IOS基于区域的防火墙：CME/CUE/GW单站点或分支机构PSTN连接配置示例

目录

简介

思科集成多业务路由器(ISR)提供可扩展的平台，可满足各种应用的数据和语音网络需求。虽然私有网络和互联网连接网络的威胁形势是一个非常动态的环境，但Cisco IOS防火墙提供状态检测和应用检测与控制(AIC)功能，以定义和实施安全网络状态，同时实现业务功能和连续性。

本文描述特定Cisco基于ISR的数据和语音应用方案的防火墙安全方面的设计和配置注意事项。为每个应用场景提供语音服务和防火墙配置。每个方案分别描述 VoIP 和安全配置，后跟整个路由器配置。您的网络可能需要对QoS和VPN等服务进行其他配置，以保持语音质量和机密性。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

IOS 防火墙背景

Cisco IOS防火墙通常部署在与设备防火墙的部署模式不同的应用场景中。典型的配置包括远程操作人员应用、小型或分行办公室站点和零售应用，非常需要低设备多个服务计数、集成和更低性能和安全功能。

虽然从成本和运营角度看，防火墙检查的应用以及ISR产品中的其他集成服务看起来很有吸引力，但必须评估特定考虑因素，以确定基于路由器的防火墙是否合适。如果部署了基于路由器的集成解决方案，应用每个附加功能会产生内存和处理成本，并可能导致转发吞吐率降低、数据包延迟增加以及在高峰负载期间丢失功能。

在路由器和设备之间做出决定时，请遵循以下准则：

- 启用了多个集成功能的路由器最适合分支机构或远程工作人员站点，其中设备较少可提供更好的解决方案。
- 高带宽、高性能应用通常能通过以下设备得到更好的解决：应应用Cisco ASA和Cisco Unified Call Manager服务器来处理NAT和安全策略应用和呼叫处理，而路由器应满足QoS策略应用、WAN终端和站点到站点VPN连接要求。

在引入Cisco IOS软件版本12.4(20)T之前，传统防火墙和基于区域的策略防火墙(ZFW)无法完全支持VoIP流量和基于路由器的语音服务所需的功能，需要在其他安全防火墙策略中开设大门来容纳语音流量，并且对不断发展的VoIP信令和媒体协议提供有限支持。

部署Cisco IOS基于区域的策略防火墙

Cisco IOS基于区域的策略防火墙与其他防火墙类似，只有在安全策略确定和描述网络安全要求时，才能提供安全防火墙。有两个到达安全策略的基本途径：*信任 角度，与怀疑角度相对*。

*信任*视角假设所有流量都是可信的，但可以明确识别为恶意或不需要的流量除外。将实施一个仅拒绝不需要的数据流的特定策略。这通常通过使用特定访问控制条目或基于签名或行为的工具来实现。此方法对现有应用的干扰较少，但需要全面了解威胁和漏洞形势，并且需要持续保持警惕，以应对新的威胁和漏洞。此外，用户社区必须在维护足够的安全性方面发挥很大作用。允许很大自由度、只对占用者进行很少控制的环境为粗心或恶意个人引起的问题提供了大量机会。此方法的另一个问题是它更依赖于提供足够的灵活性和性能以能够监视和控制所有网络数据流中的可疑数据的有效管理工具和应用程序控制。当目前的技术可以适应这些时，操作的负担会频繁地超出多数组织的极限。

可疑*视角*假设所有网络流量都是不理想的，但特别确定的良好*流量*除外。应用的策略，拒绝除明确允许的应用流量外的所有应用流量。此外，可实施应用检测和控制(AIC)来识别和拒绝专门设计为利用“良好”应用的恶意流量，以及伪装成良好流量的不需要的流量。同样，应用控制会对网络造成运营和性能负担，尽管大多数不需要的流量应由无状态过滤器(如访问控制列表(ACL)或基于区域的策略防火墙(ZFW)策略)控制，因此必须由AIC、入侵防御系统(IPS)或其他基于签名的控制(如灵活数据

包匹配(FPM)或网络)处理的流量应大幅减少基于应用识别(NBAR)。 因此，如果仅明确允许所需的应用端口（以及由已知控制连接或会话产生的动态媒体特定流量），则网络上应存在的唯一不需要的流量应落入一个特定、更易于识别的子集中，从而减轻为保持对不需要的流量的控制而施加的工程和操作负担。

本文档基于可疑角度描述VoIP安全*配*置；因此，仅允许语音网段中允许的流量。数据策略往往更为宽松，如每个应用场景配置中的注释所述。

所有安全策略部署都必须遵循闭环反馈循环；安全部署通常会影响现有应用的功能和功能，必须进行调整以尽量减少或解决此影响。

有关如何配置基于区域的策略防火墙的详细信息，请参阅《Cisco IOS防火墙基于区域的策略防火墙设计和应用指南》。

VoIP 环境中 ZFW 的注意事项

《Cisco IOS防火墙基于区域的策略防火墙设计和应用指南》简要介绍了使用安全策略来保护路由器的安全，使其能够进出路由器的自身区域，以及通过各种网络基础保护(NFP)功能提供的替代功能。基于路由器的VoIP功能托管在路由器的自身区域内，因此保护路由器的安全策略必须了解语音流量的要求，以便适应由Cisco Unified CallManager Express、可存活远程站点电话和语音网关资源发起并发往的语音信令和媒体。在Cisco IOS软件版本12.4(20)T之前，传统防火墙和基于区域的策略防火墙无法完全满足VoIP流量的要求，因此防火墙策略未优化以完全保护资源。保护基于路由器的 VoIP 资源的自身区域安全策略在很大程度上依赖于 12.4(20)T 中引入的功能。

IOS防火墙语音增强功能 — 12.4(20)T

思科IOS软件版本12.4(20)T引入了多项增强功能，以实现共存区域防火墙和语音功能。三个主要功能直接地适用获取语音应用：

- SIP 增强功能：应用层网关和应用程序检查和控制更新SIP版本以支持SIPv2，如所描述由RFC 3261扩展 SIP 信令支持以识别更多类型的呼叫流引入 SIP 应用程序检查和控制 (AIC) 以应用精确的控制来解决特定的应用程序级弱点和漏洞扩展自区域检查，以便能够识别由本地发往/源自SIP流量产生的辅助信令和媒体信道
- 对 Skinny 本地数据流和 CME 的支持更新SCCP技术的支持版本16(以前支持的版本9)引入 SCCP 应用程序检查和控制 (AIC) 以应用精确的控制来解决特定的应用程序级弱点和漏洞扩展自区域检查，以便能够识别从本地发往/源自SCCP流量产生的辅助信令和媒体信道
- H.323 v3/v4支持将H.323支持更新到v3和v4（以前支持v1和v2）引入 H.323 应用程序检查和控制 (AIC) 以应用精确的控制来解决特定的应用程序级弱点和漏洞

本文档中描述的路由器安全配置包括这些增强功能提供的功能，以及描述策略所应用的操作的说明。有关语音检测功能的完整详细信息，请参阅本文档“相关信息”部分中列出的各个功能文档。

注意事项

为了强化前面提到的要点，应用具有基于路由器的语音功能的Cisco IOS防火墙必须应用基于区域的策略防火墙。传统IOS防火墙不包含完全支持语音流量的信令复杂性和行为所需的功能。

网络地址转换

Cisco IOS网络地址转换(NAT)经常与Cisco IOS防火墙同时配置，特别是在专用网络必须与

Internet接口或者不同专用网络必须连接时，尤其是在使用重叠的IP地址空间时。Cisco IOS软件包括SIP、Skinny和H.323的NAT应用层网关(ALG)。理想情况下，IP语音的网络连接无需应用NAT即可实现，因为NAT会为故障排除和安全策略应用带来额外的复杂性，尤其是在使用NAT过载的情况下。NAT应仅作为解决网络连接问题的最后一个案例解决方案。

Cisco Unified Presence客户端

本文档不介绍支持使用带IOS防火墙的Cisco Unified Presence Client(CUPC)的配置，因为自Cisco IOS软件版本12.4(20)T1起，区域或传统防火墙尚不支持CUPC。CUPC将在未来的Cisco IOS软件版本中受支持。

CME/CUE/GW单站点或分支PSTN连接

此场景为单站点中小型企业或希望部署分布式呼叫处理、维护与公共交换电话网(PSTN)的传统连接的大型多站点组织引入了基于路由器的安全IP语音电话。 VoIP呼叫控制通过Cisco Unified Call Manager Express的应用实现。

PSTN连接可以长期维护，也可以迁移到融合语音和数据IP广域网，如本文档HQ或语音提供商部分的CME/CUE/GW单站点或分支机构中SIP中继中讨论的应用示例所述。

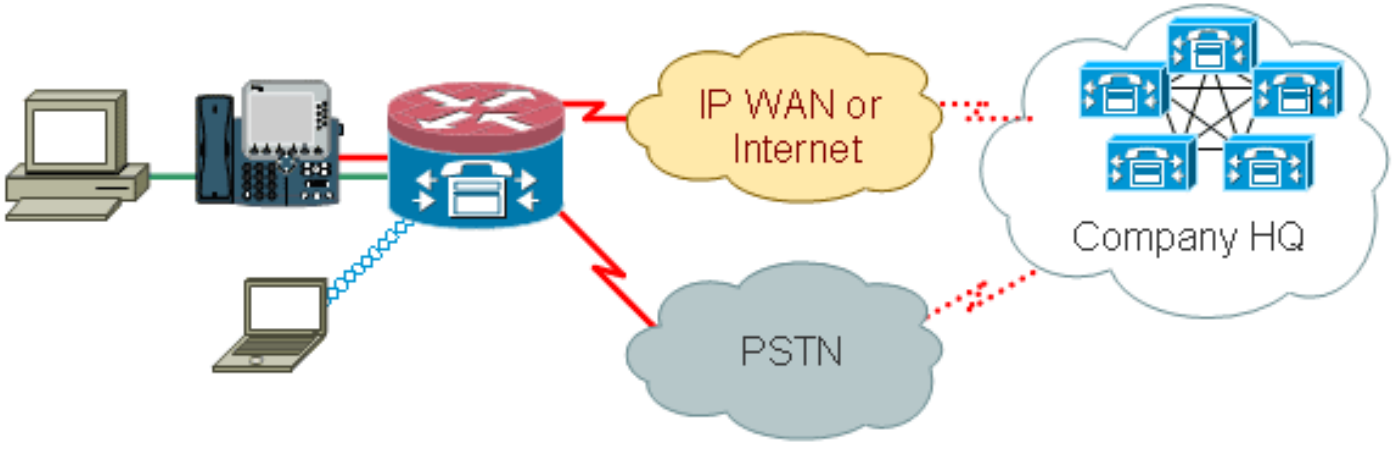
组织应考虑在站点之间使用不同VoIP环境或由于WAN数据连接不足或数据网络上VoIP使用受区域限制而无法使用VoIP的情况下实施此类应用方案。Cisco Unified CallManager Express SRND中介绍了单站点IP电话的优点和最佳实践。

方案背景

应用场景包括有线电话（语音VLAN）、有线PC（数据VLAN）和无线设备（包括VoIP设备，如IP Communicator）。

安全配置提供：

- CME和本地电话（SCCP和/或SIP）之间由路由器发起的信令检查
- 语音媒体针孔，用于在以下设备之间通信：本地有线和无线段用于 MoH 的 CME 和本地电话用于语音邮件的 CUE 和本地电话
- 将应用检测和控制(AIC)应用于：发送速率限制邀请消息确保所有 SIP 数据流上的协议符合性.



优点和缺点

场景的VoIP方面最明显的好处是，在将现有语音和数据网络基础设施集成到现有POTS/TDM环境中之后，再迁移到融合语音/数据网络以便将电话服务扩展到LAN之外的世界，从而提供迁移路径。为小型企业维护电话号码，并且现有的centrex或DID服务可保留给希望分阶段迁移到长途旁路分组电话的大型企业。

缺点包括：迁移到融合语音和数据网络时，费用旁路可实现的成本节省损失；呼叫灵活性的限制；以及缺乏通过完全融合的语音和数据网络实现的整个组织的通信集成和便携性。

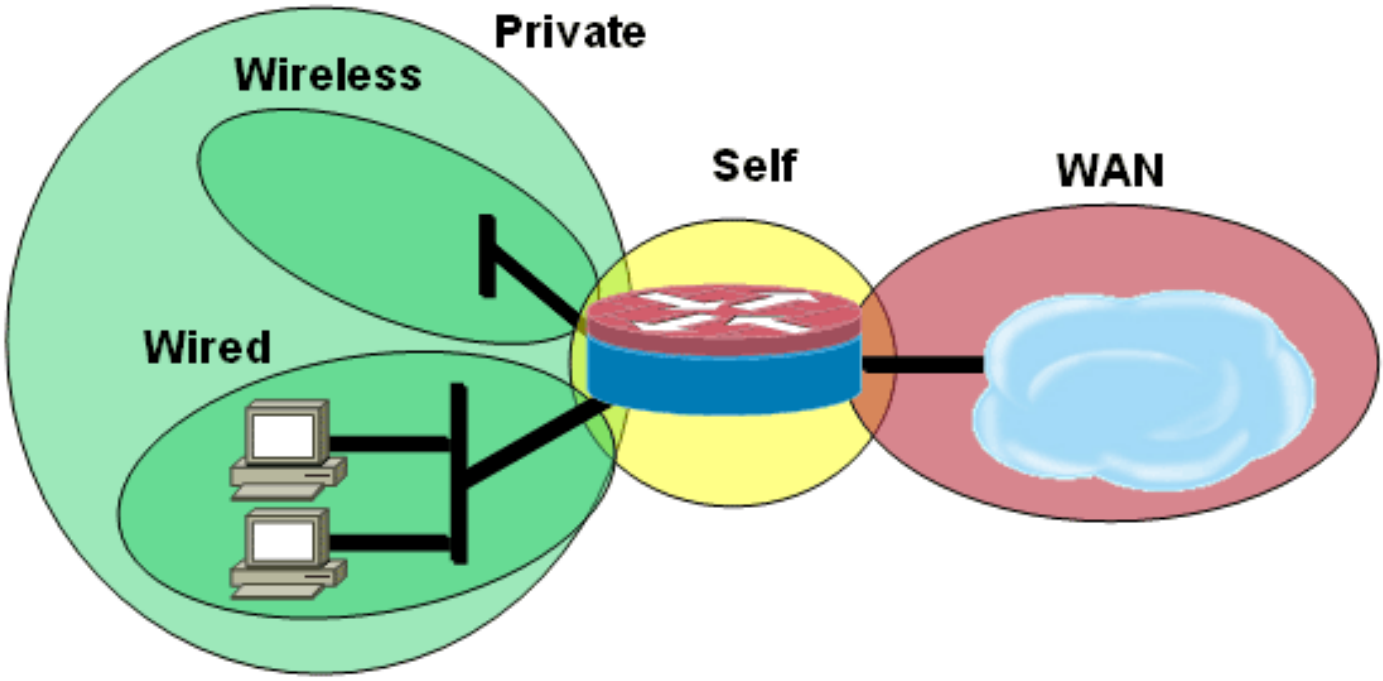
从安全角度来看，这种网络环境通过避免VoIP资源暴露到公共网络或WAN，将VoIP安全威胁降至最低。但是，路由器中嵌入的Cisco Call Manager Express仍容易受到内部威胁（如恶意流量或故障应用流量）的影响。因此，实施允许满足协议一致性检查的语音特定流量的策略，并限制特定VoIP操作（即SIP INVITE），以降低恶意或无意软件故障对VoIP资源和可用性造成负面影响的可能性。

数据策略、基于区域的防火墙、语音安全和CCME配置

此处描述的配置说明了2851，该2851具有CME和CUE连接的语音服务配置：

```
!
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
!
```

基于区域的策略防火墙配置，由有线和无线LAN网段的安全区域、私有LAN（由有线和无线网段组成）、到达不受信任Internet连接的公有WAN网段以及路由器语音资源所在的自身区域组成。



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
```

整个路由器配置

```
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
```

调配、管理和监控

Cisco Configuration Professional通常最适合调配和配置基于路由器的IP电话资源和基于区域的策略防火墙。CiscoSecure Manager不支持基于区域的策略防火墙或基于路由器的IP电话。

Cisco IOS传统防火墙支持使用Cisco Unified Firewall MIB进行SNMP监控。但是，统一防火墙MIB中尚不支持基于区域的策略防火墙。因此，防火墙监控必须通过路由器命令行界面上的统计信息或Cisco Configuration Professional等GUI工具进行处理。

思科安全监控和报告系统(CS-MARS)为基于区域的策略防火墙提供基本支持，尽管日志记录更改改善了与12.4(15)T4/T5和12.4(20)T中实施的流量的日志消息关联，但CS-MARS中尚未完全支持该关联。

验证

当前没有可用于此配置的验证过程。

故障排除

Cisco IOS区域防火墙提供**show**和**debug**命令，用于查看、监控防火墙活动并排除其故障。本节介绍提供详细故障排除信息**的区**域防火墙debug命令。

调试命令

如果您使用非典型或不受支持的配置，并且需要与Cisco TAC或其他产品的技术支持服务合作以解决互操作性问题，则使用debug命令非常有用。

注意：将**debug命**令应用于特定功能或流量可能会导致大量控制台消息，从而导致路由器控制台无响应。即使需要启用调试，您也可能希望提供替代命令行界面访问，例如不监控终端对话框的telnet窗口。您应仅在离线（实验环境）设备或计划的维护窗口中启用调试，因为启用调试可能会严重影响路由器性能。

相关信息

- Cisco Unified CallManager Express 解决方案参考网络设计指南
- 将 Cisco Unity Connection 与 Cisco Unified CME-as-SRST 集成
- Cisco Unified Communications Manager Express命令参考
- Cisco CallManager Express/Cisco Unity Express 配置示例
- Cisco CallManager Express 3.4 SNMP MIB 支持
- 区域策略防火墙设计和应用指南
- 技术支持和文档 - Cisco Systems