Cisco IOS Zone Based Firewall: CME/CUE/GW Sede singola o filiale con SIP Trunk su CCM presso la sede centrale

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, Application Inspection and Control) 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. Le configurazioni per i servizi voce e il firewall vengono fornite per ogni scenario dell'applicazione. In ogni scenario vengono descritte separatamente le configurazioni VoIP e di sicurezza, seguite dall'intera configurazione del router. È possibile che la rete richieda altre configurazioni per i servizi, ad esempio QoS e VPN, per mantenere la qualità della voce e la riservatezza.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

Convenzioni

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

Premesse

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, può 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 e di elaborazione e può contribuire a ridurre la velocità di trasmissione, a migliorare la latenza dei pacchetti e a ridurre la capacità delle funzionalità nei 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 a elevata larghezza di banda sono in genere meglio gestite con gli accessori; Cisco ASA e Cisco Unified Call Manager Server devono essere applicati per gestire l'applicazione NAT e i criteri di sicurezza e l'elaborazione delle chiamate, mentre i router soddisfano i requisiti di applicazione dei criteri QoS, terminazione della WAN e 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, che richiedevano ampi spazi vuoti nei criteri firewall altrimenti sicuri per supportare il traffico vocale, e offrivano supporto limitato per l'evoluzione dei protocolli di segnalazione e multimediali VoIP.

Distribuire Cisco IOS Zone-Based Policy Firewall

Analogamente ad altri firewall, Cisco IOS Zone-Based Policy 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 di *trust* 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 firme o comportamenti. 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 i nuovi attacchi nel momento in cui si presentano. Inoltre, la comunità degli utenti deve svolgere un ruolo di primo piano nel mantenimento di una sicurezza 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. Si tratta di una policy applicata che nega tutto il traffico delle applicazioni, 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 *buone* applicazioni, nonché il traffico indesiderato che viene mascherato come 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 deve essere controllata da filtri senza stato, ad esempio elenchi di controllo di accesso (ACL) o criteri ZFW (Zone-Based Policy Firewall). Di conseguenza, il traffico che deve essere gestito da AIC, IPS (Intrusion Prevention System) o altri controlli basati su firma, ad esempio FPM (Flexible Packet Matching) o NBAR (Network-Based Application Recognition). Se sono consentite solo le porte applicative desiderate (e il traffico dinamico specifico dei supporti derivante da sessioni o connessioni di controllo conosciute), l'unico traffico indesiderato presente sulla rete deve 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*, in modo che sia autorizzato solo il traffico autorizzato nei segmenti della rete voce. I criteri dati tendono ad essere più permissivi, come descritto nelle 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 influiscono in genere sulla capacità e sulle funzionalità delle applicazioni esistenti e devono essere regolate per ridurre al minimo o risolvere questo impatto.

Se sono necessari ulteriori elementi di sfondo per configurare il firewall dei criteri basato su aree, vedere la guida alla progettazione e all'applicazione del firewall per aree.

Considerazioni su ZFW in ambienti VoIP

La Zone Firewall Design and Application Guide offre una breve discussione sulla sicurezza dei router con l'uso dei criteri di sicurezza per e dalla zona *autonoma* del router, nonché funzionalità alternative fornite tramite varie 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 per poter 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 gestire completamente i requisiti del traffico VoIP, pertanto le policy del firewall non erano ottimizzate 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.

Funzioni vocali di IOS Firewall

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 e multimediali secondari 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 automatica della zona per riconoscere i canali di segnalazione secondari e multimediali risultanti dal traffico SCCP destinato/originato localmente
- Supporto H.323 per le versioni 3 e 4Aggiorna il supporto H.323 alle versioni 3 e 4 (versioni 1 e 2 supportate in precedenza)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 spiegazioni per descrivere l'azione applicata dalle policy. I collegamenti ipertestuali ai singoli documenti delle caratteristiche sono disponibili nella sezione Informazioni correlate di questo documento se si desidera esaminare i dettagli completi delle caratteristiche di ispezione vocale.

Avvertenze

Per rafforzare i punti citati 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 o il comportamento della segnalazione del traffico vocale.

NAT (Network Address Translation)

Il protocollo NAT (Network Address Translation) di Cisco IOS viene spesso configurato contemporaneamente al firewall di Cisco IOS, in particolare nei casi in cui le reti private devono interfacciarsi con Internet o devono connettersi reti private diverse, in particolare se lo spazio degli indirizzi IP si sovrappone. 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 poiché NAT introduce ulteriori 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 può essere applicato solo come soluzione last-case per risolvere problemi di connettività di rete.

Cisco Unified Presence Client (CUPC)

Questo documento non descrive la configurazione che supporta l'uso di Cisco Unified Presence Client (CUPC) con IOS Firewall poiché CUPC non è ancora supportato da Zone o Classic Firewall, a partire dal software Cisco IOS versione 12.4(20)T1. CUPC sarà supportato in una versione futura del software Cisco IOS.

CME/CUE/GW Sede singola o filiale con SIP Trunk su CCM presso la sede centrale o fornitore di servizi voce

Questo scenario rappresenta un compromesso tra il modello di elaborazione delle chiamate distribuite/a sito singolo/con connessione PSTN descritto in precedenza in questo documento (CME/CUE/GW a sito singolo o succursale che si connette a PSTN) e la rete voce e dati convergente/con elaborazione centralizzata delle chiamate a più siti definita nel terzo scenario descritto in questo documento. In questo scenario viene ancora utilizzato un Cisco Unified CallManager Express locale, ma la composizione del numero per lunghe distanze e la telefonia HQ/sito remoto sono supportate principalmente tramite trunk SIP da sito a sito, con composizione locale e chiamata di emergenza tramite una connessione PSTN locale. Anche nei casi in cui la maggior parte della connettività PSTN legacy viene rimossa, si consiglia un livello di capacità PSTN di base per gestire i guasti della chiamata gratuita basata su WAN e della chiamata locale, come descritto dal dial plan. Inoltre, le leggi locali in genere richiedono che venga fornito un tipo di connettività PSTN locale per supportare la composizione di emergenza (911). In questo scenario viene utilizzata l'elaborazione distribuita delle chiamate, che offre vantaggi e osserva le best practice descritte in Cisco Unified CallManager Express SRND.

Le organizzazioni possono implementare questo tipo di scenario di applicazione nelle circostanze seguenti:

- Si utilizzano ambienti VoIP diversi tra i siti, ma si desidera comunque la tecnologia VoIP al posto della rete PSTN a lunga distanza.
- Per l'amministrazione di dial-plan è necessaria l'autonomia sito per sito.
- La capacità di elaborazione completa delle chiamate è necessaria indipendentemente dalla disponibilità della WAN.

Sfondo scenario

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

La configurazione di protezione offre quanto segue:

1. Ispezione della segnalazione avviata dal router tra CME e telefoni locali (SCCP e SIP) e CME e il cluster CUCM remoto (SIP).
2. I fori dei supporti vocali per la comunicazione tra questi:Segmenti cablati e wireless localiCME e i telefoni locali per MoHCUE e i telefoni locali per la segreteria telefonicaTelefoni ed entità chiamate remote
3. Ispezione e controllo delle applicazioni (AIC), che possono essere applicate per ottenere:Numero massimo di messaggi di invitoGaranzia di conformità del protocollo su tutto il traffico SIP

Vantaggi/Svantaggi

Questa applicazione offre il vantaggio di ridurre i costi poiché trasferisce il traffico vocale da sito a sito sui collegamenti dati WAN.

Uno svantaggio di questo scenario è che sono necessari piani più dettagliati per la connettività WAN. La qualità delle chiamate da sito a sito può essere influenzata da molti fattori sulla WAN, come il traffico illegittimo/indesiderato (worm, virus, condivisione file peer-to-peer) o problemi di latenza difficili da identificare che possono verificarsi a causa della progettazione del traffico sulle reti vettore. Le connessioni WAN devono essere dimensionate in modo appropriato per offrire una larghezza di banda sufficiente sia per il traffico di voce che per quello di dati; traffico di dati con minore sensibilità alla latenza, ad esempio e-mail, traffico di file SMB/CIFS, può essere classificato come traffico con priorità inferiore per QoS al fine di preservare la qualità della voce.

Un altro problema di questo scenario è la mancanza di elaborazione centralizzata delle chiamate e le difficoltà che possono verificarsi nella risoluzione dei problemi di elaborazione delle chiamate. Questo scenario rappresenta la soluzione migliore per le aziende di grandi dimensioni, in quanto rappresenta una fase intermedia della migrazione all'elaborazione centralizzata delle chiamate. I CME Cisco locali possono essere convertiti in modo da funzionare come fallback SRST completo al termine della migrazione a Cisco CallManager.

Dal punto di vista della sicurezza, la maggiore complessità di questo ambiente rende più difficile un'implementazione efficace della sicurezza e la risoluzione dei problemi, in quanto la connettività su una WAN o su una VPN su Internet pubblica aumenta notevolmente l'ambiente di minaccia, in particolare nei casi in cui i criteri di sicurezza richiedono una prospettiva di *fiducia*, in cui vengono imposte poche restrizioni al traffico sulla WAN. A questo scopo, gli esempi di configurazione forniti da questo documento implementano una policy più *sospetta* che consente un traffico business-critical specifico, che viene quindi esaminato tramite controlli di conformità del protocollo. Inoltre, le azioni VoIP specifiche, ovvero SIP INVITE, sono limitate per ridurre la probabilità di malfunzionamenti del software dannosi o involontari che influiscono negativamente sulle risorse e sull'usabilità VoIP.

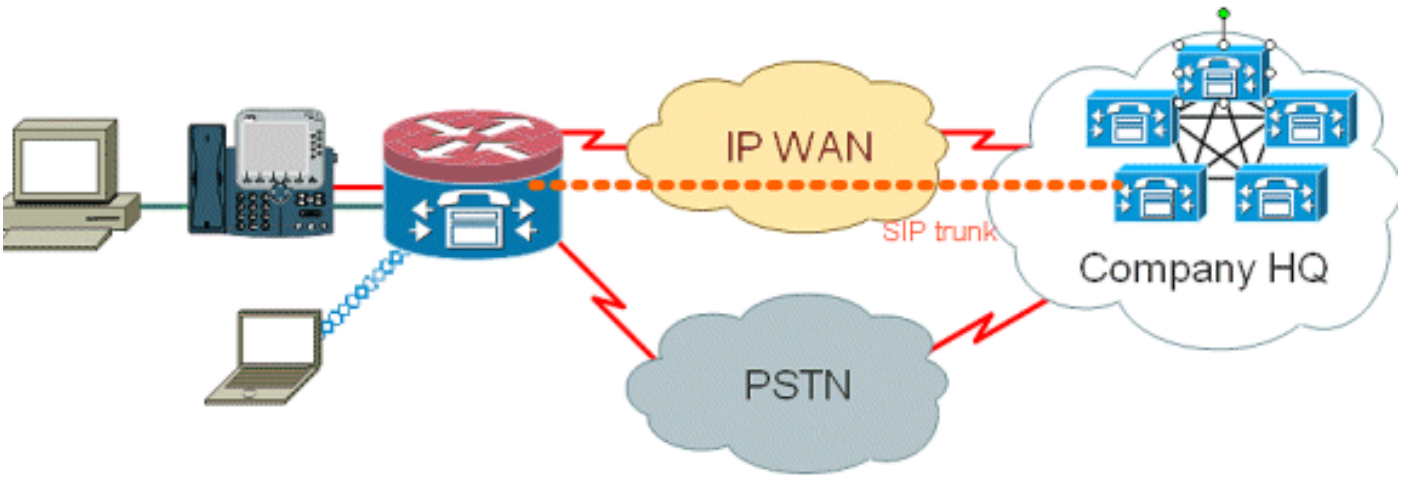
Configurazione

Configurazioni per criteri dati, firewall basato su zona, sicurezza vocale, CCME

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazioni

La configurazione descritta qui illustra un Cisco 2851 Integrated Services Router.

Nel documento vengono usate queste configurazioni:

- Configurazione servizio voce per connettività CME e CUE
- Configurazione del firewall dei criteri basata su zone
- Configurazione protezione

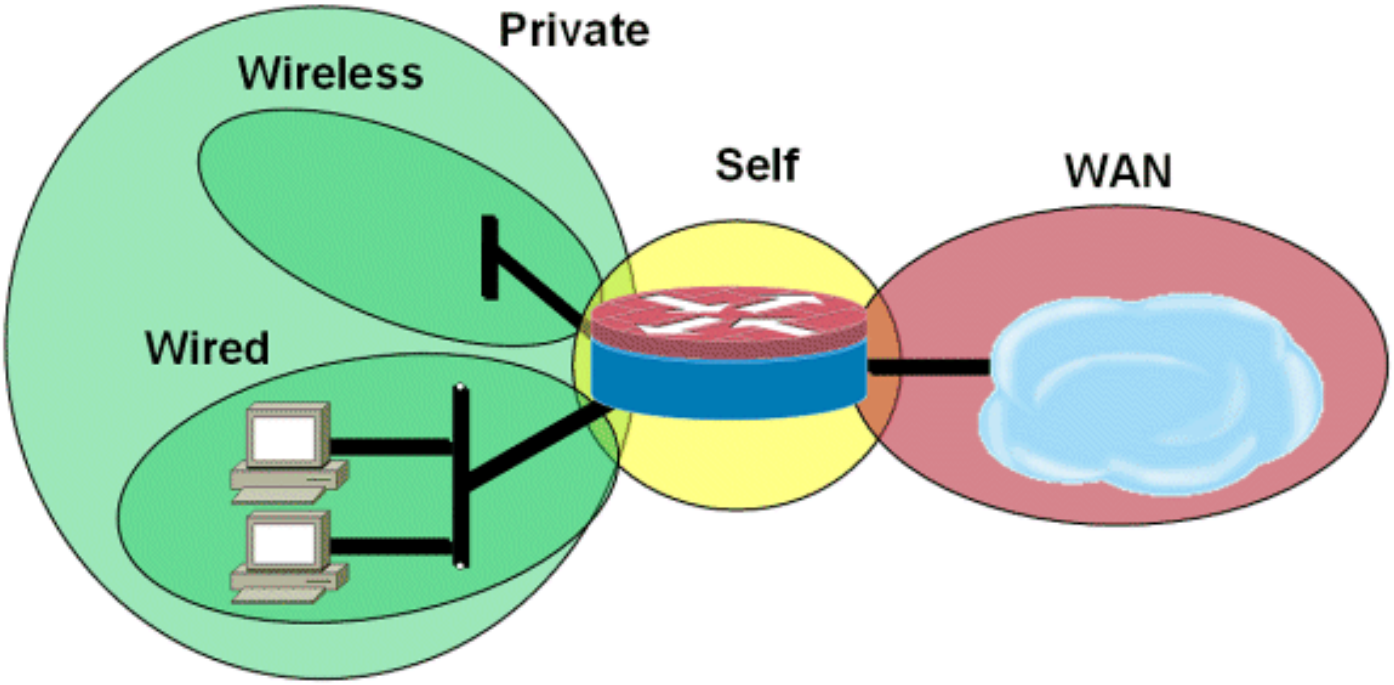
Questa è la configurazione del servizio voce per la connettività CME e CUE:

Configurazione servizio voce per 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

!
```

Questa è la 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), un segmento WAN in cui viene raggiunta la connettività WAN trusted e l'area autonoma in cui si trovano le risorse voce del router:



Questa è la configurazione di sicurezza:

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

Entire router configuration:

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

!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
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 con Cisco Configuration Professional. Cisco Secure Manager non supporta il firewall dei criteri basati sulle zone o la telefonia IP basata su router.

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

Il sistema 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.

Piani capacità

I risultati dei test sulle prestazioni delle ispezioni delle chiamate al firewall in India sono da definire.

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 descritto l'utilizzo dei comandi **show** per monitorare l'attività di base del firewall e viene fornita un'introduzione ai comandi **debug** di Zone Firewall per risolvere i problemi relativi alla configurazione o qualora il supporto tecnico richieda informazioni più dettagliate.

Comandi per la risoluzione dei problemi

Cisco IOS Firewall offre diversi comandi **show** per visualizzare la configurazione e l'attività dei criteri di sicurezza. Molti di questi comandi possono essere sostituiti con un comando più breve tramite l'applicazione del comando **alias**.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

I comandi di debug possono essere 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 a sua volta causano la mancata risposta della console del router. Nel caso in cui sia necessario eseguire il debug, è possibile 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 all'interno di una finestra di manutenzione pianificata, in quanto il debug può influire significativamente sulle prestazioni del router.

Informazioni correlate

- Guida alla progettazione della rete di riferimento per la soluzione Cisco Unified CallManager Express
- Procedure ottimali per la sicurezza di Cisco CallManager Express (CME SRND)
- 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
- Cisco IOS Firewall: Miglioramenti SIP: ALG e AIC
- Supporto software Cisco IOS Firewall H.323
- Supporto Cisco IOS Firewall per il traffico locale Skinny e CME

- Documentazione e supporto tecnico – Cisco Systems