Cisco IOS區域型防火牆：Office，帶有Cisco Unity Express/SRST/PSTN網關，可連線到集中式Cisco CallManager

目錄

簡介
必要條件
需求
採用元件
慣例
Cisco IOS防火牆背景
設定
Cisco IOS基於區域的策略防火牆的部署
注意事項
連線到集中式Cisco CallManager的Cisco Unity Express/SRST/PSTN網關的Office
布建、管理和監控
容量規劃
驗證
疑難排解
疑難排解指令
顯示命令
Debug指令
相關資訊

簡介

思科整合多業務路由器(ISR)提供可擴展的平台，以滿足各種應用的資料和語音網路需求。雖然私人網路和網際網路連線的威脅環境非常動態，但Cisco IOS®防火牆提供狀態化檢查以及應用程式檢查與控制(AIC)功能，以定義和執行安全網路狀態，同時啟用業務功能和連續性。

本文檔介紹基於Cisco ISR的特定資料和語音應用場景防火牆安全方面的設計和配置注意事項。為每個應用場景提供語音服務和防火牆配置。每個場景分別描述VoIP和安全配置，然後按整個路由器配置進行描述。您的網路可能需要對服務（如QoS和VPN）進行其他配置以保持語音品質和保密性。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

Cisco IOS防火牆背景

Cisco IOS防火牆通常部署在不同於裝置防火牆部署模式的應用場景中。典型的部署包括遠端工作人員應用程式、小型或分支辦公室站點以及零售應用程式，在這些部署中，需要低裝置數量、多服務整合和更低的效能和安全功能深度。

雖然從成本和運營角度看，防火牆檢查的應用以及ISR產品中的其他整合服務看起來頗具吸引力，但必須評估特定的考慮因素，以確定基於路由器的防火牆是否合適。如果部署了基於路由器的整合式解決方案，則應用每個附加功能會增加記憶體和處理成本，並可能導致轉發吞吐量降低、資料包延遲增加以及峰值負載期間功能丟失。當您在路由器和裝置之間進行選擇時，請遵循以下准則：

- 啟用多種整合功能的路由器最適合分支機構或遠端辦公站點，在這些站點中，裝置越少，解決方案越好
- 高頻寬、高效能應用通常可以通過裝置更好地解決。應應用Cisco ASA和Cisco Unified Call Manager Server來處理NAT和安全策略應用以及呼叫處理，同時路由器應滿足QoS策略應用、WAN終止和站點到站點VPN連線要求。

在Cisco IOS軟體版本12.4(20)T推出之前，傳統防火牆和基於區域的原則防火牆(ZFW)無法完全支援VoIP流量和基於路由器的語音服務所需的功能，而且在其他安全防火牆策略中需要較大的開口以容納語音流量，並為不斷發展的VoIP訊號傳送和媒體通訊協定提供有限的支援。

設定

Cisco IOS基於區域的策略防火牆的部署

Cisco IOS基於區域的策略防火牆與其他防火牆類似，只有在安全策略識別並描述網路信任的安全要求時，才能提供安全防火牆。制定安全策略有兩種基本方法：而不是可疑*的*視角

*trusting*視角假定所有流量都是可信任的，可明確識別為惡意或有害的流量除外。實施特定策略，僅拒絕不需要的流量。這通常通過使用特定訪問控制項或基於簽名或行為的工具來實現。此方法傾向於較少干擾現有應用程式，但需要全面瞭解威脅和漏洞情況，並需要時刻保持警惕，以便在新的威脅和漏洞出現時加以解決。此外，使用者群必須在維持足夠的安全性方面發揮重要作用。一個允許廣泛的自由而幾乎不控制居住者的環境，為疏忽或惡意的個人造成的問題提供了巨大的機會。此方法的另一個問題是，它更加依賴有效的管理工具和應用控制，這些工具和應用控制可提供足夠的靈活性和效能，以便可以監視和控制所有網路流量中的可疑資料。雖然目前已有技術可以解決這一問題，但運營負擔往往超過大多陣列織的限制。

*suspective*視角假定除明確標識的正常流量外，所有網路流量都是不需*要的*情況。應用此策略會拒絕所有應用流量（明確允許的應用流量除外）。此外，還可以實現應用檢測和控制(AIC)，以識別和拒絕專門構建的利用良好應用的惡意流*量，以及偽裝為良好流量的不需要*流量。同樣，應用控制會給網路帶來操作和效能上的負擔，儘管大多數不需要的流量應該由無狀態過濾器(如訪問控制清單(ACL)或基於區域的策略防火牆(ZFW)策略)控制，因此必須由AIC、入侵防禦系統(IPS)或其他基於特徵碼的控制措施(如靈活資料包匹配(FPM)或基於網路的應用識別(NBAR)處理的流量應該要少得多。 因此，如果僅特別允許所需的應用埠和來自已知控制連線或會話的動態媒體特定流量，則網路上

應該存在的唯一不想要的流量應落入一個特定的、更容易識別的子集中，這降低了為保持對不想要流量的控制而帶來的工程和操作負擔。

本檔案介紹基於可疑視角的VoIP安全配置；因此，只允許語音網段中允許的流量。資料策略往往更加寬容，如每個應用程式方案配置中的註釋所述。

所有安全策略部署都必須遵循閉環反饋週期；安全部署通常會影響現有應用程式的效能和功能，必須進行調整以儘量減少或解決這種影響。

有關基於區域的策略防火牆配置的更多資訊和其他背景，請參閱基於區域的策略防火牆設計和應用指南。

VoIP環境中ZFW的注意事項

前面提到的「設計和應用指南」簡要討論了路由器的安全性，使用進出路由器自身區域的安全策略，以及通過各種網路基礎保護(NFP)功能提供的備用功能。基於路由器的VoIP功能託管在路由器的自身區域內，因此保護路由器的安全策略必須瞭解對語音流量的要求，以便適應由Cisco Unified CallManager Express、Survivable Remote-Site Telephony和語音網關資源發出和發往這些裝置的語音信令和媒體。在Cisco IOS軟體版本12.4(20)T之前，傳統防火牆和基於區域的策略防火牆無法完全滿足VoIP流量的要求，因此防火牆策略未進行最佳化以完全保護資源。保護基於路由器的VoIP資源的自分割槽安全策略在很大程度上依賴於Cisco IOS軟體版本12.4(20)T中引入的功能。

Cisco IOS防火牆語音功能

Cisco IOS軟體版本12.4(20)T匯入了幾個增強功能，以便啟用共駐區防火牆和語音功能。以下三個主要功能直接適用於安全語音應用：

- SIP增強功能：應用層網關與應用檢測和控制將SIP版本支援更新為SIPv2，如RFC 3261中所述擴展SIP信令支援以識別更多種的呼叫流引入SIP應用檢測和控制(AIC)，以應用精細控制來解決特定的應用級漏洞和漏洞擴展自區域檢測，以便能夠識別由本地發往/源自本地的SIP流量產生的輔助信令和媒體通道
- 支援瘦本地流量和Cisco CallManager Express將SCCP支援更新到版本16（以前支援的版本9）引入SCCP應用檢測和控制(AIC)，以應用精細控制來解決特定的應用級漏洞和漏洞擴展自區域檢測，能夠識別由本地發往/源自SCCP流量產生的輔助信令和媒體通道
- H.323 v3/v4支援將H.323支援更新為v3和v4（以前支援的v1和v2），如中所述引入H.323應用檢測和控制(AIC)，以應用精細控制來解決特定的應用級漏洞和漏洞

本文所述的路由器安全配置包括這些增強功能提供的功能，並說明了策略應用的操作。如果您希望檢視語音檢測功能的完整詳細資訊，可在本文檔末尾的相關資訊部分找到各個功能文檔的超連結。

注意事項

應用具有路由器型語音功能的Cisco IOS防火牆時，必須應用區域型策略防火牆，以強化前面提到的要點。傳統IOS防火牆不包括充分支援語音流量的信令複雜性和行為所需的功能。

NAT

Cisco IOS網路位址轉譯(NAT)經常與Cisco IOS防火牆同時設定，尤其是當私人網路必須與Internet介面時，或是當不同的私人網路必須連線時，尤其是使用重疊的IP位址空間時。Cisco IOS軟體包括適用於SIP、Skinny和H.323的NAT應用層網關(ALG)。理想情況下，可以不應用NAT而為IP語音提供網路連線，因為NAT為故障排除和安全策略應用帶來了額外的複雜性，尤其是

使用NAT過載的情況下。NAT應僅作為解決網路連線問題的最後一個案例解決方案來應用。

CUPC

本檔案沒有說明支援將Cisco Unified Presence Client(CUPC)與Cisco IOS防火牆一起使用的組態，因為自Cisco IOS軟體版本12.4(20)T1起，區域或傳統防火牆尚未支援CUPC。將來的Cisco IOS軟體版本支援CUPC。

連線到集中式Cisco CallManager的Cisco Unity Express/SRST/PSTN網關的Office

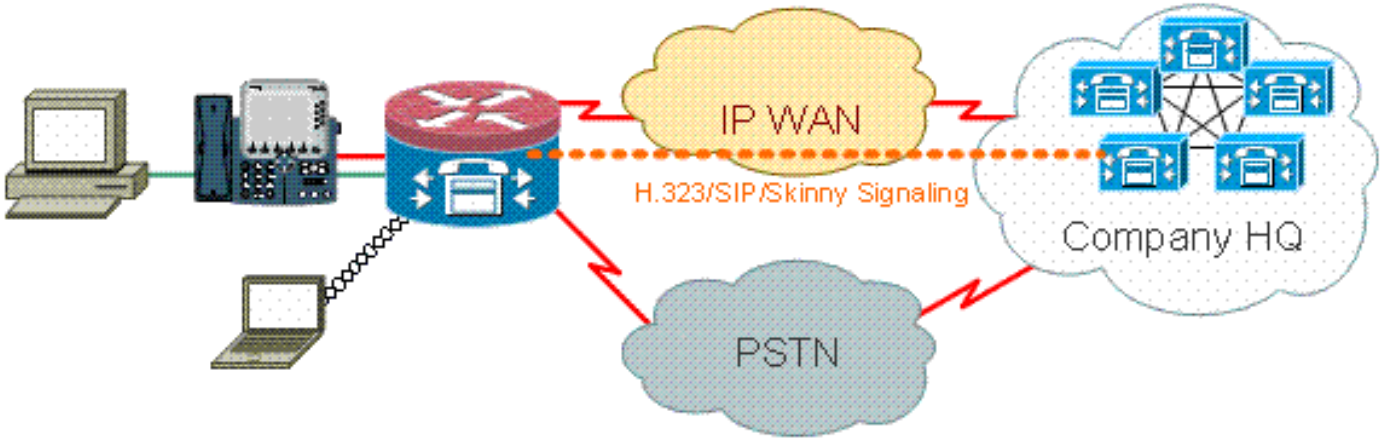
此方案與先前的應用不同，集中式呼叫控制用於所有呼叫控制，而不是基於路由器的分散式呼叫處理。分散式語音郵件已應用，但會通過路由器上的Cisco Unity Express應用。路由器為緊急撥號和本地撥號提供Survivable遠端站點電話和PSTN網關功能。建議使用特定於應用的PSTN容量級別來應對基於WAN的收費旁路撥號以及撥號方案所述的本地撥號失敗。此外，本地法律通常要求提供某種型別的本地PSTN連線以適應緊急(911)撥號。

此方案還可以將Cisco CallManager Express應用為SRST的呼叫處理代理，以應對WAN/CCM中斷期間需要更大呼叫處理能力的情況。有關詳細資訊，請參閱將Cisco Unity Connection與Cisco Unified CME-as-SRST整合。

場景背景

該應用場景包含有線電話（語音VLAN）、有線PC（資料VLAN）和無線裝置（包括IP Communicator等VoIP裝置）。

1. 本地電話與遠端CUCM集群（SCCP和SIP）之間的信令檢查
2. 檢查路由器和遠端CUCM集群之間的H.323信令。
3. 當到遠端站點的鏈路關閉且SRST處於活動狀態時，檢查本地電話與路由器之間的信令。
4. 用於以下對象之間的通訊的語音媒體針孔：本地有線和無線網段本地和遠端電話遠端MoH伺服器和本地電話用於語音郵件的遠端Unity伺服器和本地電話
5. 應用應用檢測和控制(AIC)以：速率限制邀請消息確保所有SIP流量的協定一致。



優點/缺點

此方案提供的優勢是，大多數呼叫處理都發生在中央Cisco CallManager集群中，從而降低了管理負擔。與本文檔中介紹的其他情況相比，路由器通常必須解決更少的本地語音資源檢查負擔，因為除處理來往Cisco Unity Express的流量外，大多數呼叫處理負擔並不加在路由器上，而且在出現

WAN或CUCM中斷時，本地Cisco CallManager Express/SRST被呼叫以處理呼叫處理時除外。

在典型的呼叫處理活動中，此案例的最大缺點是Cisco Unity Express位於本地路由器上。雖然從設計的角度來看這很好，例如Cisco Unity Express最接近擁有語音信箱的終端使用者，但它會產生一些額外的管理負擔，因為可以管理大量Cisco Unity Express。也就是說，中央Cisco Unity Express具有相反的缺點，因為中央Cisco Unity Express離遠端使用者更遠，在中斷期間可能無法訪問。因此，通過將Cisco Unity Express部署到遠端位置，分散式語音郵件提供的功能優勢提供了卓越的選擇。

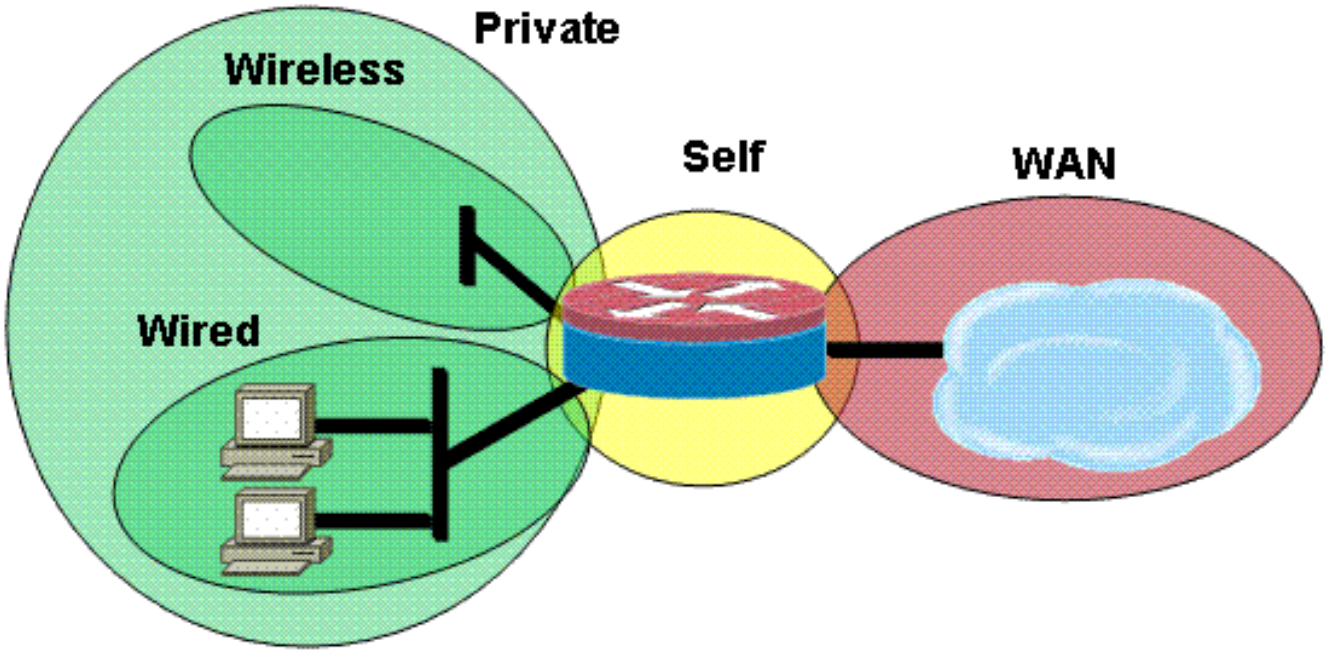
資料策略、基於區域的防火牆、語音安全、Cisco CallManager Express的配置

路由器配置基於帶有NME-X-23ES和PRI HWIC的3845:

SRST和Cisco Unity Express連線的語音服務配置：

```
!
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
!
```

以下是基於區域的策略防火牆配置的示例，包括有線和無線LAN網段的安全區域、由有線和無線網段組成的專用LAN、可達到可信WAN連線的WAN網段以及路由器語音資源所在的自身區域：



安全配置：

```
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
```

布建、管理和監控

Cisco Configuration Professional通常最能滿足基於路由器的IP電話資源和基於區域的策略防火牆的調配和配置。CiscoSecure Manager不支援基於區域的策略防火牆或基於路由器的IP電話。

Cisco IOS經典防火牆支援通過Cisco統一防火牆MIB進行SNMP監控。但是，統一防火牆MIB尚不支援基於區域的策略防火牆。因此，必須通過路由器命令列介面上的統計資訊或Cisco Configuration Professional等GUI工具處理防火牆監控。

Cisco安全監控和報告系統(CS-MARS)為基於區域的策略防火牆提供基本支援，不過CS-MARS尚未完全支援日誌記錄更改，這些更改可以改善在Cisco IOS軟體版本12.4(15)T4/T5和Cisco IOS軟體版本12.4(20)T中實施的與流量的日誌消息關聯。

容量規劃

印度TBD的防火牆呼叫檢查效能測試結果。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

Cisco IOS區域防火牆提供**show**和**debug**命令，以檢視、監控防火牆的活動並對該活動進行疑難排解。本節介紹如何使用**show**命令監控基本防火牆活動，並介紹區域防火牆的**debug**命令，以瞭解更詳細的疑難排解，或者與技術支援人員的討論是否需要詳細說明。

疑難排解指令

附註：使用 **debug** 指令之前，請先參閱有關 Debug 指令的重要資訊。

顯示命令

Cisco IOS防火牆提供多種**show**命令，以便檢視安全策略配置和活動：

許多這些命令都可以通過**alias**命令的應用用較短的命令替換。

Debug指令

Debug指令在您使用非典型或不受支援的組態時可能會很有用，而且需要與Cisco TAC或其他產品的技術支援服務協同合作，以解決互通性問題。

注意：將debug命令應用到特定功能或流量可能會導致大量控制檯消息，從而導致路由器控制檯無響應。在需要啟用調試時，可以提供備用命令列介面訪問，例如不監視終端對話方塊的telnet視窗。您應該僅在離線（實驗室環境）裝置上或計畫維護視窗中啟用調試，因為如果啟用調試，將會顯著影響路由器效能。

相關資訊

- Cisco Unified CallManager Express解決方案參考網路設計手冊
- Cisco Unified CallManager Express安全最佳實踐
- 將Cisco Unity Connection與Cisco Unified CME-as-SRST整合
- Cisco Unified Communications Manager Express命令參考
- Cisco CallManager Express/Cisco Unity Express配置示例
- Cisco CallManager Express 3.4 SNMP MIB支援
- 基於區域的策略防火牆設計和應用指南
- 適用於精簡型本地流量和CME的Cisco IOS防火牆支援
- Cisco IOS 防火牆
- 技術支援與文件 - Cisco Systems