Cisco IOS Zone Based Firewall:Cisco Unity Express/SRST/PSTN 게이트웨이가 있는 Office(중앙 집중식 Cisco CallManager 연결)

목차

소개

Cisco ISR(Integrated Service Router)은 광범위한 애플리케이션에 대한 데이터 및 음성 네트워크 요구 사항을 해결할 수 있는 확장 가능한 플랫폼을 제공합니다.프라이빗 및 인터넷 연결 네트워크의 위협 환경은 매우 동적인 환경이지만, Cisco IOS® Firewall은 안전한 네트워크 상태를 정의하고 적용하는 동시에 비즈니스 기능과 연속성을 가능하게 하는 스테이트풀 검사 및 AIC(Application Inspection and Control) 기능을 제공합니다.

이 문서에서는 특정 Cisco ISR 기반 데이터 및 음성 애플리케이션 시나리오의 방화벽 보안 측면에 대한 설계 및 구성 고려 사항에 대해 설명합니다.각 애플리케이션 시나리오에 대해 음성 서비스 및 방화벽 구성이 제공됩니다.각 시나리오에서는 VoIP 및 보안 컨피그레이션을 개별적으로 설명한 다음 전체 라우터 컨피그레이션을 기준으로 설명합니다.네트워크에서 음성 품질과 기밀성을 유지하기 위해 QoS 및 VPN 같은 서비스에 대한 다른 컨피그레이션이 필요할 수 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

Cisco IOS 방화벽 배경

Cisco IOS 방화벽은 일반적으로 어플라이언스 방화벽의 구축 모델과 다른 애플리케이션 시나리오에 구축됩니다.일반적인 구축 환경으로는 Teleworker 애플리케이션, 소규모 또는 지사 사이트, 소매 애플리케이션 등이 있는데, 여기에는 낮은 장치 수, 여러 서비스의 통합, 낮은 성능 및 보안 기능 수준이 필요합니다.

방화벽 검사 및 ISR 제품의 다른 통합 서비스와 함께 방화벽 검사를 적용하는 것이 비용 및 운영 측면에서 매력적으로 보일 수 있지만, 라우터 기반 방화벽이 적절한지 확인하기 위해 구체적인 고려 사항을 평가해야 합니다.각각의 추가 기능을 적용하면 메모리 및 처리 비용이 발생하며, 성능이 낮은 통합 라우터 기반 솔루션을 구축할 경우 최대 로드 기간 동안 전달 처리량 속도, 패킷 레이턴시 증가, 기능 기능 손실이 발생할 수 있습니다.라우터와 어플라이언스를 결정할 때 다음 지침을 준수합니다.

- 여러 개의 통합 기능이 활성화된 라우터는 더 적은 수의 장치가 더 나은 솔루션을 제공하는 지사 또는 재택 근무 사이트에 가장 적합합니다.
- 일반적으로 고대역폭 고성능 애플리케이션은 어플라이언스를 통해 더 효과적으로 대처합니다.Cisco ASA 및 Cisco Unified Call Manager Server를 적용하여 NAT 및 보안 정책 애플리케이션 및 통화 처리를 처리하고 라우터는 QoS 정책 애플리케이션, WAN 종료 및 Site-to-Site VPN 연결 요구 사항을 해결해야 합니다.

Cisco IOS Software Release 12.4(20)T가 출시되기 전에는 VoIP 트래픽 및 라우터 기반 음성 서비스에 필요한 기능을 완벽하게 지원할 수 없었고, 음성 트래픽을 수용하기 위해 보안 방화벽 정책에 대한 대규모 결원이 필요했으며, 진화하는 VoIP 신호 및 미디어 프로토콜에 대한 제한된 지원을 제공했습니다.

구성

Cisco IOS Zone-Based Policy Firewall 구축

Cisco IOS Zone-Based Policy Firewall은 다른 방화벽과 유사하게, 네트워크 신뢰의 보안 요구 사항을 파악하고 보안 정책에 따라 설명하는 경우에만 보안 방화벽을 제공할 수 있습니다.보안 정책에 도달하기 위한 두 가지 기본적인 접근 방식이 있습니다.*의심스러운* 관점과 대조적으로.

신뢰하는 *관점*은 모든 트래픽이 신뢰할 수 있다고 가정합니다. 단, 악성 또는 원치 않는 트래픽으로 구체적으로 식별될 수 있습니다.원하지 않는 트래픽만 거부하는 특정 정책이 구현됩니다.이 작업은 일반적으로 특정 액세스 제어 항목 또는 시그니처 또는 동작 기반 툴을 사용하여 수행합니다.이러한 접근 방식은 기존 애플리케이션에 방해가 되는 경향이 있지만, 위협 및 취약성 환경에 대한 포괄적인 지식이 필요하며, 새로운 위협과 익스플로잇을 나타나는 즉시 해결하기 위해 끊임없는 경계가 필요합니다.또한 사용자 커뮤니티는 적절한 보안을 유지하는 데 큰 역할을 해야 합니다.거주자에

대한 제어가 거의 없는 광범위한 자유를 허용하는 환경은 부주의한 또는 악의적인 개인들로 인해 야기되는 문제에 상당한 기회를 제공합니다.이 접근 방식의 또 다른 문제는 모든 네트워크 트래픽에서 의심스러운 데이터를 모니터링하고 제어할 수 있는 충분한 유연성과 성능을 제공하는 효과적인 관리 툴과 애플리케이션 제어에 훨씬 더 많이 의존한다는 것입니다.현재 기술을 사용할 수 있지만 운영 부담이 대부분의 조직의 한계를 초과하는 경우가 많습니다.

의심스러운 관점은 특별히 식별된 *양호한* 트래픽을 제외하고 모든 네트워크 트래픽이 바람직하지 않다고 가정합니다.이는 명시적으로 허용된 애플리케이션 트래픽을 제외한 모든 애플리케이션 트래픽을 거부하는 정책을 적용합니다.또한 AIC(Application Inspection and Control)를 구현하여 *좋은* 애플리케이션을 활용하기 위해 특별히 제작된 악성 트래픽과 *좋은* 트래픽으로 가장하는 원치 않는 트래픽을 식별하고 거부할 수 있습니다.애플리케이션 제어는 ACL(Access-Control Lists) 또는 ZFW(Zone-Based Policy Firewall) 정책과 같은 스테이트리스(stateless) 필터에 의해 제어되어야 하지만, 네트워크에 운영 및 성능 부담을 가중시킵니다. 따라서 AIC, IPS(Intrusion Prevention System) 또는 FPM(Flexible Packet Matching) 또는 NBAR(network-based application recognition)과 같은 기타 시그니처 기반 제어를 통해 처리해야 하는 트래픽이 상당히 적습니다. 따라서 원하는 애플리케이션 포트 및 알려진 제어 연결 또는 세션으로 인해 발생하는 동적 미디어별 트래픽만 특별히 허용될 경우, 네트워크에 존재해야 하는 불필요한 트래픽만 더 쉽게 인식되는 특정 하위 집합에 속해야 합니다. 그러면 원치 않는 트래픽에 대한 제어를 유지하기 위해 요구되는 엔지니어링 및 운영 부담이 줄어듭니다.

이 문서에서는 *의심스러운* 관점을 기준으로 VoIP 보안 컨피그레이션에 대해 설명합니다.따라서 음성 네트워크 세그먼트에서 허용되는 트래픽만 허용됩니다.각 애플리케이션 시나리오의 컨피그레이션에 대한 메모에 설명된 대로 데이터 정책은 더욱 허용적입니다.

모든 보안 정책 구축은 폐쇄 루프 피드백 주기를 따라야 합니다.보안 구축은 일반적으로 기존 애플리케이션의 기능 및 기능에 영향을 미치며, 이러한 영향을 최소화하거나 해결하기 위해 조정해야 합니다.

Zone-Based Policy Firewall 컨피그레이션에 대한 자세한 내용 및 추가 배경 정보는 Zone-Based Policy Firewall Design and Application Guide를 참조하십시오.

VoIP 환경에서 ZFW 고려 사항

앞서 언급한 설계 및 애플리케이션 가이드에서는 라우터의 자체 영역에 대한 보안 정책을 사용하여 라우터의 보안을 간략하게 설명하고 다양한 NFP(Network Foundation Protection) 기능을 통해 제공되는 대체 기능을 소개합니다.라우터 기반 VoIP 기능은 라우터의 자체 영역 내에서 호스팅되므로, 라우터를 보호하는 보안 정책은 Cisco Unified CallManager Express, Survivable Remote-Site Telephony 및 Voice Gateway 리소스에 의해 시작되거나 전달될 음성 신호 및 미디어를 수용하기 위해 음성 트래픽에 대한 요구 사항을 인식해야 합니다.Cisco IOS Software Release 12.4(20)T 이전 버전에서는 Classic Firewall 및 Zone-Based Policy Firewall이 VoIP 트래픽의 요구 사항을 완전히 충족할 수 없었기 때문에 리소스를 완전히 보호할 수 있도록 방화벽 정책이 최적화되지 않았습니다.라우터 기반 VoIP 리소스를 보호하는 자체 영역 보안 정책은 Cisco IOS Software Release 12.4(20)T에 도입된 기능에 크게 의존합니다.

Cisco IOS Firewall 음성 기능

Cisco IOS Software Release 12.4(20)T는 공동 상주 Zone Firewall 및 음성 기능을 활성화하기 위해 몇 가지 향상된 기능을 도입했습니다.보안 음성 애플리케이션에 3가지 주요 기능이 직접 적용됩니다.

- SIP 개선 사항:애플리케이션 레이어 게이트웨이 및 애플리케이션 검사 및 제어RFC 3261에 설명된 대로 SIP 버전 지원을 SIPv2에 업데이트SIP 신호 지원을 확장하여 더 다양한 통화 흐름을

인식합니다.특정 애플리케이션 레벨 취약성 및 익스플로잇을 해결하기 위해 세분화된 제어를 적용할 수 있는 SIP AIC(Application Inspection and Control)를 소개합니다.로컬에서/시작된 SIP 트래픽에서 발생하는 보조 신호 및 미디어 채널을 인식할 수 있도록 자체 영역 검사를 확장합니다.

- Skinny 로컬 트래픽 및 Cisco CallManager Express 지원SCCP 지원을 버전 16으로 업데이트(이전에 지원되었던 버전 9)특정 애플리케이션 레벨 취약성 및 익스플로잇을 해결하기 위해 세분화된 제어를 적용할 수 있는 SCCP AIC(Application Inspection and Control)를 소개합니다.자체 영역 검사를 확장하여 로컬로/시작된 SCCP 트래픽으로 인해 발생하는 보조 신호 및 미디어 채널을 인식할 수 있습니다.
- H.323 v3/v4 지원에서 설명한 대로 v3 및 v4(이전에 지원되었던 v1 및 v2)에 H.323 지원을 업데이트합니다.특정 애플리케이션 레벨 취약성 및 익스플로잇을 해결하기 위해 세분화된 제어를 적용할 수 있는 H.323 AIC(Application Inspection and Control)를 소개합니다.

이 문서에 설명된 라우터 보안 컨피그레이션에는 이러한 개선 사항에 의해 제공되는 기능과 정책에 의해 적용된 작업을 설명하는 설명이 포함되어 있습니다.개별 기능 문서에 대한 하이퍼링크는 음성 검사 기능에 대한 전체 세부 정보를 검토하려는 경우 이 문서 끝의 Related Information(관련 정보) 섹션에서 사용할 수 있습니다.

주의 사항

라우터 기반 음성 기능이 포함된 Cisco IOS Firewall의 애플리케이션은 앞서 언급한 사항을 보강하기 위해 Zone-Based Policy Firewall을 적용해야 합니다.기존 IOS 방화벽은 음성 트래픽의 신호 복잡성과 동작을 완전히 지원하는 데 필요한 기능을 포함하지 않습니다.

NAT

Cisco IOS NAT(Network Address Translation)는 Cisco IOS Firewall과 함께 자주 구성됩니다. 특히 사설 네트워크가 인터넷과 연결되어야 하거나, 개별 사설 네트워크가 연결해야 하는 경우, 특히 중복 IP 주소 공간이 사용 중인 경우 그렇습니다.Cisco IOS Software에는 SIP, Skinny 및 H.323용 NAT ALG(Application Layer Gateway)가 포함되어 있습니다. NAT는 문제 해결 및 보안 정책 애플리케이션, 특히 NAT 오버로드가 사용되는 경우 NAT를 사용하지 않고도 IP 음성에 대한 네트워크 연결을 수용할 수 있습니다.NAT는 네트워크 연결 문제를 해결하기 위한 마지막 사례 솔루션으로만 적용되어야 합니다.

CUPC

이 문서에서는 Cisco IOS Software Release 12.4(20)T1 현재 Zone 또는 Classic Firewall에서 CUPC를 지원하지 않으므로 Cisco IOS Firewall에서 Cisco CUPC(Unified Presence Client) 사용을 지원하는 컨피그레이션에 대해 설명하지 않습니다. CUPC는 향후 Cisco IOS Software 릴리스에서 지원됩니다.

중앙 집중식 Cisco CallManager에 연결되는 Cisco Unity Express/SRST/PSTN 게이트웨이가 있는 Office

이 시나리오는 분산 라우터 기반 통화 처리 대신 중앙 집중식 통화 제어가 모든 통화 제어에 사용된다는 점에서 이전 애플리케이션과 다릅니다.분산 음성 메일이 적용되지만 라우터의 Cisco Unity Express를 통해 전송됩니다.이 라우터는 긴급 전화 걸기 및 로컬 다이얼을 위해 Survivable Remote-Site Telephony 및 PSTN Gateway 기능을 제공합니다.다이얼 플랜에 설명된 대로 WAN 기반 유료 바이패스 다이얼링 및 로컬 영역 다이얼링 장애를 수용하려면 애플리케이션별 PSTN 용량 레벨을 사용하는 것이 좋습니다.또한 현지 법률은 일반적으로 긴급(911) 전화 걸기를 수용하기 위

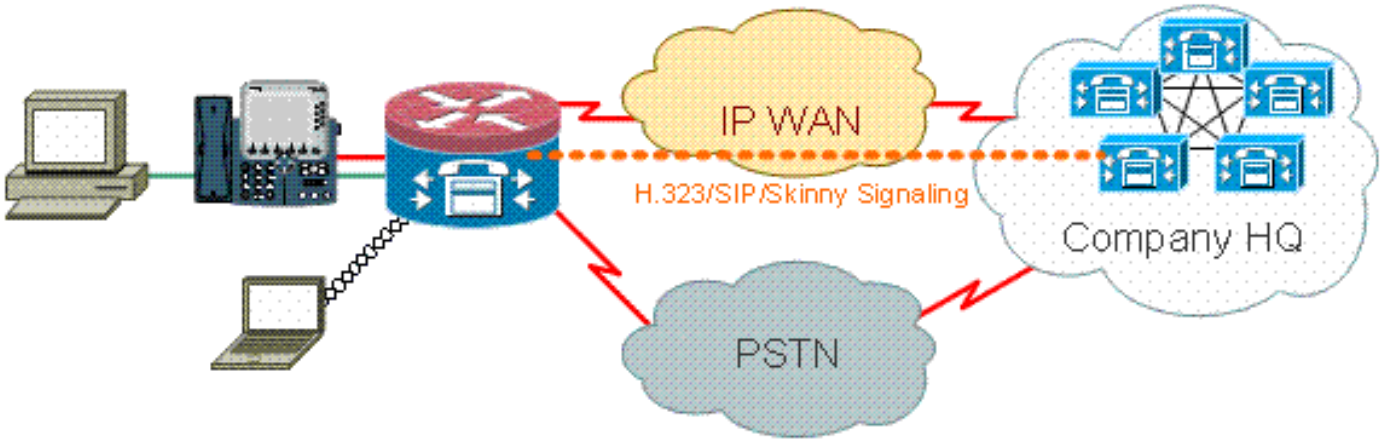
해 일종의 현지 PSTN 연결이 제공되어야 합니다.

이 시나리오는 WAN/CCM 중단 중에 더 큰 통화 처리 기능이 필요한 경우 SRST용 통화 처리 에이전트로 Cisco CallManager Express를 적용할 수도 있습니다.자세한 내용은 Cisco Unity Connection과 Cisco Unified CME-as-SRST 통합을 참조하십시오.

시나리오 배경

애플리케이션 시나리오에는 유선 전화(음성 VLAN), 유선 PC(데이터 VLAN) 및 무선 장치(IP Communicator와 같은 VoIP 장치 포함)가 포함됩니다.

1. 로컬 전화기와 원격 CUCM 클러스터(SCCP 및 SIP) 간 신호 검사
2. 라우터와 원격 CUCM 클러스터 간의 H.323 신호 처리를 검사합니다.
3. 원격 사이트에 대한 링크가 중단되고 SRST가 활성 상태일 때 로컬 전화기와 라우터 간의 신호 처리를 검사합니다.
4. 다음 사이의 통신을 위한 음성 미디어 핀홀:로컬 유무선 부문로컬 및 원격 전화원격 MoH 서버 및 로컬 전화음성 메일용 Remote Unity 서버 및 로컬 전화
5. AIC(Application Inspection and Control) 적용 대상:초대 메시지 제한모든 SIP 트래픽에 대한 프로토콜 적합성을 보장합니다.



장점/단점

이 시나리오에서는 대부분의 통화 처리가 중앙 Cisco CallManager 클러스터에서 발생하므로 관리 부담이 줄어듭니다.일반적으로 라우터는 이 문서에 설명된 다른 경우와 비교했을 때 로컬 음성 리소스 검사 부담을 덜 해결해야 합니다. Cisco Unity Express에서 송수신되는 트래픽을 처리하는 경우를 제외하고 통화 처리 부담이 라우터에 대부분 부과되지 않으며, WAN 또는 CUCM 중단이 있고 로컬 Cisco CallManager Express/SRST가 통화 처리 문제를 해결하기 위해 호출됩니다.

이 사례의 가장 큰 단점은 일반적인 통화 처리 활동 중에 Cisco Unity Express가 로컬 라우터에 있다는 것입니다.예를 들어, 설계 측면에서 보면 Cisco Unity Express는 음성 메일이 저장된 최종 사용자와 가장 가까운 위치에 있지만, 관리할 Cisco Unity Express가 많은 수가 있을 수 있으므로 관리 부담이 가중됩니다.즉, 중앙 Cisco Unity Express를 통해 반대 단점이 있습니다. 즉, 중앙 Cisco Unity Express는 원격 사용자로부터 멀리 떨어져 있으며 가동 중단 시 액세스할 수 없습니다.따라서 원격 위치에 Cisco Unity Express를 구축하면 분산 음성 메일 기능의 이점을 활용할 수 있어 탁월한 선택이 가능합니다.

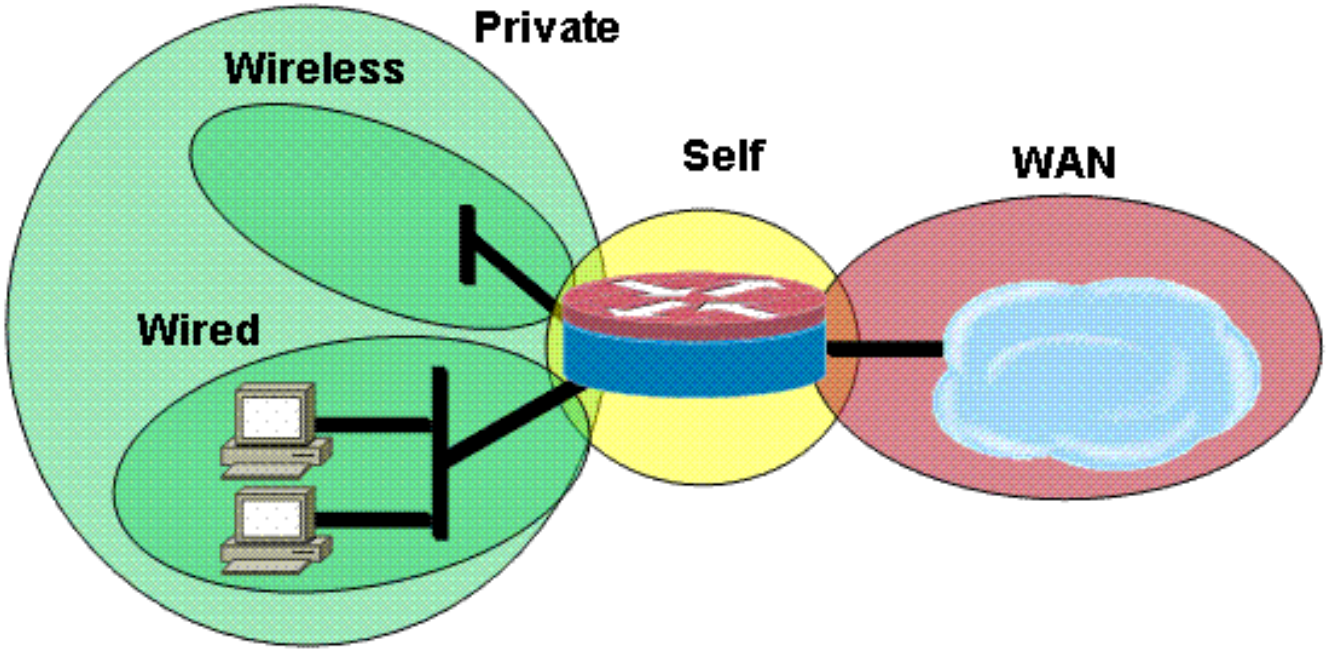
데이터 정책, 영역 기반 방화벽, 음성 보안, Cisco CallManager Express 구성

라우터 컨피그레이션은 NME-X-23ES 및 PRI HWIC가 포함된 3845를 기반으로 합니다.

SRST 및 Cisco Unity Express 연결을 위한 음성 서비스 구성:

```
!
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
!
```

다음은 유무선 LAN 세그먼트의 보안 영역, 유무선 세그먼트로 구성된 프라이빗 LAN, 신뢰할 수 있는 WAN 연결에 도달한 WAN 세그먼트, 라우터의 음성 리소스가 있는 자체 영역으로 구성된 영역 기반 정책 방화벽 컨피그레이션의 예입니다.



보안 구성:

```
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
```

프로비저닝, 관리 및 모니터링

라우터 기반 IP 텔레포니 리소스와 영역 기반 정책 방화벽 모두에 대한 프로비저닝 및 컨피그레이션은 일반적으로 Cisco Configuration Professional과 함께 사용하는 것이 가장 좋습니다.CiscoSecure Manager는 영역 기반 정책 방화벽 또는 라우터 기반 IP 텔레포니를 지원하지 않습니다.

Cisco IOS Classic Firewall은 Cisco Unified Firewall MIB를 사용하여 SNMP 모니터링을 지원합니다.그러나 Unified Firewall MIB에서는 영역 기반 정책 방화벽이 아직 지원되지 않습니다.따라서 라우터 CLI(Command Line Interface)의 통계나 Cisco Configuration Professional과 같은 GUI 툴을 통해 방화벽 모니터링을 처리해야 합니다.

Cisco CS-MARS(Secure Monitoring and Reporting System)는 Zone-Based Policy Firewall에 대한 기본 지원을 제공합니다. 그러나 Cisco IOS Software Release 12.4(15)T4/T5 및 Cisco IOS Software Release 12.4(20)T가 아직 CS-MARS에서 완전히 지원되지는 않았습니다.

용량 계획

인도 TBD의 방화벽 통화 검사 성능 테스트 결과.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

Cisco IOS Zone Firewall은 방화벽 활동을 보고 모니터링하고 문제를 해결하기 위해 **show** 및 **debug** 명령을 제공합니다.이 섹션에서는 기본 방화벽 활동을 모니터링하기 위해 **show** 명령을 사용하는 방법과 자세한 문제 해결을 위해 Zone Firewall의 **debug** 명령 소개 또는 기술 지원과의 논의가 자세한 정보를 필요로 하는 경우에 대해 설명합니다.

문제 해결 명령

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

명령 표시

Cisco IOS Firewall은 보안 정책 컨피그레이션 및 활동을 보기 위해 몇 가지 **show** 명령을 제공합니다.

이러한 명령 중 다수는 alias 명령의 응용 프로그램을 통해 더 짧은 명령으로 대체할 수 **있습니다**.

디버그 명령

디버그 명령은 암호화되지 않거나 지원되지 않는 컨피그레이션을 사용하는 경우 유용할 수 있으며, 상호 운용성 문제를 해결하기 위해 Cisco TAC 또는 기타 제품의 기술 지원 서비스와 함께 작업해야 하는 경우 유용합니다.

참고: debug 명령을 특정 기능 또는 트래픽에 적용하면 콘솔 메시지 수가 매우 많아 라우터 콘솔이 응답하지 않을 수 있습니다.디버깅을 활성화해야 하는 경우 터미널 대화 상자를 모니터링하지 않는 텔넷 창과 같은 대체 명령줄 인터페이스 액세스를 제공할 수 있습니다.디버깅을 활성화하면 라우터 성능에 큰 영향을 미칠 수 있으므로 오프라인(랩 환경) 장비 또는 계획된 유지 관리 기간 동안에만 디버그를 활성화해야 합니다.

관련 정보

- Cisco Unified CallManager Express 솔루션 참조 네트워크 설계 가이드
- Cisco Unified CallManager Express 보안 모범 사례
- Cisco Unity Connection과 Cisco Unified CME-as-SRST 통합
- Cisco Unified Communications Manager Express 명령 참조
- Cisco CallManager Express/Cisco Unity Express 컨피그레이션 예
- Cisco CallManager Express 3.4 SNMP MIB 지원
- Zone-Based Policy Firewall 설계 및 애플리케이션 가이드
- Skinny Local Traffic 및 CME를 위한 Cisco IOS Firewall 지원
- Cisco IOS Firewall
- 기술 지원 및 문서 – Cisco Systems