Firewall basado en zona de Cisco IOS: Oficina con Cisco Unity Express/SRST/PSTN Gateway con conexión a Cisco CallManager centralizado

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. 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, luego por toda la configuración del router. Su red puede requerir otras configuraciones 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.

Fondo del Firewall del IOS de Cisco

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 contribuye 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 máxima 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:

- El router con varias funciones integradas activadas es el más adecuado para sucursales o sitios de teletrabajadores donde menos dispositivos ofrecen una mejor solución
- Las aplicaciones de alto ancho de banda y alto rendimiento suelen ser mejor tratadas 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, y necesitaban grandes aperturas en políticas de firewall seguras para admitir el tráfico de voz y ofrecían compatibilidad limitada para la señalización VoIP en evolución y los protocolos de medios.

Configurar

Implementación del firewall de políticas basado en zona de Cisco IOS

Cisco IOS Zone-Based Policy Firewall, al igual que otros firewalls, sólo puede ofrecer un firewall seguro si los requisitos de seguridad de la confianza de red se identifican y describen mediante la política de seguridad. Hay dos enfoques fundamentales para llegar a una política de seguridad: la perspectiva, a diferencia de 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 y que niega todo el tráfico de la aplicación, excepto el 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 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 dinámicos 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.

Refiérase a Guía de Diseño y Aplicación de Firewall de Políticas Basadas en Zona para obtener más información y antecedentes adicionales para la configuración del Firewall de Políticas Basado en Zona.

Consideraciones para ZFW en entornos VoIP

La guía de diseño y aplicación mencionada anteriormente ofrece una breve descripción de la seguridad del 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 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 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 dependen en gran medida de las capacidades introducidas en la versión 12.4(20)T del software del IOS de Cisco.

Funciones de voz del firewall Cisco 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 aplicaciónAmplía la inspección de zona autónoma para poder reconocer canales de señalización secundaria y de medios resultantes del tráfico SIP originado/destinado localmente
- Compatibilidad con tráfico local Skinny y Cisco CallManager ExpressActualiza 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 la compatibilidad con H.323 para v3 y v4 (previamente admitida para v1 y v2), tal y como describe elPresenta 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. Los hipervínculos a los documentos de características individuales están disponibles en la sección Información Relacionada al final de este documento, si desea revisar los detalles completos para las funciones de inspección de voz.

Advertencias

La aplicación de Cisco IOS Firewall con capacidades de voz basadas en router debe aplicar el

firewall de políticas basado en zona para reforzar los puntos mencionados anteriormente. El firewall de IOS clásico no incluye la capacidad necesaria para admitir completamente las complejidades de señalización y el comportamiento del tráfico de voz.

NAT

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 una 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.

CUPC

Este documento no describe la configuración que admite el uso de Cisco Unified Presence Client (CUPC) con Cisco IOS Firewall, ya que la versión 12.4(20)T1 de Cisco IOS Software todavía no admite CUPC ni Zone ni Classic Firewall. CUPC se soporta en una futura versión de Cisco IOS Software.

Oficina con Cisco Unity Express/SRST/PSTN Gateway que se conecta a Cisco CallManager centralizado

Este escenario difiere de las aplicaciones anteriores, en que el control de llamadas centralizado se utiliza para todo el control de llamadas, en lugar del procesamiento de llamadas basado en router distribuido. Se aplica el correo de voz distribuido, pero a través de Cisco Unity Express en el router. El router proporciona la funcionalidad Survivable Remote Site Telephony y PSTN Gateway para la marcación de emergencia y la marcación local. Se recomienda un nivel específico de la capacidad PSTN de la aplicación para dar cabida a las fallas de la marcación de desvío de llamadas basada en WAN, así como a 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).

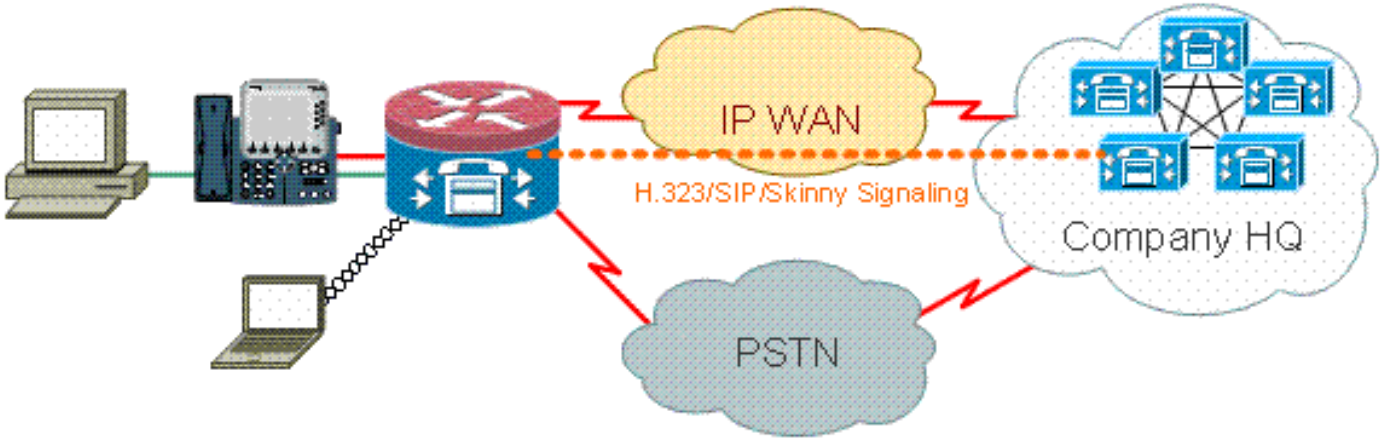
Esta situación también puede aplicar Cisco CallManager Express como agente de procesamiento de llamadas para SRST, en el caso de que se requiera una mayor capacidad de procesamiento de llamadas durante las interrupciones de WAN/CCM. Consulte Integración de Cisco Unity Connection con Cisco Unified CME-as-SRST para obtener más información.

Antecedentes del escenario

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

1. Inspección de señalización entre teléfonos locales y clúster CUCM remoto (SCCP y SIP)
2. Inspeccione la señalización H.323 entre el router y el clúster CUCM remoto.
3. Inspeccione la señalización entre los teléfonos locales y el router cuando el link al sitio remoto está inactivo y SRST está activo.

4. Los orificios de los medios de voz para la comunicación entre:Segmentos locales por cable e inalámbricosTeléfonos locales y remotosServidor MoH remoto y teléfonos localesServidor de Unity remoto y teléfonos locales para correo de voz
5. Aplicación del control e inspección de aplicaciones (AIC) a:mensajes de invitación de límite de velocidadgarantice la conformidad del protocolo en todo el tráfico SIP.



Ventajas/Desventajas

Esta situación ofrece la ventaja de que la mayoría del procesamiento de llamadas se produce en un clúster central de Cisco CallManager, que ofrece una carga de administración reducida. Normalmente, el router debería tener que hacer frente a una menor carga de inspección de recursos de voz local en comparación con los otros casos descritos en este documento, ya que la mayor parte de la carga de procesamiento de llamadas no se impone en el router, excepto por la gestión del tráfico hacia/desde Cisco Unity Express, y en los casos en que hay una interrupción de WAN o CUCM, y Cisco CallManager Express/SRST local se pone en vigor para el procesamiento de llamadas.

La mayor desventaja de este caso, durante la actividad típica de procesamiento de llamadas, es que Cisco Unity Express se encuentra en el router local. Aunque esto es bueno desde el punto de vista del diseño, por ejemplo, Cisco Unity Express se encuentra más cerca de los usuarios finales donde se mantiene el correo de voz, incurre en cierta carga de administración adicional, ya que puede haber un gran número de Cisco Unity Express que administrar. Dicho esto, con un Cisco Unity Express central para llevar los inconvenientes opuestos, en el sentido de que un Cisco Unity Express central está más lejos de los usuarios remotos y posiblemente no es accesible durante las interrupciones. Por lo tanto, las ventajas funcionales de la oferta de correo de voz distribuido mediante la implementación de Cisco Unity Express en ubicaciones remotas ofrece la mejor opción.

Configuraciones para políticas de datos, firewall basado en zonas, seguridad de voz, Cisco CallManager Express

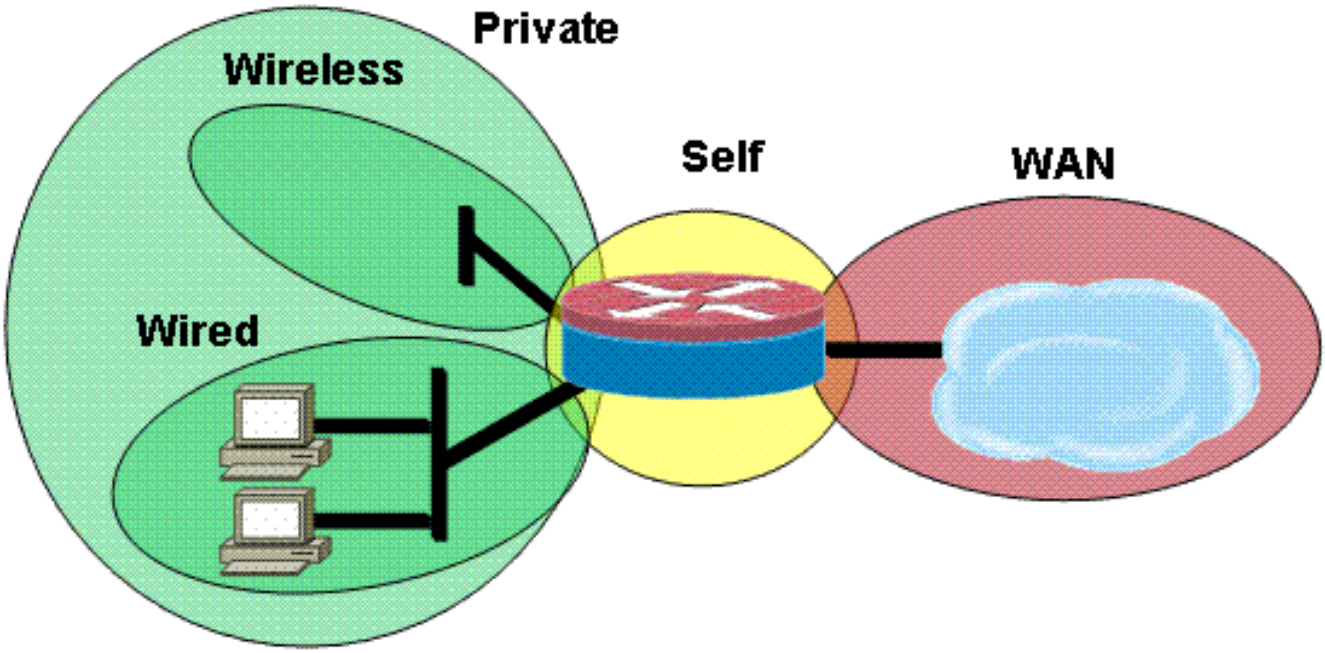
La configuración del router se basa en un 3845 con un NME-X-23ES y un PRI HWIC:

Configuración del servicio de voz para conectividad SRST y Cisco Unity Express:

```
!
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
!
```

Este es un ejemplo de la configuración de firewall de políticas basada en zonas, compuesta por zonas de seguridad para segmentos LAN por cable e inalámbricos, LAN privada, que está 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:



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 3825-srst
!
!
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
ip cef
!
!
ip domain name cisco.com
ip name-server 172.16.1.22
ip vrf acctg
 rd 0:1
!
ip vrf eng
 rd 0:2
!
ip inspect WAAS enable
!
no ipv6 cef
multilink bundle-name authenticated
!
!
voice-card 0
 no dspfarm
!
!
!
!
!
!
archive
```

```
 log config
  hidekeys
!
!
!
!
!
!
!
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 vpn
zone security eng
zone security acctg
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 Loopback101
 ip vrf forwarding acctg
 ip address 10.255.1.5 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 zone-member security acctg
!
interface Loopback102
 ip vrf forwarding eng
 ip address 10.255.1.5 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 zone-member security eng
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 media-type rj45
 no keepalive
```

```
!
interface GigabitEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 172.16.1.103 255.255.255.0
 shutdown
!
interface GigabitEthernet0/0.109
 encapsulation dot1Q 109
 ip address 172.16.109.11 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 zone-member security public
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 media-type rj45
 no keepalive
!
interface GigabitEthernet0/1.129
 encapsulation dot1Q 129
 ip address 172.17.109.2 255.255.255.0
 standby 1 ip 172.17.109.1
 standby 1 priority 105
 standby 1 preempt
 standby 1 track GigabitEthernet0/0.109
!
interface GigabitEthernet0/1.149
 encapsulation dot1Q 149
 ip address 192.168.109.2 255.255.255.0
 ip wccp 61 redirect in
 ip wccp 62 redirect out
 ip nat inside
 ip virtual-reassembly
 zone-member security private
!
interface GigabitEthernet0/1.161
 encapsulation dot1Q 161
 ip vrf forwarding acctg
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 zone-member security acctg
!
interface GigabitEthernet0/1.162
 encapsulation dot1Q 162
 ip vrf forwarding eng
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 zone-member security eng
!
interface Serial0/3/0
 no ip address
 encapsulation frame-relay
 shutdown
 frame-relay lmi-type cisco
!
interface Serial0/3/0.1 point-to-point
 ip vrf forwarding acctg
 ip address 10.255.1.1 255.255.255.252
 ip nat inside
 ip virtual-reassembly
```

```
 zone-member security acctg
 snmp trap link-status
 no cdp enable
 frame-relay interface-dlci 321 IETF
!
interface Serial0/3/0.2 point-to-point
 ip vrf forwarding eng
 ip address 10.255.1.1 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 zone-member security eng
 snmp trap link-status
 no cdp enable
 frame-relay interface-dlci 322 IETF
!
interface Integrated-Service-Engine2/0
 no ip address
 shutdown
 no keepalive
!
interface GigabitEthernet3/0
 no ip address
 shutdown
!
router eigrp 1
 network 172.16.109.0 0.0.0.255
 network 172.17.109.0 0.0.0.255
 no auto-summary
!
router eigrp 104
 network 10.1.104.0 0.0.0.255
 network 192.168.109.0
 network 192.168.209.0
 no auto-summary
!
router bgp 1109
 bgp log-neighbor-changes
 neighbor 172.17.109.4 remote-as 1109
 !
 address-family ipv4
  neighbor 172.17.109.4 activate
  no auto-summary
  no synchronization
  network 172.17.109.0 mask 255.255.255.0
 exit-address-family
!
ip forward-protocol nd
ip route vrf acctg 0.0.0.0 0.0.0.0 172.16.109.1 global
ip route vrf acctg 10.1.2.0 255.255.255.0 10.255.1.2
ip route vrf eng 0.0.0.0 0.0.0.0 172.16.109.1 global
ip route vrf eng 10.1.2.0 255.255.255.0 10.255.1.2
!
!
ip http server
no ip http secure-server
ip nat pool acctg-nat-pool 172.16.109.21 172.16.109.22 netmask 255.255.255.0
ip nat pool eng-nat-pool 172.16.109.24 172.16.109.24 netmask 255.255.255.0
ip nat inside source list 109 interface GigabitEthernet0/0.109 overload
ip nat inside source list acctg-nat-list pool acctg-nat-pool vrf acctg overload
ip nat inside source list eng-nat-list pool eng-nat-pool vrf eng overload
ip nat inside source static 172.17.109.12 172.16.109.12 extendable
!
ip access-list extended acctg-nat-list
 deny   ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
```

```
 permit ip 10.0.0.0 0.255.255.255 any
ip access-list extended eng-nat-list
 deny   ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
 permit ip 10.0.0.0 0.255.255.255 any
!
logging 172.16.1.20
access-list 1 permit any
access-list 109 deny   ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255
access-list 109 permit ip 192.168.0.0 0.0.255.255 any
access-list 111 deny   ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255
access-list 111 permit ip 192.168.0.0 0.0.255.255 any
access-list 141 permit ip 10.0.0.0 0.255.255.255 any
access-list 171 permit ip host 1.1.1.1 host 2.2.2.2
!
!
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
gateway
 timer receive-rtp 1200
!
!
alias exec sh-sess show policy-map type inspect zone-pair sessions
!
line con 0
 exec-timeout 0 0
line aux 0
line 130
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
line 194
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
line vty 0 4
 password cisco
 login
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
!
webvpn context Default_context
 ssl authenticate verify all
 !
 no inservice
!
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. 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.

CiscoSecure 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 Cisco IOS Software Release 12.4(15)T4/T5 y Cisco IOS Software Release 12.4(20)T todavía no se han admitido completamente en CS-MARS.

Planificación de capacidad

Resultados de la prueba de rendimiento de inspección de llamadas de firewall de India por determinar.

Verificación

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

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

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 una resolución de problemas más detallada, o si la discusión con el soporte técnico requiere información detallada.

Comandos para resolución de problemas

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

Comandos show

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 mediante la aplicación del comando **alias**.

Comandos de Debug

Los comandos **Debug** pueden ser útiles en el caso de que utilice una configuración atípica o no admitida, y deben 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 específicas o al tráfico 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, es posible proporcionar un acceso de interfaz de línea de comandos alternativo, como una ventana Telnet que no monitoree el diálogo de terminal. Sólo debe habilitar la depuración en equipos fuera de línea (entorno de laboratorio) o durante una ventana de mantenimiento planificada, porque si habilita la depuración, esto 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 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 de Firewall de Cisco IOS para tráfico local Skinny y CME
- Cisco IOS Firewall
- Soporte Técnico y Documentación - Cisco Systems