Usa guida di protezione avanzata di Cisco IOS XE

Sommario

Introduzione

Questo documento descrive le informazioni per proteggere i dispositivi di sistema Cisco IOS® XE e aumentare la sicurezza complessiva della documentazione della rete.

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

Strutturato attorno ai tre piani in cui è possibile categorizzare le funzioni di un dispositivo di rete, questo documento fornisce una panoramica di ogni feature inclusa e dei riferimenti agli elementi correlati.

I tre piani funzionali di una rete, ovvero il piano di gestione, il piano di controllo e il piano dati, forniscono funzionalità diverse che è necessario proteggere.

1. Management Plane: il management plane gestisce il traffico inviato al dispositivo Cisco IOS XE ed è costituito da applicazioni e protocolli quali Secure Shell (SSH) e Simple Network Management Protocol (SNMP).
2. 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).
3. 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 XE 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 stessa. 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 XE, 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 sulla sicurezza 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 Cisco Security Advisories and Responses

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 ulteriori 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 utilizzare il protocollo AAA, vedere la sezione Autenticazione, autorizzazione e accounting di questo documento.

Raccolta e monitoraggio centralizzati dei log

Per acquisire informazioni su eventi correnti, emergenti e cronologici relativi a problemi 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 XE, 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 di protezione. 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. Inoltre, quando si copiano i dati di configurazione, è necessario utilizzare protocolli di trasferimento file sicuri. Un esempio è l'uso del protocollo SCP (Secure Copy Protocol) al posto del protocollo FTP o TFTP.

Per ulteriori informazioni sulla gestione sicura dei dispositivi Cisco IOS XE, fare riferimento alla 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.

Ulteriori informazioni su questa funzione sono disponibili nella sezione Identificazione e trackback del traffico in questo documento e su Cisco IOS 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 XE, due aspetti aggiuntivi della gestione della configurazione sono critici: archiviazione della configurazione e sicurezza.

È possibile 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 XE 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 XE 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.

In queste sezioni vengono descritte in dettaglio le funzionalità e le configurazioni di sicurezza disponibili nel software Cisco IOS XE che contribuiscono a rafforzare 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:

1. Simple Network Management Protocol
2. Telnet
3. Protocollo Secure Shell
4. Protocollo di trasferimento file
5. Protocollo Hyper Text Transfer / Protocollo Secure Hyper Text Transfer
6. Protocollo Trivial File Transfer
7. Secure Copy Protocol
8. TACACS+
9. RAGGIO
10. NetFlow
11. Protocollo orario di rete
12. 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 alle risorse o ai 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 XE. 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 XE 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. Tutti i file di configurazione Cisco IOS XE che contengono password crittografate devono essere gestiti con la stessa attenzione usata per un elenco non crittografato delle stesse password.

Anche se questo algoritmo di crittografia debole non viene 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

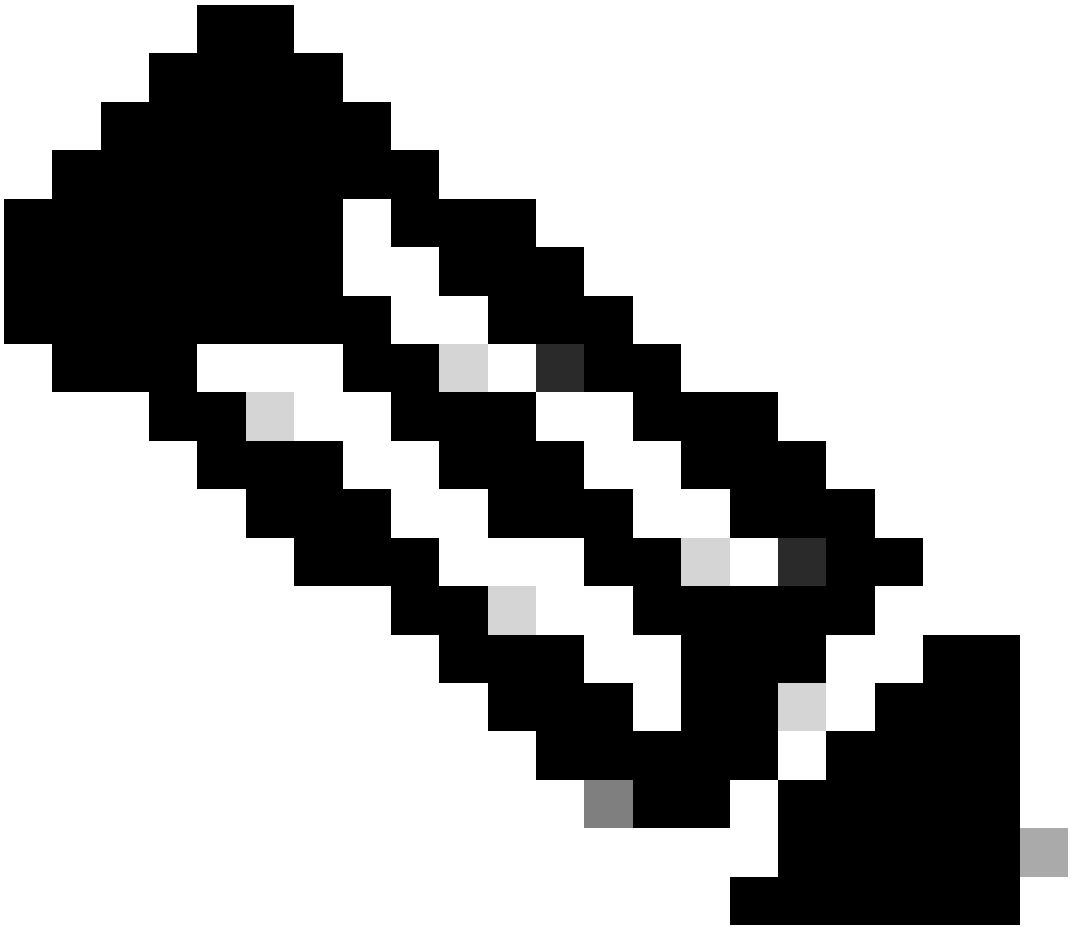
La funzione Enhanced Password Security, attiva sin dalla prima versione del software Cisco IOS XE versione 16.6.4, consente agli amministratori di configurare l'hashing MD5 delle password per il comando username. Prima di questa funzione, esistevano due tipi di password: Type 0, che è una password in testo non crittografato, e Type 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 <nome> secret <password>

Blocco nuovo tentativo password di accesso

La funzione di blocco dei tentativi di accesso tramite password, attiva dalla prima versione del software Cisco IOS XE versione 16.6.4, 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.



Nota: 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 autenticazione locale tentativi max-fail <max-try> autenticazione aaa accesso locale predefinito

username <nome> 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 XE versione 16.6.4 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.

nessun recupero password del servizio

Il software Cisco IOS XE fornisce una procedura di recupero della password che si basa sull'accesso a ROM Monitor Mode (ROMMON) e utilizza 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 attivato 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 XE dopo aver abilitato questa funzione, l'intera configurazione viene eliminata.

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:

1. echo (numero porta 7)
2. scarta (numero porta 9)
3. diurno (numero porta 13)
4. 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 XE versione 16.6.4 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:

5. Usare il comando di configurazione globale no ip finger per disabilitare il servizio Finger. Per impostazione predefinita, il software Cisco IOS XE versioni successive alla 16.1 disabilita questo servizio.
6. Usare il comando di configurazione globale no ip bootp server per disabilitare il protocollo BOOTP (Bootstrap Protocol). Per impostazione predefinita, il software Cisco IOS XE versioni successive alla 16.1 disabilita questo servizio.
7. Nel software Cisco IOS XE versione 16.6.4 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.
8. Se i servizi di inoltro DHCP non sono necessari, è possibile disabilitare i servizi DHCP. Eseguire il comando no service dhcp in modalità di configurazione globale.
9. Per disabilitare il servizio MOP (Maintenance Operation Protocol), eseguire il comando no mop enabled in modalità di configurazione interfaccia.
10. Utilizzare il comando di configurazione globale no ip domain-lookup per disabilitare i servizi di risoluzione DNS (Domain Name System).
11. 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.
12. 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.
13. A meno che i dispositivi Cisco IOS XE 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 XE di tentare di individuare un file di configurazione sulla rete con TFTP.
14. 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 di gestione della rete (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, è possibile disabilitare il CDP a livello globale 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.
15. 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. Usare 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.

16. 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 EXEC

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.

riga con 0

exec-timeout <minuti> [secondi]

vty linea 0 4

exec-timeout <minuti> [secondi]

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 XE locale.

service tcp-keepalives-in

service tcp-keepalives-out

Uso dell'interfaccia di gestione

È possibile 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 è disponibile 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.

interfaccia Loopback0

indirizzo ip 192.168.1.1 255.255.255.0

Notifiche soglia memoria

La funzione Memory Threshold Notification, aggiunta nel software Cisco IOS XE versione 16.6.4, consente di ridurre le condizioni di memoria insufficiente su un dispositivo. A tale scopo, questa funzionalità utilizza due metodi: notifica della soglia della memoria e prenotazione della 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 aumenta del 5% rispetto alla soglia specificata.

processore per il limite minimo di memoria disponibile <threshold>

i/o low-watermark disponibile in memoria <soglia>

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.

valore critico riserva di memoria <value>

Notifica soglia CPU

Introdotta nel software Cisco IOS XE versione 16.6.4, 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 XE sono supportati due metodi di soglia per l'utilizzo della CPU: Rising Threshold e Falling Threshold.

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 <indirizzo-host> <stringa-community> cpu

process cpu threshold type <tipo> rise <percentuale> interval <secondi> [fall <percentuale> interval <secondi>]

process cpu statistics limit entry-percent <numero> [size <secondi>]

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 il successo della connettività VPN che dipende dai certificati per l'autenticazione della fase 1, è necessario disporre di tempo accurato e affidabile.

1. Fuso orario NTP: quando si configura il protocollo NTP, è necessario configurare il fuso orario in modo che i timestamp possano essere correlati correttamente. 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 denominata 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 documentazione del prodotto Cisco sul fuso orario dell'orologio.
2. Autenticazione NTP: se si configura l'autenticazione NTP, questa assicura che i messaggi NTP vengano scambiati tra peer NTP attendibili.

   Configurazione di esempio che utilizza l'autenticazione NTP:

   Cliente:

   (config)#ntp authentication

   (config)#ntp authentication-key 5 md5 ciscotime

   (config)#ntp trusted-key 5

   (config)#ntp server 172.16.1.5 chiave 5 Server:

   (config)#ntp authentication

   (config)#ntp authentication-key 5 md5 ciscotime

   (config)#ntp trusted-key 5

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 facilitata 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

— Consentire le connessioni necessarie per i protocolli di routing e la gestione della rete

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

consenti host tcp <trusted-ebgp-peer> host eq 179 <indirizzo-ebgp-locale>

consenti host tcp <trusted-management-stations> qualsiasi eq 2

consenti host udp <trusted-netmgmt-servers> qualsiasi eq 161

— Nega tutto il traffico IP verso qualsiasi dispositivo di rete

deny ip any <spazio-indirizzi-infrastruttura> <maschera-caratteri-jolly>

— Consentire il traffico di transito

allow ip 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 sugli ACL dell'infrastruttura, consultare il 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 è raramente necessaria per il corretto funzionamento di una rete.

Il software Cisco IOS XE fornisce funzionalità per 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

— Autorizzare l'eco ICMP (ping) da stazioni di gestione e server attendibili

consenti host icmp <trusted-management-stations> qualsiasi eco

consenti host icmp <trusted-netmgmt-servers> qualsiasi eco

— Nega tutto il traffico IP verso qualsiasi dispositivo di rete

deny ip any <spazio-indirizzi-infrastruttura> <maschera-caratteri-jolly>

— Consentire il traffico di transito

allow ip 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 XE utilizza un metodo specifico per controllare i frammenti non iniziali rispetto agli elenchi degli accessi configurati. Il software Cisco IOS XE 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, dalla seconda 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. Lo scenario viene mostrato nella configurazione seguente:

ip access-list extended ACL-FRAGMENT-EXAMPLE

autorizzare tcp su qualsiasi 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 in modo esplicito 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

— Negare ai frammenti IP che utilizzano ACE specifiche del protocollo di supportare

— classificazione del traffico di attacco

deny tcp any fragments

nega tutti i frammenti udp

deny icmp any fragments

deny ip any fragments

— Nega tutto il traffico IP verso qualsiasi dispositivo di rete

deny ip any <spazio-indirizzi-infrastruttura> <maschera-caratteri-jolly>

— Consentire il traffico di transito

allow ip 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 il filtro delle opzioni IP

Dal software Cisco IOS XE versione 16.6.4, 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

— Nega pacchetti IP che contengono opzioni IP

deny ip any any option any-options

— Nega tutto il traffico IP verso qualsiasi dispositivo di rete

deny ip any <spazio-indirizzi-infrastruttura> <maschera-caratteri-jolly>

— Consentire il traffico di transito

allow ip any

Supporto ACL per filtrare in base al valore TTL

Dal software Cisco IOS XE versione 16.6.4, è supportato anche il filtro degli 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 che scadono è basso, ma se il numero di pacchetti che scadono è alto, la generazione e la trasmissione di questi messaggi possono consumare 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.

Nell'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

— Nega pacchetti IP con valori TTL insufficienti per attraversare la rete

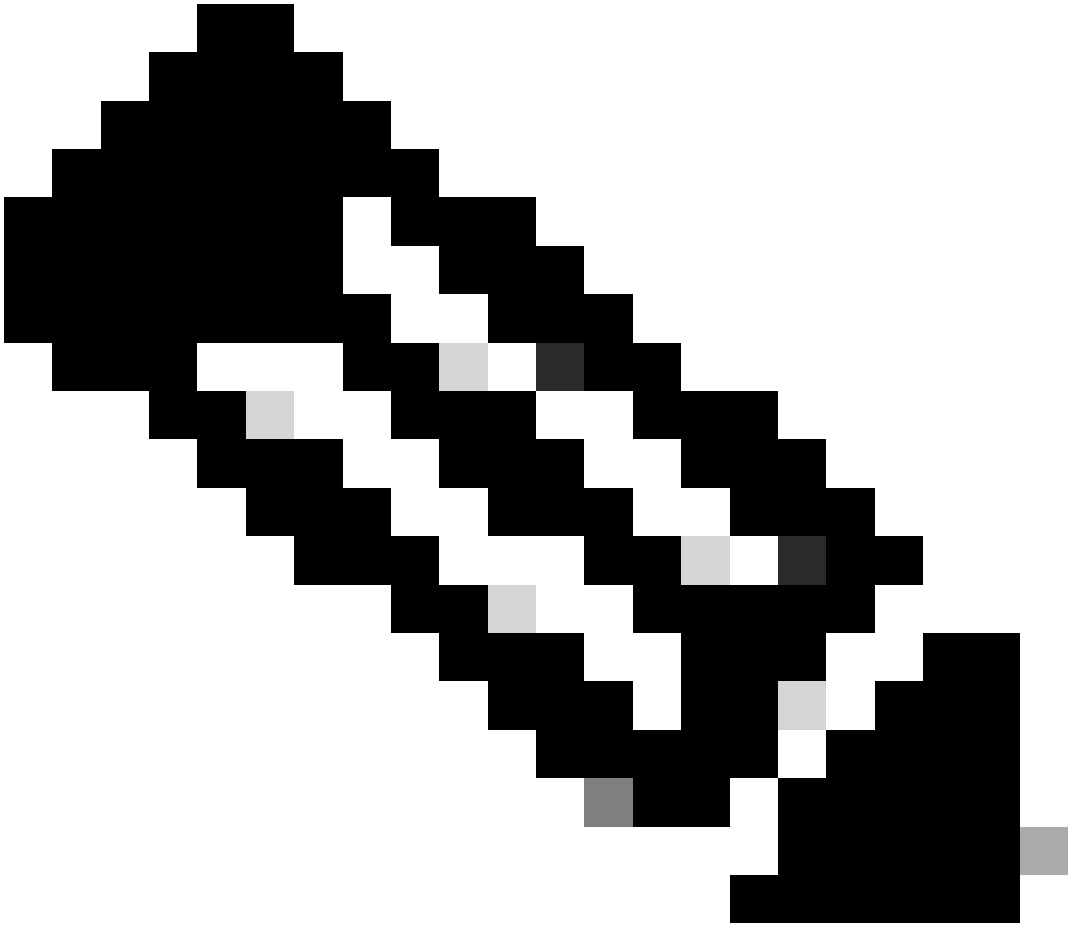
deny ip any ttl lt 6

— Nega tutto il traffico IP verso qualsiasi dispositivo di rete

deny ip any <spazio-indirizzi-infrastruttura> <mask>

— Consentire il traffico di transito

allow ip any



Nota: alcuni protocolli utilizzano in modo legittimo pacchetti con valori TTL bassi. eBGP è uno di questi protocolli. Per ulteriori informazioni sull'attenuazione degli attacchi TTL basati sulla scadenza, fate riferimento a TTL Expiry Attack Identification and Mitigation (Identificazione e mitigazione degli attacchi TTL in scadenza).

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 XE versione 16.6.4 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:

host control-plane

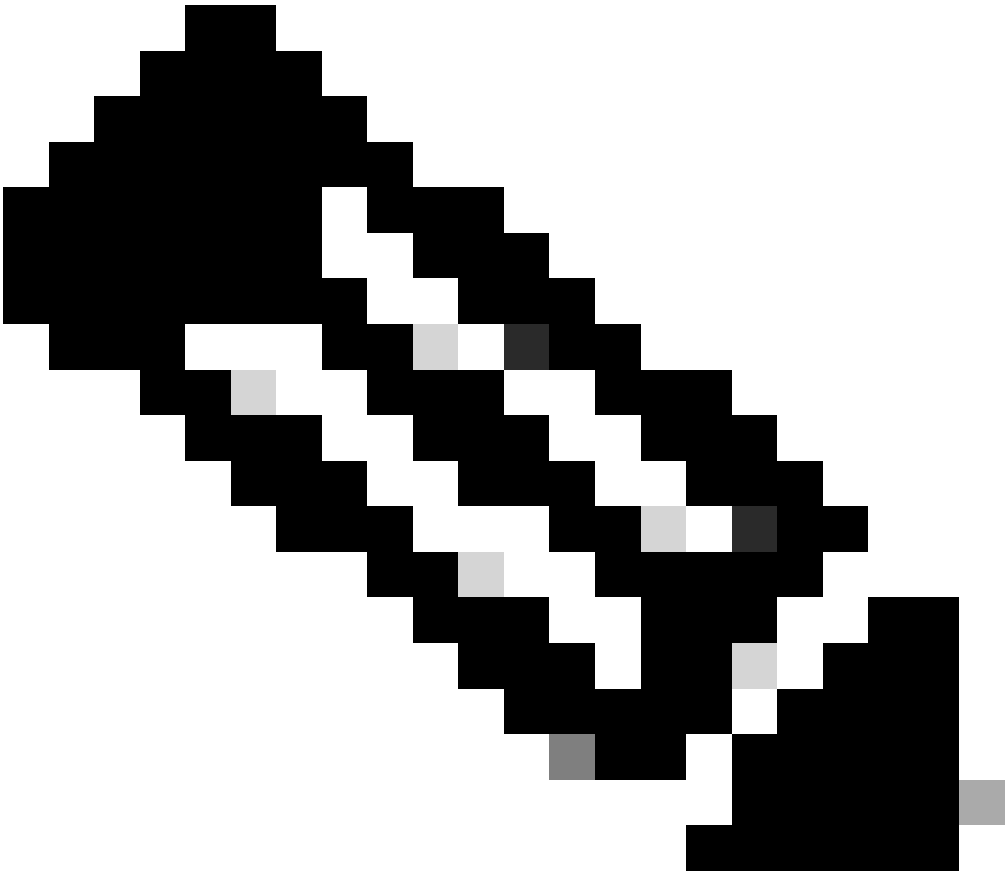
interfaccia di gestione Gigabit Ethernet 0/1 per https ssh

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-XE. La funzione CPPr divide il piano di controllo in categorie separate denominate sottointerfacce. Esistono tre sottointerfacce del control plane: Host, Transit e CEF-Exception. Inoltre, CPPr include le seguenti funzioni aggiuntive di protezione del control plane:

1. Funzione di filtro delle porte: questa funzione consente di controllare o ignorare i pacchetti diretti alle porte TCP e UDP chiuse o non in ascolto.
2. 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.

   Il protocollo 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, fare riferimento a Control Plane Policing.

Sessioni di gestione della 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 XE supporta 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.

Il software Cisco IOS XE 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 XE:

ip domain-name example.com

crypto key generate rsa module 2048

ip ssh timeout 60

tentativi di autenticazione ip ssh 3

interfaccia-origine ip ssh Gigabit Ethernet 0/1

vty linea 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 module 2048

ip http secure-server

SSHv2

La funzione SSHv2 è stata introdotta in Cisco IOS XE nella prima release 16.6.4, che consente all'utente di configurare SSHv2. SSH viene eseguito su un livello di trasporto affidabile e fornisce solide funzionalità 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 XE abilita SSH versione 1.9. SSH v1 e SSH v2 sono compatibili con entrambe le connessioni. 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 XE:

hostname router

ip domain-name example.com

crypto key generate rsa module 2048

ip ssh timeout 60

tentativi di autenticazione ip ssh 3

interfaccia-origine ip ssh Gigabit Ethernet 0/1

ip ssh versione 2

vty linea 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 XE SSHv2 supporta metodi di autenticazione interattivi da tastiera e basati su password. La funzione SSHv2 Enhancements for RSA Keys supporta anche l'autenticazione con chiave pubblica basata su RSA per il client e il 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 XE.

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 XE 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 sessione continua; in caso contrario viene terminata e viene visualizzato il messaggio Autenticazione server non riuscita.

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

Configurare un nome host per il dispositivo

hostname router

Configurare un nome di dominio

ip domain-name example.com

Abilitare il server SSH per l'autenticazione locale e remota sul router che usa

usare il comando "crypto key generate".

Per SSH versione 2, le dimensioni del modulo devono essere almeno 768 bit

crypto key generate rsa usage-keys label modulo sshkeys 2048

Specificare il nome della coppia di chiavi RSA (in questo caso, "sshkeys") da utilizzare per SSH

ip ssh rsa keypair-name sshkeys

Configurare un timeout ssh (in secondi).

L'uscita successiva abilita un timeout di 120 secondi per le connessioni SSH.

ip ssh timeout 120

Configurare un limite di cinque tentativi di autenticazione.

tentativi di autenticazione ip ssh 5

Configurare SSH versione 2.

ip ssh versione 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 Cisco IOS XE SSH 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.

Configurare un nome host per il dispositivo.

hostname router

Configurare un nome di dominio.

ip domain name cisco.com

Generare una coppia di chiavi RSA che utilizzi un modulo di 2048 bit.

crypto key generate rsa module 2048

Configurare le chiavi SSH-RSA per l'autenticazione di server e utente sul server SSH.

catena di pubkey ip ssh

Configurare il nome utente SSH.

Configurare le chiavi SSH-RSA per l'autenticazione di server e utente sul server SSH.

catena di pubkey ip ssh

Configurare il nome utente SSH.

username ssh-user

Specificare la chiave pubblica RSA del dispositivo peer remoto.

È quindi necessario configurare il comando key-string

(seguita dalla chiave pubblica RSA del peer remoto) o

key-hash (seguito dal tipo di chiave SSH e dalla versione).

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

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

hostname router

ip domain-name cisco.com

Generare una coppia di chiavi RSA.

crypto key generate rsa

Configurare le chiavi SSH-RSA per l'autenticazione di server e utente sul server SSH.

catena di pubkey ip ssh

Abilitare il server SSH per l'autenticazione a chiave pubblica sul router.

server SSH-nome-server

Specificare la chiave pubblica RSA del peer remoto.

È quindi necessario configurare il comando key-string

(seguita dalla chiave pubblica RSA del peer remoto) o thea

key-hash <tipo-chiave> <nome-chiave> seguito dalla chiave SSH

tipo e versione).

Verificare che venga eseguita l'autenticazione del server. La connessione è

terminato in caso di errore.

ip ssh stricthostkeycheck

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

Porte console e AUX

Nei dispositivi Cisco IOS XE, 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 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 necessario, un amministratore può rimuovere la possibilità di eseguire la procedura di recupero della password che utilizza il comando di configurazione globale no service password-recovery; tuttavia, dopo aver abilitato il comando no service password-recovery, 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 l'accesso non autorizzato. Una porta AUX può essere disabilitata con questi comandi:

linea ausiliaria 0

input trasporto none

output trasporto none

no exec-timeout 0 1

nessuna password

Controllare le righe vty e tty

Le sessioni di gestione interattive nel software Cisco IOS XE utilizzano un tty o un tty virtuale (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 XE hanno un numero limitato di linee vty; il numero di linee 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.

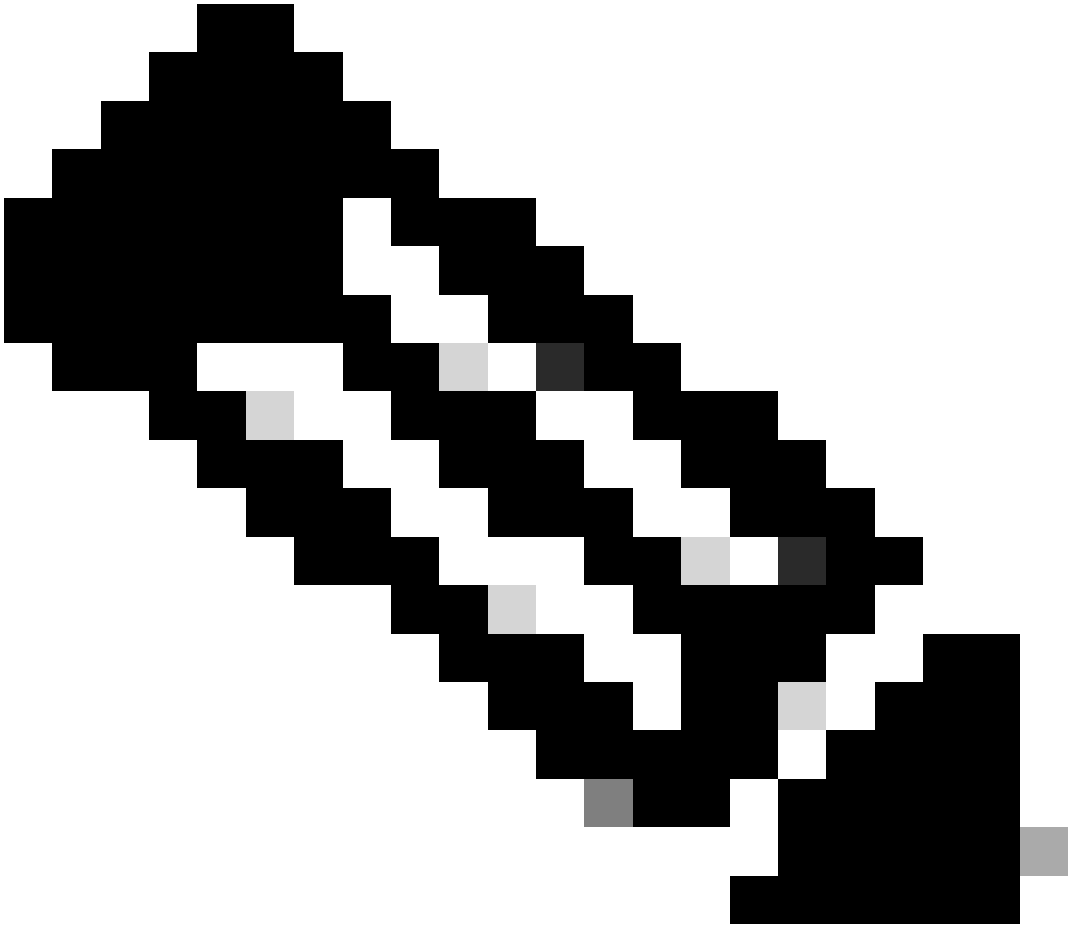
il comando exec-timeout deve essere usato per disconnettere le sessioni sulle righe vty o tty lasciate inattive. Anche il comando service tcp-keepalives-in deve essere usato per abilitare i pacchetti TCP keepalive sulle connessioni in arrivo al dispositivo. In questo modo il dispositivo sull'estremità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

Controllo del trasporto per le linee vty e tty

È possibile 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 possibile usare transport input ssh anziché protocolli non crittografati, ad esempio Telnet e rlogin. La configurazione none dell'input di trasporto può essere abilitata su un tty, il che in effetti disabilita l'uso della linea tty per le connessioni alla console inversa.

Entrambe le linee vty e tty consentono a un 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 possibile 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 può essere imposto utilizzando l'output del trasporto ssh.



> Nota: se supportato, IPSec può essere utilizzato per connessioni di accesso remoto crittografate e sicure a un dispositivo. Se si utilizza IPSec, viene aggiunto un ulteriore sovraccarico della CPU al dispositivo. Tuttavia, è necessario applicare il protocollo SSH come protocollo di trasporto anche quando si utilizza IPSec.

Banner di 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. Uno dei metodi per inviare questa notifica è inserire le informazioni in un messaggio banner configurato con il comando Cisco IOS XE Software banner login.

Gli obblighi di notifica legale sono complessi, variano in base alla giurisdizione e alla situazione e possono 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 le informazioni seguenti:

1. Notare che il sistema deve essere connesso o utilizzato solo da personale specificamente autorizzato e forse anche informazioni su chi può autorizzare l'uso.
2. Si noti che qualsiasi utilizzo non autorizzato del sistema è illegale e può essere soggetto a sanzioni civili e penali.
3. 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.
4. 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 può 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 XE possono utilizzare per autenticare gli utenti di gestione su un server AAA remoto. Questi utenti di gestione possono accedere al dispositivo IOS-XE 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, cripta 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+ può 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 XE con una configurazione simile a quella dell'esempio seguente:

aaa new-model

gruppo predefinito di accesso autenticazione aaa tacacs+

tacacs server <nome_server>

 address ipv4 <indirizzo_ip_server_tacacs>

Chiave <chiave>

La configurazione precedente può essere utilizzata come punto di partenza per un modello di autenticazione AAA specifico dell'organizzazione.

Un elenco di metodi è un elenco sequenziale che descrive i metodi di autenticazione da sottoporre a query 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 XE 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 XE può fare affidamento sui protocolli di autenticazione secondari. Le configurazioni tipiche includono l'uso dell'autenticazione locale o l'abilitazione dell'autenticazione 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 XE che supportano l'utilizzo di password segrete per gli utenti definiti localmente, può essere consigliabile eseguire il fallback all'autenticazione locale. In questo modo, è possibile 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 la propria 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 sulla password configurata localmente con il comando enable secret:

enable secret <password>

aaa new-model

autenticazione aaa login gruppo predefinito tacacs+ enable

tacacs server <nome_server>

address ipv4 <indirizzo_ip_server_tacacs>

Chiave <chiave>

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 possibile evitare l'uso di password di tipo 7 a meno che non sia richiesto da una funzionalità in uso sul dispositivo Cisco IOS XE.

Il tipo 9 (scrypt) può essere utilizzato 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 generale 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 XE 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 gruppo predefinito tacacs+ none

comandi autorizzazione aaa 0 gruppo predefinito tacacs+ nessuno

comandi autorizzazione aaa 1 gruppo predefinito tacacs+ none

comandi di autorizzazione aaa 15 gruppi predefiniti tacacs+ none

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

Accounting comando TACACS+

Quando è configurata, 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.

acs+ gruppo start-stop predefinito esecuzione accounting aaa

comandi di accounting aaa 0 gruppo start-stop predefinito tacacs+

comandi di accounting aaa 1 gruppo start-stop predefinito tacacs+

comandi di accounting aaa 15 gruppo start-stop predefinito 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 possono 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:

1. Disponibilità dei server AAA durante potenziali errori di rete
2. Posizionamento geograficamente distribuito dei server AAA
3. Caricamento su singoli server AAA in condizioni di stato stazionario e di errore
4. Latenza di rete tra server di accesso alla rete e server AAA
5. 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-XE. 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. Tali informazioni possono essere protette da utenti malintenzionati che desiderano utilizzare questi dati per eseguire attacchi alla rete.

Stringhe della community SNMP

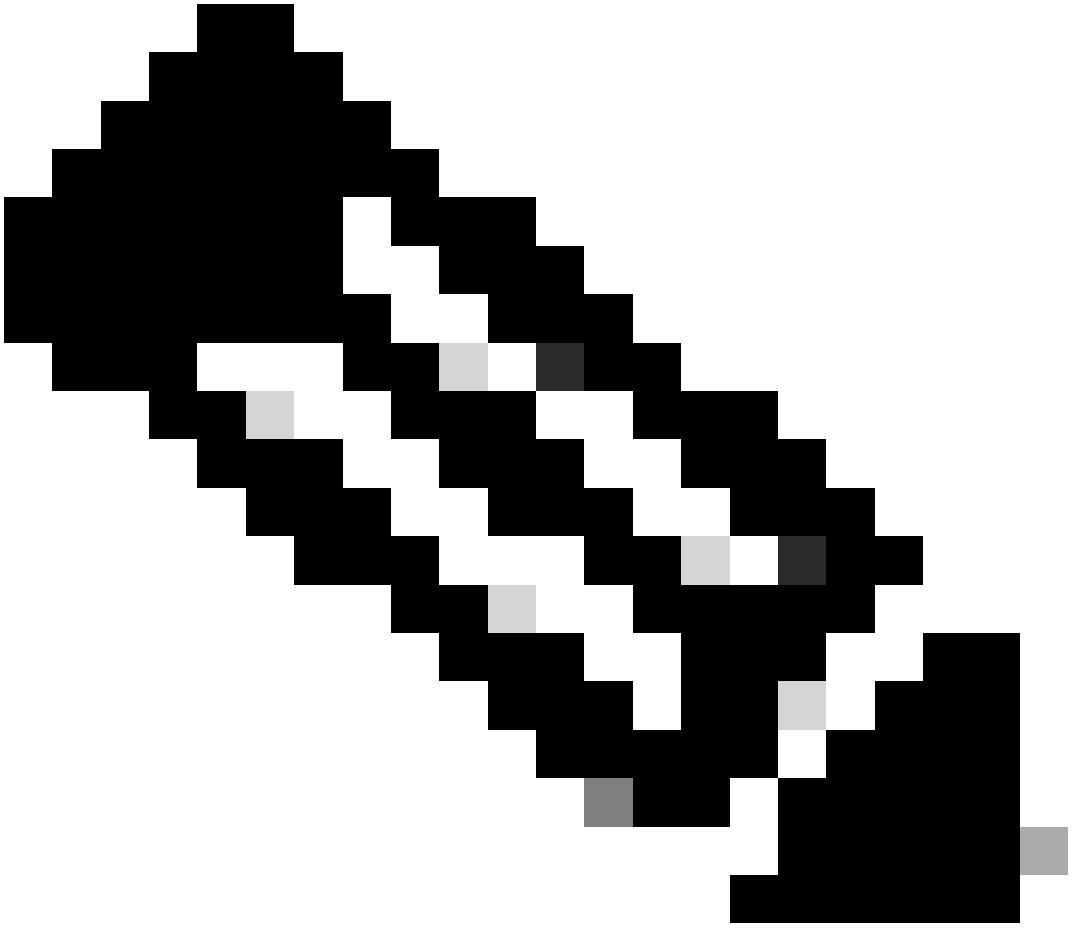
Le stringhe della community sono password applicate a un dispositivo IOS-XE per limitare l'accesso, sia di sola lettura che di lettura/scrittura, ai dati SNMP sul dispositivo. Queste stringhe della community, come tutte le password, possono essere scelte con cura per evitare che siano insignificanti. Le stringhe della community possono essere modificate a intervalli regolari e in conformità con i criteri di sicurezza delle reti.

Ad esempio, le stringhe possono 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:

RO snmp-server community READONLY

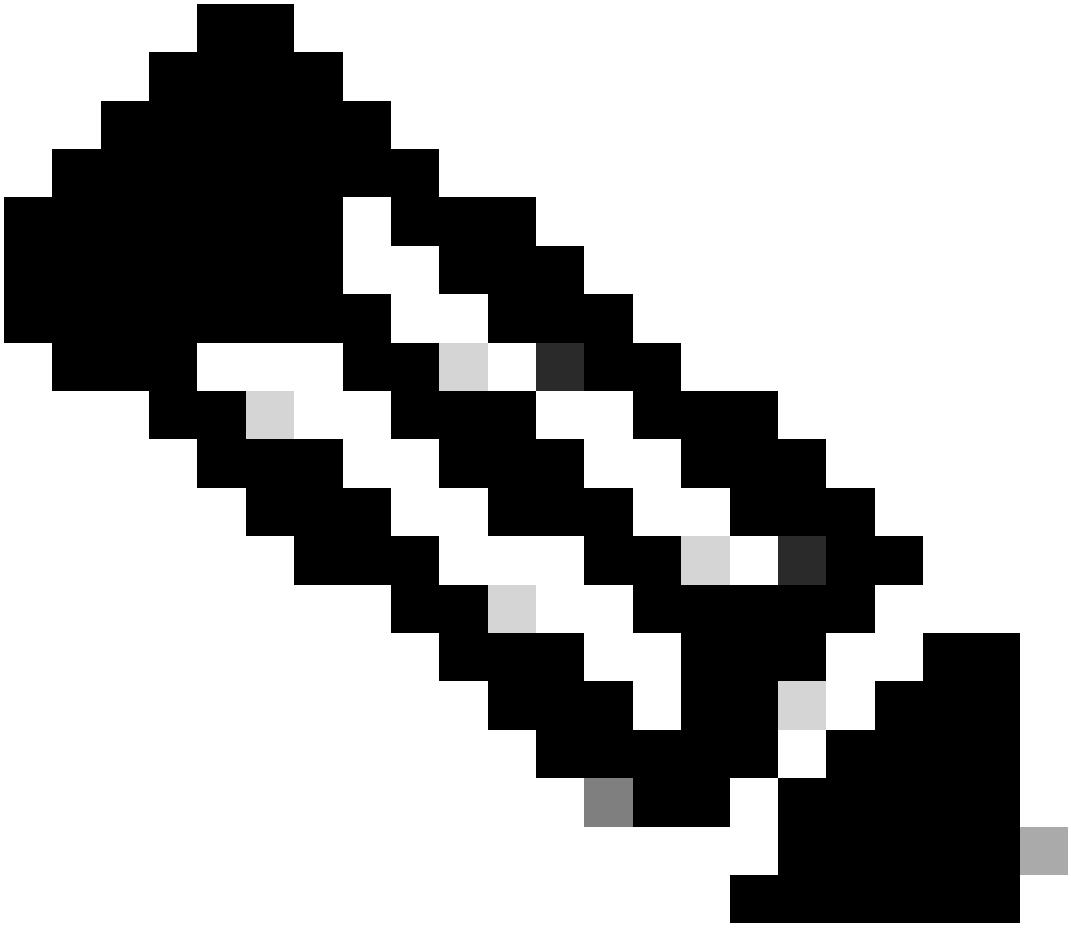
community snmp-server READWRITE RW



Nota: per spiegare chiaramente l'uso di queste stringhe, sono stati scelti gli esempi di stringhe della community precedenti. Per gli ambienti di produzione, le stringhe della community possono essere scelte con cautela e possono essere costituite da una serie di simboli alfabetici, numerici e non alfanumerici. Per ulteriori informazioni sulla selezione di password non banali, consultare la sezione Suggerimenti per la creazione di password sicure.

Stringhe della community SNMP con ACL

Oltre alla stringa della community, è possibile 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 appropriata per accedere alle informazioni SNMP richieste.

access-list 98 allow 192.168.100.0 0.0.0.255

access-list 99 allow 192.168.100.1

snmp-server community READONLY RO 98

community snmp-server READWRITE RW 99

Per ulteriori informazioni su questa funzione, fare riferimento alla community snmp-server nella guida di riferimento dei comandi di Cisco IOS XE Network Management.

ACL di infrastruttura

È possibile 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-XE. Un

iACL può 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 <nome_vista> <nome_famiglia_vista_mib> [include/exclude]

snmp-server community <stringa_community>view <nome_visualizzazione> 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. L'SNMPv3 è costituito da tre opzioni di configurazione principali:

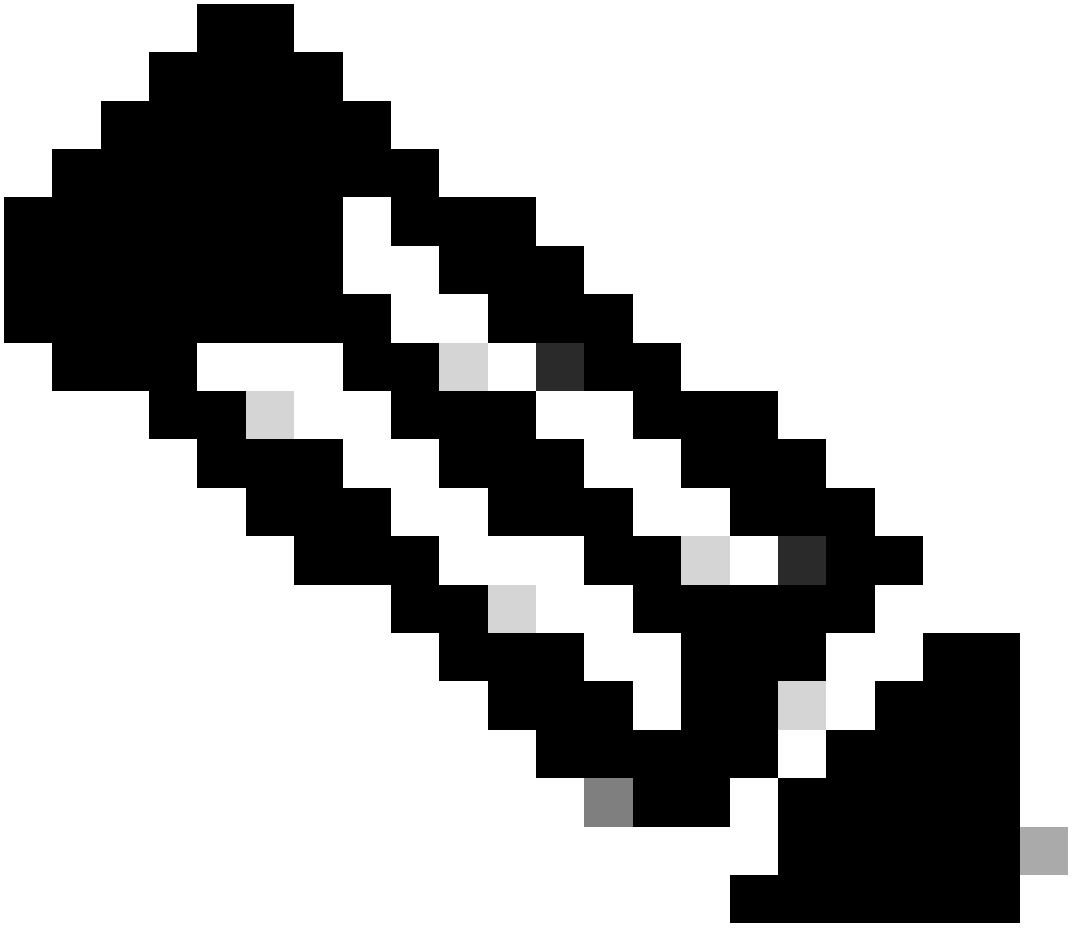
1. no auth - Questa modalità non richiede alcuna autenticazione né crittografia dei pacchetti SNMP.
2. auth: questa modalità richiede l'autenticazione del pacchetto SNMP senza crittografia.
3. priv: questa modalità richiede sia l'autenticazione che la crittografia (privacy) di ciascun pacchetto SNMP.

   Per utilizzare i meccanismi di protezione SNMPv3 per l'autenticazione o l'autenticazione e la crittografia, è necessario che esista un ID motore autorevole per gestire i pacchetti SNMP. Per impostazione predefinita, l'ID 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

ID motore SNMP locale: 8000000903000152BD35496

ID motore remoto - Porta IP-addr



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 XE per SNMPv3 con un gruppo di server SNMP AUTHGROUP e abilita solo l'autenticazione per questo gruppo con la parola chiave auth:

gruppo snmp-server AUTHGROUP v3 auth

Questo comando configura un dispositivo Cisco IOS XE per SNMPv3 con un gruppo di server SNMP.

PRIVGROUP e abilita l'autenticazione e la crittografia per questo gruppo con la parola chiave priv:

gruppo snmp-server 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:

utente snmp-server snmpv3utente PRIVGROUP v3 auth md5 authpassword priv 3des privpassword

Tenere presente 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 dell'utente non può essere visualizzata dalla configurazione. Per visualizzare gli utenti configurati, immettere il comando show snmp user come mostrato nell'esempio:

router#show snmp user

Nome utente: snmpv3ID motore utente: 80000009030000152BD35496

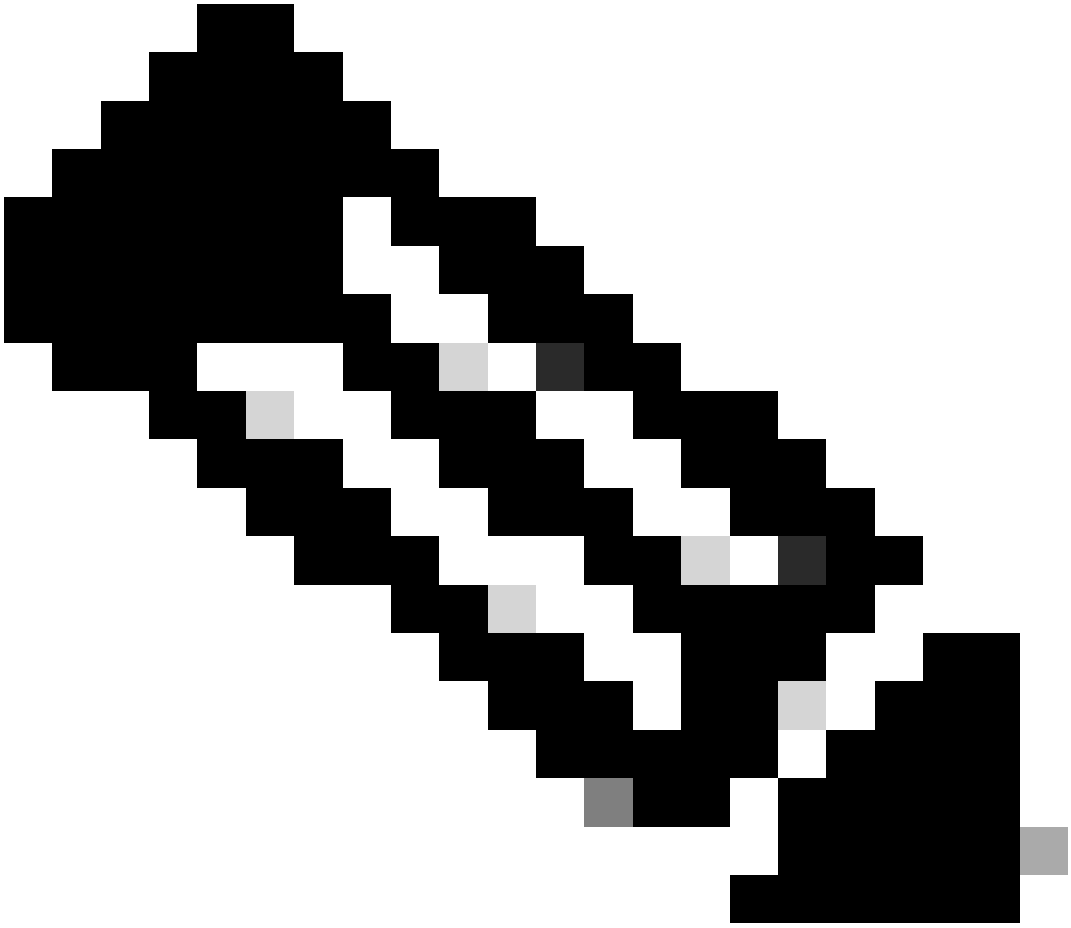
tipo di storage: attivo non volatile

Protocollo di autenticazione: MD5
Protocollo di privacy: 3DES
Nome-gruppo: 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 XE 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.



> Nota: 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:

host control-plane

interfaccia di gestione Fast Ethernet0/0 per consentire 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 XE e la rete in cui è distribuito. Il software Cisco IOS XE offre diverse opzioni di registrazione

flessibili che possono contribuire a raggiungere gli obiettivi di visibilità e gestione della rete 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 e a ridurre al minimo l'impatto della registrazione su un dispositivo Cisco IOS XE.

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 out-of-band) possono essere estese in modo da includere il traffico syslog.

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

logging host <indirizzo-ip>

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

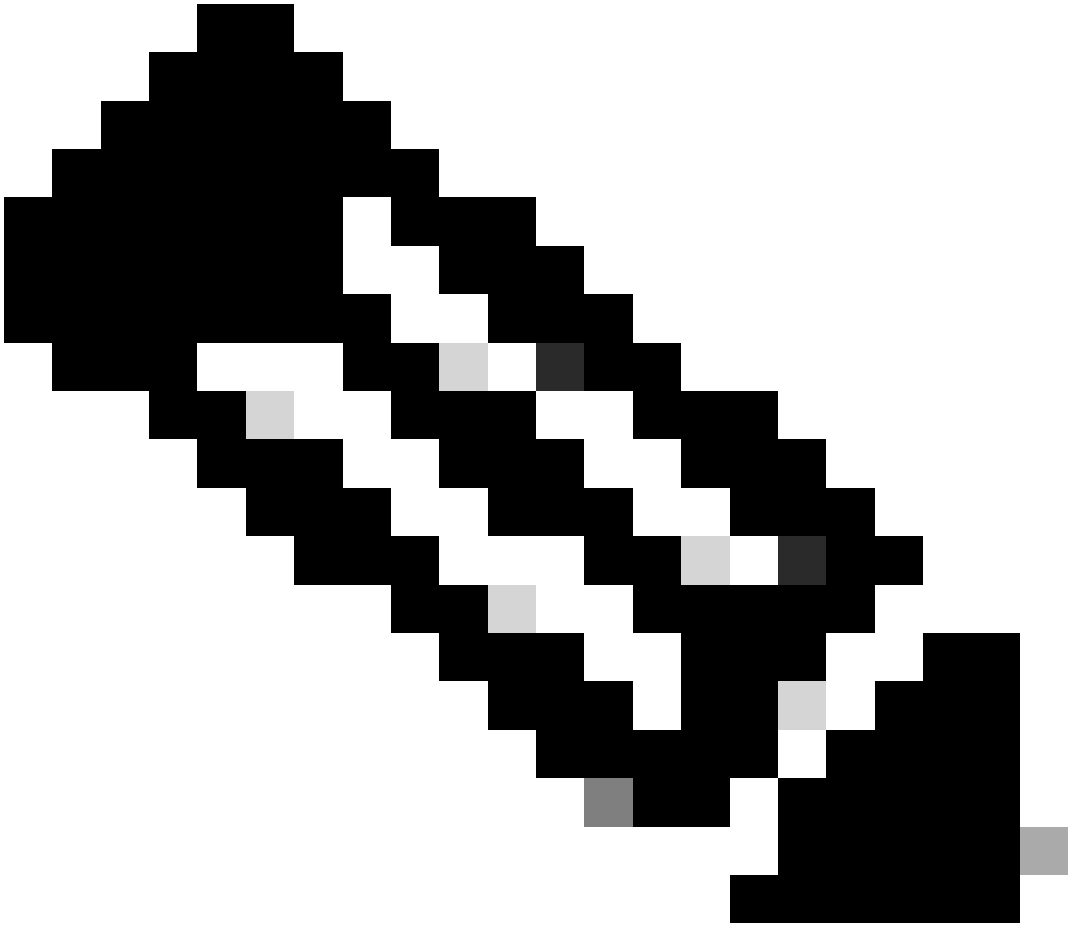
La funzione Logging to Local Nonvolatile Storage (ATA Disk) consente il salvataggio dei messaggi di registrazione del sistema su un disco flash ATA (Advanced Technology Attachment). I messaggi salvati su un'unità ATA vengono mantenuti dopo il riavvio di un router.

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

logging buffered.

registrazione url persistente disco0:/syslog dimensione 134217728 filesize 16384

Prima di registrare i messaggi scritti su un file sul disco ATA, il software Cisco IOS XE verifica 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 un sovraccarico 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 in un archivio non volatile locale.

Livello di registrazione

A ogni messaggio di log generato da un dispositivo Cisco IOS XE viene assegnata una delle otto priorità che vanno 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):

registrazione trap 6

registrazione memorizzata nel buffer 6

Non accedere alle sessioni di console o di monitoraggio

Con il software Cisco IOS XE, 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-XE 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:

nessuna console di registrazione

nessun monitoraggio di registrazione

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

Usa registrazione nel buffer

Il software Cisco IOS XE 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 della console o di monitoraggio.

Durante la configurazione della registrazione nel buffer, sono disponibili due opzioni di configurazione: la dimensione del buffer di registrazione e la gravità dei messaggi memorizzati 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 i messaggi di livello da 0

(emergenze) a 6 (di tipo informativo) sono memorizzati:

log nel buffer 16384 6

Per ulteriori informazioni sulla registrazione nel buffer, fare riferimento a Cisco IOS XE Setting the Message Display Destination Device (Impostazione del dispositivo di destinazione di visualizzazione dei messaggi).

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.

Se eseguito 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:

log interfaccia di origine Loopback 0

Per ulteriori informazioni, fare riferimento a Cisco IOS XE Embedded Syslog Manager.

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 possono essere configurati in modo da includere la data e l'ora con una precisione di millisecondi e da includere il fuso orario in uso sul dispositivo.

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

servizio timestamp 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):

orologio fuso orario PST -8

servizio timestamp log datetime msec localtime show-timezone

Gestione configurazione software Cisco IOS XE

Il software Cisco IOS XE include diverse funzionalità che possono abilitare una forma di gestione della configurazione su un dispositivo Cisco IOS XE. 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 XE versione 16.6.4 e successive, le funzionalità di sostituzione e ripristino della configurazione consentono di archiviare la configurazione del dispositivo Cisco IOS XE 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 XE 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. Inoltre, indica al dispositivo Cisco IOS XE di archiviare le configurazioni archiviate come file denominati archived-config-N sul disco0: 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.

archivio

path disk0:configurazione archiviata

massimo 14

periodo 1440

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 XE versione 16.6.4, la funzione Accesso esclusivo alle modifiche alla configurazione assicura che solo un amministratore apporti modifiche alla configurazione di un dispositivo Cisco IOS XE alla volta. Questa funzione consente di eliminare l'impatto indesiderato delle modifiche simultanee apportate ai componenti di configurazione correlati. Questa funzione, configurata con il comando di configurazione globale in modalità esclusiva, 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:

modalità di configurazione esclusiva

Software Cisco con firma digitale

Aggiunta nel software Cisco IOS XE versione 16.1 e successive, la funzionalità software Cisco con firma digitale semplifica l'utilizzo del software Cisco IOS XE con firma digitale e quindi sicuro, tramite la crittografia asimmetrica protetta (chiave pubblica).

Un'immagine con firma digitale trasporta 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 manomessa 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 XE 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 isr4300-universalk9.16.06.04.SPA.bin nella memoria flash con le chiavi nell'archivio chiavi del dispositivo:

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

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

Una nuova immagine (isr4300-universalk9.16.10.03.SPA.bin) può quindi essere copiata nella memoria flash per essere caricata e la firma dell'immagine viene verificata con la nuova chiave speciale aggiunta

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

Notifica e registrazione delle modifiche alla configurazione

La funzionalità di notifica e registrazione delle modifiche alla configurazione, aggiunta nel software Cisco IOS XE versione 16.6.4, consente di registrare le modifiche alla configurazione apportate a un dispositivo Cisco IOS XE. Il registro viene mantenuto sul dispositivo Cisco IOS XE 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 nascondono le chiavi e le voci di dimensione di registrazione vengono utilizzati per migliorare la configurazione predefinita in quanto 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 XE 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.

archivio

configurazione log

attivazione registrazione

dimensioni registrazione 200

hidekey

notifica syslog

Dopo aver abilitato la funzione Configuration Change Notification and Logging, è possibile usare il comando show archive log config all in modalità di esecuzione privilegiata 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 per spostare i dati dall'origine alla destinazione. Ciò include protocolli di routing come il Border Gateway Protocol, nonché protocolli come ICMP e il Resource Reservation Protocol (RSVP).

È importante che gli eventi nei piani di gestione e di dati non influiscano negativamente sul piano di controllo. Quando un evento del piano dati, ad esempio un attacco DoS, colpisce il piano di controllo, l'intera rete può diventare instabile. Queste informazioni sulle funzionalità e sulle configurazioni del software Cisco IOS XE possono contribuire 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 router può generare un messaggio di reindirizzamento ICMP 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 che funziona correttamente, un router invia i reindirizzamenti solo agli host delle proprie subnet locali. In altre parole, i reindirizzamenti ICMP non possono mai oltrepassare un limite di layer 3.

I messaggi di reindirizzamento ICMP sono di due tipi: reindirizzamento per un indirizzo host e reindirizzamento per 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 XE 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 accetta la responsabilità di instradare i pacchetti verso la 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'autore dell'attacco. Il proxy ARP può essere disabilitato con il comando di configurazione interfaccia no ip proxy-arp.

Per ulteriori informazioni su questa funzione, fare riferimento a Abilitazione e disabilitazione di ARP proxy.

Messaggi di controllo NTP

Le query NTP Control Message sono funzioni di NTP che hanno assistito nelle funzioni di gestione della rete (NM) prima che fossero creati e utilizzati NM migliori. A meno che l'organizzazione non stia ancora utilizzando NTP per le funzioni NM, le procedure consigliate per la sicurezza della rete consentono di disabilitarle completamente tutte insieme. Se li si utilizza, è possibile che si tratti di un servizio di tipo solo rete interna bloccato dal firewall o da un altro dispositivo esterno. Sono stati addirittura rimossi da tutte le versioni IOS e IOS-XE ad eccezione di quelle standard, in quanto IOS-XR e NX-OS non le supportano.

Se si sceglie di disabilitare questa funzione, il comando è

```
Router (config)# senza controllo modalità consentita ntp
```

Questo comando viene quindi visualizzato in running-config come controllo di modalità non consentita ntp 0. In questo modo, i messaggi di controllo NTP sono stati disabilitati sul dispositivo e il dispositivo è stato protetto dagli attacchi.

Limita impatto CPU del 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 la manutenzione e l'operatività degli altri due piani.

Informazioni sul traffico del Control Plane

Per proteggere correttamente il control plane del dispositivo Cisco IOS XE, 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 XE e deve essere gestito direttamente dalla CPU del dispositivo Cisco IOS XE. 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 XE, inclusi 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 XE stesso, che richiede un'elaborazione speciale da parte della CPU. Sebbene non sia un elenco esaustivo di CPU che influisce 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:

1. Log lista di controllo dell'accesso: il traffico di log 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.
2. Unicast Reverse Path Forwarding (Unicast RPF) - RPF unicast, utilizzato in combinazione con un ACL, può causare la commutazione di determinati pacchetti.
3. Opzioni IP - Tutti i pacchetti IP con opzioni incluse devono essere elaborati dalla CPU.
4. Frammentazione: tutti i pacchetti IP che richiedono la frammentazione devono essere passati alla CPU per essere elaborati.
5. 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 danno luogo all'elaborazione della CPU.
6. ICMP Unreachables - I pacchetti che causano messaggi ICMP "destinazione irraggiungibile" a causa di routing, MTU o filtro vengono elaborati dalla CPU.
7. Traffico che richiede una richiesta ARP - Le destinazioni per cui non esiste una voce ARP richiedono l'elaborazione da parte della CPU.
8. 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 XE:
9. 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.
10. Il comando show interface switching restituisce informazioni sul numero di pacchetti elaborati da un dispositivo.
11. Il comando show ip traffic fornisce informazioni sul numero di pacchetti IP: se la destinazione è locale (ossia, il traffico di ricezione adiacente), le opzioni che richiedono la frammentazione vengono inviate allo spazio degli indirizzi di broadcast che vengono inviate allo spazio degli indirizzi multicast.
12. Il traffico di ricezione adiacente può essere identificato usando il comando show ip cache flow. Tutti i flussi destinati al dispositivo Cisco IOS XE hanno un'interfaccia di destinazione (DstIf) locale.
13. Control Plane Policing può essere usato per identificare il tipo e la velocità del traffico che raggiunge il control plane del dispositivo Cisco IOS XE. 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

L'rACL protegge il dispositivo dal traffico dannoso prima che questo 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 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 possono 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:

— Autorizzare SSH dagli host attendibili autorizzati al dispositivo.

access-list 151 allow tcp 192.168.100.0 0.0.0.255 any eq 22

— negare il collegamento SSH da tutte le altre origini al punto di ripristino.

access-list 151 deny tcp any eq 22

— autorizzare tutto il resto del traffico diretto al dispositivo.

— in base alle policy e alle configurazioni di sicurezza.

access-list 151 allow ip any

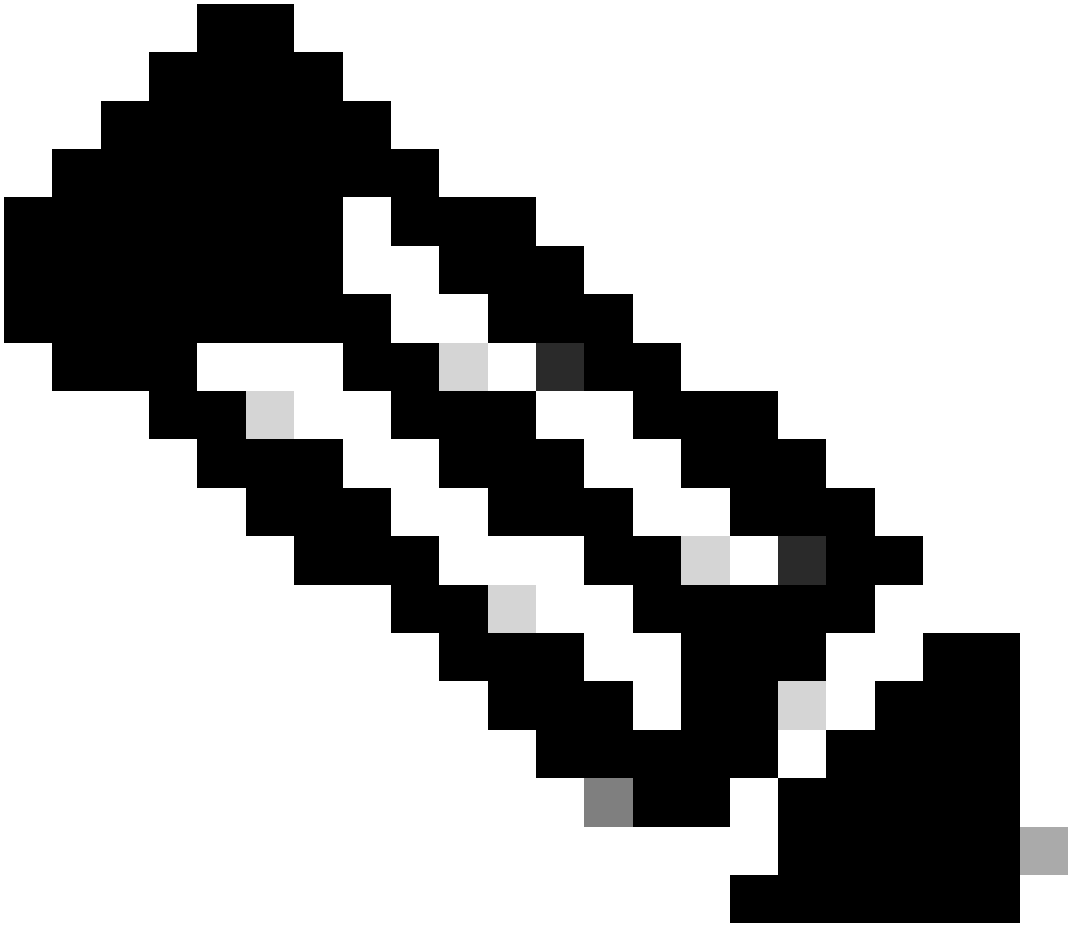
— Applica l'elenco degli accessi al percorso di ricezione.

ip receive access-list 151

Per identificare e autorizzare il traffico legittimo su un dispositivo e rifiutare tutti i pacchetti indesiderati, consultare gli Access Control List.

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 XE.



Nota: se si elimina il traffico proveniente da indirizzi IP sconosciuti o non attendibili, gli host con indirizzi IP assegnati in modo dinamico potrebbero non essere in grado di connettersi al dispositivo Cisco IOS XE.

access-list 152 deny tcp <indirizzi-attendibili> <maschera> any eq 22

access-list 152 permetta tcp any eq 22

access-list 152 deny ip any

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

mappa criteri 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 da parte della 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 nella versione software Cisco IOS XE.

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

Control Plane Protection

La funzionalità Control Plane Protection (CPPr), introdotta nel software Cisco IOS XE versione 16.6.4, può essere utilizzata per limitare o controllare il traffico aereo destinato alla CPU del dispositivo Cisco IOS XE. 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, la CPPr comprende le seguenti funzioni di protezione del control plane:

1. Funzione di filtro delle porte: questa funzione consente di controllare e scartare i pacchetti inviati a porte TCP o UDP chiuse o non in ascolto.
2. Funzione di soglia della coda: questa funzione limita il numero di pacchetti per un protocollo specificato che sono 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 (HWRL) specifici della 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 dispositivi HWRL possono proteggere il dispositivo Cisco IOS XE da una serie di attacchi che richiedono l'elaborazione dei pacchetti da parte della CPU.

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 preso di mira dagli utenti non autorizzati per la sua ubiquità e la natura complessa e dimenticata 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 in base al sistema operativo e in genere varia da 64 a 255. Un pacchetto viene scartato quando il relativo 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 dei router peer; tuttavia, una volta abilitata, 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>

neighbors <indirizzo-ip> remote-as <asn-remota>

neighbors <indirizzo-ip> ttl-security hops <conteggio-hop>

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> neighbors <indirizzo-ip> remote-as <asn-remota>

neighbor <indirizzo-ip> password <segreto>

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 utente 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: il 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> neighbors <indirizzo-ip> remote-as <asn-remota>

neighbor <indirizzo-ip> maximum-prefix <soglia-arresto> <percentuale-registro>

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 possibile utilizzare gli elenchi di prefissi per garantire l'invio del traffico di rete sui percorsi desiderati. È possibile applicare gli elenchi di prefissi a ogni peer eBGP sia in entrata che 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 possibile configurare un elenco di prefissi in modo da bloccare specificamente 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. È possibile configurare gli elenchi di prefissi in uscita in modo da consentire in modo specifico 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 allow 0.0.0.0/0

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

router bgp <asn>

router adiacente <indirizzo-ip> prefix-list BGP-PL-INBOUND in

router adiacente <indirizzo-ip> prefix-list BGP-PL-OUTBOUND out

Per una copertura completa del filtro dei prefissi BGP, consultare il documento sul filtro delle route in uscita basato sul prefisso.

Filtra 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 allow

ip as-path access-list 2 allow

router bgp <asn>

neighbors <indirizzo-ip> remote-as 65501

neighbor <indirizzo-ip> filter-list 1 in

router adiacente <indirizzo-ip> 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.

Quando si aggiungono 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. Dal momento che 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 che utilizza MD5:

key chain <nome-chiave>

key <identificatore-chiave>

key-string <password>

interface <interface> modalità di autenticazione ip eigrp <as-number> md5

ip authentication key-chain eigrp <as-number> <nome-chiave>

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

key chain <nome-chiave>

key <identificatore-chiave>

key-string <password>

interface <interface> modalità di autenticazione ip rip md5

ip rip authentication key-chain <nome-chiave>

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

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

router ospf <process-id>

network 10.0.0.0 0.255.255.255 area 0 area 0 autenticazione 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> impostazione predefinita interfaccia passiva

no passive-interface <interfaccia> (interfaccia passiva)

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 <nome-elenco>

seq 10 allow <prefisso>

router eigrp <numero-as>

interfaccia passiva predefinita

no passive-interface <interfaccia> (interfaccia passiva)

prefisso distribute-list <nome-elenco> out <interfaccia>

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

ip prefix-list <nome-elenco> seq 10 allow <prefisso>

router eigrp <numero-as>

interfaccia passiva predefinita

no passive-interface <interfaccia> (interfaccia passiva)

prefisso distribute-list <nome-elenco> in <interfaccia>

Per ulteriori informazioni su come controllare la pubblicità e l'elaborazione degli aggiornamenti del routing, fare riferimento a EIGRP Route filtering.

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

ip prefix-list <nome-elenco> seq 10 allow <prefisso>

router ospf <process-id>

area <id-area> filter-list prefix <nome-elenco> 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 <id-processo> max-lsa <numero-massimo>

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 XE 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 Fast Ethernet 1

descrizione *** Autenticazione GLBP ***

glbp 1 authentication md5 key-string <segreto glbp>

glbp 1 ip 10.1.1.1

interface Fast Ethernet 2

descrizione *** Autenticazione HSRP ***

standby 1 autenticazione md5 key-string <hsrp-secret>

standby 1 ip 10.2.2.1

interface Fast Ethernet 3

descrizione *** Autenticazione VRRP ***

vrp 1 authentication md5 key-string <segreto vrp>

vrp 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. Per questo motivo, quando si protegge un dispositivo di rete, è importante proteggere di preferenza i piani di gestione e di controllo rispetto al piano dati.

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.

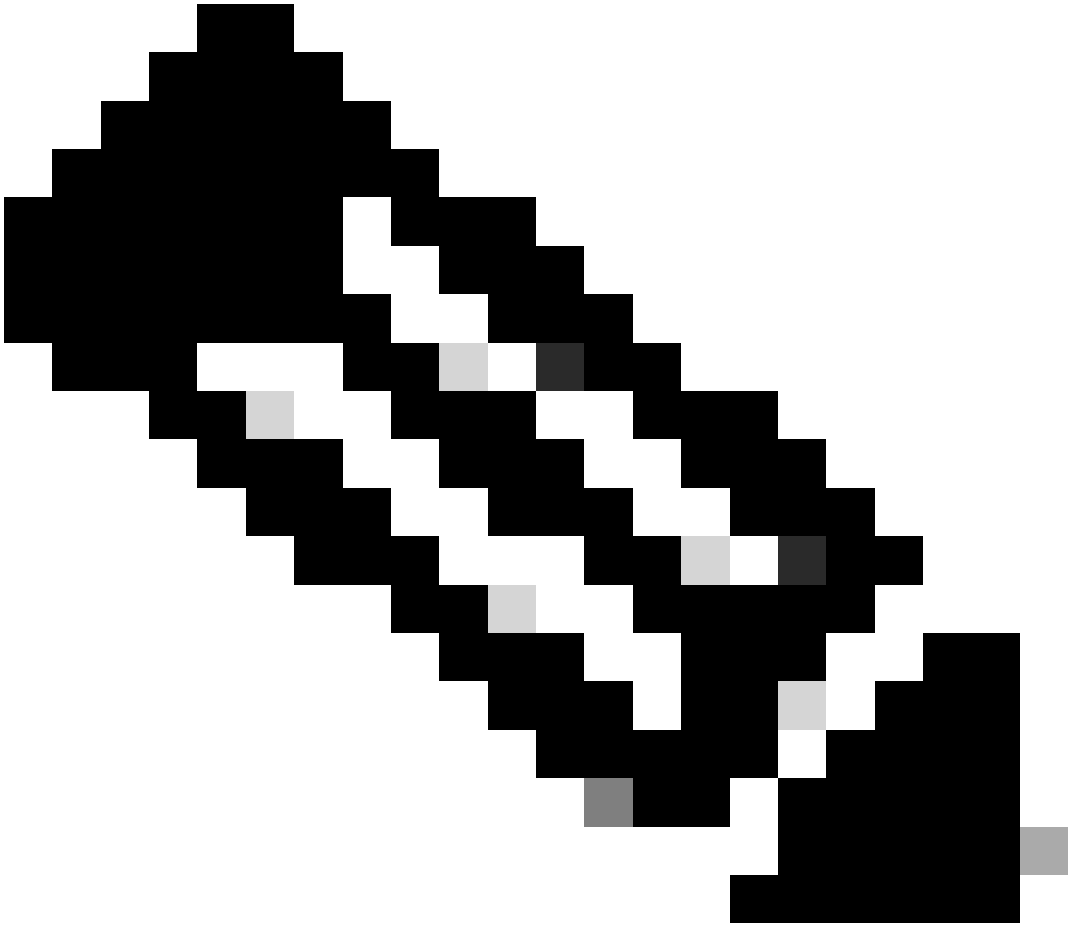
Caduta selettiva opzioni IP

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 XE, 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 XE versione 16.6.4 e successive. Nella prima forma di questo comando, ip options drop, tutti i pacchetti IP che contengono opzioni IP ricevute dal dispositivo Cisco IOS XE, 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 XE 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 vivamente di eliminare la forma di questo comando. Questa condizione viene dimostrata nell'esempio di configurazione:

opzioni ip ignorate



Nota: alcuni protocolli, ad esempio l'RSVP, fanno un uso legittimo delle 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 XE, è disabilitato con il comando di configurazione globale no ip source-route.

L'esempio di configurazione riportato di seguito illustra l'utilizzo del 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 XE invia un reindirizzamento se riceve un pacchetto che deve essere indirizzato tramite l'interfaccia su cui è stato ricevuto.

In alcune situazioni, è possibile che un utente non autorizzato faccia in modo che il dispositivo Cisco IOS XE 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 Fast Ethernet 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 che includono l'attacco del mirino.

Nelle versioni correnti del software Cisco IOS XE, questa funzionalità è disabilitata per impostazione predefinita; tuttavia, è possibile abilitarla tramite il comando di configurazione dell'interfaccia ip direct-broadcast. Nelle versioni precedenti alla 12.0, il software Cisco IOS XE dispone di questa funzionalità abilitata per impostazione predefinita.

Se una rete richiede assolutamente una funzionalità di trasmissione diretta, il suo utilizzo può 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 allow udp 192.168.1.0 0.0.0.255 any

interface Fast Ethernet 0

ip direct-broadcast 100

Filtra il traffico di transito con ACL transit

È possibile 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 questo filtro su un dispositivo Cisco IOS XE 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 contro lo spoofing di questo documento.

Per ulteriori informazioni sugli ACL, fare riferimento a Access Control List transit: Filtering at Your Edge.

Filtro pacchetti ICMP

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

Il software Cisco IOS XE offre la funzionalità di filtrare specificamente i messaggi ICMP per nome, 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

— Consenti pacchetti ICMP solo da reti attendibili

consenti host icmp <trusted-networks> qualsiasi

— Nega tutto il traffico IP verso qualsiasi dispositivo di rete

deny icmp 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 possono essere filtrati esplicitamente nella parte superiore di qualsiasi ACL configurato.

L'ACL 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

— Negare ai frammenti IP che utilizzano ACE specifiche del protocollo di supportare

— classificazione del traffico di attacco

deny tcp any fragments

nega tutti i frammenti udp

deny icmp any fragments

deny ip any fragments

Per ulteriori informazioni sulla gestione di pacchetti IP frammentati da parte degli ACL, consultare il documento sull'elaborazione dei frammenti nella lista degli accessi.

Supporto ACL per il filtro delle opzioni IP

Nel software Cisco IOS XE versione 16.6.4 e successive, il software Cisco IOS XE 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 di alterare in altro modo le caratteristiche di transito di un pacchetto. Per questi motivi, i pacchetti con opzioni IP possono 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

— Nega pacchetti IP che contengono opzioni IP

deny ip any any option any-options

Protezioni anti-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 XE 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: loose o strict. 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 <interfaccia>

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.

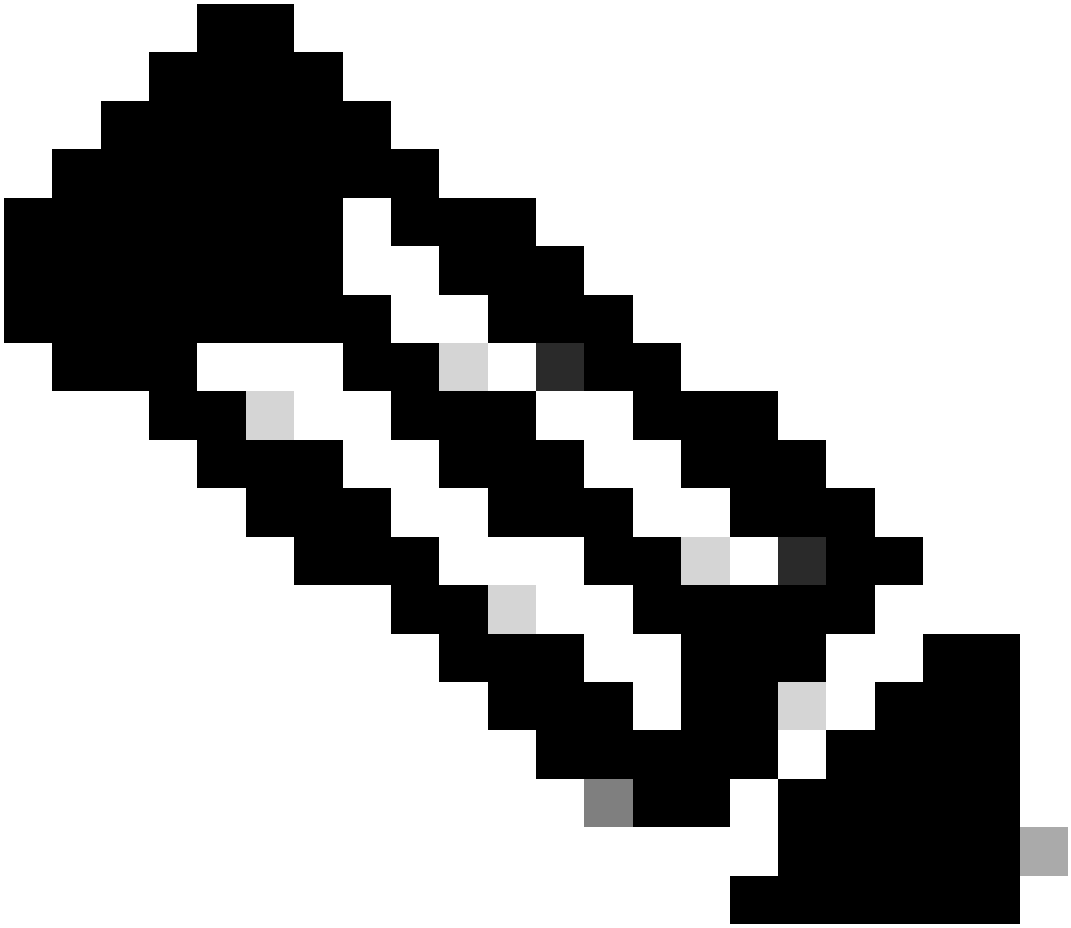
Protezione origine IP

IP Source Guard è un mezzo efficace per prevenire lo spoofing che può essere utilizzato se si ha il 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:

snooping ip dhcp

ip dhcp snooping vlan <vlan-range>



> Nota: per supportare IP Source Guard, lo chassis/router richiede un modulo di switching di livello 2.

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 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 funzione di 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> portaswitch

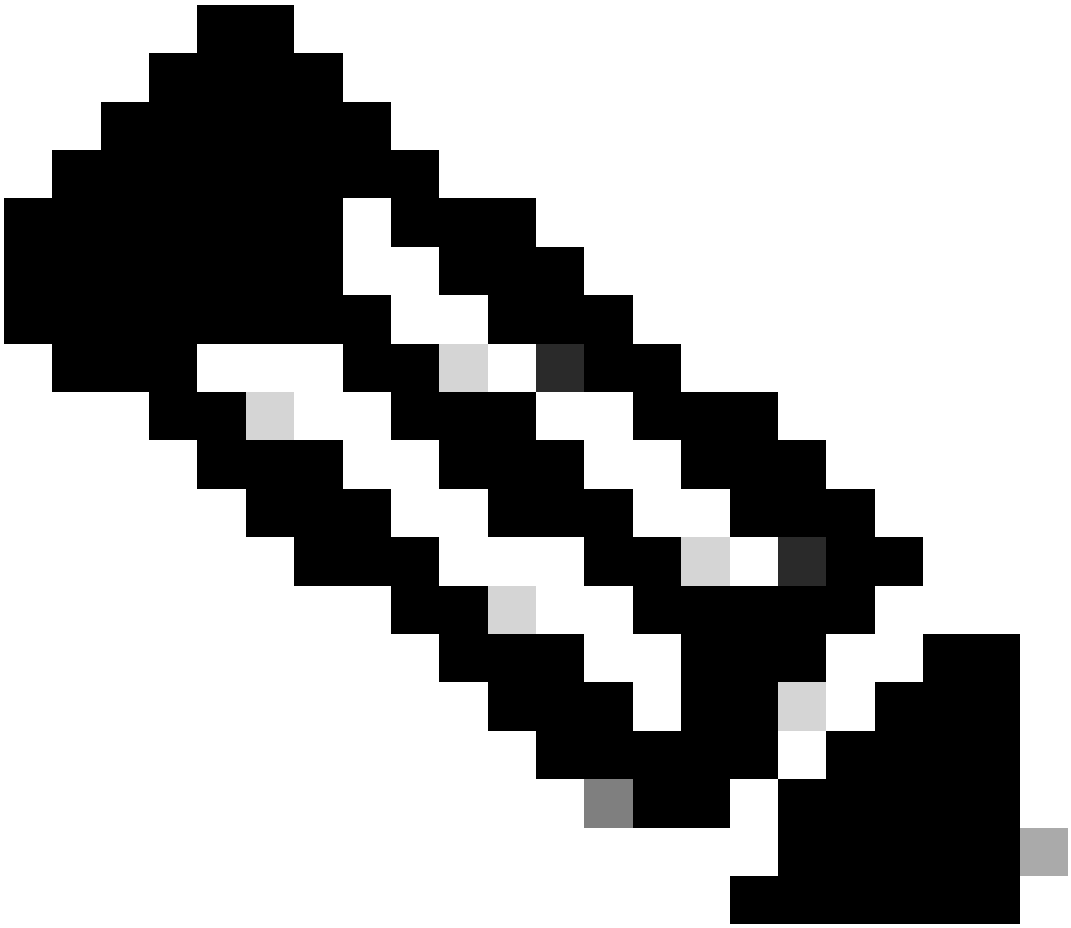
accesso in modalità switchport

switchport port-security

switchport port-security mac-address sticky

switchport port-security maximum <numero>

switchport-violazione della sicurezza <modalità di violazione>



Nota: per supportare la sicurezza delle porte, lo chassis/router richiede un modulo di switching di livello 2.

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

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 al traffico in entrata sull'interfaccia desiderata. Gli ACE che compongono 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 <interfaccia>

ip access-group ACL-ANTISPOOF-IN in

Per ulteriori informazioni su come configurare gli elenchi di controllo di accesso, consultare il documento sulla configurazione degli ACL IPv4.

Limitazione dell'impatto della CPU sul 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 avere un impatto sulle operazioni della CPU di un dispositivo. Il piano dati, costituito dal traffico che attraversa il dispositivo di rete, può 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

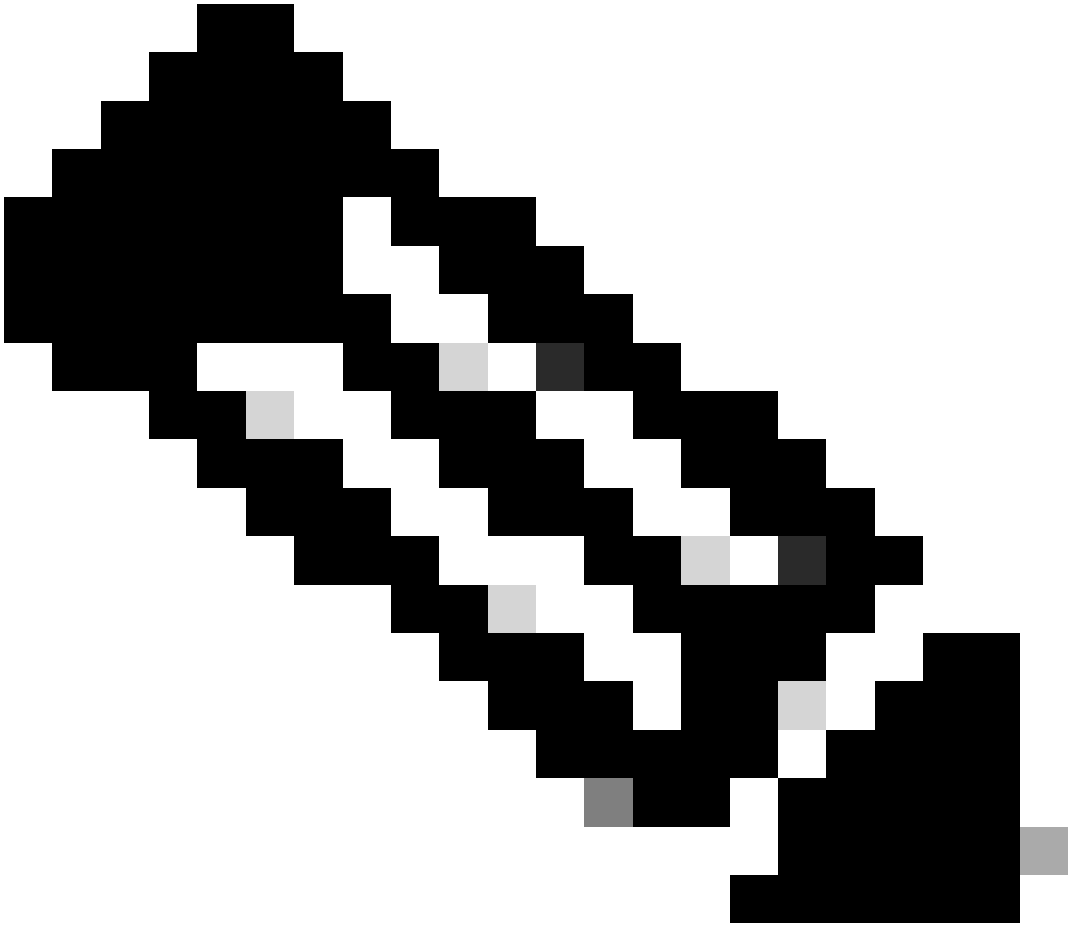
un'elaborazione speciale della CPU e sono commutati dal processo da parte della CPU:

1. Log ACL: il traffico di log 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.
2. L'uso combinato di RPF unicast e RPF unicast con un ACL può causare la commutazione di alcuni pacchetti.
3. Opzioni IP - Tutti i pacchetti IP con opzioni incluse devono essere elaborati dalla CPU.
4. Frammentazione: tutti i pacchetti IP che richiedono la frammentazione devono essere passati alla CPU per essere elaborati.
5. Scadenza TTL (Time-to-Live): 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), con conseguente elaborazione da parte della CPU.
6. ICMP Unreachables - I pacchetti che causano messaggi ICMP "destinazione irraggiungibile" a causa di routing, MTU o filtro vengono elaborati dalla CPU.
7. Traffico che richiede una richiesta ARP: le destinazioni per le quali non esiste una voce ARP richiedono l'elaborazione da parte della CPU.
8. Traffico non IP - Tutto il traffico non IP viene elaborato dalla CPU.

   Per ulteriori informazioni su Protezione avanzata piano dati, vedere la sezione Protezione avanzata piano dati generale di questo documento.

Filtra in base al valore TTL

È possibile usare la funzione di supporto ACL per il filtro sul valore TTL, introdotta nel software Cisco IOS XE versione 16.6.4, 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 e che quindi protegga il control plane dei dispositivi dell'infrastruttura a valle dagli attacchi TTL in scadenza.



Nota: 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.

— Creare un criterio ACL che filtra i pacchetti IP con un valore TTL.

— inferiore a 6

ip access-list extended ACL-TRANSIT-IN

deny ip any ttl lt 6

allow ip any

— Applica l'elenco degli accessi all'interfaccia nella direzione in entrata.

interfaccia Gigabit Ethernet 0/0

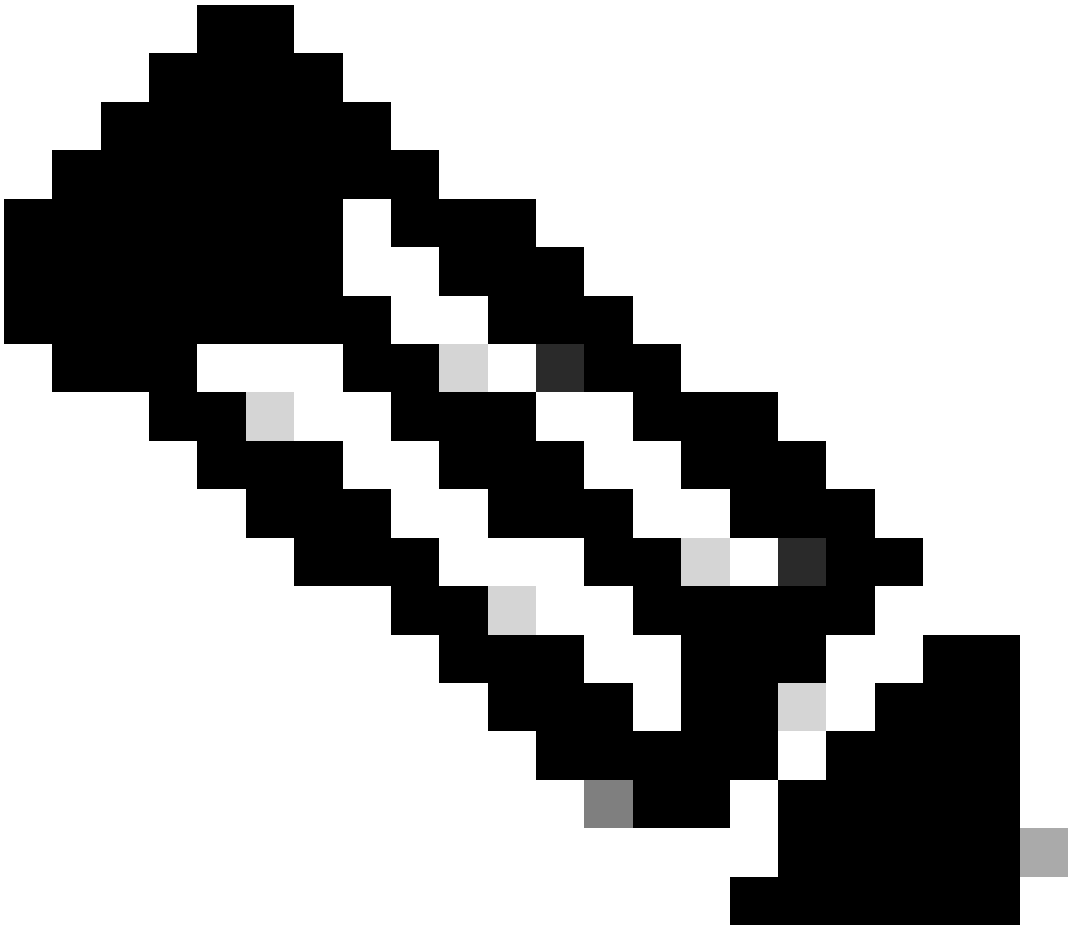
ip access-group ACL-TRANSIT-IN in

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.

Filtra in base alla presenza di opzioni IP

Nel software Cisco IOS XE versione 16.6.4 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.



Nota: 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 non possono 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 funzione ACL IP Options Selective Drop potrebbe causare il rifiuto di questo traffico e questi protocolli non possono 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

allow ip any

interfaccia Gigabit Ethernet 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:

1. 0 Fine elenco opzioni (eool)
2. 7 Record Route (record-route)
3. Timestamp 68 (timestamp)
4. 131 - Loose Source Route (lsr)
5. 137 - SSR (Strict Source Route)

ip access-list extended ACL-TRANSIT-IN

deny ip any option eool

deny ip any any option record-route

deny ip any any option timestamp

deny ip any option lsr

deny ip any option ssr

allow ip any

interfaccia Gigabit Ethernet 0/0

ip access-group ACL-TRANSIT-IN in

Per ulteriori informazioni sulle opzioni IP degli ACL, vedere la sezione Protezione avanzata del piano dati in questo documento.

Un'altra funzionalità del software Cisco IOS XE che può essere utilizzata per filtrare i pacchetti con opzioni IP è CoPP. Sul software Cisco IOS XE versione 16.6.4 e successive, 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 XE versione 16.6.4, può utilizzare un criterio dell'elenco degli accessi per filtrare i pacchetti contenenti 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

consenti ip qualsiasi opzione qualsiasi

class-map ACL-IP-OPTIONS-CLASS

match access-group name ACL-IP-OPTIONS-ANY

mappa-criteri COPP-POLICY

class ACL-IP-OPTIONS-CLASS

Police 80000 conforme trasmettere superare goccia

piano di controllo

input di service-policy COPP-POLICY!

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

1. 0 Fine elenco opzioni (eool)
2. 7 Record Route (record-route)
3. Timestamp 68 (timestamp)
4. 131 Loose Source Route (lsr)
5. 137 Strict Source Route (ssr)

ip access-list extended ACL-IP-OPTIONS

allow ip any option eool

allow ip any any option record-route

consenti ip con qualsiasi opzione timestamp

consenti ip any option lsr

consenti ip con qualsiasi opzione ssr

class-map ACL-IP-OPTIONS-CLASS

match access-group name ACL-IP-OPTIONS

mappa-criteri COPP-POLICY

class ACL-IP-OPTIONS-CLASS

Police 80000 conforme trasmettere superare goccia

piano di controllo

input criteri servizio 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 XE versione 16.6.4 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 XE. Anche se simile al CoPP, il CPPr ha la capacità di limitare o controllare il traffico che utilizza una granularità più fine rispetto al CoPP. Il CPPr divide il control plane aggregato in tre categorie separate 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

allow ip 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

allow ip 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

allow ip any option eool

allow ip any any option record-route

consenti ip con qualsiasi opzione timestamp

consenti ip any option lsr

consenti ip con qualsiasi opzione ssr

class-map ACL-IP-OPTIONS-CLASS

match access-group name ACL-IP-OPTIONS

mappa-criteri CPPR-CEF-EXCEPTION-POLICY

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

cascata conforme-azione Police 80000

class ACL-IP-OPTIONS-CLASS

cascata conforme-azione Police 8000

mappa-politica CPPR-TRANSIT-POLICY

class ACL-IP-TTL-LOW-CLASS

cascata conforme-azione Police 8000

transito sul control plane

input dei criteri dei servizi 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 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 feature CPPr, fate riferimento a Control Plane Policing.

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 XE. NetFlow può fornire visibilità su tutto il traffico della rete. Inoltre, NetFlow può essere implementato con collector in grado di fornire analisi automatiche e di analisi dei trend 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 di 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, attraverso i trend a lungo termine, possono fornire il comportamento della rete e l'analisi dell'utilizzo. 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 i dati del 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 XE, il comando per abilitare NetFlow su un'interfaccia è ip route-cache flow anziché ip flow {ingress | in uscita}.

ip flow-export destination <indirizzo-ip> <porta-udp>

ip flow-export versione <versione>

interface <interfaccia>

ip flow <ingess|uscita>

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 (2662860 pacchetti totali):

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 .003 .000 .001 .000 .000

512 544 576 1024 1536 2048 2560 3072 3584 4096 4608

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

Cache IP Flow Switching, 4456704 byte

55 attivi, 65481 inattivi, 1014683 aggiunti

41000680 polling ager, 0 errori allocazione flusso

Timeout flussi attivi tra 2 minuti

Timeout flussi inattivi in 60 secondi

Cache IP Sub Flow, 336520 byte

110 attivo, 16274 inattivo, 2029366 aggiunto, 1014683 aggiunto al flusso

0 errori di allocazione, 0 libera forza 1 blocco, 15 blocchi aggiunti ultima cancellazione di statistiche mai

Protocollo Totale Flussi Pacchetti Byte Pacchetti Attivi (Sec) Inattivi (Sec)

— Flussi /Sec /Flow /Pkt /Sec /Flow /Flow

TCP-Telnet 1512 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 7155 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 14 0.0 1 40 0.0 0.0 62.4

TCP-NNTP 120 0.0 1 42 0.0 0.7 61.4

TCP-altro 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 1989 0,0 37 33 0,9 26,0 53,9

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

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

SrcIf IndirizzoIPorigDstIf IndirizzoIPorig Pr Pacchetti DstP SrcP

Gi0/1 192.168.128.21 Locale 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 Locale 192.168.206.20 01 000 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 Flexible 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 suddivisa in protocolli o porte specifiche. Questa classificazione più granulare del traffico in voci ACE specifiche può aiutare a comprendere il traffico di rete, in quanto ogni categoria di traffico ha un proprio contatore di visite. L'amministratore può anche separare 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 usando 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

nota Contenuto esistente di ACL

nota Classificazione del traffico TCP specifico per SMB

nega tcp any eq 139

nega tcp any eq 445

deny ip any any

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

EXEC. Per cancellare i contatori dell'ACL, usare il comando clear ip access-list counters aclname EXEC.

router#show access-list ACL-SMB-CLASSIFY Elenco accessi IP esteso ACL-SMB-CLASSIFY

10 nega tcp any eq 139 (10 corrispondenze)

20 deny tcp any eq 445 (9 corrispondenze)

30 deny ip any any (184 corrispondenze)

Per ulteriori informazioni su come abilitare le funzionalità di log negli ACL, fare riferimento a Descrizione della registrazione nella lista di controllo dell'accesso.

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 <nome-acl> allow <protocollo> <indirizzo-origine> <porta-origine> <indirizzo-destinazione> <porta-destinazione> !

interface <type> <slot/port> modalità di accesso switchport accesso vlan <vlan_number> gruppo di accesso ip <acl-name> in !

Per ulteriori informazioni sulla configurazione degli ACL, consultare la sezione Configurazione della sicurezza di rete con gli ACL delle porte di.

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. Le VLAN isolate possono essere utilizzate su reti non attendibili, ad esempio reti che supportano gli utenti guest.

Nell'esempio di configurazione, la VLAN 11 è configurata come VLAN isolata e associata alla VLAN 20 primaria. Nell'esempio, l'interfaccia Fast Ethernet 1/1 è configurata anche come porta isolata nella VLAN 11:

vlan 11 private-vlan isolata

vlan 20 private-vlan primary private-vlan association 11

descrizione interfaccia Fast Ethernet 1/1 *** Porta in VLAN isolata *** modalità switchport 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 rispetto alla VLAN 20 primaria.

vlan 12 private-vlan community

vlan 20 private-vlan primary private-vlan association 12

descrizione interfaccia Fast Ethernet 1/2 *** Porta nella VLAN della community *** modalità switchport modalità host vlan privata switchport vlan privata associazione host 20 12

Conclusioni

Questo documento offre un'ampia panoramica dei metodi che possono essere utilizzati per proteggere un dispositivo di sistema Cisco IOS XE. Se si proteggono i dispositivi, si 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: checklist di protezione avanzata dei dispositivi Cisco IOS XE

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 XE, anche se una funzionalità non è stata implementata perché non era applicabile. Si consiglia agli amministratori di valutare ogni opzione in relazione ai potenziali rischi prima di implementarla.

Piano di gestione

1. Password
   Abilita hashing MD5 (opzione segreta) per abilitare le password degli utenti localiConfigurare il blocco dei tentativi di reimpostazione della passwordDisabilitare il recupero della password (prendere in considerazione i rischi)
2. Disabilita servizi inutilizzati
3. Configurare i pacchetti TCP keepalive per le sessioni di gestione
4. Impostazione delle notifiche di soglia della memoria e della CPU
5. Configurazione
   Notifiche di soglia della memoria e della CPU Memoria riservata per l'accesso alla console Rilevatore di perdite di memoria Rilevamento di overflow del buffer Raccolta avanzata informazioni arresto anomalo
6. Uso degli iACL per limitare l'accesso alla gestione
7. Filtro (considerare i rischi)
   pacchetti ICMPframmenti IPopzioni IPvalore TTL nei pacchetti
8. Control Plane Protection
   Configurare il filtro delle porteConfigurare le soglie della coda
9. Accesso alla gestione
   Utilizzare Management Plane Protection per limitare le interfacce di gestioneImpostare il timeout di esecuzioneUtilizzare un protocollo di trasporto crittografato (ad esempio SSH) per l'accesso CLIcontrollare il trasporto per le linee vty e tty (opzione della classe di accesso)Avvertire che utilizzare i banner
10. AAA
    Usare AAA per l'autenticazione e il fallbackUsare AAA (TACACS+) per l'autorizzazione dei comandiUsare AAA per l'accountingUsare server AAA ridondanti
11. SNMP
    Configurazione delle community SNMPv2 e applicazione degli ACLconfigurazione di SNMPv3
12. Registrazione
    Configurare la registrazione centralizzataImpostare i livelli di registrazione per tutti i componenti rilevantiImpostare l'origine della registrazione interfacciaConfigurare la granularità dei timestamp di registrazione
13. Gestione della configurazione

Sostituire e ripristinare lo stato precedenteAccesso esclusivo alle modifiche alla configurazioneConfigurazione della resilienza del softwareNotifiche delle modifiche alla configurazione.

Piano di controllo

1. Disabilita (considera rischio)
   Reindirizzamenti ICMPicmp non raggiungibiliARP proxy
2. Configura autenticazione NTP se viene utilizzato NTP
3. Configura Control Plane Policing/Protection (filtro porte, soglie coda)
4. 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)
5. Configurare i limitatori di velocità hardware
6. Protocolli di ridondanza Secure First Hop (GLBP, HSRP, VRRP)

Piano dati

1. Configura eliminazione selettiva opzioni IP
2. Disabilita (considera rischio)
   instradamento sorgente IPtrasmissioni dirette IPreindirizzamenti ICMP
3. Limita trasmissioni dirette IP
4. Configurazione degli ACL (considerare i rischi)
   Filtra ICMPFiltra frammenti IPopzioni di filtro IPvalori di filtro TTL
5. Configurare le protezioni anti-spoofing necessarie
   ACLsIP Source GuardDynamic ARP InspectionUnicast RPFProtezione porte
6. Control Plane Protection (control-plane cef-exception)
7. Configurazione di NetFlow e degli ACL di classificazione per l'identificazione del traffico
8. Configurazione degli ACL di controllo dell'accesso richiesti (mappe VLAN, PACL, MAC)
9. Configurazione di VLAN private

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).