# Cisco IOS Zone Based Firewall: Office con Cisco Unity Express/SRST/PSTN Gateway con connessione a Cisco CallManager centralizzato

## 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, il firewall Cisco IOS® 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, quindi viene descritta l'intera configurazione del router. Per mantenere la qualità e la riservatezza della voce, la rete può 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.

## Convenzioni

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

# Sfondo di Cisco 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 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 in cui 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, e richiedevano ampie aperture in policy firewall altrimenti sicure per supportare il traffico vocale; inoltre, offrivano un supporto limitato per l'evoluzione dei protocolli multimediali e di segnalazione VoIP.

# Configurazione

## Distribuzione di 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 dell'attendibilità della rete sono identificati e descritti dai criteri di sicurezza. Esistono due approcci fondamentali per giungere a una politica di sicurezza: rispetto 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. Si tratta di un 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 *buone* applicazioni, 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 consentiti, 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 per la sicurezza influiscono in genere sulle funzionalità delle applicazioni esistenti e devono essere regolate per ridurre al minimo o risolvere questo impatto.

Per ulteriori informazioni e ulteriori informazioni di base sulla configurazione del firewall dei criteri basato su zone, consultare la guida alla progettazione e all'applicazione di firewall dei criteri basati su zone.

## Considerazioni su ZFW in ambienti VoIP

La guida alla progettazione e all'applicazione sopra menzionata offre una breve descrizione della sicurezza del router con l'utilizzo di policy di sicurezza da e verso l'area 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, 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, pertanto le policy del firewall non erano ottimizzate per proteggere completamente le risorse. Le policy di sicurezza basate sull'area autonoma che proteggono le risorse VoIP basate su router si basano in gran parte sulle funzionalità introdotte nel software Cisco IOS versione 12.4(20)T.

### Funzioni vocali di Cisco IOS Firewall

Il software Cisco IOS versione 12.4(20)T ha introdotto diversi miglioramenti per abilitare le funzionalità vocali e del 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 di zona per essere in grado di riconoscere i canali di segnalazione e multimediali secondari risultanti dal traffico SIP destinato/originato localmente
- Supporto per Skinny Local Traffic e Cisco CallManager ExpressAggiorna 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), come descritto inIntroduce 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. I collegamenti ipertestuali ai singoli documenti delle caratteristiche sono disponibili nella sezione Informazioni correlate alla fine del presente documento, se si desidera esaminare i dettagli completi delle caratteristiche di ispezione vocale.

## Avvertenze

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

### NAT

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 ulteriore 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.

### CUPC

Questo documento non descrive la configurazione che supporta l'uso di Cisco Unified Presence Client (CUPC) con Cisco 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 è supportato in una versione futura del software Cisco IOS.

## Office con Cisco Unity Express/SRST/PSTN Gateway per la connessione a Cisco CallManager centralizzato

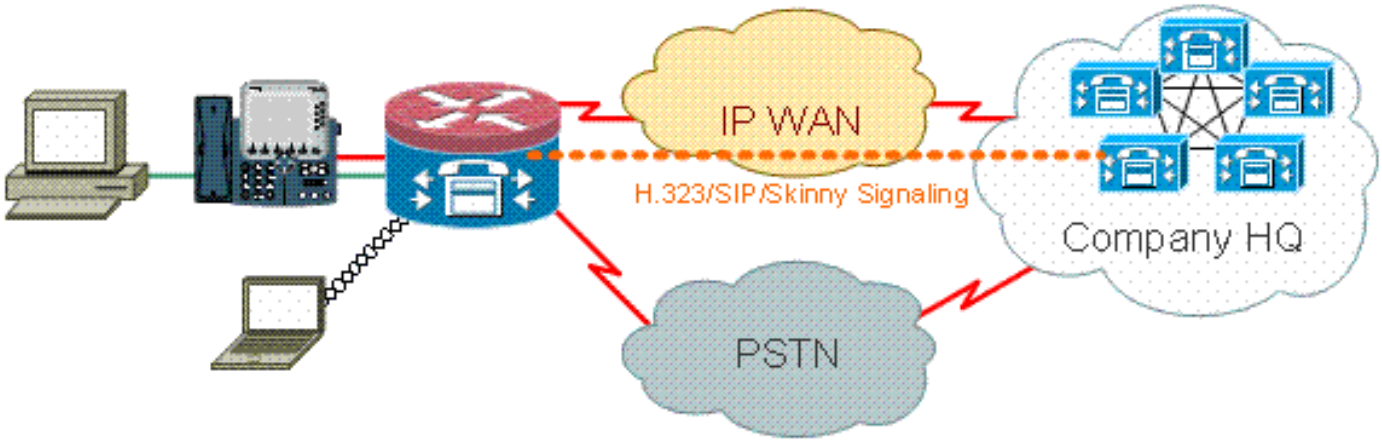
Questo scenario differisce dalle applicazioni precedenti, in quanto il controllo delle chiamate centralizzato viene utilizzato per il controllo di tutte le chiamate, anziché per l'elaborazione distribuita basata su router. Viene applicata la segreteria telefonica distribuita, ma tramite Cisco Unity Express sul router. Il router offre la funzionalità Survivable Remote-Site Telephony e PSTN Gateway per la composizione di emergenze e la composizione locale. Si consiglia un livello di capacità PSTN specifico dell'applicazione per gestire gli errori della composizione del numero verde basata sulla WAN e della composizione per area 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).

Questo scenario può anche applicare Cisco CallManager Express come agente di elaborazione delle chiamate per SRST, nel caso in cui sia necessaria una maggiore capacità di elaborazione delle chiamate durante le interruzioni WAN/CCM. per ulteriori informazioni, fare riferimento a Integrazione di Cisco Unity Connection con Cisco Unified CME-as-SRST.

### Sfondo scenario

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

1. Ispezione della segnalazione tra telefoni locali e cluster CUCM remoto (SCCP e SIP)
2. Esaminare la segnalazione H.323 tra il router e il cluster CUCM remoto.
3. Ispezionare la segnalazione tra i telefoni locali e il router quando il collegamento al sito remoto è inattivo e SRST è attivo.
4. Punti deboli dei supporti vocali per la comunicazione tra:Segmenti cablati e wireless localiTelefoni locali e remotiServer MoH remoto e telefoni localiServer Unity remoto e telefoni locali per segreteria telefonica
5. Applica ispezione e controllo applicazione (AIC) a:messaggi invito limite di velocitàverificare la conformità del protocollo su tutto il traffico SIP.




## Vantaggi/Svantaggi

Questo scenario offre il vantaggio che la maggior parte dell'elaborazione delle chiamate si verifica in un cluster Cisco CallManager centrale, con un conseguente riduzione del carico di gestione. In genere, il router deve gestire meno il carico di ispezione delle risorse vocali locali rispetto agli altri casi descritti in questo documento, in quanto la maggior parte del carico di elaborazione delle chiamate non viene imposto sul router, ad eccezione della gestione del traffico da/verso Cisco Unity Express e nei casi in cui si verifica un'interruzione della WAN o del CUCM e in cui viene chiamata in vigore la funzionalità locale Cisco CallManager Express/SRST per gestire l'elaborazione delle chiamate.

Il maggiore inconveniente in questo caso, durante la tipica attività di elaborazione delle chiamate, è che Cisco Unity Express si trova sul router locale. Benché ciò sia positivo dal punto di vista della progettazione, ad esempio, Cisco Unity Express si trova nella posizione più vicina agli utenti finali in cui risiede la casella vocale, ma comporta un ulteriore onere di gestione, in quanto può essere gestito da un elevato numero di Cisco Unity Express. Detto questo, con un Cisco Unity Express centrale che presenta gli svantaggi opposti, in quanto un Cisco Unity Express centrale è più lontano dagli utenti remoti e probabilmente non è accessibile durante le interruzioni. Pertanto, i vantaggi funzionali dell'offerta di segreteria telefonica distribuita, offerti dall'implementazione di Cisco Unity Express in sedi remote, offrono una scelta superiore.

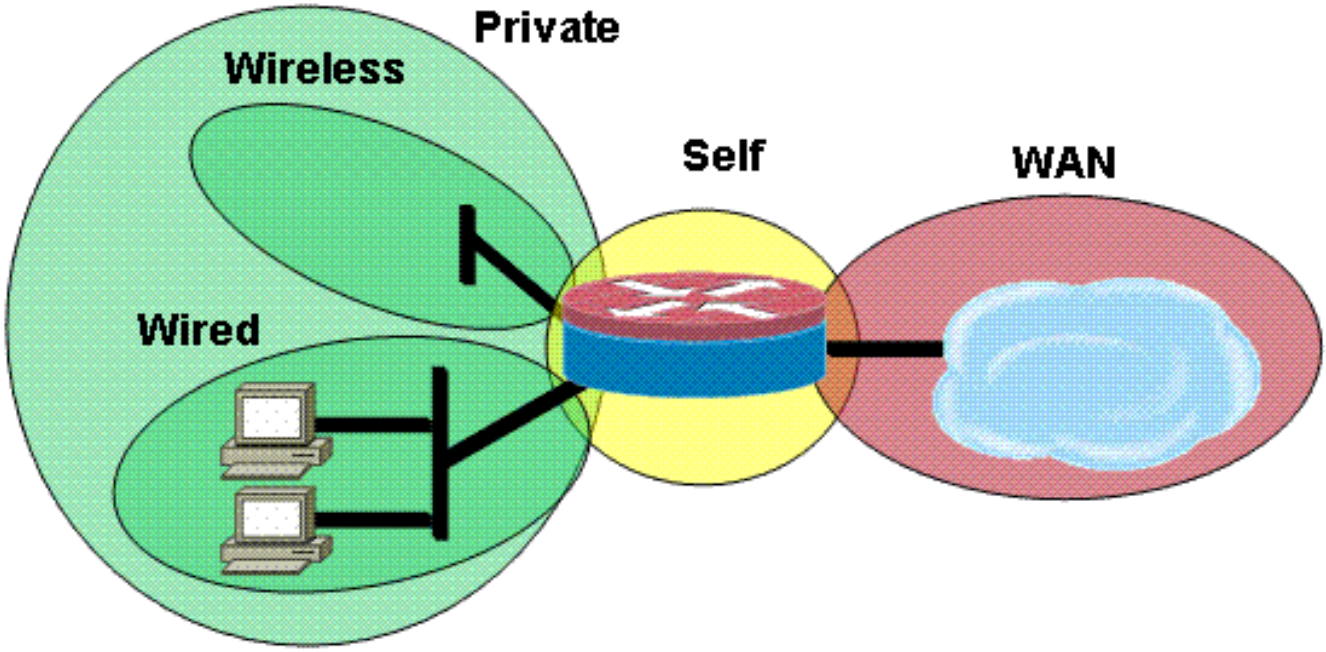
## Configurazioni per criteri dati, firewall basato su zone, sicurezza vocale, Cisco CallManager Express

La configurazione del router è basata su uno switch 3845 con NME-X-23ES e PRI HWIC:

Configurazione del servizio voce per la connettività SRST e Cisco Unity Express:

```
!
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
!
```

Questo è un esempio di Configurazione del firewall dei criteri basata su zone, composta da zone di sicurezza per i 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 vocali 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
```

Entire router configuration:

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 3825-srst
!
!
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
ip cef
!
!
ip domain name cisco.com
ip name-server 172.16.1.22
ip vrf acctg
 rd 0:1
!
ip vrf eng
 rd 0:2
!
ip inspect WAAS enable
!
no ipv6 cef
multilink bundle-name authenticated
!
!
voice-card 0
 no dspfarm
!
!
!
!
!
!
archive
 log config
  hidekeys
!
!
!
!
!
!
!
```

```
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 vpn
zone security eng
zone security acctg
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 Loopback101
 ip vrf forwarding acctg
 ip address 10.255.1.5 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 zone-member security acctg
!
interface Loopback102
 ip vrf forwarding eng
 ip address 10.255.1.5 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 zone-member security eng
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 media-type rj45
 no keepalive
!
interface GigabitEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 172.16.1.103 255.255.255.0
 shutdown
!
interface GigabitEthernet0/0.109
 encapsulation dot1Q 109
 ip address 172.16.109.11 255.255.255.0
```

```
 ip nat outside
 ip virtual-reassembly
 zone-member security public
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 media-type rj45
 no keepalive
!
interface GigabitEthernet0/1.129
 encapsulation dot1Q 129
 ip address 172.17.109.2 255.255.255.0
 standby 1 ip 172.17.109.1
 standby 1 priority 105
 standby 1 preempt
 standby 1 track GigabitEthernet0/0.109
!
interface GigabitEthernet0/1.149
 encapsulation dot1Q 149
 ip address 192.168.109.2 255.255.255.0
 ip wccp 61 redirect in
 ip wccp 62 redirect out
 ip nat inside
 ip virtual-reassembly
 zone-member security private
!
interface GigabitEthernet0/1.161
 encapsulation dot1Q 161
 ip vrf forwarding acctg
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 zone-member security acctg
!
interface GigabitEthernet0/1.162
 encapsulation dot1Q 162
 ip vrf forwarding eng
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 zone-member security eng
!
interface Serial0/3/0
 no ip address
 encapsulation frame-relay
 shutdown
 frame-relay lmi-type cisco
!
interface Serial0/3/0.1 point-to-point
 ip vrf forwarding acctg
 ip address 10.255.1.1 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 zone-member security acctg
 snmp trap link-status
 no cdp enable
 frame-relay interface-dlci 321 IETF
!
interface Serial0/3/0.2 point-to-point
 ip vrf forwarding eng
 ip address 10.255.1.1 255.255.255.252
 ip nat inside
```

```
 ip virtual-reassembly
 zone-member security eng
 snmp trap link-status
 no cdp enable
 frame-relay interface-dlci 322 IETF
!
interface Integrated-Service-Engine2/0
 no ip address
 shutdown
 no keepalive
!
interface GigabitEthernet3/0
 no ip address
 shutdown
!
router eigrp 1
 network 172.16.109.0 0.0.0.255
 network 172.17.109.0 0.0.0.255
 no auto-summary
!
router eigrp 104
 network 10.1.104.0 0.0.0.255
 network 192.168.109.0
 network 192.168.209.0
 no auto-summary
!
router bgp 1109
 bgp log-neighbor-changes
 neighbor 172.17.109.4 remote-as 1109
 !
 address-family ipv4
  neighbor 172.17.109.4 activate
  no auto-summary
  no synchronization
  network 172.17.109.0 mask 255.255.255.0
 exit-address-family
!
ip forward-protocol nd
ip route vrf acctg 0.0.0.0 0.0.0.0 172.16.109.1 global
ip route vrf acctg 10.1.2.0 255.255.255.0 10.255.1.2
ip route vrf eng 0.0.0.0 0.0.0.0 172.16.109.1 global
ip route vrf eng 10.1.2.0 255.255.255.0 10.255.1.2
!
!
ip http server
no ip http secure-server
ip nat pool acctg-nat-pool 172.16.109.21 172.16.109.22 netmask 255.255.255.0
ip nat pool eng-nat-pool 172.16.109.24 172.16.109.24 netmask 255.255.255.0
ip nat inside source list 109 interface GigabitEthernet0/0.109 overload
ip nat inside source list acctg-nat-list pool acctg-nat-pool vrf acctg overload
ip nat inside source list eng-nat-list pool eng-nat-pool vrf eng overload
ip nat inside source static 172.17.109.12 172.16.109.12 extendable
!
ip access-list extended acctg-nat-list
 deny   ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
 permit ip 10.0.0.0 0.255.255.255 any
ip access-list extended eng-nat-list
 deny   ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
 permit ip 10.0.0.0 0.255.255.255 any
!
logging 172.16.1.20
access-list 1 permit any
access-list 109 deny   ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255
access-list 109 permit ip 192.168.0.0 0.0.255.255 any
```

```
access-list 111 deny   ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255
access-list 111 permit ip 192.168.0.0 0.0.255.255 any
access-list 141 permit ip 10.0.0.0 0.255.255.255 any
access-list 171 permit ip host 1.1.1.1 host 2.2.2.2
!
!
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
gateway
 timer receive-rtp 1200
!
!
alias exec sh-sess show policy-map type inspect zone-pair sessions
!
line con 0
 exec-timeout 0 0
line aux 0
line 130
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
line 194
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
line vty 0 4
 password cisco
 login
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
!
webvpn context Default_context
 ssl authenticate verify all
 !
 no inservice
!
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 nel software Cisco IOS versione 12.4(15)T4/T5 e nel software Cisco IOS versione 12.4(20)T non sono ancora state completamente supportate in CS-MARS.

### Pianificazione della capacità

Risultati del test sulle prestazioni delle ispezioni delle chiamate al firewall da India a BD.

## Verifica

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

## Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Cisco IOS Zone Firewall fornisce i 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 un'introduzione ai comandi **debug** di Zone Firewall per procedure di risoluzione dei problemi più dettagliate o quando l'assistenza tecnica richiede informazioni dettagliate.

### Comandi per la risoluzione dei problemi

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

### Comandi show

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**.

### Comandi 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. Se è necessario attivare 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. È consigliabile abilitare il debug solo sulle apparecchiature offline (ambiente lab) o durante un intervento di manutenzione pianificato, in quanto l'abilitazione del debug può influire significativamente sulle prestazioni del router.

## Informazioni correlate

- Guida alla progettazione della rete di riferimento per la soluzione Cisco Unified CallManager Express
- Best practice per la sicurezza di 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
- Supporto Cisco IOS Firewall per il traffico locale Skinny e CME
- Cisco IOS Firewall
- Documentazione e supporto tecnico – Cisco Systems