Cisco IOS Zone-Based ファイアウォール：中央集中型 Cisco CallManager への接続が動作する Cisco Unity Express/SRST/PSTN ゲートウェイのオフィス

内容

概要

Cisco Integrated Service Router（ISR）は、さまざまなアプリケーションのデータおよび音声ネットワークの要件に対応する、スケーラブルなプラットフォームを提供します。プライベートおよびインターネットに接続されたネットワークの脅威の状況は非常に動的ですが、Cisco IOS® Firewallは、ステートフルインスペクションおよびApplication Inspection and Control(AIC)機能を提供して、セキュアなネットワークポスチャを定義および適用し、ビジネス機能と継続性をを可能します。

このドキュメントでは、特定の Cisco ISR ベースのデータおよび音声アプリケーションのシナリオに関して、ファイアウォール セキュリティの設計および設定の考慮事項について説明します。音声サービスおよびファイアウォールの設定は、アプリケーションのシナリオごとに示されます。各シナリオでは、VoIP およびセキュリティの設定が個別に説明され、その後、ルータ全体の設定が説明されます。ネットワークには、音声品質と機密性を維持するためのサービス（QoS、VPN など）の設定が必要なことがあります。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

Cisco IOS Firewall のバックグラウンド

Cisco IOS Firewall は、通常、アプライアンス ファイアウォールの導入モデルとは異なるアプリケーションのシナリオで導入されます。典型的な導入には、少ないデバイス数、複数サービスの統合、低いパフォーマンスとセキュリティ機能深度が好まれる、在宅勤務者アプリケーション、小規模オフィスやブランチオフィスのサイト、およびリテール アプリケーションが含まれます。

ファイアウォール インスペクションのアプリケーションと ISR 製品の他の統合サービスの組み合わせは、コストと運用面で魅力的に思えますが、ルータベースのファイアウォールが適切であるかどうかを判断するためには、個別の考慮事項を検討する必要があります。能力が足りない統合型のルータベース ソリューションを導入した場合、各追加機能のアプリケーションにより、メモリコストと処理コストが増え、転送スループット率の低下、パケット遅延の増加、および最大負荷時の機能の損失が発生する可能性があります。ルータとアプライアンスの間で判断を下す場合は、次のガイドラインに従ってください。

- デバイスが少ない方がソリューションとして優れているブランチ オフィスや在宅勤務者のサイトには、複数の統合機能に対応したルータが最も適しています。
- 一般的に、高帯域幅、高性能のアプリケーションがアプライアンスでの処理には適しています。Cisco ASA および Cisco Unified CallManager サーバは、NAT、セキュリティ ポリシー アプリケーション、および呼処理を処理するために適用する必要があります。ルータは、QoS ポリシー アプリケーション、WAN の終端、およびサイト間 VPN 接続の要件に対応します。

Cisco IOS Software Release 12.4(20)T が登場する前は、Classic Firewall とゾーンベース ポリシー ファイアウォール（ZFW）では、VoIP トラフィックおよびルータベースの音声サービスに必要な機能を完全にはサポートできず、音声トラフィックに対応するためには、他の点ではセキュアなファイアウォール ポリシーに大きな穴を開ける必要があり、発達する VoIP シグナリングとメディア プロトコルのサポートは限定されていました。

設定

Cisco IOS ゾーンベース ポリシー ファイアウォールの導入

Cisco IOS ゾーンベース ポリシー ファイアウォールは、他のファイアウォールと同様、ネットワーク *trustingare のセキュリティ要件がセキュリティ ポリシーによって特定および記述されている場合にのみ、セキュアなファイアウォールを提供できます。*セキュリティ ポリシーに対する 2 つの基本的なアプローチは次のとおりです。観点：*疑いの観点とは対照的。*

*信頼の観点では、悪意のあるトラフィックまたは不要なトラフィックと明確に特定できるものを除き、すべてのトラフィックが信頼できると仮定されます。*不要なトラフィックのみを拒否する特定のポリシーが実装されます。これは、通常、特定のアクセス制御エントリ、またはシグニチャや動作ベースのツールで実行されます。このアプローチの場合、既存アプリケーションへの影響は少ない傾向にありますが、脅威と脆弱性の展望に関する包括的な専門知識が必要であり、新たな脅威に対応し、現れる脅威をエクスプロイトするために常に警戒している必要があります。また、ユーザ コミュニティが、セキュリティの適切な維持の大部分を担当する必要があります。利用者に対する制限が少なく、自由度の高い環境では、多くの場合、不注意または悪意のある人物によって問題が引き起こされます。このアプローチのさらなる問題点は、すべてのネットワーク トラフィック内の疑わしいデータのモニタとコントロールを可能にするための、十分な柔軟性と性能を提供する効率的な管理ツールとアプリケーション制御への依存度がさらに増す点です。現在は、この点に対応するためのテクノロジーがありますが、多くの場合、運用上の負担はほとんどの組織の限界を超えています。

*疑いの観点では、望ましいトラフィックだと明確に識別されたものを除き、すべてのネットワーク トラフィックが望ましくないと仮定されます。*これは、明示的に許可されたトラフィックを除き、すべてのアプリケーション トラフィックを拒否するために適用されるポリシーです。また、Application Inspection and Control（AIC）は、*望ましいアプリケーション、および望ましいトラフィックとしてマスカレードされている不要なトラフィックをエクスプロイトするために作成された、悪意のあるトラフィックを識別および拒否するために実装できます。*繰り返しになりますが、望ましくないトラフィックの大部分は、アクセス コントロール リスト（ACL）やゾーンベース ポリシー ファイアウォール（ZFW）ポリシーなどのステートレス フィルタによって制御される必要がありますが、アプリケーション制御を行うことで、ネットワークに対する運用およびパフォーマンスの負担は生じます。したがって、AIC、侵入防御システム（IPS）、または Flexible Packet Matching（FPM）や Network-Based Application Recognition（NBAR; ネットワークベースのアプリケーション認識）などの他のシグニチャベース コントロールで処理する必要があるトラフィックは大幅に減少する必要があります。 したがって、希望するアプリケーション ポート、および既知の制御接続やセッションから生じる動的なメディア固有のトラフィックが具体的に許可されている場合、ネットワーク上に存在する必要がある不要なトラフィックのみ、個別のより認識しやすいサブセットに分類されます。その結果、望ましくないトラフィックに対するコントロールを維持するために必要なエンジニアリングおよび運用上の負担が軽減されます。

このドキュメントでは、*疑いの観点に基づいた VoIP セキュリティの設定について説明しています。*そのため、音声ネットワーク セグメントで許容されるトラフィックのみ許可されます。各アプリケーション シナリオの設定の「注」で説明されているように、データ ポリシーは許可されやすい傾向にあります。

すべてのセキュリティ ポリシーの導入は、クローズドループ フィードバック サイクルに従う必要があります。セキュリティの導入は、通常、既存アプリケーションの機能に影響を及ぼします。また、その影響を最小限に抑える、または解消するための調整が必要になります。

ゾーンベース ポリシー ファイアウォールの設定の詳細および追加のバックグラウンド情報については、『ゾーンベース ポリシー ファイアウォールの設計およびアプリケーション ガイドライン』を参照してください。

VoIP 環境内の ZFW の考慮事項

前述の『設計およびアプリケーション ガイド』には、ルータのセルフ ゾーンとの通信にセキュリティ ポリシーを使用するルータのセキュリティの概要、さまざまな Network Foundation Protection（NFP）機能によって提供される代替機能の概要が記載されています。ルータベースの VoIP 機能は、ルータのセルフ ゾーン内でホストされているため、Cisco Unified CallManager Express、Survivable Remote Site Telephony、および音声ゲートウェイ リソースによって生成され、これらのリソース宛に送信される音声信号とメディアに対応するためには、ルータを保護するセキュリティ ポリシーが音声トラフィックの要件を認識する必要があります。Cisco IOS Software Release 12.4(20)T、Classic Firewall、およびゾーンベース ポリシー ファイアウォールが登場する前は、VoIP トラフィックの要件に完全に対応することができなかったため、ファイアウォール ポリシーはリソースを完全に保護するように最適化されていませんでした。ルータベースの VoIP リソースを保護するセルフゾーン セキュリティ ポリシーは、Cisco IOS Software Release 12.4(20)T で導入された機能に大きく依存しています。

Cisco IOS Firewall の音声機能

Cisco IOS Software Release 12.4(20)T では、Zone Firewall と音声機能の共存を可能にするために複数の機能が強化されています。3 つの主要機能は、セキュアな音声アプリケーションに直接適用されます。

- SIP の機能強化：アプリケーション層ゲートウェイおよび Application Inspection and ControlRFC 3261 で定義されている、SIPv2 への SIP バージョンのサポートを更新より広範なコール フローを認識するために、SIP シグナリングのサポートを拡大固有のアプリケーションレベルの脆弱性およびエクスプロイトに対応するためのきめ細かい制御を適用するために、SIP Application Inspection and Control（AIC）を導入ローカルに送受信される SIP トラフィックによって生じるセカンダリ シグナリングおよびメディア チャネルを認識できるようにするために、セルフゾーン検査を拡大
- Skinny Local Traffic および Cisco CallManager Express のサポートバージョン 16 に対する SCCP のサポートを更新（以前のサポート バージョンは 9）固有のアプリケーションレベルの脆弱性およびエクスプロイトに対応するためのきめ細かい制御を適用するために、SCCP Application Inspection and Control（AIC）を導入ローカルに送受信される SCCP トラフィックによって生じるセカンダリ シグナリングおよびメディア チャネルを認識できるようにするために、セルフゾーン検査を拡大
- H.323 v3/v4 のサポートv3 および v4 に対する H.323 のサポートを更新（以前のサポート対象は v2 および v1）固有のアプリケーションレベルの脆弱性およびエクスプロイトに対応するためのきめ細かい制御を適用するために、H.323 Application Inspection and Control（AIC）を導入

このドキュメントで説明されているルータのセキュリティ設定には、これらの機能強化によってもたらされる機能、およびポリシーによって適用されるアクションに関する説明が含まれています。音声検査機能の詳細を確認する場合は、このドキュメントの最後にある「関連情報」の項に記載されている個々の機能ドキュメントのハイパーリンクをクリックしてください。

警告

ルータベースの音声機能を持つ Cisco IOS Firewall アプリケーションの場合は、ゾーンベース ポリシー ファイアウォールを適用して、前述した点を強化する必要があります。Classic IOS Firewall には、シグナリングの複雑さと音声トラフィックの動作を完全にサポートするために必要な機能は含まれていません。

NAT

Cisco IOS ネットワーク アドレス変換（NAT）は、Cisco IOS Firewall と共に設定されることがよくあります。特に、プライベート ネットワークがインターネットとインターフェイス接続する必要がある場合、または異種プライベート ネットワークを接続する必要がある場合（特に、オーバーラップ IP アドレス空間が使用されている場合）に設定されます。Cisco IOSソフトウェアには、SIP、Skinny、およびH.323用のNATアプリケーション層ゲートウェイ(ALG)が含まれています。NATではトラブルシューティングやセキュリティポリシーアプリケーションが複雑になるため、IP音声のネットワーク接続はNATの適用なしで行えます。NAT は、ネットワークの接続性の問題に対しては最後の解決策としてのみ適用する必要があります。

CUPC

このドキュメントでは、Cisco IOSファイアウォールでCisco Unified Presence Client(CUPC)の使用をサポートする設定については説明しません。CUPCは、Cisco IOSソフトウェアリリース12.4(20)T1でゾーンまたはクラシックファイアウォールでサポートされていません。

中央集中型 Cisco CallManager に接続する Cisco Unity Express/SRST/PSTN ゲートウェイがあるオフィス

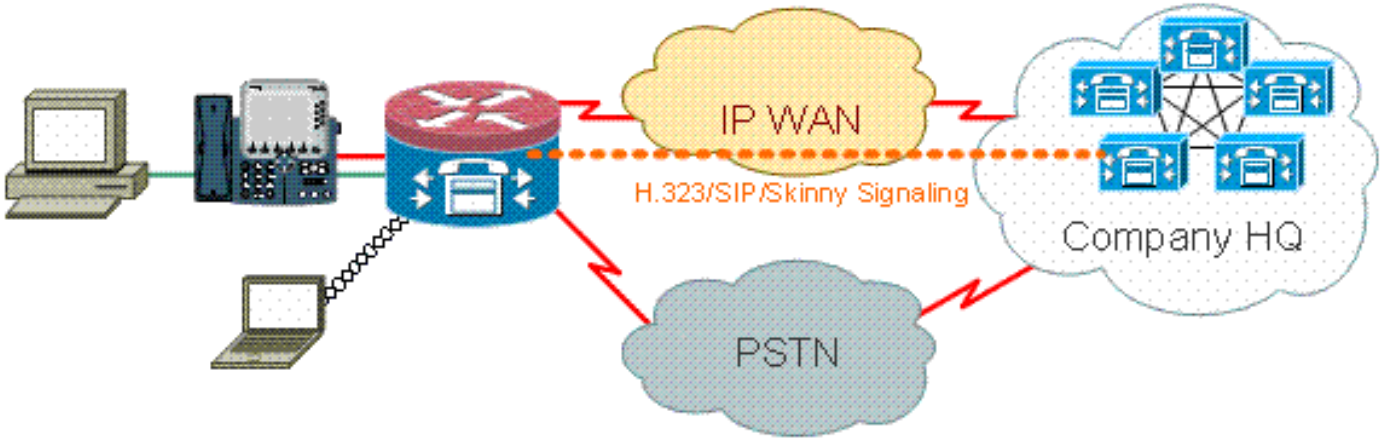
このシナリオは、分散型のルータベースの呼処理の代わりに、すべてのコール制御に集中型のコール制御が使用される点で、前述のアプリケーションのシナリオとは異なります。分散型ボイス メールが適用されますが、ルータ上の Cisco Unity Express を介して適用されます。ルータは、緊急のダイヤルとローカル ダイヤルのための Survivable Remote Site Telephony および PSTN ゲートウェイ機能を提供します。ダイヤル プランの説明に従い、WAN ベースのトール バイパス ダイヤル、およびローカルエリア ダイヤルの障害に対応するために、用途別レベルの PSTN 機能を適用することを推奨します。また、一般的に、各地域の法律では、緊急（911）ダイヤルに対応するために、何らかのローカル PSTN 接続を提供することが求められます。

このシナリオでは、WAN/CCM の停止時に、大規模な呼処理機能が必要な場合に、SRST の呼処理エージェントとして Cisco CallManager Express を適用することもできます。詳細については、「Cisco Unity Connection と Cisco Unified CME の SRST として統合」を参照してください。

シナリオのバックグラウンド

アプリケーションのシナリオには、有線電話機（音声 VLAN）、有線 PC（データ VLAN）、およびワイヤレス デバイス（IP Communicator などの VoIP デバイスを含む）が含まれています。

1. ローカル電話機とリモート CUCM クラスタ間のシグナリング インスペクション（SCCP および SIP）
2. ルータとリモート CUCM クラスタ間の H.323 シグナリングを検査します。
3. リモート サイトへのリンクがダウンし、SRST がアクティブである場合にローカルの電話機とルータ間のシグナリングを検査します。
4. 次の間における通信の音声メディア ピンホール：ローカルの有線およびワイヤレス セグメントローカルおよびリモートの電話機リモート MOH サーバとローカル電話機ボイス メール用のリモート Unity サーバおよびローカル電話機
5. Application Inspection and Control（AIC）の適用先：招待メッセージのレート制限すべての SIP トラフィックのプロトコル準拠の保証



長所/短所

このシナリオでは、管理上の負担が軽減される、呼処理の大部分が中央の Cisco CallManager クラスタで行われる点の利点が示されます。一般的に、呼処理の負担の大部分は、ルータには課せられないため、ローカルの音声リソースの検査に対するルータの負担は、このドキュメントで説明されている他のケースと比べて少なくなります。ただし、Cisco Unity Express との間でトラフィックを処理する場合、WAN または CUCM が停止している場合、およびローカルの Cisco CallManager Express/SRST が呼処理に対応するためにコールされた場合を除きます。

一般的な呼処理アクティビティ中におけるこのケースの最大の欠点は、Cisco Unity Express がローカル ルータ上に存在する点です。一方、Cisco Unity Express がボイス メールを保持しているエンドユーザの近くにある点などは、設計上の観点からは良い点ですが、管理上の負担が増し、多数の Cisco Unity Express を管理する必要が生じます。したがって、中央の Cisco Unity Express により利点をもたらすためには、中央の Cisco Unity Express をリモート ユーザから遠い位置に配置することになり、停電中にもアクセスできないようにします。そのため、リモート ロケーションへの Cisco Unity Express の導入による分散型ボイス メールの機能上の利点は、豊富な選択肢が提供される点にあります。

データ ポリシー、ゾーンベース ファイアウォール、音声セキュリティ、Cisco CallManager Express の設定

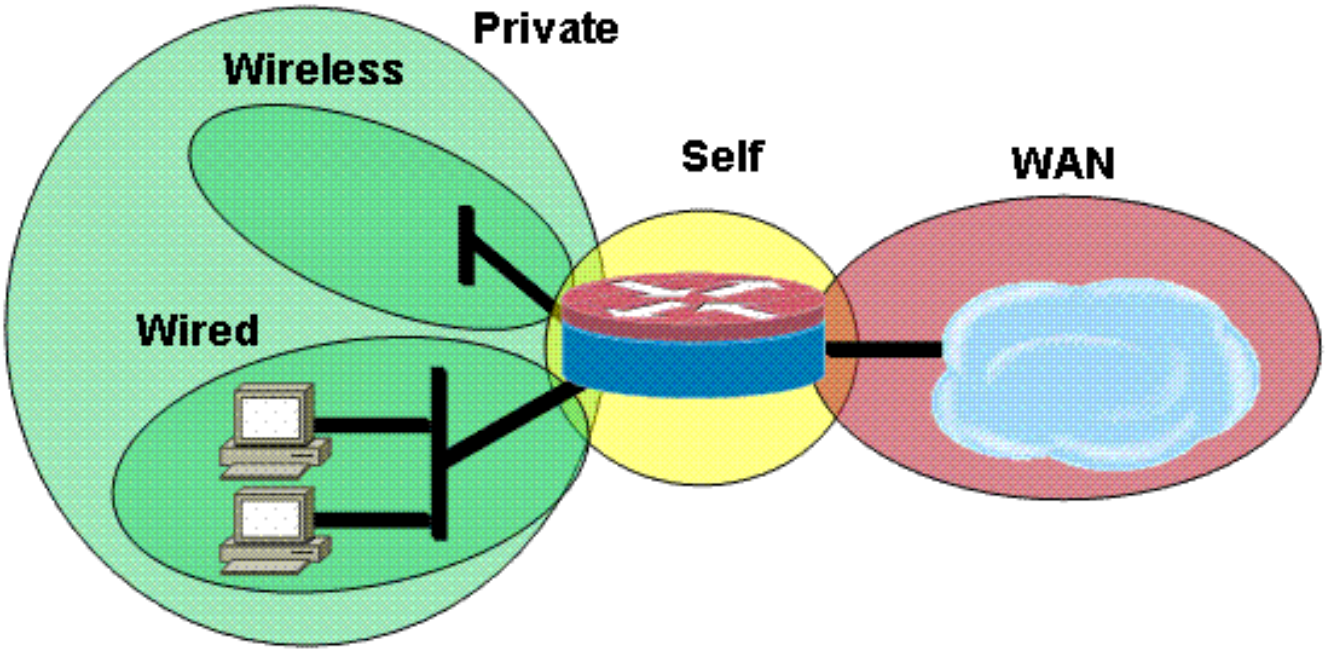
ルータ設定は、NME-X-23ES および PRI HWIC を搭載した 3845 に基づいています。

SRST および Cisco Unity Express 接続向けの音声サービスの設定：

```
!
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
!
```

これは、有線/無線 LAN セグメント、プライベート LAN のセキュリティ ゾーンで構成されたゾーンベース ポリシー ファイアウォールの設定の例です。これは、有線/無線セグメント、信頼できる WAN 接続で接続可能な WAN セグメント、およびルータの音声リソースが存在するセルフ ゾ

ーンで構成されています。



セキュリティの設定：

```
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
```

プロビジョニング、管理、およびモニタリング

ルータベースの IP テレフォニー リソースおよびゾーンベース ポリシー ファイアウォールの両方のプロビジョニングと設定は、一般的に、Cisco Configuration Professional を使用して適用するのが最適です。Cisco Secure Manager は、ゾーンベース ポリシー ファイアウォールまたはルータベースの IP テレフォニーをサポートしていません。

Cisco IOS Classic Firewall は、Cisco Unified Firewall MIB による SNMP モニタリングをサポートしています。ただし、ゾーンベース ポリシー ファイアウォールは、Unified Firewall MIB ではサポートされていません。そのため、ファイアウォールのモニタリングは、ルータのコマンドライン インターフェイス（CLI）の統計情報を用いて、または Cisco Configuration Professional など

の GUI ツールを使用して行う必要があります。

Cisco Secure Monitoring And Reporting System（CS-MARS）は、ゾーンベース ポリシー ファイアウォールに対する基本的なサポートを提供します。ただし、Cisco IOS Software Release 12.4(15)T4/T5 および Cisco IOS Software Release 12.4(20)T に実装されている、トラフィックへのログメッセージの相関関係を向上するロギングの変更は、CS-MARS では完全にはサポートされていません。

キャパシティ プランニング

India TBD のファイアウォールのコール インスペクション パフォーマンス テストの結果。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

Cisco IOS Zone Firewall には、ファイアウォールのアクティビティを表示、モニタ、およびトラブルシューティングするための **show および debug コマンドがあります。**この項では、**show コマンドを使用したファイアウォールの基本アクティビティのモニタ方法について説明し、より詳細なトラブルシューティングを行うために、またはテクニカル サポートとの話し合いにおいて詳細な情報が必要な場合に使用する** Zone Firewall の**debug コマンドを紹介します。**

トラブルシューティングのためのコマンド

注：debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

show コマンド

Cisco IOS Firewall には、セキュリティ ポリシーの設定とアクティビティを表示するための複数の **show コマンドがあります。**

show コマンドの多くは、**alias コマンドを利用することで、短いコマンドと置き換えることができます。**

デバッグ コマンド

debug コマンドは、特殊またはサポートされていない設定を使用していて、Cisco TAC または他の製品のテクニカル サポート サービスと協力して相互運用性に関する問題を解決する必要がある場合に役立ちます。

注：特定の機能またはトラフィックに**debug**コマンドを適用すると、非常に大量のコンソールメッセージが発生し、ルータのコンソールが応答しなくなる可能性があります。デバッグを有効にする必要がある場合は、端末のダイアログをモニタしない Telnet ウィンドウなどの、代替のコマンドライン インターフェイス（CLI）アクセスを提供することもできます。デバッグを有効にすると、ルータのパフォーマンスに大きな影響を及ぼすことがあるため、デバッグは、オフライン

（ラボ環境）機器に対して、または計画された保守時間枠にのみ有効にする必要があります。

関連情報

- Cisco Unified CallManager Express ソリューションのリファレンス ネットワーク設計ガイド
- Cisco Unified CallManager Express のセキュリティのベスト プラクティス
- Cisco Unity Connection と Cisco Unified CME の SRST としての統合
- Cisco Unified Communications Manager Express のコマンドリファレンス
- Cisco CallManager Express および Cisco Unity Express の設定例
- Cisco CallManager Express 3.4 SNMP MIB に関するサポート ページ
- ゾーンベース ポリシー ファイアウォールの設計と適用ガイド
- Skinny Local Traffic および CME 向けの Cisco IOS Firewall に関するサポート ページ
- Cisco IOS ファイアウォール
- テクニカル サポートとドキュメント – Cisco Systems