IOS區域型防火牆：CME/CUE/GW單站點或分支機構PSTN連線配置示例

目錄

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偵測和控制(AIC)功能，以定義和執行安全網路態勢，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，然後是整個路由器配置。您的網路可能需要對QoS和VPN等服務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。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

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。

IOS防火牆背景

Cisco IOS防火牆通常部署在應用場景中，這些應用場景不同於裝置防火牆的部署模式。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。

雖然從成本和運營的角度來看，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，則應用每項附加功能將產生記憶體和處理成本，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，裝置較少可以提供更好的解決方案。
- 高頻寬、高效能應用通常可以通過以下裝置更好地滿足需求：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。

在引入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(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，需要在其他安全防火牆策略中增加較大的開口以容納語音流量，並為不斷發展的VoIP信令和媒體協定提供有限的支援。

部署Cisco IOS基於區域的策略防火牆

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：*信任*角度，而不是可疑*的*角度。

*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。應用的策略，拒絕所有應用流量，但明確允許的應用流量除外。此外，可以實施應用檢測和控制(AIC)來識別和拒絕專門設計來利用「好」應用的惡意流量，以及偽裝為好流量的不需要的流量。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，如果僅專門允許所需的應用埠（以及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。

有關如何配置基於區域的策略防火牆的詳細資訊，請參閱Cisco IOS防火牆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

Cisco IOS防火牆基於區域的策略防火牆設計和應用指南簡要討論了如何通過使用安全策略來保護路由器進出路由器自身*區，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12.4(20)T中引入的功能。

IOS防火牆語音增強功能 — 12.4(20)T

Cisco IOS軟體版本12.4(20)T匯入了幾種增強功能，可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，能夠識別由本地發往/源自SIP流量產生的輔助信令和媒體通道
- 支援精簡型本地流量和CME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）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。有關語音檢測功能的完整詳細資訊，請參閱本文檔的相關資訊部分中列出的各個功能文檔。

注意事項

為了強化前面提到的觀點，應用具有基於路由器的語音功能的Cisco IOS防火牆必須應用基於區域的策略防火牆。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。

網路位址轉譯

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，特別是在使用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。

Cisco Unified Presence使用者端

本檔案沒有說明支援將Cisco Unified Presence Client(CUPC)與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。未來版本的Cisco IOS軟體將支援CUPC。

CME/CUE/GW單站點或分支PSTN連線

此方案為希望部署分散式呼叫處理、維護與公共交換電話網路(PSTN)的舊式連線的單站點中小型企業或大型多站點組織引入基於路由器的安全IP語音電話。 VoIP呼叫控制通過應用Cisco Unified Call Manager Express實現。

PSTN連線可以長期保持或可以遷移到融合的語音和資料IP廣域網，如本文檔的CME/CUE/GW單站點或具有SIP中繼的分支機構到HQ或語音提供商的CCM部分中所述的應用示例所述。

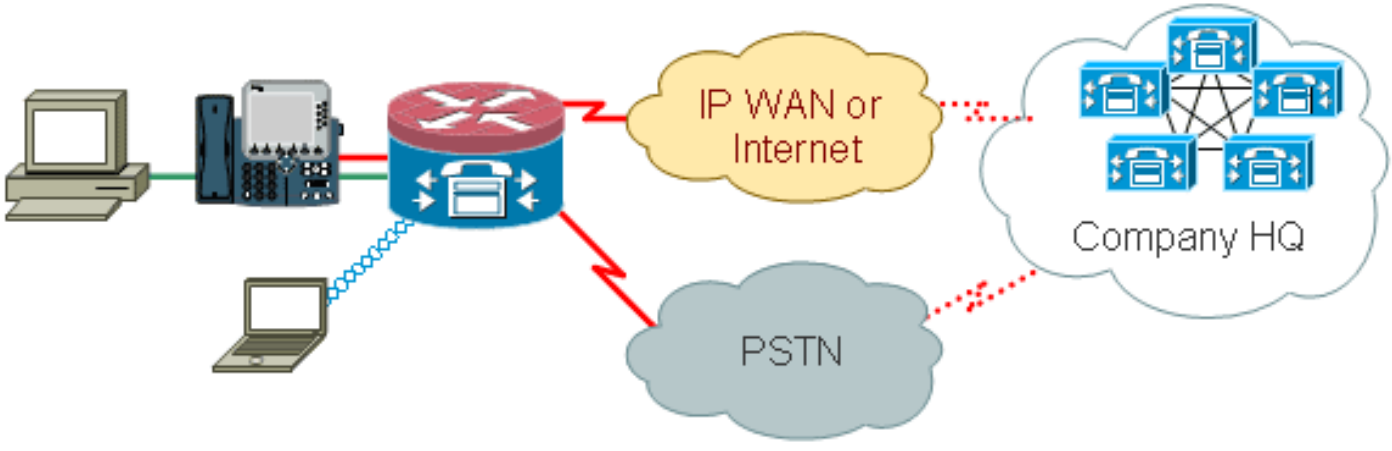
如果站點間使用不同的VoIP環境，或者VoIP由於WAN資料連線不充分或由於資料網路上的VoIP使用受到特定於區域設定的限制而不可行，組織應考慮實施此類應用場景。Cisco Unified CallManager Express SRND中介紹了單站點IP電話的優勢和最佳實踐。

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）。

安全配置提供：

- CME和本地電話（SCCP和/或SIP）之間的路由器啟動的信令檢查
- 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CME和MoH的本地電話CUE和本地語音郵件電話
- 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。



優點和缺點

方案的VoIP方面最明顯的好處是，在將現有語音和資料網路基礎設施整合到現有POTS/TDM環境中，然後遷移到融合語音/資料網路，從而為LAN以外的世界提供電話服務之前，提供了遷移路徑。為小型企業維護電話號碼，並且對於希望分階段遷移到收費旁路資料包電話的大型組織，可以保留現有的centrex或DID服務。

缺點包括：採用融合語音和資料網路後，通過收費旁路可以節省成本；呼叫靈活性受到限制；缺乏組織範圍的通訊整合；以及採用完全融合的語音和資料網路後可實現的可移植性。

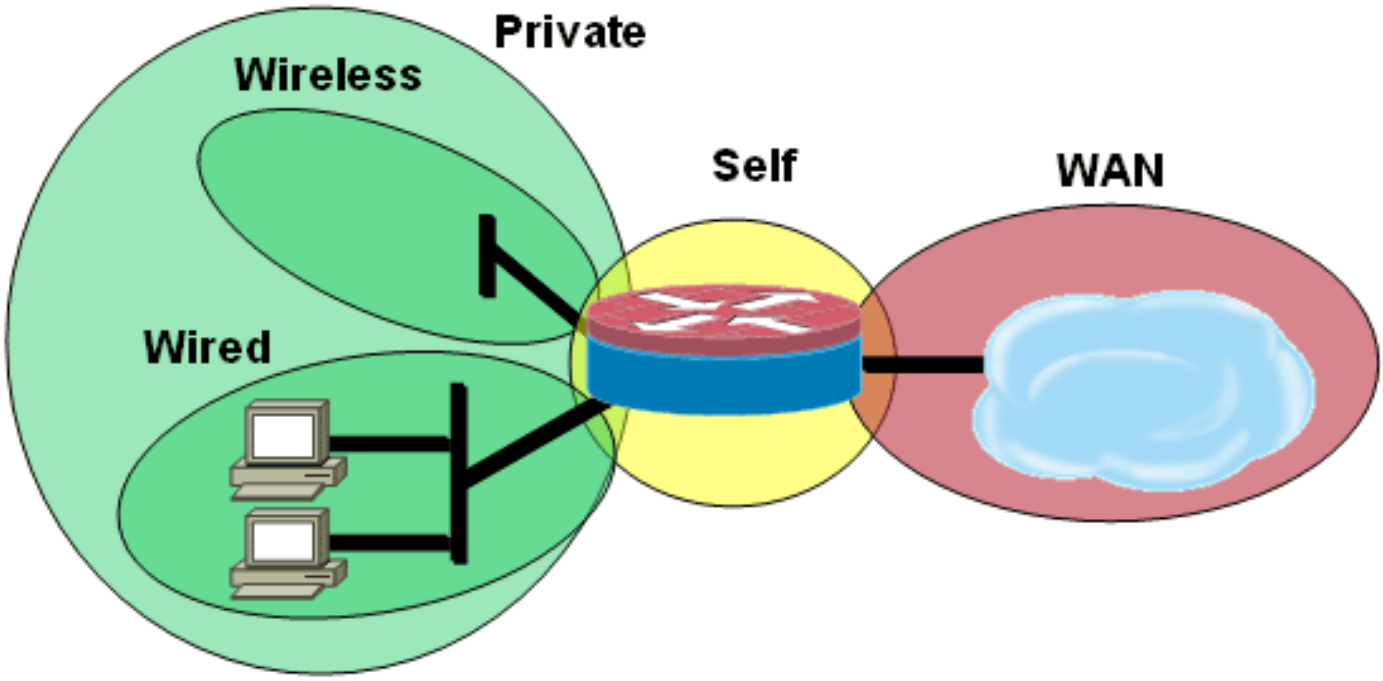
從安全形度來看，此類網路環境通過避免VoIP資源暴露到公共網路或WAN，將VoIP安全威脅降至最低。但是，嵌入在路由器中的Cisco Call Manager Express仍然容易受到內部威脅（如惡意流量或應用程式流量故障）的影響。因此，實施允許滿足協定一致性檢查的語音特定流量的策略，並且限制特定VoIP操作（即SIP INVITE）以減少惡意或無意的軟體故障對VoIP資源和可用性產生負面影響的可能性。

資料策略、基於區域的防火牆、語音安全和CCME配置

此處描述的配置說明了2851的CME和CUE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
!
```

基於區域的策略防火牆配置，由有線和無線LAN網段的安全區域、專用LAN（由有線和無線網段組成）、到達不受信任的Internet連線的公共WAN網段以及路由器語音資源所在的自身區域組成。



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
```

整個路由器配置

```
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
```

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使用Cisco Configuration Professional等GUI工具處理防火牆監控。

思科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，儘管在12.4(15)T4/T5和12.4(20)T中實施的日誌記錄更改尚未在CS-MARS中得到完全支援，這些更改改進了日誌消息與流量的關聯。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

Cisco IOS Zone Firewall提供**show**和**debug**命令，以檢視、監控防火牆的活動並對此進行故障排除。本節介紹用於提供詳細故障排除資訊的Zone Firewall **debug**命令。

Debug指令

Debug命令在您使用非典型或不受支援的組態且需要與Cisco TAC或其他產品的技術支援服務合作以解決互通性問題時非常有用。

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。即使您需要啟用調試，您也可能想要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）裝置上或計畫維護時段啟用調試，因為啟用調試可能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
- 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
- 技術支援與文件 - Cisco Systems