Firewall basado en zona de Cisco IOS: CME/CUE/GW Un solo sitio o sucursal con enlace troncal SIP a CCM en la sede central

Contenido

Introducción

Los routers de servicios integrados (ISR) de Cisco ofrecen una plataforma escalable para hacer frente a los requisitos de red de voz y datos para una amplia gama de aplicaciones. Aunque el panorama de amenazas de las redes privadas y conectadas a Internet es un entorno muy dinámico, Cisco IOS® Firewall ofrece funciones de inspección y control de aplicaciones (AIC) con información de estado para definir y aplicar una condición de red segura, al tiempo que permite la capacidad y continuidad empresarial.

Este documento describe consideraciones de diseño y configuración para los aspectos de seguridad del firewall de escenarios específicos de aplicaciones de voz y datos basados en Cisco ISR. Las configuraciones para los servicios de voz y el firewall se proporcionan para cada escenario de aplicación. Cada escenario describe las configuraciones de VoIP y seguridad por separado, seguidas de la configuración completa del router. Es posible que su red requiera otra configuración para servicios, como QoS y VPN, para mantener la calidad de voz y la confidencialidad.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

Fondo del Firewall IOS

El firewall de Cisco IOS se suele implementar en escenarios de aplicaciones que difieren de los modelos de implementación de firewalls de dispositivos. Las implementaciones típicas incluyen aplicaciones de teletrabajador, sitios de oficinas pequeñas o sucursales y aplicaciones minoristas, en las que se desea un número reducido de dispositivos, integración de varios servicios y un menor rendimiento y una mayor capacidad de seguridad.

Aunque la aplicación de la inspección de firewall, junto con otros servicios integrados en los productos ISR, puede parecer atractiva desde la perspectiva de costes y de funcionamiento, se deben evaluar consideraciones específicas para determinar si un firewall basado en router es apropiado. La aplicación de cada función adicional conlleva costes de procesamiento y memoria, y probablemente puede contribuir a reducir las tasas de rendimiento de reenvío, a aumentar la latencia de paquetes y a la pérdida de capacidad de funciones dentro de los períodos de carga pico si se implementa una solución integrada basada en router con bajo consumo de energía. Observe estas pautas cuando decide entre un router y un dispositivo:

- Los routers con varias funciones integradas habilitadas son los más adecuados para sucursales o teletrabajadores, donde un número menor de dispositivos ofrece una mejor solución.
- Las aplicaciones de alto ancho de banda y alto rendimiento se suelen abordar mejor con los dispositivos; Cisco ASA y Cisco Unified Call Manager Server deben aplicarse para gestionar la aplicación de políticas de seguridad y NAT y el procesamiento de llamadas, mientras que

los routers abordan la aplicación de políticas de QoS, la terminación de WAN y los requisitos de conectividad VPN de sitio a sitio.

Antes de la introducción de la versión 12.4(20)T del software Cisco IOS, el firewall clásico y el firewall de políticas basado en zonas (ZFW) no eran capaces de admitir completamente las capacidades necesarias para el tráfico VoIP y los servicios de voz basados en router, que requerían grandes brechas en las políticas de firewall seguras para admitir el tráfico de voz, y ofrecían compatibilidad limitada para la señalización VoIP en evolución y los protocolos multimedia.

Implementar firewall de políticas basado en zonas de Cisco IOS

Cisco IOS Zone-Based Policy Firewall, al igual que otros firewalls, solo puede ofrecer un firewall seguro si los requisitos de seguridad de la red se identifican y describen mediante la política de seguridad. Hay dos enfoques fundamentales para llegar a una política de seguridad: la perspectiva *de confianza*, en contraposición a la *perspectiva* sospechosa.

La perspectiva *de confianza* asume que todo el tráfico es confiable, excepto aquello que se puede identificar específicamente como malicioso o no deseado. Se implementa una política específica que niega solamente el tráfico no deseado. Esto se consigue normalmente mediante el uso de entradas de control de acceso específicas o herramientas basadas en firma o comportamiento. Este enfoque tiende a interferir menos con las aplicaciones existentes, pero requiere un conocimiento exhaustivo del panorama de amenazas y vulnerabilidades, y requiere una vigilancia constante para hacer frente a las nuevas amenazas y vulnerabilidades a medida que aparecen. Además, la comunidad de usuarios debe desempeñar un papel importante en el mantenimiento de una seguridad adecuada. Un entorno que permite una amplia libertad con escaso control para los ocupantes ofrece una oportunidad sustancial para los problemas causados por individuos descuidados o maliciosos. Un problema adicional de este enfoque es que se basa mucho más en herramientas de administración y controles de aplicaciones eficaces que ofrecen suficiente flexibilidad y rendimiento para poder supervisar y controlar los datos sospechosos en todo el tráfico de red. Aunque actualmente se dispone de tecnología para hacer frente a esta situación, la carga operacional suele superar los límites de la mayoría de las organizaciones.

La perspectiva *sospechosa* asume que todo el tráfico de red no es deseado, excepto para el *buen* tráfico *identificado específicamente*. Se trata de una política que se aplica, que niega todo el tráfico de la aplicación, excepto aquélla que se permite explícitamente. Además, la inspección y el control de aplicaciones (AIC) se pueden implementar para identificar y denegar el tráfico malintencionado diseñado específicamente para explotar *buenas* aplicaciones, así como el tráfico no deseado que se muestra como *buen* tráfico. Nuevamente, los controles de aplicaciones imponen cargas operativas y de rendimiento en la red, aunque la mayoría del tráfico no deseado debe controlarse mediante filtros sin información de estado, como las listas de control de acceso (ACL) o la política de firewall de políticas basado en zonas (ZFW), por lo que hay mucho menos tráfico que debe gestionar AIC, el sistema de prevención de intrusiones (IPS) u otros controles basados en firmas, como la coincidencia de paquetes flexible (FPM) o el reconocimiento de aplicaciones basado en red (NBAR) ... Si sólo se permiten específicamente los puertos de aplicación deseados (y el tráfico específico de medios dinámico derivado de conexiones o sesiones de control conocidas), el único tráfico no deseado que está presente en la red debe caer en un subconjunto específico y más fácilmente reconocido, lo que reduce la carga de ingeniería y operativa impuesta para mantener el control sobre el tráfico no deseado.

Este documento describe las configuraciones de seguridad de VoIP basadas en la perspectiva *sospechosa*, por lo que sólo se permite el tráfico que está permitido en los segmentos de red de voz. Las políticas de datos tienden a ser más permisivas, como se describe en las notas de la

configuración de cada escenario de aplicación.

Todas las implementaciones de políticas de seguridad deben seguir un ciclo de retroalimentación de bucle cerrado; las implementaciones de seguridad suelen afectar a la capacidad y funcionalidad de las aplicaciones existentes y deben ajustarse para minimizar o resolver este impacto.

Si necesita información adicional para configurar el firewall de políticas basado en zona, revise la Guía de diseño y aplicación de Zone Firewall.

Consideraciones para ZFW en entornos VoIP

La Guía de diseño y aplicación de firewall de zona ofrece un breve debate sobre la seguridad del router con el uso de políticas de seguridad hacia y desde la *zona* propia del router, así como capacidades alternativas que se proporcionan a través de diversas funciones de Network Foundation Protection (NFP). Las capacidades de VoIP basadas en router se alojan dentro de la zona *automática* del router, por lo que las políticas de seguridad que protegen el router deben ser conscientes de los requisitos del tráfico de voz para acomodar la señalización de voz y los medios originados por Cisco Unified CallManager Express, Survivable Remote-Site Telephony y los recursos de la Gateway de voz. Antes de la versión 12.4(20)T del software Cisco IOS, el firewall clásico y el firewall de políticas basado en zonas no podían satisfacer por completo los requisitos del tráfico VoIP, por lo que las políticas de firewall no estaban optimizadas para proteger por completo los recursos. Las políticas de seguridad de zona autónoma que protegen los recursos VoIP basados en router se basan en gran medida en las capacidades introducidas en 12.4(20)T.

Funciones de voz del firewall IOS

La versión 12.4(20)T del software Cisco IOS introdujo varias mejoras para habilitar las capacidades de voz y firewall de zona co-residentes. Tres funciones principales se aplican directamente a las aplicaciones de voz seguras:

- Mejoras de SIP: Control e inspección de aplicaciones y gateway de capa de aplicaciónActualiza el soporte de la versión SIP para SIPv2, como se describe en RFC 3261Amplía el soporte de señalización SIP para reconocer una mayor variedad de flujos de llamadasIntroduce el control e inspección de aplicaciones SIP (AIC) para aplicar controles granulares para hacer frente a vulnerabilidades y vulnerabilidades específicas de nivel de aplicaciónExpande la inspección de zona autónoma para poder reconocer canales de medios y señalización secundarios que resultan del tráfico SIP originado/destinado localmente
- Compatibilidad con tráfico local Skinny y CMEActualiza el soporte SCCP a la versión 16 (versión 9 previamente admitida)Presenta el control e inspección de aplicaciones (AIC) de SCCP para aplicar controles granulares con el fin de hacer frente a vulnerabilidades y vulnerabilidades específicas de nivel de aplicaciónExpande la inspección de zona autónoma para poder reconocer canales de señalización secundaria y medios que resultan del tráfico SCCP originado/destinado localmente
- Soporte de H.323 para las versiones 3 y 4Actualiza el soporte de H.323 a las versiones 3 y 4 (versiones 1 y 2 previamente admitidas)Presenta H.323 Application Inspection and Control (AIC) para aplicar controles granulares con el fin de hacer frente a vulnerabilidades y vulnerabilidades específicas en el nivel de las aplicaciones

Las configuraciones de seguridad del router descritas en este documento incluyen las capacidades ofrecidas por estas mejoras con explicaciones para describir la acción aplicada por

las políticas. Los hipervínculos a los documentos de características individuales están disponibles en la sección Información Relacionada de este documento si desea revisar los detalles completos de las funciones de inspección de voz.

Advertencias

Para reforzar los puntos mencionados anteriormente, la aplicación del Cisco IOS Firewall con capacidades de voz basadas en router debe aplicar el firewall de políticas basado en zona. El firewall de IOS clásico no incluye la capacidad necesaria para admitir completamente las complejidades de señalización o el comportamiento del tráfico de voz.

traducción de Dirección de Red (NAT)

La traducción de direcciones de red (NAT) de Cisco IOS se configura con frecuencia de forma simultánea con el firewall de Cisco IOS, especialmente en los casos en que las redes privadas deben interactuar con Internet, o si se deben conectar redes privadas dispares, especialmente si el espacio de direcciones IP se superpone. El software Cisco IOS incluye los gateways de capa de aplicación NAT (ALG) para SIP, Skinny y H.323. Lo ideal es que la conectividad de red para voz IP se pueda alojar sin la aplicación de NAT, ya que NAT introduce complejidad adicional en la resolución de problemas y en las aplicaciones de políticas de seguridad, especialmente en los casos en que se utiliza sobrecarga de NAT. NAT sólo se puede aplicar como solución en el último caso para abordar las preocupaciones de conectividad de red.

Cliente Cisco Unified Presence (CUPC)

Este documento no describe la configuración que admite el uso de Cisco Unified Presence Client (CUPC) con IOS Firewall, ya que CUPC todavía no es compatible con Zone o Classic Firewall, a partir de la versión 12.4(20)T1 del software Cisco IOS. CUPC será compatible en una futura versión del software Cisco IOS.

CME/CUE/GW Un solo sitio o sucursal con enlace troncal SIP a CCM en la sede central o proveedor de voz

Este escenario ofrece un compromiso entre el modelo conectado a PSTN/procesamiento de llamadas distribuido/de un solo sitio descrito anteriormente en este documento (CME/CUE/GW de un solo sitio o sucursal que se conecta a PSTN) y la red convergente de voz y datos de procesamiento de llamadas centralizada/multisitio definida en el tercer escenario descrito en este documento. Esta situación todavía utiliza un Cisco Unified CallManager Express local, pero la marcación de larga distancia y la telefonía de HQ/sitio remoto se acomodan principalmente a través de líneas troncales SIP de sitio a sitio, con marcación de emergencia y de marcado local a través de una conexión PSTN local. Incluso en los casos en los que se elimina la mayoría de la conectividad PSTN heredada, se recomienda un nivel básico de capacidad PSTN para admitir el fallo en la marcación de desvío de llamadas basada en WAN, así como la marcación de área local como se describe en el plan de marcación. Además, las leyes locales suelen exigir que se proporcione algún tipo de conectividad PSTN local para admitir la marcación de emergencia (911). Este escenario emplea el procesamiento de llamadas distribuido, que ofrece ventajas y observa las prácticas recomendadas tal como se describe en el SRND de Cisco Unified CallManager Express.

Las organizaciones pueden implementar este tipo de escenario de aplicación en estas

circunstancias:

- Se utilizan entornos VoIP diferentes entre sitios, pero VoIP sigue siendo deseable en lugar de PSTN de larga distancia.
- Se necesita autonomía sitio a sitio para la administración del plan de marcación.
- Se necesita una capacidad de procesamiento de llamadas completa independientemente de la disponibilidad de la WAN.

Antecedentes del escenario

El escenario de la aplicación incorpora teléfonos con cables (VLAN de voz), PC con cables (VLAN de datos) y dispositivos inalámbricos (que incluyen dispositivos VoIP, como IP Communicator).

La configuración de seguridad proporciona lo siguiente:

1. Inspección de señalización iniciada por el router entre CME y los teléfonos locales (SCCP y SIP) y CME y el clúster CUCM remoto (SIP).
2. Los medios de voz distinguen entre sí para la comunicación entre estos:Segmentos locales por cable e inalámbricosCME y los teléfonos locales para MoHCUE y los teléfonos locales para el correo de vozTeléfonos y entidades de llamada remotas
3. Control e inspección de aplicaciones (AIC), que se pueden aplicar para lograr estos objetivos:Mensajes de invitación de límite de velocidadGarantizar la conformidad del protocolo en todo el tráfico SIP

Ventajas/Desventajas

Esta aplicación ofrece la ventaja de reducir costes, ya que transporta tráfico de voz de sitio a sitio en enlaces de datos WAN.

Una desventaja de esta situación es que se necesitan planes más detallados para la conectividad WAN. La calidad de las llamadas de sitio a sitio puede verse afectada por muchos factores en la WAN, como el tráfico ilegítimo o no deseado (gusanos, virus, intercambio de archivos de igual a igual) o la dificultad para identificar los problemas de latencia que pueden surgir como resultado de la ingeniería del tráfico en las redes de operadores. Las conexiones WAN se deben dimensionar adecuadamente para ofrecer un ancho de banda suficiente tanto para el tráfico de voz como de datos; el tráfico de datos menos sensible a la latencia, por ejemplo, el correo electrónico, el tráfico de archivos SMB/CIFS, se puede clasificar como tráfico de menor prioridad para QoS a fin de preservar la calidad de voz.

Otro problema con este escenario es la falta de procesamiento centralizado de llamadas y las dificultades que pueden surgir en la resolución de problemas de fallas de procesamiento de llamadas. Por lo tanto, este escenario funciona mejor para las organizaciones más grandes como un paso intermedio en una migración al procesamiento centralizado de llamadas. Los CME de Cisco locales se pueden convertir para que actúen como reserva SRST con todas las funciones a medida que se completa la migración a Cisco CallManager.

Desde el punto de vista de la seguridad, la mayor complejidad de este entorno dificulta aún más la implementación y resolución de problemas de seguridad efectiva, ya que la conectividad a través de una WAN o VPN en Internet pública aumenta drásticamente el entorno de amenazas, especialmente en los casos en los que la política de seguridad requiere una perspectiva *de*

confianza, donde se imponen pocas restricciones al tráfico a través de la WAN. Con esto en mente, los ejemplos de configuración proporcionados por este documento implementan una política más *sospechosa* que permite tráfico específico crítico para el negocio, que luego es examinado por verificaciones de conformidad del protocolo. Además, las acciones específicas de VoIP, es decir, SIP INVITE, se limitan a reducir la probabilidad de que se produzcan fallos de software malintencionados o no intencionados que afecten negativamente a los recursos y la capacidad de uso de VoIP.

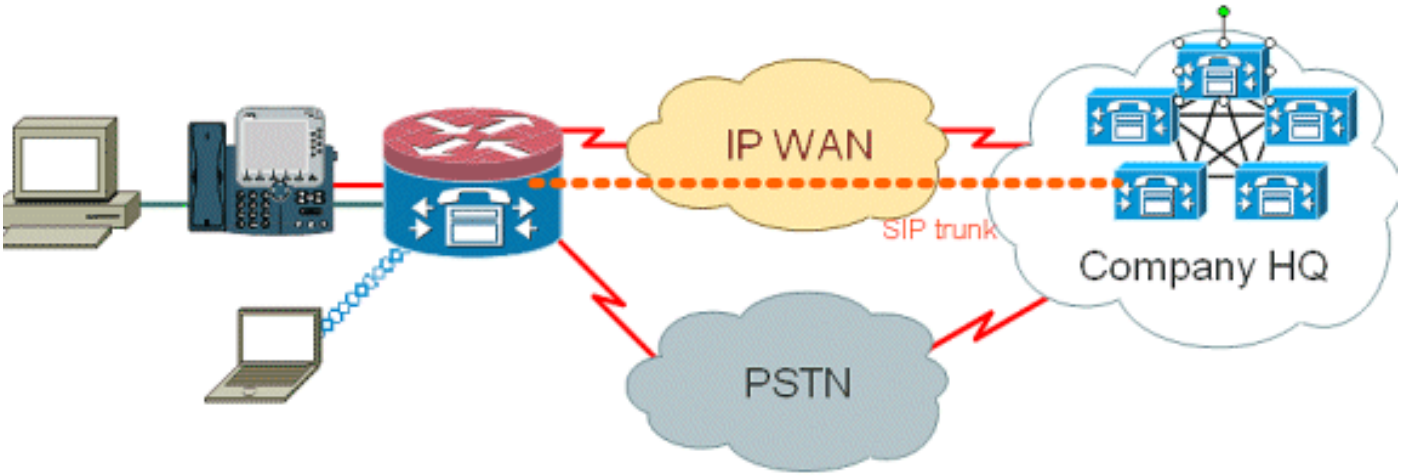
Configurar

Configuraciones para políticas de datos, firewall basado en zonas, seguridad de voz, CCME

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

La configuración que se describe aquí ilustra un router de servicios integrados Cisco 2851.

En este documento, se utilizan estas configuraciones:

- Configuración del servicio de voz para la conectividad CME y CUE
- Configuración de firewall de políticas basado en zona
- Configuración de Seguridad

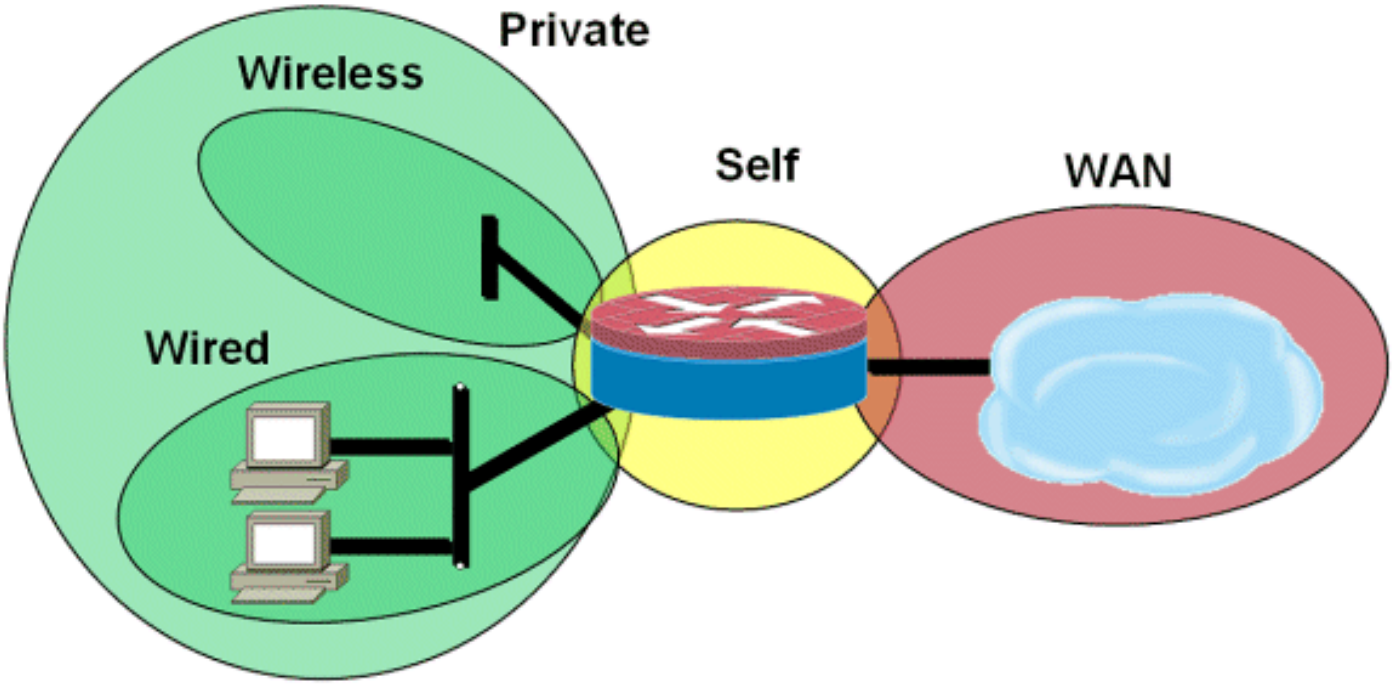
Esta es la configuración del servicio de voz para la conectividad CME y CUE:

Configuración del servicio de voz para la conectividad CME y 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

!
```

Se trata de la configuración de firewall de políticas basada en zonas, compuesta por zonas de seguridad para segmentos LAN por cable e inalámbricos, LAN privada (compuesta por segmentos por cable e inalámbricos), un segmento WAN en el que se alcanza la conectividad WAN de confianza y la zona autónoma en la que se encuentran los recursos de voz del router:



Esta es la configuración de seguridad:

Configuración de Seguridad

```
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
```

Aprovisionamiento, gestión y supervisión

El aprovisionamiento y la configuración de los recursos de telefonía IP basada en router y de firewall de políticas basado en zona se adaptan mejor en general con Cisco Configuration Professional. Cisco Secure Manager no admite firewall de políticas basadas en zonas ni telefonía IP basada en router.

El Cisco IOS Classic Firewall admite la supervisión SNMP con Cisco Unified Firewall MIB, pero Zone-Based Policy Firewall todavía no se admite en Unified Firewall MIB. Como tal, la supervisión del firewall se debe gestionar a través de estadísticas en la interfaz de línea de comandos del router o con herramientas GUI, como Cisco Configuration Professional.

Cisco Secure Monitoring And Reporting System (CS-MARS) ofrece soporte básico para el firewall de políticas basado en zonas, aunque los cambios de registro que mejoraron la correlación de mensajes de registro con el tráfico, que se implementaron en 12.4(15)T4/T5 y 12.4(20)T, todavía no se han admitido completamente en CS-MARS.

Planes de capacidad

Los resultados de las pruebas de rendimiento de inspección de llamadas de firewall de la India son TBD.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Cisco IOS Zone Firewall proporciona los comandos **show** y **debug** para ver, monitorear y resolver problemas de la actividad del firewall. Esta sección describe el uso de los comandos **show** para monitorear la actividad básica del firewall, y una introducción a los comandos **debug** del firewall de zona para resolver problemas de su configuración o si la discusión con el soporte técnico requiere información más detallada.

Comandos para resolución de problemas

El Cisco IOS Firewall ofrece varios comandos **show** para ver la actividad y la configuración de la política de seguridad. Muchos de estos comandos se pueden reemplazar con un comando más corto a través de la aplicación del comando **alias**.

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos **debug**.

Los comandos de depuración pueden ser útiles en el caso de que esté utilizando una configuración atípica o no admitida, y necesiten trabajar con el TAC de Cisco u otros servicios de soporte técnico de productos para resolver problemas de interoperabilidad.

Nota: La aplicación de los comandos **debug** a capacidades o tráfico específicos puede causar un gran número de mensajes de consola, lo que hace que la consola del router deje de responder. En el caso de que necesite depurar, puede proporcionar acceso de interfaz de línea de comandos alternativo, como una ventana Telnet que no monitoree el diálogo de terminal. Habilite solamente la depuración en equipos fuera de línea (entorno de laboratorio) o dentro de una ventana de mantenimiento planificada, ya que la depuración puede afectar sustancialmente al rendimiento del router.

Información Relacionada

- Guía de diseño de red de referencia de la solución Cisco Unified CallManager Express
- Prácticas recomendadas de seguridad de Cisco CallManager Express (CME SRND)
- Integración de Cisco Unity Connection con Cisco Unified CME-as-SRST
- Referencia de Comandos de Cisco Unified Communications Manager Express
- Ejemplo de configuración de Cisco CallManager Express/Cisco Unity Express
- Soporte de MIB SNMP de Cisco CallManager Express 3.4
- Guía de Aplicación y Diseño de Zone-Based Policy Firewall
- Firewall de Cisco IOS: Mejoras de SIP: ALG y AIC
- Soporte del Firewall H.323 del IOS de Cisco
- Soporte de Firewall de Cisco IOS para tráfico local Skinny y CME
- Soporte Técnico y Documentación - Cisco Systems