Pare-feu basé sur la zone Cisco IOS : Office avec passerelle Cisco Unity Express/SRST/PSTN avec connexion à la solution Cisco CallManager centralisé

Contenu

Introduction
Conditions préalables
Conditions requises
Components Used
Conventions
Arrière-plan du pare-feu Cisco IOS
Configuration
Déploiement de Cisco IOS Zone-Based Policy Firewall
Cavates
Bureau avec la passerelle Cisco Unity Express/SRST/PSTN qui se connecte à Cisco CallManager centralisé
Provisionnement, gestion et surveillance
Planification de capacité
Vérification
Dépannage
Dépannage des commandes
Commandes show
Commandes de débogage
Informations connexes

Introduction

Les routeurs à services intégrés (ISR) de Cisco offrent une plate-forme évolutive qui répond aux besoins du réseau voix et données pour un large éventail d'applications. Bien que le paysage des menaces des réseaux privés et connectés à Internet soit un environnement très dynamique, Cisco IOS® Firewall offre des fonctionnalités d'inspection dynamique et d'inspection et de contrôle des applications (AIC) pour définir et appliquer une position réseau sécurisée, tout en permettant la continuité et la capacité de l'entreprise.

Ce document décrit les considérations de conception et de configuration pour les aspects de sécurité du pare-feu de scénarios spécifiques d'applications vocales et de données basées sur Cisco ISR. La configuration des services vocaux et du pare-feu est fournie pour chaque scénario d'application. Chaque scénario décrit les configurations VoIP et de sécurité séparément, puis par l'ensemble de la configuration du routeur. Votre réseau peut nécessiter d'autres configurations pour des services tels que QoS et VPN afin de préserver la qualité et la confidentialité de la voix.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Arrière-plan du pare-feu Cisco IOS

Le pare-feu Cisco IOS est généralement déployé dans des scénarios d'applications qui diffèrent des modèles de déploiement des pare-feu d'appareils. Les déploiements typiques incluent les applications de télétravail, les sites de petites ou de filiales et les applications de vente au détail, où le nombre d'appareils est faible, l'intégration de plusieurs services, et où les performances et les capacités de sécurité sont réduites.

Bien que l'application de l'inspection par pare-feu, ainsi que d'autres services intégrés dans les produits ISR, puisse paraître attrayante du point de vue du coût et du fonctionnement, des considérations spécifiques doivent être évaluées afin de déterminer si un pare-feu basé sur un routeur est approprié. L'application de chaque fonctionnalité supplémentaire entraîne des coûts de mémoire et de traitement et contribue probablement à réduire le débit de transfert, à augmenter la latence des paquets et à réduire la capacité des fonctionnalités pendant les périodes de pointe si une solution intégrée sous-alimentée basée sur un routeur est déployée. Respectez ces consignes lorsque vous décidez entre un routeur et une appliance :

- Les routeurs dotés de plusieurs fonctionnalités intégrées sont les mieux adaptés aux sites de filiales ou de télétravailleurs où moins de périphériques offrent une meilleure solution
- Les applications hautes performances à bande passante élevée sont généralement mieux gérées avec les appliances. Cisco ASA et Cisco Unified Call Manager Server doivent être appliqués pour gérer la NAT et l'application de stratégie de sécurité et le traitement des appels, tandis que les routeurs répondent aux besoins en termes d'application de stratégie QoS, de terminaison WAN et de connectivité VPN site à site.

Avant l'introduction du logiciel Cisco IOS Version 12.4(20)T, le pare-feu classique et le pare-feu ZFW (Zone-Based Policy Firewall) n'étaient pas en mesure de prendre pleinement en charge les fonctionnalités requises pour le trafic VoIP et les services vocaux basés sur les routeurs, et nécessitaient de grandes ouvertures dans des politiques de pare-feu par ailleurs sécurisées afin de prendre en charge le trafic voix.

Configuration

Déploiement de Cisco IOS Zone-Based Policy Firewall

Cisco IOS Zone-Based Policy Firewall, comme d'autres pare-feu, ne peut offrir un pare-feu sécurisé que si les exigences de sécurité du réseau trustingare sont identifiées et décrites par la stratégie de sécurité. Il existe deux approches fondamentales pour élaborer une politique de sécurité : la perspective, par opposition à la perspective *suspecte*.

La perspective *de confiance* suppose que tout le trafic est fiable, sauf celui qui peut être spécifiquement identifié comme malveillant ou indésirable. Une politique spécifique est mise en oeuvre qui refuse uniquement le trafic indésirable. Cela se fait généralement au moyen d'entrées de contrôle d'accès spécifiques ou d'outils basés sur les signatures ou les comportements. Cette approche tend à interférer moins avec les applications existantes, mais elle nécessite une connaissance approfondie du paysage des menaces et des vulnérabilités et nécessite une vigilance constante pour faire face aux nouvelles menaces et aux nouvelles attaques à mesure qu'elles apparaissent. En outre, la communauté d'utilisateurs doit jouer un rôle important dans le maintien d'une sécurité adéquate. Un environnement qui offre une liberté étendue et peu de contrôle aux occupants offre des possibilités substantielles de problèmes causés par des individus négligents ou malveillants. Un autre problème de cette approche est qu'elle repose davantage sur des outils de gestion et des contrôles d'application efficaces qui offrent une flexibilité et des performances suffisantes pour être en mesure de surveiller et de contrôler les données suspectes dans tout le trafic réseau. Bien que la technologie soit actuellement disponible pour y faire face, la charge opérationnelle dépasse souvent les limites de la plupart des organisations.

La perspective *suspecte* suppose que tout le trafic réseau est indésirable, sauf pour le *bon* trafic spécifiquement identifié. Il s'agit d'une stratégie qui est appliquée et qui refuse tout trafic d'application, à l'exception de celle explicitement autorisée. En outre, l'inspection et le contrôle des applications (AIC) peuvent être mis en oeuvre pour identifier et refuser le trafic malveillant spécifiquement conçu pour exploiter de *bonnes* applications, ainsi que le trafic indésirable qui se déguise en *bon* trafic. Là encore, les contrôles d'application imposent des contraintes opérationnelles et de performances au réseau, bien que la plupart du trafic indésirable doive être contrôlé par des filtres sans état tels que les listes de contrôle d'accès (ACL) ou la politique ZFW (Zone-Based Policy Firewall), de sorte qu'il doit y avoir beaucoup moins de trafic qui doit être géré par AIC, le système de prévention des intrusions (IPS) ou d'autres contrôles basés sur les signatures tels que la technologie FPM (Flexible Packet NBAR). Ainsi, si seuls les ports d'application souhaités et le trafic dynamique spécifique au support provenant de connexions ou de sessions de contrôle connues sont spécifiquement autorisés, le seul trafic indésirable qui doit être présent sur le réseau doit tomber dans un sous-ensemble spécifique, plus facilement reconnu, ce qui réduit la charge d'ingénierie et d'exploitation imposée pour maintenir le contrôle du trafic indésirable.

Ce document décrit les configurations de sécurité VoIP basées sur la perspective *suspecte* ; ainsi, seul le trafic autorisé dans les segments de réseau vocal est autorisé. Les politiques de données ont tendance à être plus permissives, comme le décrivent les notes de configuration de chaque scénario d'application.

Tous les déploiements de stratégie de sécurité doivent suivre un cycle de rétroaction en boucle fermée ; les déploiements de sécurité affectent généralement les capacités et les fonctionnalités des applications existantes et doivent être ajustés afin de minimiser ou résoudre cet impact.

Référez-vous au Guide de conception et d'application du pare-feu de stratégie basé sur les zones pour plus d'informations et d'arrière-plan supplémentaires pour la configuration du pare-feu de stratégie basé sur les zones.

Considérations relatives au ZFW dans les environnements VoIP

Le Guide de conception et d'application mentionné précédemment présente brièvement la sécurité du routeur en ce qui concerne l'utilisation de stratégies de sécurité à destination et en provenance de la zone autonome du routeur, ainsi que les autres fonctionnalités fournies par le biais de diverses fonctions NFP (Network Foundation Protection). Les fonctionnalités VoIP basées sur un routeur sont hébergées dans la zone autonome du routeur. Les politiques de sécurité qui protègent le routeur doivent donc être conscientes des exigences du trafic vocal, afin de prendre en charge la signalisation vocale et les supports provenant et destinés aux ressources Cisco Unified CallManager Express, Survivable Remote-Site Telephony et Voice Gateway. Avant la version 12.4(20)T du logiciel Cisco IOS, le pare-feu classique et le pare-feu de stratégie basé sur les zones ne pouvaient pas répondre entièrement aux exigences du trafic VoIP, de sorte que les politiques de pare-feu n'étaient pas optimisées pour protéger pleinement les ressources. Les politiques de sécurité de zone autonome qui protègent les ressources VoIP basées sur les routeurs reposent largement sur les fonctionnalités introduites dans le logiciel Cisco IOS Version 12.4(20)T.

Fonctionnalités vocales du pare-feu Cisco IOS

Le logiciel Cisco IOS Version 12.4(20)T a introduit plusieurs améliorations afin d'activer les fonctionnalités voix et de pare-feu de zone corésidentes. Trois fonctions principales s'appliquent directement aux applications vocales sécurisées :

- Améliorations SIP : Contrôle et inspection des applications et de la passerelle de couche applicationMet à jour la prise en charge de la version SIP vers SIPv2, comme décrit dans la RFC 3261Étend la prise en charge de la signalisation SIP pour reconnaître une plus grande variété de flux d'appelsIntroduction de SIP Application Inspection and Control (AIC) pour appliquer des contrôles granulaires afin de traiter des vulnérabilités et des exploits spécifiques au niveau des applicationsÉtend l'inspection de zone autonome afin de pouvoir reconnaître les canaux de signalisation et de support secondaires résultant du trafic SIP destiné/originaire localement
- Prise en charge du trafic local maigre et de Cisco CallManager ExpressMet à jour la prise en charge de SCCP vers la version 16 (version 9 précédemment prise en charge)Introduit l'inspection et le contrôle des applications (AIC) SCCP afin d'appliquer des contrôles granulaires pour traiter des vulnérabilités et des exploits spécifiques au niveau des applicationsDéveloppe l'inspection de zone autonome pour être en mesure de reconnaître les canaux de signalisation et de média secondaires résultant du trafic SCCP destiné/originaire localement
- Support H.323 v3/v4Met à jour la prise en charge H.323 vers v3 et v4 (précédemment pris en charge v1 et v2), comme décrit parIntroduit l'inspection et le contrôle des applications (AIC) H.323 pour appliquer des contrôles granulaires afin de traiter des vulnérabilités et des exploits spécifiques au niveau des applications

Les configurations de sécurité des routeurs décrites dans ce document incluent les fonctionnalités offertes par ces améliorations, avec une explication pour décrire l'action appliquée par les politiques. Des liens hypertexte vers les documents de fonction individuels sont disponibles dans la section Informations connexes à la fin de ce document, si vous souhaitez consulter les détails complets des fonctions d'inspection vocale.

Cavates

L'application du pare-feu Cisco IOS avec des fonctionnalités vocales basées sur routeur doit appliquer le pare-feu de stratégie basé sur les zones afin de renforcer les points précédemment

mentionnés. Le pare-feu IOS classique n'inclut pas la capacité nécessaire pour prendre en charge pleinement la complexité de signalisation et le comportement du trafic vocal.

NAT

La traduction d'adresses de réseau (NAT) Cisco IOS est fréquemment configurée simultanément avec le pare-feu Cisco IOS, en particulier dans les cas où les réseaux privés doivent interagir avec Internet ou si des réseaux privés disparates doivent se connecter, en particulier si l'espace d'adresses IP se chevauche est utilisé. Le logiciel Cisco IOS inclut des passerelles de couche application NAT (ALG) pour SIP, Skinny et H.323. Idéalement, la connectivité réseau pour la voix IP peut être prise en charge sans l'application de NAT, car la NAT introduit une complexité supplémentaire dans les applications de dépannage et de stratégie de sécurité, en particulier dans les cas où la surcharge NAT est utilisée. La fonction NAT ne doit être appliquée qu'en dernier cas pour répondre aux problèmes de connectivité réseau.

CUPC

Ce document ne décrit pas la configuration qui prend en charge l'utilisation de Cisco Unified Presence Client (CUPC) avec Cisco IOS Firewall, car CUPC n'est pas encore pris en charge par Zone ou Classic Firewall à partir de la version 12.4(20)T1 du logiciel Cisco IOS. CUPC est pris en charge dans une prochaine version du logiciel Cisco IOS.

Bureau avec la passerelle Cisco Unity Express/SRST/PSTN qui se connecte à Cisco CallManager centralisé

Ce scénario diffère des applications précédentes, dans la mesure où le contrôle centralisé des appels est utilisé pour tout le contrôle des appels, au lieu du traitement distribué des appels basé sur le routeur. La messagerie vocale distribuée est appliquée, mais via Cisco Unity Express sur le routeur. Le routeur fournit la fonctionnalité Survivable Remote Site Telephony et la passerelle RTPC pour la numérotation d'urgence et la numérotation locale. Il est recommandé d'utiliser un niveau de capacité RTPC spécifique à l'application pour répondre aux défaillances de la numérotation de contournement WAN, ainsi que de la numérotation locale, comme décrit par le plan de numérotation. En outre, les lois locales exigent généralement qu'une sorte de connectivité RTPC locale soit fournie pour prendre en charge la numérotation d'urgence (911).

Ce scénario peut également appliquer Cisco CallManager Express en tant qu'agent de traitement des appels pour SRST, dans le cas où une capacité de traitement des appels plus importante est requise pendant les pannes WAN/CCM. Référez-vous à Intégration de Cisco Unity Connection à Cisco Unified CME-as-SRST pour plus d'informations.

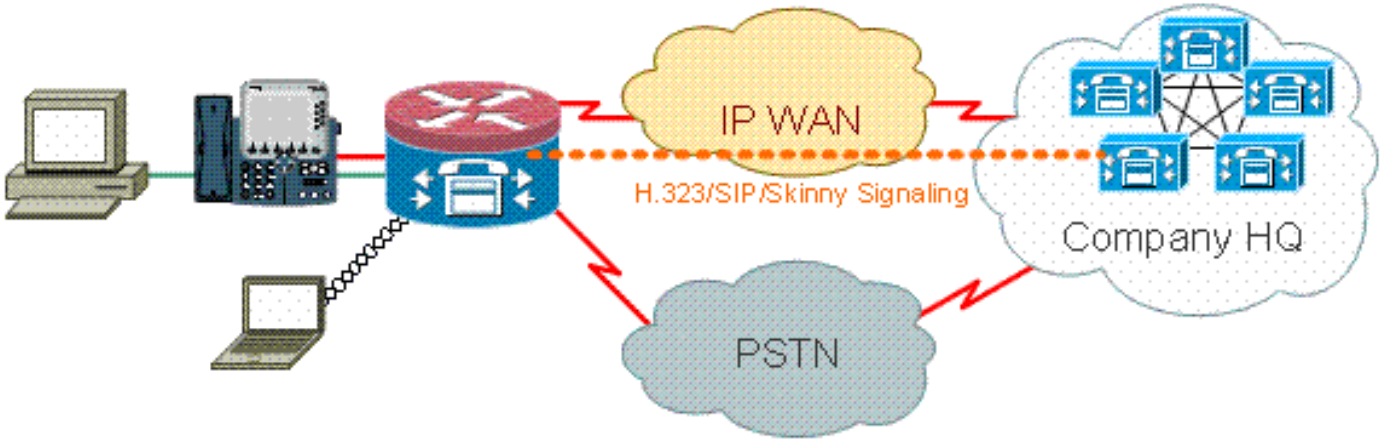
Arrière-plan du scénario

Le scénario d'application intègre des téléphones filaires (VLAN voix), des PC filaires (VLAN données) et des périphériques sans fil (y compris des périphériques VoIP tels qu'IP Communicator).

1. Inspection de signalisation entre les téléphones locaux et le cluster CUCM distant (SCCP et SIP)
2. Inspectez la signalisation H.323 entre le routeur et la grappe CUCM distante.
3. Inspectez la signalisation entre les téléphones locaux et le routeur lorsque la liaison au site

distant est arrêtée et que SRST est actif.

4. Les supports vocaux permettent de détecter les trous de communication entre :Segments filaires et sans fil locauxTéléphones locaux et distantsServeur MoH distant et téléphones locauxServeur Remote Unity et téléphones locaux pour la messagerie vocale
5. Appliquer l'inspection et le contrôle des applications (AIC) à :messages d'invitation de limite de débitassurer la conformité du protocole sur tout le trafic SIP.



Avantages/inconvénients

Ce scénario offre l'avantage que la majorité du traitement des appels se produit dans un cluster Cisco CallManager central, ce qui réduit la charge de gestion. En règle générale, le routeur doit gérer moins de charge d'inspection des ressources vocales locales que les autres cas décrits dans ce document, car la majeure partie de la charge de traitement des appels n'est pas imposée au routeur, sauf pour le traitement du trafic en provenance et à destination de Cisco Unity Express, et dans les cas de panne WAN ou CUCM, et Cisco CallManager Express/SRST local est appelé en vigueur pour le traitement des appels.

Le principal inconvénient de ce cas, lors d'une activité de traitement des appels classique, est que Cisco Unity Express est situé sur le routeur local. Bien que cela soit utile du point de vue de la conception, par exemple, Cisco Unity Express est situé le plus près des utilisateurs finaux où se trouve la messagerie vocale, il est soumis à une charge de gestion supplémentaire, en ce sens qu'il peut y avoir un grand nombre de Cisco Unity Express à gérer. Ceci dit, avec un Cisco Unity Express central pour supporter les inconvénients opposés, en ce sens qu'un Cisco Unity Express central est plus éloigné des utilisateurs distants et n'est peut-être pas accessible pendant les pannes. Ainsi, les avantages fonctionnels de l'offre de messagerie vocale distribuée par le déploiement de Cisco Unity Express sur des sites distants offrent un choix idéal.

Configurations pour les politiques de données, le pare-feu basé sur les zones, la sécurité vocale, Cisco CallManager Express

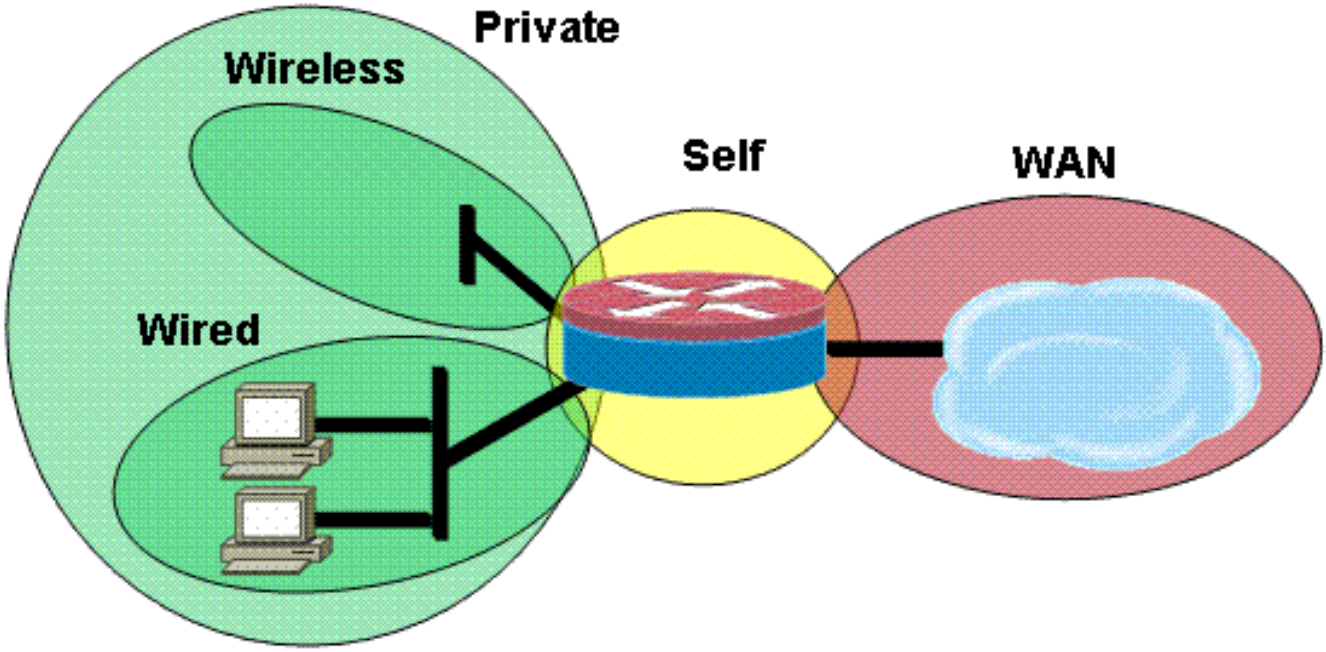
La configuration du routeur est basée sur un 3845 avec un NME-X-23ES et une carte HWIC PRI :

Configuration du service vocal pour la connectivité SRST et 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
!
```

Ceci est un exemple de la configuration Zone-Based Policy Firewall, composée de zones de sécurité pour les segments LAN filaires et sans fil, LAN privé, composé de segments filaires et sans fil, d'un segment WAN où la connectivité WAN fiable est atteinte et de la zone libre où se trouvent les ressources vocales du routeur :



Configuration de la sécurité :

```
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
```

Provisionnement, gestion et surveillance

Le provisionnement et la configuration des ressources de téléphonie IP basées sur les routeurs et du pare-feu de stratégie basé sur les zones sont généralement mieux adaptés à Cisco Configuration Professional. CiscoSecure Manager ne prend pas en charge le pare-feu Zone-Based Policy ni la téléphonie IP basée sur routeur.

Cisco IOS Classic Firewall prend en charge la surveillance SNMP avec la MIB Cisco Unified Firewall. Cependant, le pare-feu de stratégie basé sur les zones n'est pas encore pris en charge dans la MIB du pare-feu unifié. En tant que tel, la surveillance du pare-feu doit être gérée à l'aide de statistiques sur l'interface de ligne de commande du routeur, ou à l'aide d'outils graphiques tels que Cisco Configuration Professional.

CiscoSecure Monitoring And Reporting System (CS-MARS) offre une prise en charge de base du pare-feu de stratégie basé sur les zones, bien que les modifications de journalisation qui ont amélioré la corrélation des messages de journal avec le trafic mis en oeuvre dans le logiciel Cisco IOS Version 12.4(15)T4/T5 et le logiciel Cisco IOS Version 12.4(20)T n'aient pas encore été entièrement pris en charge dans CS-MARS.

Planification de capacité

Résultats des tests de performances d'inspection des appels de pare-feu en Inde à déterminer.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Cisco IOS Zone Firewall fournit des commandes **show** et **debug** afin d'afficher, de surveiller et de dépanner l'activité du pare-feu. Cette section décrit l'utilisation des commandes **show** afin de surveiller l'activité de base du pare-feu, ainsi qu'une introduction aux commandes **debug** du pare-feu de zone pour un dépannage plus détaillé, ou si la discussion avec le support technique nécessite des informations détaillées.

Dépannage des commandes

Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Commandes show

Cisco IOS Firewall propose plusieurs commandes **show** afin d'afficher la configuration et l'activité de la stratégie de sécurité :

La plupart de ces commandes peuvent être remplacées par une commande plus courte via l'application de la commande **alias**.

Commandes de débogage

Les commandes de **débogage** peuvent être utiles si vous utilisez une configuration atypique ou non prise en charge et que vous devez travailler avec le centre d'assistance technique de Cisco ou d'autres produits afin de résoudre les problèmes d'interopérabilité.

Remarque : l'application des commandes **debug** à des fonctionnalités ou un trafic spécifiques peut provoquer un très grand nombre de messages de console, ce qui fait que la console du routeur ne répond plus. Si vous devez activer le débogage, il est possible de fournir un autre accès à l'interface de ligne de commande, tel qu'une fenêtre telnet qui ne surveille pas la boîte de dialogue de terminal. Vous devez uniquement activer le débogage sur un équipement hors ligne (environnement de travaux pratiques) ou pendant une fenêtre de maintenance planifiée, car si vous activez le débogage, cela peut affecter considérablement les performances du routeur.

Informations connexes

- Guide de conception du réseau de référence de la solution Cisco Unified CallManager Express
- Meilleures pratiques de sécurité Cisco Unified CallManager Express
- Intégration de Cisco Unity Connection à Cisco Unified CME-as-SRST
- Référence des commandes de Cisco Unified Communications Manager Express
- Exemple de configuration de Cisco CallManager Express/Cisco Unity Express
- Prise en charge de la MIB SNMP de Cisco CallManager Express 3.4
- Guide de conception et d'application du pare-feu de stratégie basé sur la zone
- Prise en charge du pare-feu Cisco IOS pour le trafic local maigre et CME
- Cisco IOS Firewall
- Support et documentation techniques - Cisco Systems