Firewall basado en zona IOS: Ejemplo de Configuración de Conexión PSTN de Sucursal o Sitio Único de CME/CUE/GW

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, a la vez 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. Se proporciona la configuración para los servicios de voz y el firewall 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.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

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

Fondo del Firewall IOS

Cisco IOS Firewall 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 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 contribuirá a reducir las tasas de rendimiento de reenvío, a aumentar la latencia de paquetes y a la pérdida de capacidad de funciones durante los períodos de carga pico si se implementa una solución integrada basada en router con bajo consumo de energía.

Siga estas instrucciones cuando decida entre un router y un dispositivo:

- Los routers con varias funciones integradas habilitadas son los más adecuados para sucursales o teletrabajadores, donde menos dispositivos ofrecen 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 routers, por lo que se necesitaban grandes aperturas en políticas de firewall seguras para admitir el tráfico de voz y

ofrecer compatibilidad limitada para la señalización VoIP en evolución y los protocolos multimedia.

Implementación de Cisco IOS Zone-Based Policy Firewall

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*. Política que se aplica que niega todo el tráfico de la aplicación excepto el que está permitido explícitamente. Además, la inspección y el control de aplicaciones (AIC) se pueden implementar para identificar y denegar el tráfico malintencionado diseñado específicamente para explotar aplicaciones "buenas", así como el tráfico no deseado que se muestra como tráfico bueno. 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 estado, como las listas de control de acceso (ACL) o la política de firewall de políticas basado en zonas (ZFW), por lo que debe haber un tráfico sustancialmente menor que debe ser manejado por 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). Por lo tanto, 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 debería estar presente en la red debería 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 tanto, 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.

Para obtener más información sobre cómo configurar el firewall de políticas basado en zona, refiérase a la Guía de Diseño y Aplicación de Firewall de Políticas Basado en Zona de Cisco IOS.

Consideraciones para ZFW en entornos VoIP

La Guía de diseño y aplicación de firewall de Cisco IOS basada en zona ofrece una breve explicación para proteger el router con el uso de políticas de seguridad hacia y desde la *zona autónoma* del router, así como capacidades alternativas que se proporcionan a través de diversas funciones de Network Foundation Protection (NFP). Las funciones 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 poder acomodar la señalización de voz y los medios originados y destinados a los recursos de Cisco Unified CallManager Express, Survivable Remote Site Telephony y Voice Gateway. 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.

Mejoras de voz del firewall IOS - 12.4(20)T

La versión 12.4(20)T del software del IOS de Cisco 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 aplicaciónAmplía la inspección de zona autónoma para poder reconocer canales de medios y señalización secundarios resultantes del tráfico SIP originado o 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 aplicaciónAmplía la inspección de zona autónoma para poder reconocer canales de medios y señalización secundarios resultantes del tráfico SCCP originado/destinado localmente
- Compatibilidad con H.323 v3/v4Actualiza el soporte de H.323 para v3 y v4 (previamente soportado para v1 y v2)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 una explicación para describir la acción aplicada por las políticas. Para obtener detalles completos sobre las funciones de inspección de voz, consulte los documentos de características individuales enumerados en la sección Información Relacionada de este documento.

Advertencias

Para reforzar los puntos mencionados anteriormente, la aplicación de 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 y el comportamiento del tráfico de voz.

Traducción de direcciones de red

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

Cliente de Cisco Unified Presence

Este documento no describe las configuraciones que admiten el uso de Cisco Unified Presence Client (CUPC) con IOS Firewall, ya que el 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.

Conexión CME/CUE/GW PSTN de sucursal o sitio único

Esta situación introduce telefonía de voz sobre IP basada en router segura para pequeñas y medianas empresas de un solo sitio o para organizaciones de varios sitios que deseen implementar el procesamiento de llamadas distribuidas, manteniendo las conexiones heredadas a la Red de telefonía pública conmutada (PSTN). El control de llamadas VoIP se adapta mediante la aplicación de Cisco Unified Call Manager Express.

La conectividad PSTN se puede mantener a largo plazo o se puede migrar a una red convergente de área extensa IP de voz y datos, como se describe en el ejemplo de aplicación que se describe en la sección CME/CUE/GW Single Site o Branch Office with SIP Trunk to CCM at HQ or Voice Provider de este documento.

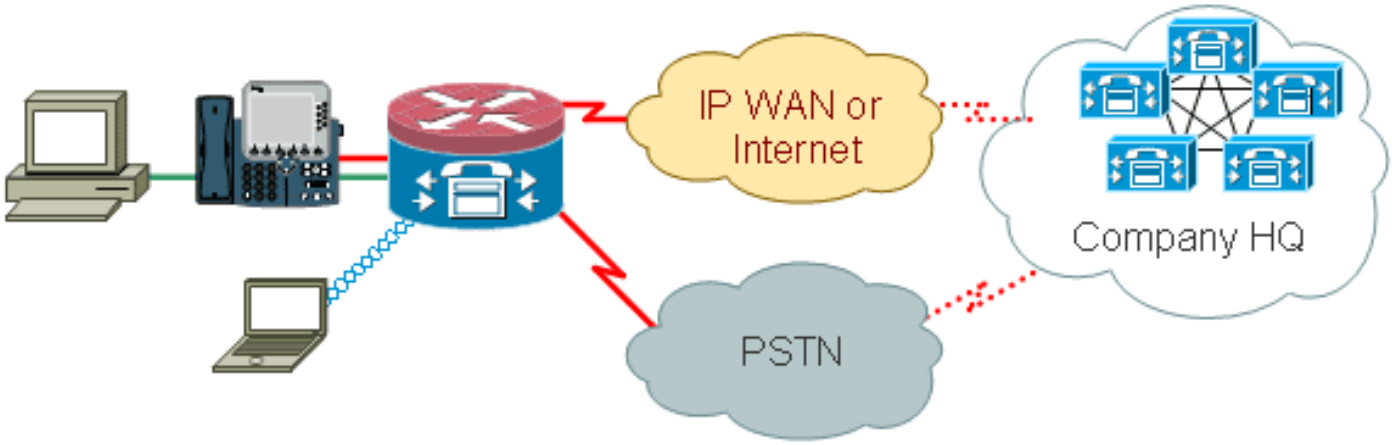
Las organizaciones deben considerar la implementación de este tipo de escenario de aplicación en circunstancias en las que se utilizan entornos VoIP dispares entre sitios o si VoIP no es práctico debido a una conectividad de datos WAN inadecuada o a restricciones específicas de la configuración regional sobre el uso de VoIP en redes de datos. Las ventajas y las prácticas recomendadas de telefonía IP de un solo sitio se describen en el SRND de Cisco Unified CallManager Express.

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:

- Inspección de señalización iniciada por el router entre CME y los teléfonos locales (SCCP y/o SIP)
- Los orificios de los medios de voz para la comunicación entre:Segmentos locales por cable e inalámbricosCME y los teléfonos locales para MoHCUE y los teléfonos locales para el correo de voz
- Aplicación del control e inspección de aplicaciones (AIC) a:Mensajes de invitación de límite de velocidadGarantizar la conformidad del protocolo en todo el tráfico SIP.



Ventajas y desventajas

La ventaja más obvia del aspecto VoIP del escenario es la ruta de migración que ofrece la integración de la infraestructura de red de voz y datos existente en un entorno POTS/TDM existente, antes de pasar a una red convergente de voz/datos para servicios de telefonía al mundo más allá de la LAN. Los números de teléfono se mantienen para las empresas más pequeñas y se puede dejar el servicio centrex o DID existente para las organizaciones más grandes que deseen realizar una migración por etapas a la telefonía de paquetes de desvío de llamadas.

Entre las desventajas se incluyen la pérdida de ahorros de costes que se podrían conseguir con la derivación de tarifas al pasar a una red convergente de voz y datos, así como las limitaciones en cuanto a la flexibilidad de las llamadas y la falta de portabilidad e integración de las comunicaciones en toda la organización que se podrían conseguir con una red de voz y datos totalmente convergente.

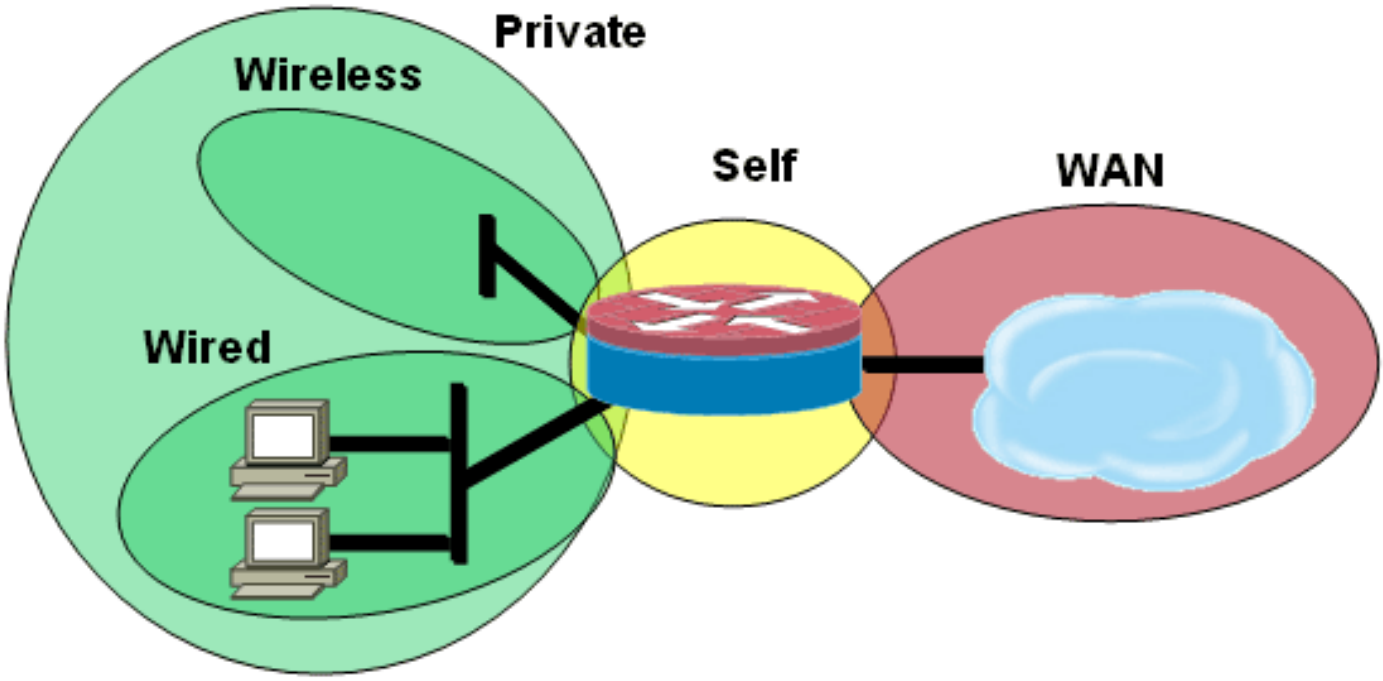
Desde el punto de vista de la seguridad, este tipo de entorno de red minimiza las amenazas de seguridad VoIP, ya que evita la exposición de los recursos VoIP a la red pública o a la WAN. Sin embargo, Cisco Call Manager Express integrado en el router seguiría siendo vulnerable a amenazas internas como tráfico malintencionado o tráfico de aplicaciones que funciona mal. Por lo tanto, se implementa una política que permite el tráfico específico de voz que cumple con las verificaciones de conformidad del protocolo, y las acciones específicas de VoIP (es decir, SIP INVITE) son limitadas para reducir la probabilidad de que el software malintencionado o no funcione de manera negativa, afectando los recursos y la capacidad de uso de VoIP.

Políticas de datos, firewall basado en zonas, seguridad de voz y configuraciones de CCME

La configuración descrita aquí ilustra un 2851 con una configuración de 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
!
```

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 público en el que se alcanza la conectividad a Internet no fiable y la zona autónoma en la que se encuentran los recursos de voz del router.



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
```

Configuración del router completo

```
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
```

Aprovisionamiento, gestión y supervisión

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

Cisco IOS Classic Firewall admite la supervisión SNMP con Cisco Unified Firewall MIB. Sin embargo, el firewall de políticas basado en zonas todavía no se admite en la MIB de firewall unificado. Por lo tanto, 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.

CiscoSecure Monitoring And Reporting System (CS-MARS) ofrece compatibilidad básica 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.

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 proporciona una introducción a los comandos **debug** de Zone Firewall que proporcionan información detallada sobre la solución de problemas.

Comandos de Debug

Los comandos de depuración son útiles en el caso de que utilice 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 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 habilitar la depuración, puede que desee proporcionar acceso alternativo a la interfaz de línea de comandos, como una ventana telnet que no monitoree el diálogo de terminal. Sólo debe habilitar el debug en equipos sin conexión (entorno de laboratorio) o durante una ventana de mantenimiento planificada, ya que habilitar el debug puede afectar sustancialmente al rendimiento del router.

Información Relacionada

- Guía de diseño de red de referencia de la solución Cisco Unified CallManager Express
- 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
- Soporte Técnico y Documentación - Cisco Systems