IOS Zone-Based Firewall: Esempio di configurazione della connessione PSTN CME/CUE/GW per un singolo sito o filiale

Sommario

Introduzione

I Cisco Integrated Service Router (ISR) offrono una piattaforma scalabile per soddisfare i requisiti di rete voce e dati per una vasta gamma di applicazioni. Sebbene lo scenario delle minacce delle reti private e connesse a Internet sia molto dinamico, Cisco IOS Firewall offre funzionalità di ispezione stateful e di controllo e ispezione delle applicazioni (AIC) per definire e applicare una postura di rete sicura, garantendo al contempo funzionalità e continuità aziendali.

In questo documento vengono descritte le considerazioni di progettazione e configurazione per gli aspetti di sicurezza del firewall di scenari specifici di applicazioni voce e dati basati su Cisco ISR. Per ogni scenario applicativo vengono fornite le configurazioni per i servizi voce e il firewall. In ogni scenario vengono descritte separatamente le configurazioni VoIP e di sicurezza, seguite dall'intera configurazione del router. Per mantenere la qualità della voce e la riservatezza, la rete potrebbe richiedere altre configurazioni per servizi quali QoS e VPN.

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.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Sfondo di IOS Firewall

Cisco IOS Firewall viene in genere implementato in scenari applicativi diversi dai modelli di implementazione dei firewall per appliance. Le implementazioni tipiche includono applicazioni Teleworker, uffici di piccole o filiali e applicazioni per la vendita al dettaglio, dove è necessario un numero ridotto di dispositivi, l'integrazione di più servizi e una riduzione delle prestazioni e della profondità delle funzionalità di sicurezza.

Anche se l'applicazione dell'ispezione del firewall, insieme ad altri servizi integrati nei prodotti ISR, potrebbe sembrare interessante dal punto di vista economico e operativo, è necessario valutare considerazioni specifiche per determinare se un firewall basato su router è appropriato. L'applicazione di ciascuna funzionalità aggiuntiva comporta costi di memoria ed elaborazione e contribuisce probabilmente a ridurre la velocità di trasmissione, a migliorare la latenza dei pacchetti e a perdere la funzionalità durante i periodi di picco di carico se viene installata una soluzione basata su router integrato sottoalimentata.

Quando si sceglie tra un router e un accessorio, attenersi alle seguenti linee guida:

- I router con più funzionalità integrate abilitate sono ideali per le filiali o i siti di telelavoro dove un numero inferiore di dispositivi offre una soluzione migliore.
- Le applicazioni ad alte prestazioni e larghezza di banda elevata sono in genere meglio gestite con gli accessori: Cisco ASA e Cisco Unified Call Manager Server devono essere applicati per gestire l'applicazione dei criteri di sicurezza NAT e l'elaborazione delle chiamate, mentre i router soddisfano i requisiti dell'applicazione dei criteri QoS, della terminazione della WAN e della connettività VPN da sito a sito.

Prima dell'introduzione del software Cisco IOS versione 12.4(20)T, il firewall classico e ZFW (Zone-Based Policy Firewall) non erano in grado di supportare completamente le funzionalità richieste per il traffico VoIP e i servizi voce basati su router, richiedendo ampie aperture in policy firewall altrimenti sicure per supportare il traffico vocale e offrendo supporto limitato per l'evoluzione dei protocolli di segnalazione e multimediali VoIP.

Implementazione di Cisco IOS Zone-Based Policy Firewall

Il firewall dei criteri basati sulle zone di Cisco IOS, simile ad altri firewall, può offrire un firewall sicuro solo se i requisiti di sicurezza della rete sono identificati e descritti dai criteri di sicurezza. Esistono due approcci fondamentali per giungere a una politica di sicurezza: la prospettiva della *fiducia*, in contrapposizione alla prospettiva *sospetta*.

La prospettiva *trusting* presuppone che tutto il traffico sia attendibile, ad eccezione di quello che può essere identificato specificamente come dannoso o indesiderato. Vengono implementati criteri specifici che negano solo il traffico indesiderato. A tale scopo, vengono in genere utilizzate voci di controllo di accesso specifiche o strumenti basati su firma o comportamento. Questo approccio tende a interferire meno con le applicazioni esistenti, ma richiede una conoscenza completa del panorama delle minacce e delle vulnerabilità, e richiede una vigilanza costante per affrontare le nuove minacce e gli attacchi nel momento in cui si presentano. Inoltre, la comunità degli utenti deve svolgere un ruolo di primo piano nel mantenimento di una protezione adeguata. Un ambiente che permette un'ampia libertà con uno scarso controllo per gli occupanti offre un'opportunità sostanziale per i problemi causati da individui imprudenti o malintenzionati. Un ulteriore problema di questo approccio è che si basa molto di più su strumenti di gestione e controlli delle applicazioni efficaci che offrono flessibilità e prestazioni sufficienti per monitorare e controllare i dati sospetti in tutto il traffico di rete. Sebbene la tecnologia sia attualmente disponibile per risolvere questo problema, il carico operativo spesso supera i limiti della maggior parte delle organizzazioni.

La prospettiva *sospetta* presume che tutto il traffico di rete sia indesiderato, ad eccezione del traffico *buono* identificato in modo specifico. Criterio applicato che nega tutto il traffico dell'applicazione ad eccezione di quello esplicitamente consentito. Inoltre, è possibile implementare l'ispezione e il controllo delle applicazioni (AIC) per identificare e negare il traffico dannoso appositamente creato per sfruttare le applicazioni "buone", nonché il traffico indesiderato mascherato da traffico buono. Anche in questo caso, i controlli delle applicazioni impongono un carico operativo e prestazionale sulla rete, anche se la maggior parte del traffico indesiderato dovrebbe essere controllato da filtri senza stato, ad esempio gli elenchi di controllo di accesso (ACL) o i criteri ZFW (Zone-Based Policy Firewall). Di conseguenza, dovrebbe esserci una quantità sostanzialmente inferiore di traffico che deve essere gestito da AIC, dal sistema di prevenzione delle intrusioni (IPS) o da altri controlli basati su firma, ad esempio FPM (Flexible Packet Matching) o NBAR (Network-Based Application Recognition). Pertanto, se solo le porte applicative desiderate (e il traffico dinamico specifico dei supporti derivante da sessioni o connessioni di controllo conosciute) sono specificamente consentite, l'unico traffico indesiderato che dovrebbe essere presente sulla rete dovrebbe rientrare in un sottoinsieme specifico e più facilmente riconoscibile, il che riduce il carico di lavoro e di progettazione imposto per mantenere il controllo sul traffico indesiderato.

Questo documento descrive le configurazioni di sicurezza VoIP basate su una prospettiva *sospetta*; pertanto, è consentito solo il traffico autorizzato nei segmenti della rete voce. I criteri dati tendono ad essere più permissivi, come descritto dalle note nella configurazione di ogni scenario di applicazione.

Tutte le installazioni di politiche di sicurezza devono seguire un ciclo di feedback a circuito chiuso; le implementazioni di protezione in genere influiscono sulla capacità e sulle funzionalità delle applicazioni esistenti e devono essere regolate per ridurre al minimo o risolvere questo impatto.

Per ulteriori informazioni su come configurare il firewall dei criteri basato sulle zone, vedere la guida alla progettazione e all'applicazione di firewall dei criteri basati sulle zone di Cisco IOS Firewall.

Considerazioni su ZFW in ambienti VoIP

La Guida alla progettazione e all'applicazione di firewall per le policy basate sulle zone di Cisco IOS Firewall offre una breve discussione sulla sicurezza del router con l'utilizzo di policy di sicurezza per e dalla zona *autonoma* del router, nonché funzionalità alternative fornite tramite diverse funzionalità di Network Foundation Protection (NFP). Le funzionalità VoIP basate su router sono ospitate nell'area autonoma del router, quindi i criteri di sicurezza che proteggono il router devono essere a conoscenza dei requisiti per il traffico vocale, al fine di supportare la segnalazione vocale e i supporti originati e destinati alle risorse Cisco Unified CallManager Express, Survivable Remote-Site Telephony e Voice Gateway. Nelle versioni precedenti al software Cisco IOS versione 12.4(20)T, il firewall classico e il firewall dei criteri basati su zone non erano in grado di soddisfare completamente i requisiti del traffico VoIP, quindi i criteri del firewall non erano ottimizzati per proteggere completamente le risorse. I criteri di sicurezza basati su zone autonome che proteggono le risorse VoIP basate su router dipendono in larga misura dalle funzionalità introdotte nella versione 12.4(20)T.

Miglioramenti voce di IOS Firewall - 12.4(20)T

Il software Cisco IOS versione 12.4(20)T ha introdotto diversi miglioramenti per abilitare le funzionalità voce e firewall nelle zone condivise. Tre caratteristiche principali si applicano direttamente alle applicazioni voce protette:

- Miglioramenti SIP: Gateway a livello di applicazione e controllo e ispezione delle applicazioniAggiorna il supporto della versione SIP per SIPv2, come descritto nella RFC 3261Amplia il supporto di segnalazione SIP per riconoscere una più ampia varietà di flussi di chiamateIntroduce SIP Application Inspection and Control (AIC) per applicare controlli granulari per affrontare vulnerabilità e exploit specifici a livello di applicazioneEspande l'ispezione automatica della zona per riconoscere i canali di segnalazione secondari e multimediali risultanti dal traffico SIP destinato/originato localmente
- Supporto per Skinny Local Traffic e CMEAggiorna il supporto SCCP alla versione 16 (versione 9 supportata in precedenza)Introduce SCCP Application Inspection and Control (AIC) per applicare controlli granulari per affrontare vulnerabilità e exploit specifici a livello di applicazioneEspande l'ispezione di zona per riconoscere i canali di segnalazione e multimediali secondari risultanti dal traffico SCCP destinato/originato localmente
- Supporto H.323 v3/v4Aggiorna il supporto H.323 per v3 e v4 (precedentemente supportati v1 e v2)Introduce H.323 Application Inspection and Control (AIC) per applicare controlli granulari per affrontare vulnerabilità e exploit specifici a livello di applicazione

Le configurazioni di sicurezza dei router descritte in questo documento includono le funzionalità offerte da questi miglioramenti, con una spiegazione dell'azione applicata dalle policy. Per ulteriori informazioni sulle funzioni di ispezione vocale, consultare i documenti relativi alle singole funzioni elencati nella sezione Informazioni correlate di questo documento.

Avvertenze

Per rafforzare i punti menzionati in precedenza, l'applicazione di Cisco IOS Firewall con funzionalità voce basate su router deve applicare Zone-Based Policy Firewall. Il firewall IOS classico non include la funzionalità necessaria per supportare completamente la complessità e il comportamento della segnalazione del traffico vocale.

Network Address Translation

Cisco IOS Network Address Translation (NAT) viene spesso configurato contemporaneamente a Cisco IOS Firewall, in particolare nei casi in cui le reti private devono interfacciarsi con Internet o devono connettersi reti private diverse, in particolare se viene utilizzato uno spazio degli indirizzi IP sovrapposto. Il software Cisco IOS include NAT Application Layer Gateway (ALG) per SIP, Skinny e H.323. Idealmente, la connettività di rete per la voce IP può essere ospitata senza l'applicazione di NAT, in quanto NAT introduce una maggiore complessità per la risoluzione dei problemi e le applicazioni di policy di sicurezza, in particolare nei casi in cui viene utilizzato il sovraccarico NAT. NAT deve essere applicato solo come soluzione last case per risolvere i problemi di connettività di rete.

Cisco Unified Presence Client

Questo documento non descrive configurazioni che supportano l'uso di Cisco Unified Presence Client (CUPC) con IOS Firewall, in quanto CUPC non è ancora supportato da Zone o Classic Firewall come dal software Cisco IOS versione 12.4(20)T1. CUPC sarà supportato in una versione futura del software Cisco IOS.

Connessione PSTN CME/CUE/GW a sito singolo o a filiale

In questo scenario viene introdotta una telefonia Voice-over-IP basata su router sicura per le piccole e medie imprese con un singolo sito o per le organizzazioni più grandi che desiderano implementare l'elaborazione distribuita delle chiamate, mantenendo le connessioni preesistenti alla PSTN (Public Switched Telephone Network). Il controllo delle chiamate VoIP è supportato dall'applicazione di Cisco Unified Call Manager Express.

La connettività PSTN può essere mantenuta nel lungo periodo o può essere migrata a una rete WAN IP convergente voce e dati, come descritto nell'esempio di applicazione descritto nella sezione CME/CUE/GW Single Site o Branch Office con SIP Trunk su CCM presso la sede centrale o il provider vocale di questo documento.

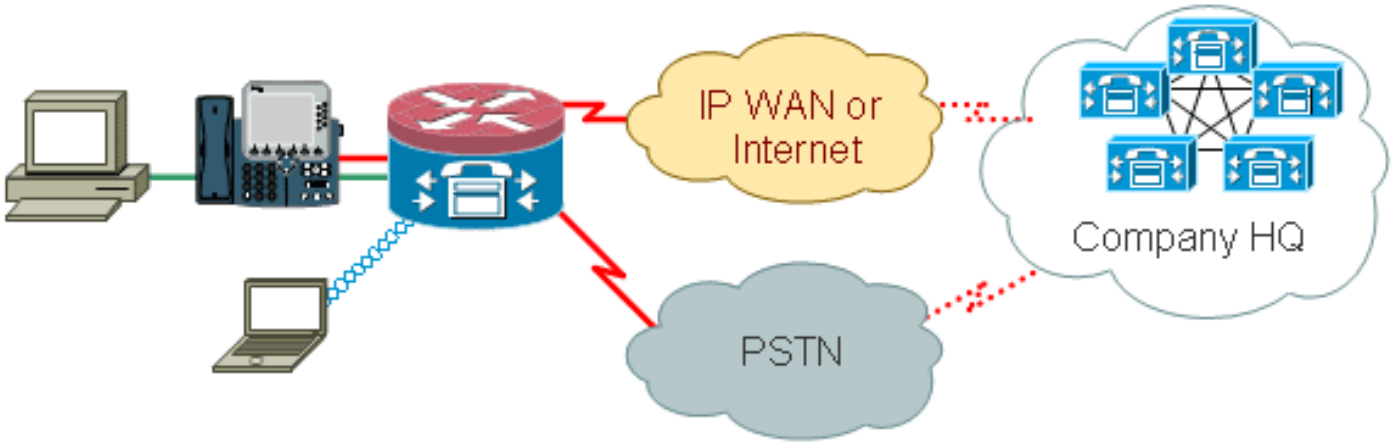
Le organizzazioni dovrebbero prendere in considerazione l'implementazione di questo tipo di scenario applicativo in circostanze in cui vengono utilizzati ambienti VoIP diversi tra i siti o in cui il VoIP è impraticabile a causa di una connettività dei dati WAN inadeguata o di restrizioni specifiche delle impostazioni locali sull'utilizzo del VoIP nelle reti di dati. I vantaggi e le best practice della telefonia IP su un singolo sito sono descritti nella SRND di Cisco Unified CallManager Express.

Sfondo scenario

Lo scenario applicativo incorpora telefoni cablati (VLAN voce), PC cablati (VLAN dati) e dispositivi wireless (che includono dispositivi VoIP come IP Communicator).

La configurazione di protezione fornisce:

- Ispezione della segnalazione avviata dal router tra CME e telefoni locali (SCCP e/o SIP)
- Punti deboli dei supporti vocali per la comunicazione tra:Segmenti cablati e wireless localiCME e i telefoni locali per MoHCUE e i telefoni locali per la segreteria telefonica
- Applica ispezione e controllo applicazione (AIC) a:Numero massimo di messaggi di invitoGaranzia di conformità del protocollo su tutto il traffico SIP.



Vantaggi e svantaggi

Il vantaggio più ovvio dell'aspetto VoIP dello scenario è il percorso di migrazione offerto dall'integrazione dell'infrastruttura di rete voce e dati esistente in un ambiente POTS/TDM esistente, prima del passaggio a una rete voce/dati convergente per i servizi di telefonia al mondo oltre la LAN. I numeri di telefono vengono conservati per le aziende più piccole e i servizi esistenti centrex o DID possono essere mantenuti per le aziende più grandi che desiderano una migrazione graduale per ignorare i pacchetti di telefonia.

Gli svantaggi includono la perdita di risparmi sui costi che potrebbero essere realizzati con il toll bypass passando a una rete voce e dati convergente, oltre ai limiti sulla flessibilità delle chiamate e la mancanza di integrazione e portabilità delle comunicazioni a livello di organizzazione che potrebbero essere realizzati con una rete voce e dati completamente convergente.

Dal punto di vista della sicurezza, questo tipo di ambiente di rete riduce al minimo le minacce alla sicurezza VoIP, evitando l'esposizione delle risorse VoIP alla rete pubblica o alla WAN. Tuttavia, il Call Manager Express di Cisco incorporato nel router sarebbe ancora vulnerabile a minacce interne, quali traffico dannoso o traffico delle applicazioni non funzionante. Pertanto, viene implementata una policy che consente al traffico specifico della voce che soddisfa i controlli di conformità del protocollo e le azioni VoIP specifiche (ad esempio SIP INVITE) sono limitate in modo da ridurre la probabilità di malfunzionamenti del software dannosi o non intenzionali che influiscono negativamente sulle risorse VoIP e sulla fruibilità.

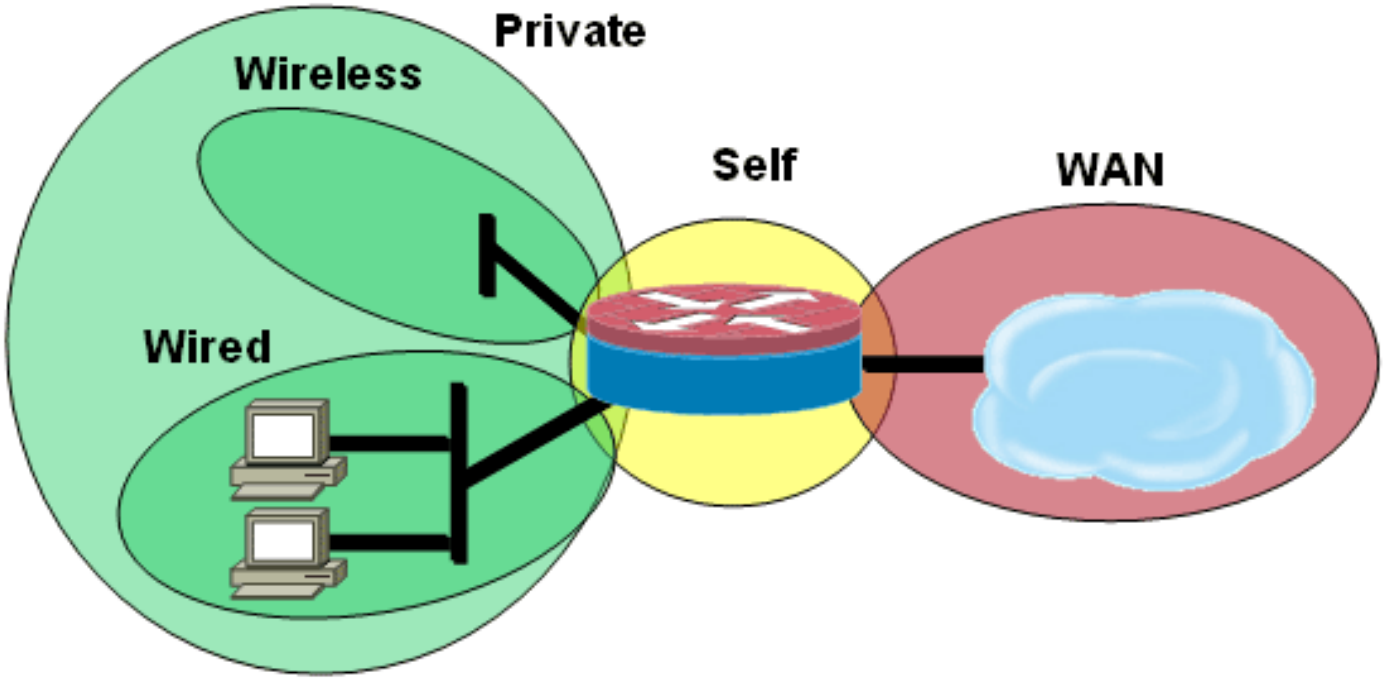
Policy dei dati, firewall basato su zone, sicurezza vocale e configurazioni CCME

La configurazione qui descritta mostra un 2851 con una configurazione Voice Service per la connettività CME e CUE:

```
!
telephony-service
 load 7960-7940 P00308000400
 max-ephones 24
 max-dn 24
 ip source-address 192.168.112.1 port 2000
 system message CME2
 max-conferences 12 gain -6
 transfer-system full-consult
 create cnf-files version-stamp 7960 Jun 10 2008 15:47:13
!
```

Configurazione del firewall dei criteri basata su zone, composta da zone di sicurezza per segmenti

LAN cablati e wireless, LAN privata (composta da segmenti cablati e wireless), segmento WAN pubblico a cui viene raggiunta la connettività Internet non attendibile e zona autonoma in cui si trovano le risorse voce del router.



Configurazione protezione

```
class-map type inspect match-all acl-cmap
 match access-group 171
class-map type inspect match-any most-traffic-cmap
 match protocol tcp
 match protocol udp
 match protocol icmp
 match protocol ftp
!
!
policy-map type inspect most-traffic-pmap
 class type inspect most-traffic-cmap
  inspect
 class class-default
  drop
policy-map type inspect acl-pass-pmap
 class type inspect acl-cmap
  pass
!
zone security private
zone security public
zone security wired
zone security wireless
!
zone-pair security priv-pub source private destination
public
 service-policy type inspect most-traffic-pmap
zone-pair security priv-vpn source private destination
vpn
 service-policy type inspect most-traffic-pmap
zone-pair security acctg-pub source acctg destination
public
 service-policy type inspect most-traffic-pmap
zone-pair security eng-pub source eng destination public
```

```
 service-policy type inspect most-traffic-pmap
!
!
!
interface GigabitEthernet0/0
 ip virtual-reassembly
 zone-member security eng
```

Intera configurazione router

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 2851-cme2
!
!
logging message-counter syslog
logging buffered 51200 warnings
!
no aaa new-model
clock timezone mst -7
clock summer-time mdt recurring
!
dot11 syslog
ip source-route
!
!
ip cef
no ip dhcp use vrf connected
!
ip dhcp pool pub-112-net
   network 172.17.112.0 255.255.255.0
   default-router 172.17.112.1
   dns-server 172.16.1.22
   option 150 ip 172.16.1.43
   domain-name bldrtme.com
!
ip dhcp pool priv-112-net
   network 192.168.112.0 255.255.255.0
   default-router 192.168.112.1
   dns-server 172.16.1.22
   domain-name bldrtme.com
   option 150 ip 192.168.112.1
!
!
ip domain name yourdomain.com
!
no ipv6 cef
multilink bundle-name authenticated
!
!
!
!
voice translation-rule 1
 rule 1 // /1001/
!
!
voice translation-profile default
 translate called 1
!
!
```

```
voice-card 0
 no dspfarm
!
!
!
!
!
interface GigabitEthernet0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-GE 0/0$
 ip address 172.16.112.10 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.132
 encapsulation dot1Q 132
 ip address 172.17.112.1 255.255.255.0
!
interface GigabitEthernet0/1.152
 encapsulation dot1Q 152
 ip address 192.168.112.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface FastEthernet0/2/0
!
interface FastEthernet0/2/1
!
interface FastEthernet0/2/2
!
interface FastEthernet0/2/3
!
interface Vlan1
 ip address 198.41.9.15 255.255.255.0
!
router eigrp 1
 network 172.16.112.0 0.0.0.255
 network 172.17.112.0 0.0.0.255
 no auto-summary
!
ip forward-protocol nd
ip http server
ip http access-class 23
ip http authentication local
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
ip http path flash:/gui
!
!
ip nat inside source list 111 interface
GigabitEthernet0/0 overload
!
access-list 23 permit 10.10.10.0 0.0.0.7
access-list 111 deny   ip 192.168.112.0 0.0.0.255
192.168.0.0 0.0.255.255
access-list 111 permit ip 192.168.112.0 0.0.0.255 any
!
!
```

```
!
!
!
!
tftp-server flash:/phone/7940-7960/P00308000400.bin
alias P00308000400.bin
tftp-server flash:/phone/7940-7960/P00308000400.loads
alias P00308000400.loads
tftp-server flash:/phone/7940-7960/P00308000400.sb2
alias P00308000400.sb2
tftp-server flash:/phone/7940-7960/P00308000400.sbn
alias P00308000400.sbn
!
control-plane
!
!
!
voice-port 0/0/0
 connection plar 3035452366
 description 303-545-2366
 caller-id enable
!
voice-port 0/0/1
 description FXO
!
voice-port 0/1/0
 description FXS
!
voice-port 0/1/1
 description FXS
!
!
!
!
!
dial-peer voice 804 voip
 destination-pattern 5251...
 session target ipv4:172.16.111.10
!
dial-peer voice 50 pots
 destination-pattern A0
 port 0/0/0
 no sip-register
!
!
!
!
telephony-service
 load 7960-7940 P00308000400
 max-ephones 24
 max-dn 24
 ip source-address 192.168.112.1 port 2000
 system message CME2
 max-conferences 12 gain -6
 transfer-system full-consult
 create cnf-files version-stamp 7960 Jun 10 2008
15:47:13
!
!
ephone-dn  1
 number 1001
 trunk A0
!
!
```

```
ephone-dn  2
 number 1002
!
!
ephone-dn  3
 number 3035452366
 label 2366
 trunk A0
!
!
ephone  1
 device-security-mode none
 mac-address 0003.6BC9.7737
 type 7960
 button  1:1 2:2 3:3
!
!
!
ephone  2
 device-security-mode none
 mac-address 0003.6BC9.80CE
 type 7960
 button  1:2 2:1 3:3
!
!
!
ephone  5
 device-security-mode none
!
!
!
line con 0
 exec-timeout 0 0
 login local
line aux 0
line vty 0 4
 access-class 23 in
 privilege level 15
 login local
 transport input telnet ssh
line vty 5 15
 access-class 23 in
 privilege level 15
 login local
 transport input telnet ssh
!
ntp server 172.16.1.1
end
```

Provisioning, gestione e monitoraggio

Il provisioning e la configurazione sia per le risorse di telefonia IP basate su router che per il firewall dei criteri basato su zone sono generalmente più adatti a Cisco Configuration Professional. Cisco Secure Manager non supporta il firewall per i criteri basati sulle zone o la telefonia IP basata su router.

Cisco IOS Classic Firewall supporta il monitoraggio SNMP con Cisco Unified Firewall MIB. Tuttavia, il firewall dei criteri basato su zone non è ancora supportato nel MIB del firewall unificato. Di conseguenza, il monitoraggio del firewall deve essere gestito tramite le statistiche sull'interfaccia della riga di comando del router o con strumenti GUI come Cisco Configuration

Professional.

Cisco Secure Monitoring And Reporting System (CS-MARS) offre supporto di base per il firewall delle policy basato su zone, anche se le modifiche di registrazione che hanno migliorato la correlazione tra i messaggi di log e il traffico implementate nelle versioni 12.4(15)T4/T5 e 12.4(20)T non sono ancora state completamente supportate in CS-MARS.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Cisco IOS Zone Firewall fornisce comandi **show** e **debug** per visualizzare, monitorare e risolvere i problemi relativi all'attività del firewall. In questa sezione viene fornita un'introduzione ai comandi di **debug di** Zone Firewall che forniscono informazioni dettagliate sulla risoluzione dei problemi.

Comandi debug

I comandi di debug sono utili nel caso in cui si utilizzi una configurazione atipica o non supportata e si abbia la necessità di utilizzare Cisco TAC o i servizi di supporto tecnico di altri prodotti per risolvere i problemi di interoperabilità.

Nota: l'applicazione dei comandi di **debug** a funzionalità o traffico specifici può causare un numero elevato di messaggi della console, che causano la mancata risposta della console del router. Nel caso in cui sia necessario attivare il debug, potrebbe essere necessario fornire un accesso alternativo all'interfaccia della riga di comando, ad esempio una finestra telnet che non monitora la finestra di dialogo del terminale. Abilitare il debug solo sulle apparecchiature offline (ambiente lab) o durante un intervento di manutenzione pianificato, in quanto l'abilitazione del debug potrebbe influire sostanzialmente sulle prestazioni del router.

Informazioni correlate

- Guida alla progettazione della rete di riferimento per la soluzione Cisco Unified CallManager Express
- Integrazione di Cisco Unity Connection con Cisco Unified CME-as-SRST
- Guida di riferimento ai comandi di Cisco Unified Communications Manager Express
- Esempio di configurazione di Cisco CallManager Express/Cisco Unity Express
- Supporto MIB SNMP Cisco CallManager Express 3.4
- Guida alla progettazione e all'applicazione di firewall per i criteri basati su zone
- Documentazione e supporto tecnico – Cisco Systems