Firewall baseado em zona do Cisco IOS: CME/CUE/GW Single Site ou Branch Office com Tronco SIP para CCM no HQ

Contents

Introduction

Os Cisco Integrated Service Routers (ISRs) oferecem uma plataforma escalável para atender aos requisitos de rede de dados e voz para uma ampla variedade de aplicativos. Embora o cenário de ameaças de redes privadas e conectadas à Internet seja um ambiente muito dinâmico, o Cisco IOS® Firewall oferece recursos de inspeção stateful e inspeção e controle de aplicativos (AIC) para definir e aplicar uma postura de rede segura, enquanto permite a capacidade e a continuidade dos negócios.

Este documento descreve as considerações de projeto e configuração para aspectos de segurança de firewall de cenários específicos de aplicativos de voz e dados baseados em Cisco ISR. As configurações para serviços de voz e firewall são fornecidas para cada cenário de aplicativo. Cada cenário descreve as configurações de VoIP e de segurança separadamente, seguidas por toda a configuração do roteador. A sua rede possivelmente pode exigir outra configuração para serviços, como QoS e VPN, para manter a qualidade e a confidencialidade da voz.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Plano de Fundo do Firewall IOS

O Cisco IOS Firewall é normalmente implantado em cenários de aplicativos que diferem dos modelos de implantação de firewalls de dispositivos. As implantações típicas incluem aplicativos para funcionários remotos, escritórios remotos ou pequenos e aplicativos de varejo, onde se deseja uma baixa contagem de dispositivos, integração de vários serviços e menor desempenho e profundidade de recursos de segurança.

Embora a aplicação da inspeção de firewall, juntamente com outros serviços integrados nos produtos ISR, possa parecer atraente do ponto de vista de custo e operacional, considerações específicas devem ser avaliadas para determinar se um firewall baseado em roteador é apropriado. A aplicação de cada recurso adicional incorre em custos de memória e processamento, e pode provavelmente contribuir para taxas de transferência de encaminhamento reduzidas, maior latência de pacotes e perda de capacidade de recurso em períodos de pico de carga se uma solução baseada em roteador integrado com baixa energia for implantada. Observe estas diretrizes ao decidir entre um roteador e um dispositivo:

- Os roteadores com vários recursos integrados habilitados são mais adequados para filiais ou escritórios remotos, onde menos dispositivos oferecem uma solução melhor.
- Aplicativos de alta largura de banda e alto desempenho são geralmente mais bem tratados com dispositivos; O Cisco ASA e o Cisco Unified Call Manager Server devem ser aplicados para lidar com o NAT e o processamento de aplicativos e chamadas de políticas de segurança, enquanto os roteadores lidam com a aplicação de política de QoS, terminação de

WAN e requisitos de conectividade de VPN site a site.

Antes da introdução do Cisco IOS Software versão 12.4(20)T, o Classic Firewall e o Zone-Based Policy Firewall (ZFW) não podiam suportar totalmente os recursos necessários para tráfego VoIP e serviços de voz baseados em roteador, o que exigia grandes lacunas nas políticas de firewall seguras para acomodar tráfego de voz, e oferecia suporte limitado para a sinalização VoIP em evolução e protocolos de mídia.

Implantar o firewall de política baseado em zona do Cisco IOS

O Cisco IOS Zone-Based Policy Firewall, semelhante a outros firewalls, só pode oferecer um firewall seguro se os requisitos de segurança da rede forem identificados e descritos pela política de segurança. Há duas abordagens fundamentais para chegar a uma política de segurança: a perspectiva *confiável*, em oposição à perspectiva *suspeita*.

A perspectiva *confiável* pressupõe que todo o tráfego é confiável, exceto o que pode ser especificamente identificado como mal-intencionado ou indesejado. Uma política específica é implementada que nega apenas o tráfego indesejado. Isso normalmente é feito por meio do uso de entradas de controle de acesso específicas ou ferramentas baseadas em assinatura ou comportamento. Essa abordagem tende a interferir menos nos aplicativos existentes, mas exige um conhecimento abrangente do cenário de ameaças e vulnerabilidades e exige vigilância constante para lidar com novas ameaças e explorações à medida que elas surgem. Além disso, a comunidade de usuários deve desempenhar um papel importante na manutenção da segurança adequada. Um ambiente que permite ampla liberdade com pouco controle para os ocupantes oferece oportunidades substanciais para problemas causados por indivíduos descuidados ou mal-intencionados. Um problema adicional dessa abordagem é que ela depende muito mais de ferramentas de gerenciamento eficazes e controles de aplicativos que oferecem flexibilidade e desempenho suficientes para poder monitorar e controlar dados suspeitos em todo o tráfego de rede. Embora a tecnologia esteja atualmente disponível para acomodar isso, a carga operacional frequentemente excede os limites da maioria das empresas.

A perspectiva *suspeita* pressupõe que todo o tráfego de rede é indesejado, exceto para o *bom* tráfego *identificado especificamente*. É uma política aplicada, que nega todo o tráfego de aplicativos, exceto aquela explicitamente permitida. Além disso, a AIC (Application Inspection and Control, inspeção e controle de aplicativos) pode ser implementada para identificar e negar o tráfego mal-intencionado criado especificamente para explorar *bons* aplicativos, bem como o tráfego indesejado que se mascara como um *bom* tráfego. Novamente, os controles de aplicativos impõem carga operacional e de desempenho na rede, embora a maioria do tráfego indesejado deva ser controlada por filtros stateless, como listas de controle de acesso (ACLs) ou política de firewall de política baseada em zona (ZFW), de modo que há muito menos tráfego que deve ser tratado pelo AIC, sistema de prevenção de invasão (IPS) ou outros controles baseados em assinatura, como correspondência de pacotes flexível (FPM) ou reconhecimento de aplicativos baseados em rede (NBAR) . Se apenas as portas de aplicativos desejadas (e o tráfego específico de mídia dinâmico proveniente de conexões ou sessões de controle conhecidas) forem especificamente permitidos, o único tráfego indesejado presente na rede deverá cair em um subconjunto específico e mais facilmente reconhecido, o que reduz a carga operacional e de engenharia imposta para manter o controle sobre o tráfego indesejado.

Este documento descreve as configurações de segurança de VoIP com base na perspectiva *suspeita*, de modo que somente o tráfego permitido nos segmentos de rede de voz é permitido. As políticas de dados tendem a ser mais permissivas, conforme descrito pelas notas na configuração de cada cenário de aplicação.

Todas as implantações de políticas de segurança devem seguir um ciclo de feedback de loop fechado; as implantações de segurança normalmente afetam a capacidade e a funcionalidade dos aplicativos existentes e devem ser ajustadas para minimizar ou resolver esse impacto.

Se precisar de informações adicionais para configurar o firewall de política baseado em zona, consulte o Guia de design e aplicação do firewall de zona.

Considerações para ZFW em ambientes VoIP

O Zone Firewall Design and Application Guide oferece uma breve discussão sobre a segurança do roteador com o uso de políticas de segurança para e da zona *própria* do roteador, bem como recursos alternativos que são fornecidos através de vários recursos do Network Foundation Protection (NFP). Os recursos de VoIP baseados em roteador são hospedados na zona *autossuficiente* do roteador, portanto, as políticas de segurança que protegem o roteador devem estar cientes dos requisitos de tráfego de voz para acomodar a sinalização de voz e a mídia originada e destinada ao Cisco Unified CallManager Express, Survivable Remote-Site Telephony e aos recursos de Gateway de Voz. Antes da versão 12.4(20)T do software Cisco IOS, o firewall clássico e o firewall de política baseado em zona não podiam acomodar totalmente os requisitos do tráfego VoIP, portanto, as políticas de firewall não foram otimizadas para proteger totalmente os recursos. As políticas de segurança de zona autônoma que protegem os recursos VoIP baseados em roteador dependem muito dos recursos introduzidos no 12.4(20)T.

Recursos de voz do firewall IOS

O Cisco IOS Software Release 12.4(20)T introduziu vários aprimoramentos para ativar o Zone Firewall co-residente e os recursos de voz. Três recursos principais se aplicam diretamente a aplicativos de voz seguros:

- Aprimoramentos SIP: Inspeção e Controle de Aplicativos e Gateway da Camada de AplicaçãoAtualiza o suporte da versão SIP para SIPv2, conforme descrito pelo RFC 3261Amplia o suporte de sinalização SIP para reconhecer uma variedade maior de fluxos de chamadasApresenta o SIP Application Inspection and Control (AIC) para aplicar controles granulares para lidar com vulnerabilidades e explorações específicas no nível do aplicativoExpande a inspeção de zona automática para poder reconhecer a sinalização secundária e os canais de mídia que resultam do tráfego SIP com origem/destino local
- Suporte para tráfego local Skinny e CMEAtualiza o suporte do SCCP para a versão 16 (versão 9 suportada anteriormente)Apresenta o AIC (Application Inspection and Control, inspeção e controle de aplicativos) do SCCP para aplicar controles granulares para lidar com vulnerabilidades e explorações específicas no nível do aplicativoExpande a inspeção de zona automática para poder reconhecer a sinalização secundária e os canais de mídia que resultam do tráfego SCCP com origem/destino local
- Suporte H.323 para versões 3 e 4Atualiza o suporte do H.323 para as versões 3 e 4 (versões 1 e 2 com suporte anterior)Apresenta o AIC (Application Inspection and Control, inspeção e controle de aplicativos) H.323 para aplicar controles granulares para lidar com vulnerabilidades específicas em nível de aplicativos e explorações

As configurações de segurança do roteador descritas neste documento incluem recursos oferecidos por esses aprimoramentos com explicações para descrever a ação aplicada pelas políticas. Hiperlinks para os documentos de recursos individuais estão disponíveis na seção Informações Relacionadas deste documento se você quiser revisar os detalhes completos dos recursos de inspeção de voz.

Caveats

Para reforçar os pontos mencionados anteriormente, a aplicação do Cisco IOS Firewall com recursos de voz baseados em roteador deve aplicar o Zone-Based Policy Firewall. O firewall IOS clássico não inclui a capacidade necessária para suportar totalmente as complexidades de sinalização ou o comportamento do tráfego de voz.

Tradução de Endereço de Rede (NAT)

A Conversão de Endereço de Rede (NAT - Network Address Translation) do Cisco IOS é frequentemente configurada simultaneamente com o Cisco IOS Firewall, especialmente nos casos em que as redes privadas devem fazer interface com a Internet ou se redes privadas diferentes devem se conectar, especialmente se o espaço de endereço IP se sobrepuser. O software Cisco IOS inclui os gateways da camada de aplicação (ALGs) NAT para SIP, Skinny e H.323. Idealmente, a conectividade de rede para voz IP pode ser acomodada sem a aplicação do NAT, pois o NAT apresenta complexidade adicional para a solução de problemas e aplicativos de política de segurança, especialmente nos casos em que a sobrecarga de NAT é usada. O NAT só pode ser aplicado como uma solução de último caso para resolver problemas de conectividade de rede.

Cisco Unified Presence Client (CUPC)

Este documento não descreve a configuração que suporta o uso do Cisco Unified Presence Client (CUPC) com IOS Firewall, pois o CUPC ainda não é suportado pelo Zone ou Classic Firewall, a partir do Cisco IOS Software Release 12.4(20)T1. O CUPC será suportado em uma versão futura do Cisco IOS Software.

CME/CUE/GW Single Site ou Branch Office com Tronco SIP para CCM em HQ ou Provedor de Voz

Esse cenário oferece um comprometimento entre o modelo conectado PSTN/processamento de chamadas distribuído/de local único descrito anteriormente neste documento (CME/CUE/GW Single Site ou Branch Office que se conecta ao PSTN) e a rede de voz e dados convergente/processamento de chamadas de vários locais/centralizados definida no terceiro cenário descrito neste documento. Esse cenário ainda usa um Cisco Unified CallManager Express local, mas a discagem de longa distância e a telefonia de HQ/local remoto são acomodadas principalmente através de troncos SIP de site a site, com discagem local e discagem de emergência através de uma conexão PSTN local. Mesmo nos casos em que a maioria da conectividade PSTN antiga é removida, recomenda-se um nível básico de capacidade PSTN para acomodar falhas na discagem de desvio de tarifa baseada em WAN, bem como na discagem de área local, conforme descrito pelo plano de discagem. Além disso, as leis locais geralmente exigem que algum tipo de conectividade PSTN local seja fornecido para acomodar a discagem de emergência (911). Este cenário emprega o processamento de chamadas distribuídas, que oferece benefícios e observa as melhores práticas conforme descrito no Cisco Unified CallManager Express SRND.

As organizações podem implementar esse tipo de cenário de aplicação nessas circunstâncias:

- Ambientes VoIP diferentes são usados entre locais, mas VoIP ainda é desejado no lugar da PSTN de longa distância.

- A autonomia local por local é necessária para a administração do plano de discagem.
- O recurso completo de processamento de chamadas é necessário independentemente da disponibilidade da WAN.

Histórico do cenário

O cenário do aplicativo incorpora telefones com fio (VLAN de voz), PCs com fio (VLAN de dados) e dispositivos sem fio (que incluem dispositivos VoIP, como o IP Communicator).

A configuração de segurança oferece:

1. Inspeção de sinalização iniciada pelo roteador entre o CME e os telefones locais (SCCP e SIP) e o CME e o cluster remoto do CUCM (SIP).
2. Orifícios de mídia de voz para comunicação entre estes:Segmentos locais com e sem fioCME e os telefones locais para MoHCUE e os telefones locais para correio de vozTelefones e entidades de chamada remota
3. AIC (Application Inspection and Control, inspeção e controle de aplicativos), que pode ser aplicada para alcançar estes objetivos:Limite de taxa de mensagens de conviteGarantir a conformidade do protocolo em todo o tráfego SIP

Vantagens/Desvantagens

Esse aplicativo oferece o benefício de custos reduzidos, já que transporta tráfego de voz site a site em enlaces de dados da WAN.

Uma desvantagem desse cenário é que são necessários planos mais detalhados para a conectividade da WAN. A qualidade da chamada de site a site pode ser afetada por muitos fatores na WAN, como tráfego ilegítimo/indesejado (worms, vírus, compartilhamento de arquivos ponto a ponto) ou problemas de latência difíceis de identificar que podem surgir como resultado da engenharia de tráfego em redes de operadoras. As conexões WAN devem ser dimensionadas adequadamente para oferecer largura de banda suficiente para tráfego de voz e dados; menos tráfego de dados sensível à latência, por exemplo, e-mail, tráfego de arquivos SMB/CIFS, pode ser classificado como tráfego de prioridade mais baixa para QoS a fim de preservar a qualidade de voz.

Outro problema com esse cenário é a falta de processamento centralizado de chamadas e as dificuldades que podem surgir na solução de problemas de falhas de processamento de chamadas. Como tal, esse cenário funciona melhor para empresas maiores como uma etapa intermediária na migração para o processamento centralizado de chamadas. Os Cisco CMEs locais podem ser convertidos para atuar como fallback de SRST completo quando a migração para o Cisco CallManager for concluída.

Do ponto de vista da segurança, o aumento da complexidade desse ambiente torna a implementação de segurança efetiva e a solução de problemas mais difíceis porque a conectividade em uma WAN, ou sobre VPN na Internet pública, aumenta drasticamente o ambiente de ameaças, particularmente nos casos em que a política de segurança requer uma perspectiva de *confiança*, onde pouca restrição é imposta ao tráfego sobre a WAN. Com isso em mente, os exemplos de configuração fornecidos por este documento implementam uma política mais *suspeita* que permite tráfego crítico para os negócios específico, que é então examinado por verificações de conformidade de protocolo. Além disso, ações VoIP específicas, ou seja, CONVITE SIP, são limitadas para reduzir a probabilidade de defeitos de software mal-

intencionados ou não intencionais que afetam negativamente os recursos de VoIP e a usabilidade.

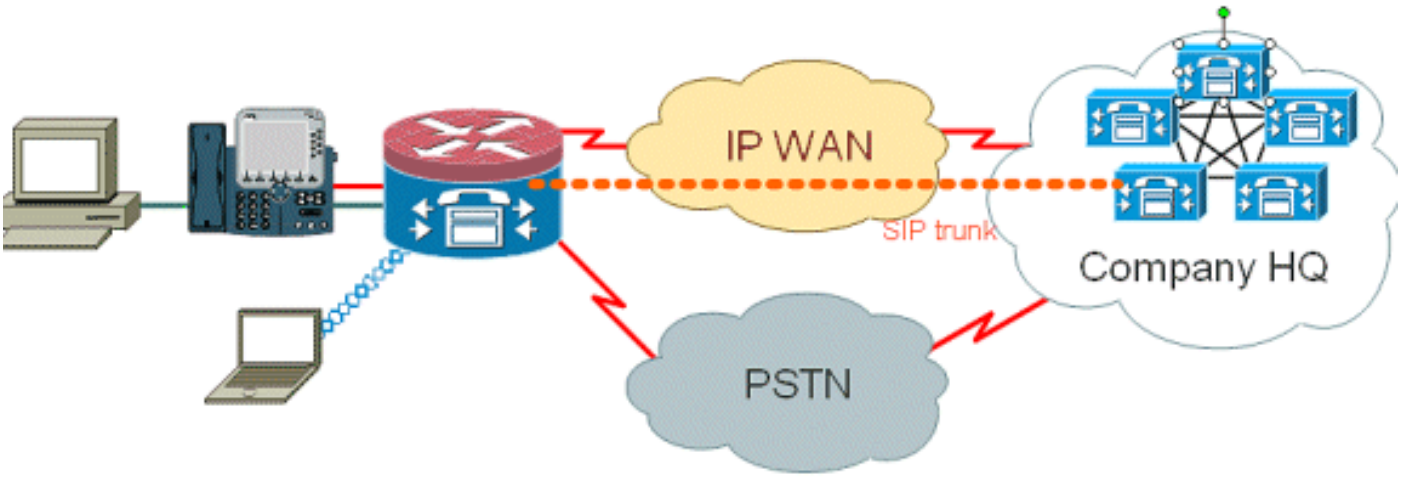
Configurar

Configurações para políticas de dados, firewall baseado em zona, segurança de voz, CCME

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

A configuração descrita aqui ilustra um Cisco 2851 Integrated Services Router.

Este documento utiliza as seguintes configurações:

- Configuração do serviço de voz para conectividade CME e CUE
- Configuração do firewall de política baseada em zona
- Configuração de segurança

Esta é a configuração do serviço de voz para conectividade CME e CUE:

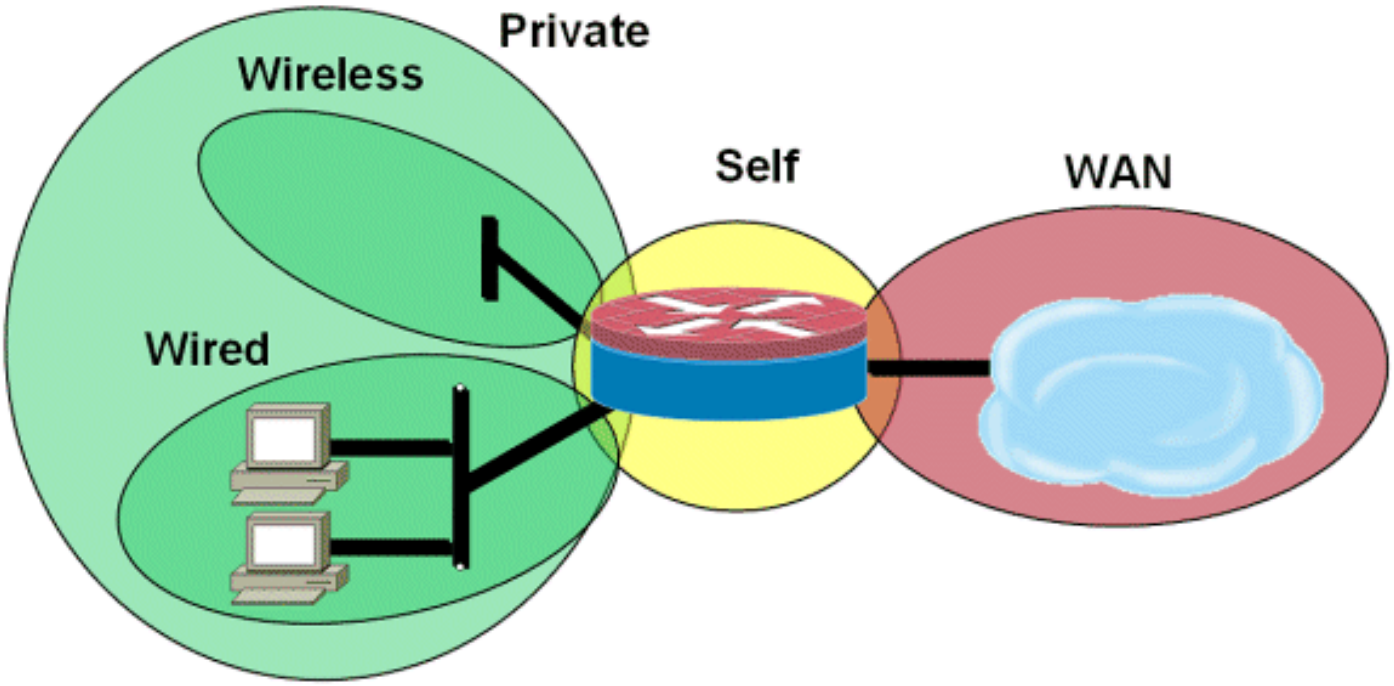
Configuração do serviço de voz para conectividade CME e CUE

```
!
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

!
```

Esta é a Configuração do Firewall de Política Baseada em Zona, composta de zonas de segurança para segmentos de LAN com e sem fio, LAN privada (composta de segmentos com e sem fio), um segmento de WAN onde a conectividade de WAN confiável é alcançada e a zona automática onde os recursos de voz do roteador estão localizados:



Esta é a configuração de segurança:

Configuração de segurança

```
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
```

Provisionar, gerenciar e monitorar

O provisionamento e a configuração para recursos de telefonia IP baseados em roteador e firewall de política baseada em zona geralmente são mais bem acomodados com o Cisco Configuration Professional. O Cisco Secure Manager não suporta firewall de política baseada em zona ou telefonia IP baseada em roteador.

O Cisco IOS Classic Firewall suporta monitoramento SNMP com o Cisco Unified Firewall MIB, mas o firewall de política baseado em zona ainda não é suportado no Unified Firewall MIB. Como tal, o monitoramento de firewall deve ser tratado por meio de estatísticas na interface de linha de comando do roteador ou com ferramentas GUI, como o Cisco Configuration Professional.

O Cisco Secure Monitoring And Reporting System (CS-MARS) oferece suporte básico para o Zone-Based Policy Firewall, embora as alterações de registro que melhoraram a correlação da mensagem de registro com o tráfego, que foram implementadas em 12.4(15)T4/T5 e 12.4(20)T, ainda não tenham sido totalmente suportadas no CS-MARS.

Planos de capacidade

Os resultados do teste de desempenho de inspeção de chamadas de firewall da Índia são a serem definidos.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

O Cisco IOS Zone Firewall fornece comandos **show** e **debug** para exibir, monitorar e solucionar problemas da atividade do firewall. Esta seção descreve o uso dos comandos **show** para monitorar a atividade básica do firewall e uma introdução aos comandos **debug** do Zone Firewall para solucionar problemas de configuração ou se a discussão com o suporte técnico exigir informações mais detalhadas.

Comandos para Troubleshooting

O Cisco IOS Firewall oferece vários comandos **show** para exibir a configuração e a atividade da política de segurança. Muitos desses comandos podem ser substituídos por um comando mais curto através da aplicação do comando **alias**.

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

Os comandos de depuração podem ser úteis no caso de você estar usando uma configuração atípica ou não suportada e precisarem trabalhar com o Cisco TAC ou com os serviços de suporte técnico de outros produtos para resolver problemas de interoperabilidade.

Observação: a aplicação de comandos **debug** a recursos ou tráfego específicos pode causar um grande número de mensagens do console, o que faz com que o console do roteador não responda. Mesmo que você precise depurar, você pode fornecer acesso alternativo à interface de linha de comando, como uma janela Telnet que não monitore a caixa de diálogo do terminal. Somente habilite a depuração em equipamentos off-line (ambiente de laboratório) ou em uma janela de manutenção planejada, uma vez que a depuração pode afetar substancialmente o desempenho do roteador.

Informações Relacionadas

- Guia de projeto de rede de referência da solução Cisco Unified CallManager Express
- Práticas recomendadas de segurança do Cisco CallManager Express (CME SRND)
- Integração do Cisco Unity Connection com o Cisco Unified CME-as-SRST

- Referência de comandos do Cisco Unified Communications Manager Express
- Exemplo de configuração do Cisco CallManager Express/Cisco Unity Express
- Suporte MIB SNMP Cisco CallManager Express 3.4
- Guia de aplicativos e design de firewall de política baseada em zona
- Firewall do Cisco IOS: Aprimoramentos SIP: ALG e AIC
- Software Cisco IOS Firewall H.323 Suporte
- Suporte do Cisco IOS Firewall para tráfego local Skinny e CME
- Suporte Técnico e Documentação - Cisco Systems