi che usano spazio degli indirizzi noto, non usato o non attendibile. In genere, questi ACL anti-spoofing vengono applicati al traffico in entrata ai limiti della rete come componente di un ACL più grande. Gli ACL anti-spoofing richiedono un monitoraggio regolare in quanto possono essere modificati frequentemente. È possibile ridurre al minimo lo spoofing nel traffico proveniente dalla rete locale se si applicano ACL in uscita che limitano il traffico a indirizzi locali validi.

Nell'esempio viene mostrato come usare gli ACL per limitare lo spoofing IP. Questo ACL viene applicato in entrata sull'interfaccia desiderata. Gli ACE che costituiscono questo ACL non sono completi. Se si configurano questi tipi di ACL, cercare un riferimento aggiornato e completo.

```
!

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
!
```

Per ulteriori informazioni su come configurare gli Access Control List, consultare il documento sulla configurazione degli ACL IP di uso comune.

L'elenco ufficiale degli indirizzi Internet non assegnati è gestito dal Team Cymru. Per ulteriori informazioni sul filtro degli indirizzi inutilizzati, consultare la pagina di riferimento di Bogon .

Limita impatto CPU del traffico del piano dati

Lo scopo principale dei router e degli switch è inoltrare i pacchetti e i frame attraverso il dispositivo alle destinazioni finali. Questi pacchetti, che attraversano i dispositivi distribuiti in tutta la rete, possono influire sulle operazioni della CPU di un dispositivo. Il piano dati, costituito dal traffico che attraversa il dispositivo di rete, deve essere protetto per garantire il funzionamento dei piani di gestione e di controllo. Se il traffico di transito può causare l'elaborazione del traffico di commutazione da parte di un dispositivo, è possibile che il piano di controllo di un dispositivo ne subisca le conseguenze, con conseguenti interruzioni operative.

Funzioni e tipi di traffico che influiscono sulla CPU

Sebbene non esaustivo, questo elenco include i tipi di traffico del piano dati che richiedono un'elaborazione speciale della CPU e sono commutati dal processo da parte della CPU:

- **Registrazione ACL**: il traffico di registrazione ACL è costituito da qualsiasi pacchetto generato a causa di una corrispondenza (autorizzazione o negazione) di una voce ACE in cui viene utilizzata la parola chiave **log**.
- **RPF unicast** - RPF unicast utilizzato in combinazione con un ACL potrebbe causare la commutazione di processo di alcuni pacchetti.
- **Opzioni IP** - Tutti i pacchetti IP con opzioni incluse devono essere elaborati dalla CPU.
- **Frammentazione**: tutti i pacchetti IP che richiedono la frammentazione devono essere passati alla CPU per essere elaborati.
- **Time-to-Live (TTL) Expiry**: i pacchetti il cui valore TTL è minore o uguale a 1 richiedono l'invio di messaggi ICMP (Internet Control Message Protocol Time Exceeded) (ICMP Type 11, Code 0), che danno luogo all'elaborazione della CPU.
- **ICMP Unreachables**: i pacchetti che causano messaggi ICMP "destinazione irraggiungibile" a causa di routing, MTU o filtro, vengono elaborati dalla CPU.
- **Traffico che richiede una richiesta ARP** - Le destinazioni per cui non esiste una voce ARP richiedono l'elaborazione da parte della CPU.
- **Traffico non IP**: tutto il traffico non IP viene elaborato dalla CPU.

Per ulteriori informazioni sulla protezione avanzata del piano dati, *vedere* la sezione Protezione avanzata del piano dati in questo documento.

Filtra in base al valore TTL

Èpossibile usare la funzione di supporto ACL per il filtro sul valore TTL, introdotta nel software Cisco IOS versione 12.4(2)T, in un elenco di accessi IP esteso per filtrare i pacchetti in base al valore TTL. Questa funzione può essere utilizzata per proteggere un dispositivo che riceve il traffico di transito il cui valore TTL è zero o uno. È possibile anche filtrare i pacchetti in base ai valori TTL in modo da garantire che il valore TTL non sia inferiore al diametro della rete, proteggendo così il control plane dei dispositivi dell'infrastruttura a valle dagli attacchi TTL in scadenza.

Alcune applicazioni e strumenti, ad esempio **traceroute,** usano i pacchetti TTL in scadenza a scopo di test e diagnostica. Alcuni protocolli, ad esempio IGMP, utilizzano legittimamente il valore TTL 1.

Nell'esempio, questo ACL crea un criterio che filtra i pacchetti IP quando il valore TTL è inferiore a 6.

```
!
!--- 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
!
```

Per ulteriori informazioni sul filtro dei pacchetti basato sul valore TTL, consultare il documento sull'identificazione e mitigazione degli attacchi TTL.

Per ulteriori informazioni su questa funzione, fare riferimento al supporto ACL per il filtro sul valore TTL.

Nel software Cisco IOS versione 12.4(4)T e successive, il protocollo FPM (Flexible Packet Matching) consente agli amministratori di effettuare corrispondenze su bit arbitrari di un pacchetto. Questo criterio FPM elimina i pacchetti con un valore TTL inferiore a sei.

```
!

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
!
```

Per ulteriori informazioni su questa funzione, consultare il documento Flexible Packet Matching, *disponibile nella home page di* Cisco IOS Flexible Packet Matching.

Filtra in base alla presenza di opzioni IP

Nel software Cisco IOS versione 12.3(4)T e successive, è possibile usare il supporto ACL per la funzionalità Filtering IP Options (Opzioni IP filtro) in un elenco di accessi IP esteso con nome per filtrare i pacchetti IP con opzioni IP presenti. È possibile anche filtrare i pacchetti IP basati sulla presenza di opzioni IP per evitare che il control plane dei dispositivi dell'infrastruttura debba elaborare questi pacchetti a livello di CPU.

Il supporto ACL per il filtro delle opzioni IP può essere usato solo con ACL estesi con nome. Si noti inoltre che RSVP, Multiprotocol Label Switching Traffic Engineering, IGMP versioni 2 e 3 e altri protocolli che utilizzano pacchetti con opzioni IP potrebbero non funzionare correttamente se i pacchetti di questi protocolli vengono scartati. Se questi protocolli sono in uso nella rete, è possibile usare il supporto ACL per il filtro delle opzioni IP; tuttavia, la funzionalità ACL IP Options Selective Drop potrebbe causare il rifiuto del traffico e i protocolli potrebbero non funzionare correttamente. Se non sono in uso protocolli che richiedono opzioni IP, il metodo preferibile per eliminare questi pacchetti è ACL IP Options Selective Drop.

Nell'esempio di ACL viene creato un criterio che filtra i pacchetti IP che contengono opzioni IP:

```
!

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 questo esempio viene mostrato un ACL che filtra i pacchetti IP con cinque opzioni IP specifiche. I pacchetti contenenti queste opzioni vengono rifiutati:

- 0 Fine elenco opzioni (eool)
- 7 Record Route (record-route)
- Timestamp 68 (timestamp)
- 131 - Loose Source Route (lsr)
- 137 - SSR (Strict Source Route)

```
!

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
!
```

Per ulteriori informazioni sulla rimozione selettiva delle opzioni IP degli ACL, *vedere* la sezione Protezione avanzata del piano dati generale di questo documento.

Per ulteriori informazioni, fare riferimento al documento Access Control List transit: filtraggio sul perimetro della rete per ulteriori informazioni sul filtraggio del traffico di transito e sui perimetro della rete.

Un'altra funzionalità del software Cisco IOS che può essere utilizzata per filtrare i pacchetti con opzioni IP è CoPP. Nel software Cisco IOS versione 12.3(4)T e successive, il protocollo CoPP consente agli amministratori di filtrare il flusso del traffico dei pacchetti del control plane. Un dispositivo che supporta CoPP e ACL per il filtro delle opzioni IP, introdotto nel software Cisco IOS versione 12.3(4)T, può usare un criterio dell'elenco degli accessi per filtrare i pacchetti che contengono opzioni IP.

Questo criterio CoPP ignora i pacchetti di transito ricevuti da un dispositivo quando sono presenti opzioni IP:

```
!

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
!
```

Il criterio CoPP ignora i pacchetti di transito ricevuti da un dispositivo quando sono presenti le seguenti opzioni IP:

- 0 Fine elenco opzioni (eool)
- 7 Record Route (record-route)
- Timestamp 68 (timestamp)
- 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
!
```

Nei criteri CoPP precedenti, le voci dell'elenco di controllo di accesso (ACE, Access Control List) che corrispondono ai pacchetti con l'azione di autorizzazione determinano lo scarto di questi pacchetti da parte della funzione di eliminazione della mappa dei criteri, mentre i pacchetti che corrispondono all'azione di negazione (non visualizzata) non sono interessati dalla funzione di eliminazione della mappa dei criteri.

Per ulteriori informazioni sulla funzionalità CoPP, fare riferimento a Distribuzione di Control Plane Policing.

Control Plane Protection

Nel software Cisco IOS versione 12.4(4)T e successive, la protezione del piano di controllo (CPPr) può essere utilizzata per limitare o controllare il traffico del piano di controllo da parte della CPU di un dispositivo Cisco IOS. Anche se simile al CoPP, il CPPr ha la capacità di limitare o controllare il traffico usando una granularità più fine rispetto al CoPP. La funzione CPPr divide il piano di controllo aggregato in tre categorie distinte di piani di controllo, note come sottointerfacce: Esistono sottointerfacce host, transit e CEF-Exception.

Il criterio CPPr rifiuta i pacchetti in transito ricevuti da un dispositivo il cui valore TTL è inferiore a 6 e i pacchetti in transito o non in transito ricevuti da un dispositivo il cui valore TTL è zero o uno. Il criterio CPPr ignora anche i pacchetti con opzioni IP selezionate ricevuti dal dispositivo.

```
!

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
!
```

Nel criterio CPPr precedente, le voci dell'elenco di controllo di accesso che corrispondono ai pacchetti con l'azione di autorizzazione determinano l'eliminazione di questi pacchetti tramite la funzione di eliminazione della mappa dei criteri, mentre i pacchetti che corrispondono all'azione di negazione (non visualizzata) non sono interessati dalla funzione di eliminazione della mappa dei criteri.

Per ulteriori informazioni sulla funzione CPPr, fare riferimento a Descrizione di Control Plane Protection *e* Control Plane Protection.

Identificazione e tracciamento del traffico

In alcuni casi, è necessario identificare rapidamente e rintracciare il traffico di rete, in particolare durante la risposta a un problema o durante prestazioni di rete insoddisfacenti. NetFlow e gli ACL di classificazione sono i due metodi principali per raggiungere questo scopo con il software Cisco

IOS. NetFlow può fornire visibilità su tutto il traffico della rete. Inoltre, NetFlow può essere implementato con collector in grado di fornire analisi dei trend e analisi automatizzate a lungo termine. Gli ACL di classificazione sono un componente degli ACL e richiedono una pre-pianificazione per identificare il traffico specifico e gli interventi manuali durante l'analisi. In queste sezioni viene fornita una breve panoramica di ciascuna funzionalità.

NetFlow

NetFlow identifica le attività di rete anomale e relative alla sicurezza monitorando i flussi di rete. I dati NetFlow possono essere visualizzati e analizzati dalla CLI, oppure possono essere esportati in un sistema di raccolta NetFlow commerciale o freeware per l'aggregazione e l'analisi. I collector NetFlow, tramite i trend a lungo termine, possono fornire analisi del comportamento e dell'utilizzo della rete. NetFlow funziona eseguendo analisi di attributi specifici all'interno dei pacchetti IP e creando flussi. La versione 5 è la più utilizzata di NetFlow, tuttavia la versione 9 è più estendibile. I flussi NetFlow possono essere creati con dati di traffico campionati in ambienti con grandi volumi di dati.

Il CEF, o CEF distribuito, è un prerequisito per abilitare NetFlow. NetFlow può essere configurato su router e switch.

Nell'esempio viene illustrata la configurazione di base di questa funzionalità. Nelle versioni precedenti del software Cisco IOS, il comando per abilitare NetFlow su un'interfaccia è **ip route-cache flow** anziché **ip flow {ingress | In uscita}**.

```
!

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

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

Questo è un esempio di output di NetFlow dalla CLI. L'attributo SrcIf può essere utile nel traceback.

```
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
```

Per ulteriori informazioni sulle funzionalità di NetFlow, fare riferimento a Cisco IOS NetFlow.

Per una panoramica tecnica *di* NetFlow, *consultare il documento* Introduzione a Cisco IOS NetFlow.

ACL di classificazione

Gli ACL di classificazione forniscono visibilità sul traffico che attraversa un'interfaccia. Gli ACL di classificazione non alterano i criteri di sicurezza di una rete e sono in genere costruiti per classificare singoli protocolli, indirizzi di origine o destinazioni. Ad esempio, una voce ACE che consente tutto il traffico potrebbe essere separata in protocolli o porte specifiche. Questa classificazione più granulare del traffico in ACE specifiche può aiutare a comprendere il traffico di rete, in quanto ogni categoria di traffico ha un proprio contatore di visite. Inoltre, è possibile che un amministratore separi il rifiuto implicito presente alla fine di un ACL in ACE granulari per identificare i tipi di traffico negato.

L'amministratore può velocizzare la risposta all'evento imprevisto utilizzando gli ACL di classificazione con i comandi **show access-list** e **clear ip access-list counters** EXEC.

Nell'esempio viene mostrata la configurazione di un ACL di classificazione per identificare il traffico SMB prima di un rifiuto predefinito:

```
!

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
!
```

Per identificare il traffico che usa un ACL di classificazione, usare il comando **show access-list**/acl-

name in modalità di esecuzione. Per cancellare i contatori dell'ACL, usare il comando **clear ip access-list counters** in modalità di esecuzione nome ACL.

```
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)
```

Per ulteriori informazioni su come abilitare le funzionalità di log negli ACL, fare riferimento a Descrizione della funzione di log delle liste di controllo dell'accesso.

Controllo degli accessi con mappe VLAN e elenchi dei controlli degli accessi alle porte

Gli Access Control Lists (VACL) delle VLAN, o mappe VLAN e ACL delle porte (PACL), offrono la possibilità di applicare il controllo dell'accesso al traffico non indirizzato più vicino ai dispositivi endpoint rispetto agli elenchi di controllo degli accessi applicati alle interfacce indirizzate.

In queste sezioni viene fornita una panoramica delle funzionalità, dei vantaggi e dei potenziali scenari di utilizzo di VACL e PACL.

Controllo degli accessi con mappe VLAN

I VACL o le mappe VLAN che si applicano a tutti i pacchetti che entrano nella VLAN, offrono la capacità di imporre il controllo dell'accesso sul traffico intra-VLAN. Ciò non è possibile con gli ACL sulle interfacce di routing. Ad esempio, è possibile usare una mappa VLAN per impedire agli host contenuti nella stessa VLAN di comunicare tra loro, riducendo in questo modo le opportunità per gli attacchi locali o i worm di sfruttare un host sullo stesso segmento di rete. Per impedire ai pacchetti di usare una mappa VLAN, è possibile creare un elenco di controllo di accesso (ACL) che corrisponda al traffico e, nella mappa VLAN, impostare l'azione su drop. Dopo aver configurato una mappa VLAN, tutti i pacchetti che entrano nella VLAN vengono valutati in sequenza rispetto alla mappa VLAN configurata. Le mappe di accesso VLAN supportano gli elenchi di accesso IPv4 e MAC; tuttavia, non supportano la registrazione o gli ACL IPv6.

In questo esempio viene utilizzato un elenco degli accessi esteso con nome che illustra la configurazione di questa funzionalità:

```
!

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>
!
```

Nell'esempio viene mostrato come usare una mappa VLAN per bloccare le porte TCP 139 e 445 e il protocollo vines-ip:

```
!

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
!
```

Per ulteriori informazioni sulla configurazione delle mappe VLAN, fare riferimento a Configurazione della sicurezza di rete con gli ACL.

Controllo dell'accesso con i PACL

I PACL possono essere applicati solo alla direzione in entrata sulle interfacce fisiche di layer 2 di uno switch. Analogamente alle mappe VLAN, i PACL offrono il controllo dell'accesso sul traffico non indirizzato o di livello 2. La sintassi per la creazione dei PACL, che ha la precedenza sulle mappe VLAN e sugli ACL del router, è la stessa degli ACL del router. Se un ACL viene applicato a un'interfaccia di layer 2, viene chiamato PACL. La configurazione implica la creazione di un ACL IPv4, IPv6 o MAC e la relativa applicazione all'interfaccia di layer 2.

In questo esempio viene usato un elenco degli accessi esteso con nome per illustrare la configurazione di questa funzione:

```
!

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
!
```

Per ulteriori informazioni sulla configurazione dei PACL, *consultare* la sezione Configurazione della sicurezza di rete con gli ACL sulle porte.

Controllo degli accessi con MAC

Gli elenchi di controllo di accesso MAC o gli elenchi estesi possono essere applicati sulle reti IP con questo comando in modalità di configurazione interfaccia:

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

> **Nota:** I pacchetti di layer 3 devono essere classificati come pacchetti di layer 2. Il comando è supportato nel software Cisco IOS versione 12.2(18)SXD (per Sup 720) e nel software Cisco IOS versione 12.2(33)SRA o successive.

Questo comando di interfaccia deve essere applicato all'interfaccia in entrata e indica al motore di inoltro di non ispezionare l'intestazione IP. Di conseguenza, è possibile utilizzare un elenco degli accessi MAC nell'ambiente IP.

Uso di VLAN private

Le VLAN private (PVLAN) sono una funzione di sicurezza di layer 2 che limita la connettività tra workstation o server all'interno di una VLAN. Senza le PVLAN, tutti i dispositivi di una VLAN di layer 2 possono comunicare liberamente. Esistono situazioni di rete in cui la sicurezza può essere migliorata limitando la comunicazione tra i dispositivi su una singola VLAN. Ad esempio, le PVLAN vengono spesso utilizzate per impedire la comunicazione tra i server in una subnet accessibile pubblicamente. Se un singolo server viene compromesso, la mancanza di connettività ad altri server dovuta all'applicazione di PVLAN potrebbe contribuire a limitare il compromesso a un unico server.

Esistono tre tipi di VLAN private: VLAN isolate, VLAN di comunità e VLAN primarie. La configurazione delle PVLAN utilizza le VLAN primaria e secondaria. La VLAN primaria contiene tutte le porte promiscue, descritte più avanti, e include una o più VLAN secondarie, che possono essere VLAN isolate o di comunità.

VLAN isolate

La configurazione di una VLAN secondaria come VLAN isolata impedisce completamente la comunicazione tra i dispositivi della VLAN secondaria. Può esistere una sola VLAN isolata per VLAN primaria e solo le porte promiscue possono comunicare con le porte di una VLAN isolata. È consigliabile utilizzare VLAN isolate su reti non attendibili, ad esempio reti che supportano utenti guest.

Questo esempio di configurazione configura la VLAN 11 come VLAN isolata e la associa alla VLAN 20 primaria. L'esempio seguente configura anche l'interfaccia Fast Ethernet 1/1 come porta isolata nella VLAN 11:

```
!

vlan 11
```

```
private-vlan isolated
!

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

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

VLAN della community

Una VLAN secondaria configurata come VLAN di comunità consente la comunicazione tra i membri della VLAN e con qualsiasi porta promiscua nella VLAN primaria. Tuttavia, non è possibile comunicare tra due VLAN della community o da una VLAN della community a una VLAN isolata. È necessario usare le VLAN di comunità per raggruppare i server che devono essere connessi tra loro, ma nei casi in cui non è richiesta la connettività a tutti gli altri dispositivi della VLAN. Questo scenario è comune in una rete accessibile pubblicamente o in qualsiasi punto in cui i server forniscono contenuto a client non attendibili.

Nell'esempio, viene configurata una singola VLAN della community e la porta dello switch Fast Ethernet 1/2 viene configurata come membro di tale VLAN. La VLAN della community, VLAN 12, è una VLAN secondaria della VLAN 20 principale.

```
!

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
!
```

Porte promiscue

Le porte degli switch inserite nella VLAN principale sono note come porte promiscue. Le porte promiscue possono comunicare con tutte le altre porte nelle VLAN primaria e secondaria. Le interfacce router o firewall sono i dispositivi più comuni presenti sulle VLAN.

Questo esempio di configurazione combina i precedenti esempi di VLAN isolata e di comunità e aggiunge la configurazione dell'interfaccia Fast Ethernet 1/12 come porta promiscua:

```
!

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
!
```

Quando si implementano le PVLAN, è importante verificare che la configurazione di layer 3 in uso supporti le restrizioni imposte dalle PVLAN e non consenta di sovvertire la configurazione. Il filtro di layer 3 con un ACL del router o un firewall può impedire la sovversione della configurazione della PVLAN.

Per ulteriori informazioni sull'uso e la configurazione delle VLAN private, fare riferimento alla sezione PVLAN (VLAN private) - promiscue, isolate, condivise nella home page Sicurezza LAN.

Conclusioni

Questo documento offre un'ampia panoramica dei metodi che possono essere usati per proteggere un dispositivo di sistema Cisco IOS. Se si proteggono i dispositivi, aumenta la sicurezza complessiva delle reti gestite. In questa panoramica, viene descritta la protezione dei piani di gestione, controllo e dati e vengono forniti suggerimenti per la configurazione. Se possibile, vengono forniti dettagli sufficienti per la configurazione di ciascuna feature associata. Tuttavia, in tutti i casi, vengono forniti riferimenti completi per fornire le informazioni necessarie per un'ulteriore valutazione.

Riconoscimenti

Alcune descrizioni delle caratteristiche riportate in questo documento sono state scritte dai team di sviluppo di informazioni Cisco.

Appendice Lista di controllo per la protezione avanzata dei dispositivi Cisco IOS

Questo elenco di controllo è una raccolta di tutte le fasi di protezione avanzata presentate in questa guida. Gli amministratori possono usarlo come promemoria di tutte le funzionalità di protezione avanzata usate e considerate per un dispositivo Cisco IOS, anche se una funzionalità non è stata implementata perché non era applicabile. Si consiglia agli amministratori di valutare ogni opzione per i potenziali rischi prima di implementarla.

Piano di gestione

- Password

  Abilita hashing MD5 (opzione segreta) per abilitare le password degli utenti localiConfigurare il blocco dei tentativi di reimpostazione passwordDisabilita recupero password (considerare i rischi)

- Disabilita servizi inutilizzati
- Configurare i pacchetti TCP keepalive per le sessioni di gestione
- Impostazione delle notifiche di soglia della memoria e della CPU
- Configurazione

  Notifiche di soglia della memoria e della CPURiserva di memoria per l'accesso alla consoleRilevatore di perdita di memoriaRilevamento overflow bufferRaccolta avanzata crashinfo

- Uso degli iACL per limitare l'accesso alla gestione
- Filtro (considerare i rischi)

  Pacchetti ICMPFrammenti IPOpzioni IPValore TTL nei pacchetti

- Control Plane Protection

  Configura filtro porteConfigura soglie della coda

- Accesso alla gestione

  Utilizzare Management Plane Protection per limitare le interfacce di gestioneImposta timeout esecuzioneUso di un protocollo di trasporto crittografato (ad esempio SSH) per l'accesso CLIControllo del trasporto per le linee vty e tty (opzione classe di accesso)Avvisa tramite banner

- AAA

  Usa AAA per autenticazione e fallbackUtilizzare AAA (TACACS+) per l'autorizzazione dei comandiUsa AAA per contabilitàUso di server AAA ridondanti

- SNMP

  Configurazione delle community SNMPv2 e applicazione degli ACLConfigurazione di SNMPv3

- Registrazione

  Configurazione della registrazione centralizzataImpostazione dei livelli di registrazione per tutti i componenti rilevantiImposta interfaccia origine registrazioneConfigura granularità timestamp registrazione

- Gestione della configurazione

  Sostituzione e rollbackAccesso esclusivo alle modifiche alla configurazioneConfigurazione resilienza softwareNotifiche delle modifiche alla configurazione

Piano di controllo

- Disabilita (considera rischio)

  Messaggi di reindirizzamento ICMPICMP non raggiungibiliProxy ARP

- Configura autenticazione NTP se viene utilizzato NTP

- Configura Control Plane Policing/Protection (filtro porte, soglie coda)

- Protocolli di routing sicuri

  BGP (TTL, MD5, prefissi massimi, elenchi di prefissi, ACL di percorsi di sistema)IGP (MD5, interfaccia passiva, filtro route, consumo risorse)

- Configurare i limitatori di velocità hardware

- Protocolli di ridondanza Secure First Hop (GLBP, HSRP, VRRP)

Piano dati

- Configura eliminazione selettiva opzioni IP

- Disabilita (considera rischio)

  Routing origine IPTrasmissioni dirette IPMessaggi di reindirizzamento ICMP

- Limita trasmissioni dirette IP

- Configurazione degli ACL (considerare i rischi)

Filtra ICMPFiltra frammenti IPOpzioni IP filtroFiltra valori TTL

- Configurare le protezioni anti-spoofing necessarie

  ACLProtezione origine IPIspezione ARP dinamicaRPF unicastSicurezza porta

- Control Plane Protection (control-plane cef-exception)
- Configurazione di NetFlow e degli ACL di classificazione per l'identificazione del traffico
- Configurazione degli ACL di controllo dell'accesso richiesti (mappe VLAN, PACL, MAC)
- Configurazione di VLAN private