Cisco IOS Zone-Based ファイアウォール：HQ の CCM に対する SIP トランクがある CME/CUE/GW の 1 つの場所またはブランチ オフィス

内容

概要
前提条件
要件
使用するコンポーネント
表記法
背景説明
IOS ファイアウォールの背景説明
Cisco IOS ゾーンベース ポリシー ファイアウォールの導入
VoIP 環境内の ZFW の考慮事項
IOS ファイアウォールの音声機能
警告
ネットワーク アドレス変換（NAT）
Cisco Unified Presence Client（CUPC）
HQ または音声プロバイダーの CCM への SIP トランクがある CME/CUE/GW 単一サイトまたはブランチ オフィス
シナリオのバックグラウンド
長所/短所
設定
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、CCME の設定
ネットワーク図
設定
プロビジョニング、管理、モニタ
キャパシティ プラン
確認
トラブルシュート
トラブルシューティングのためのコマンド
関連情報

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 ネットワークとインターネット接続ネットワークに関する脅威の展望は非常に動的な情勢ではありますが、Cisco IOS® Firewall は、セキュアなネットワーク ポスチャを定義および適用するための

ステートフル インスペクション機能と Application Inspection and Control（AIC）機能を提供し、同時にビジネス遂行能力とビジネスの継続性の実現を可能にします。

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。

背景説明

IOS ファイアウォールの背景説明

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 バージョン 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。

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。*信頼の観点*と、*対照的な疑いの観点*。

*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）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します。 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不要なトラフィックのみ、より認識しやすい個別のサブセットに分類される必要があります。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て VoIP セキュリティ設定を説明します。したがって音声ネットワーク セグメントで許容されるトラフィックだけが許可されます。*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に関するその他の背景説明が必要な場合は、『ゾーン 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』を参照してください。

VoIP 環境内の ZFW の考慮事項

『ゾーン 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』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 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 ソフトウェア バージョン 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、12.4(20)T で導入された機能に大きく依存しています。

IOS ファイアウォールの音声機能

Cisco IOS Software Release 12.4(20)T では、ゾーン ファイアウォール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 CME 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 でのバージョン 3 および 4 のサポートH.323 のサポートをバージョン 3 および 4 に更新（以前のサポート バージョンは 1 と 2）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「関連情報」の項で個々の機能ドキュメントへのハイパーリンクをクリックしてください。

警告

前述のポイントを強調するために、ルータベースの音声機能を備えたCisco IOS Firewallを適用するには、ゾーンベースポリシーファイアウォールを適用する必要があります。従来のIOSファイアウォールには、シグナリングの複雑さや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。

ネットワーク アドレス変換（NAT）

Cisco IOSネットワークアドレス変換(NAT)は、Cisco IOSファイアウォールと同時に頻繁に設定されます。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する必要がある場合、または異なるプライベートネットワークが接続する必要がある場合は、IPアドレス空間が重複します。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、NATを適用しなくてもネットワーク接続を可能にします。NATは、ネットワーク接続の問題に対処する最後のケースのソリューションとしてのみ適用できます。

Cisco Unified Presence Client（CUPC）

このドキュメントでは、Cisco IOSソフトウェアリリース12.4(20)T1では、CUPCが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ないため、IOSファイアウォールでの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。

HQ または音声プロバイダーの CCM への SIP トランクがある CME/CUE/GW 単一サイトまたはブランチ オフィス

このシナリオでは、このドキュメントで前述した単一サイト/分散型コール処理/PSTN接続モデル（CME/CUE/GW単一サイトまたはPSTNに接続するブランチオフィス）と、このドキュメントで説明する3番目のシナリオで定義された複数サイト/集中型コール処理/音声およびネットワークのの間ののの間のこのシナリオでは引き続きローカルのCisco Unified CallManager Expressを使用しますが、長距離ダイヤルとHQ/リモートサイトのテレフォニーは、主にサイト間SIPトランクを介して対応し、ローカルPSTN接続を介して緊急ダイヤルします。レガシーPSTN接続の大部分が削除された場合でも、ダイヤルプランで説明されているように、WANベースのトールバイパスダイヤルとローカルエリアダイヤルの障害に対応するために、基本的なレベルのPSTN容量を推奨します。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、分散型コール処理を使用します。これにより、Cisco Unified CallManager Express SRNDで説明されている利点とベストプラクティスが得られます。

組織は、次の状況でこのタイプのアプリケーションシナリオを実装できます。

- サイト間では異なるVoIP環境が使用されますが、長距離のPSTNの代わりにVoIPが望まれます。
- ダイヤルプランの管理には、サイトごとの自律性が必要です。
- WANの可用性に関係なく、完全なコール処理機能が必要です。

シナリオのバックグラウンド

アプリケーションシナリオには、有線電話（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）が含まれます。

セキュリティ設定には、次の機能があります。

1. CMEとローカル電話（SCCPおよびSIP）およびCMEとリモートCUCMクラスタ(SIP)間のルータ開始シグナリングインスペクション。
2. 次の間の通信用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CMEとMoHのローカル電話ボイスメール用のCUEおよびローカル電話電話機およびリモートコールエンティティ
3. Application Inspection and Control（AIC；アプリケーションインスペクションおよび制御）。次の実現に適用できます。招待メッセージのレート制限すべてのSIPトラフィックでプロトコル準拠を保証

長所/短所

このアプリケーションは、WANデータリンク上でサイト間の音声トラフィックを伝送するため、コスト削減のメリットがあります。

このシナリオの欠点は、WAN接続の詳細な計画が必要になることです。サイト間コールの品質は、不正/不要なトラフィック（ワーム、ウイルス、ピアツーピアファイル共有）や、キャリアネットワークのトラフィックエンジニアリングの結果として発生する遅延の問題を特定することが困難など、WAN上の多くの要因によって影響を受けます。音声トラフィックとデータトラフィックの両方に十分な帯域幅を提供するには、WAN接続のサイズを適切に設定する必要があります。遅延の影響を受けにくいデータトラフィック（電子メール、SMB/CIFSファイルトラフィックなど）は、音声品質を維持するために、QoSの優先度の低いトラフィックとして分類できます。

このシナリオに関するもう1つの問題は、集中呼処理の欠如と、コール処理障害のトラブルシューティングで発生する可能性のある問題です。そのため、このシナリオは、中央集中型コール処理への移行の中間段階として、大規模な組織に最適です。ローカルCisco CMEは、Cisco CallManagerへの移行が完了すると、フル機能のSRSTフォールバックとして機能するように変換できます。

セキュリティの観点からは、この環境の複雑さが増すと、効果的なセキュリティの実装とトラブルシューティングが困難になります。これは、WANまたはパブリックインターネット上のVPNを介した接続が、特に信頼の観点を必要とする場合にす。このことを念頭に置いて、このドキュメントで提供する設定例では、特定のビジネスクリティカルなトラフィックを許可するより疑いのあるポリシーを実装し、次にプロトコル準拠チェックで調べます。さらに、特定のVoIPアクション、つまりSIP INVITEは、VoIPリソースとユーザビリティに悪影響を与える悪意のある、または意図しないソフトウェアの誤動作の可能性を減らすために制限されています。

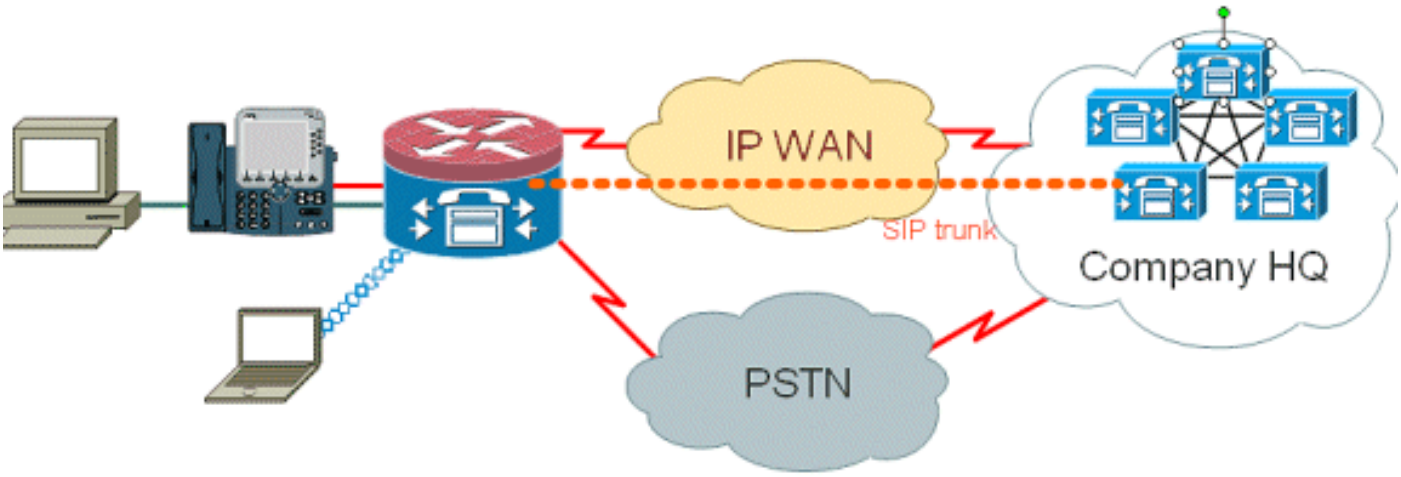
設定

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、CCME の設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



設定

ここで説明する設定は、Cisco 2851サービス統合型ルータを示しています。

このドキュメントでは、次の構成を使用します。

- CMEおよびCUE接続の音声サービス設定
- ゾーンベースポリシーファイアウォールの設定
- セキュリティ設定

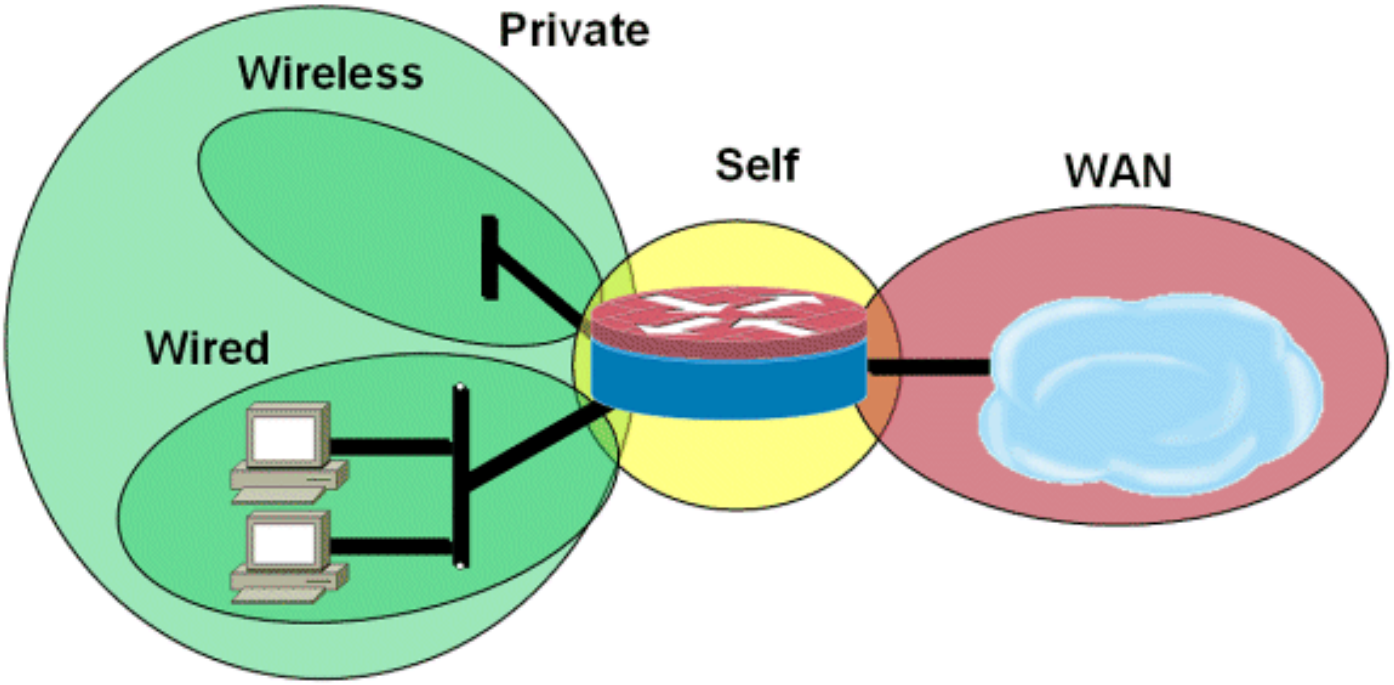
CMEおよびCUE接続の音声サービス設定を次に示します。

CMEおよびCUE接続の音声サービス設定

```
!
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、有線および無線LANセグメントのセキュリティゾーン、プライベートLAN（有線および無線セグメントで構成）、信頼できるWAN接続に到達するWANセグメント、およびルータの音声リソースが配置されるセルフゾーンで構成されるゾーンベースポリシーファイアウォール設定です。



これはセキュリティ設定です。

セキュリティ設定

```
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 2851-cme2
!
!
logging message-counter syslog
logging buffered 51200 warnings
!
no aaa new-model
clock timezone mst -7
clock summer-time mdt recurring

!
dot11 syslog
ip source-route

!
!
ip cef
no ip dhcp use vrf connected

!
ip dhcp pool pub-112-net
network 172.17.112.0 255.255.255.0
default-router 172.17.112.1
dns-server 172.16.1.22
option 150 ip 172.16.1.43
domain-name bldrtme.com

!

ip dhcp pool priv-112-net
network 192.168.112.0 255.255.255.0
default-router 192.168.112.1
dns-server 172.16.1.22
domain-name bldrtme.com
option 150 ip 192.168.112.1

!
!
ip domain name yourdomain.com

!

no ipv6 cef
multilink bundle-name authenticated

!
!
!
!

voice translation-rule 1
rule 1 // /1001/

!
!
```

```
voice translation-profile default
translate called 1

!
!

voice-card 0
no dspfarm

!
!
!
!
!

interface GigabitEthernet0/0
description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-GE 0/0$
ip address 172.16.112.10 255.255.255.0
ip nat outside
ip virtual-reassembly
duplex auto
speed auto

!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
 !
interface GigabitEthernet0/1.132
encapsulation dot1Q 132
ip address 172.17.112.1 255.255.255.0

!

interface GigabitEthernet0/1.152
encapsulation dot1Q 152
ip address 192.168.112.1 255.255.255.0
ip nat inside
ip virtual-reassembly

!

interface FastEthernet0/2/0

!

interface FastEthernet0/2/1

!

interface FastEthernet0/2/2

!

interface FastEthernet0/2/3

!

interface Vlan1
ip address 198.41.9.15 255.255.255.0

!
```

```
router eigrp 1
network 172.16.112.0 0.0.0.255
network 172.17.112.0 0.0.0.255
no auto-summary
!

ip forward-protocol nd
ip http server ip http access-class 23
ip http authentication local
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
ip http path flash:/gui

 !!

ip nat inside source list 111 interface
GigabitEthernet0/0 overload

!

access-list 23 permit 10.10.10.0 0.0.0.7
access-list 111 deny
ip 192.168.112.0 0.0.0.255 192.168.0.0 0.0.255.255
access-list 111 permit ip 192.168.112.0 0.0.0.255 any

!
!
!
!
!
!tftp-server flash:/phone/7940-7960/
P00308000400.bin alias P00308000400.bin
tftp-server flash:/phone/7940-7960/
P00308000400.loads alias P00308000400.loads
tftp-server flash:/phone/7940-7960/
P00308000400.sb2 alias P00308000400.sb2
tftp-server flash:/phone/7940-7960/
P00308000400.sbn alias P00308000400.sbn

!

control-plane

!
!
!

voice-port 0/0/0
connection plar 3035452366
description 303-545-2366
caller-id enable

!

voice-port 0/0/1 description FXO

!

voice-port 0/1/0
description FXS

!
```

```
voice-port 0/1/1 description FXS


!
!
!
!
!
dial-peer voice 804 voip
destination-pattern 5251...
session target ipv4:172.16.111.10
!
dial-peer voice 50 pots
destination-pattern A0
port 0/0/0
no sip-register

!
!
!
!

telephony-service
load 7960-7940 P00308000400
max-ephones 24
max-dn 24
ip source-address 192.168.112.1 port 2000
system message CME2
max-conferences 12 gain -6
transfer-system full-consult
create cnf-files version-stamp
7960 Jun 10 2008 15:47:13

 !!

ephone-dn 1
number 1001
trunk A0

!
!

ephone-dn 2
number 1002

!
!
ephone-dn 3
number 3035452366
label 2366
trunk A0

!
!

ephone 1
device-security-mode none
mac-address 0003.6BC9.7737
type 7960
button 1:1 2:2 3:3

!
!
!
```

```
ephone 2
device-security-mode none
mac-address 0003.6BC9.80CE
type 7960
button 1:2 2:1 3:3

!
!
!

ephone 5
device-security-mode none

!
!
!

line con 0
exec-timeout 0 0
login local
line aux 0
line vty 0 4
access-class 23 in
privilege level 15
login local
transport input telnet ssh

line vty 5 15
access-class 23 in
privilege level 15
login local
transport input telnet ssh

!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
ntp server 172.16.1.1
end
```

プロビジョニング、管理、モニタ

ルータベースのIPテレフォニーリソースと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、一般にCisco Configuration Professionalで最適です。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が、Unified Firewall MIBではゾーンベースポリシーファイアウォールはサポートされていません。したがって、ファイアウォールの監視は、ルータのコマンドラインインターフェイス(CLI)の統計情報を通じて、またはCisco Configuration ProfessionalなどのGUIツールを使用して処理する必要があります。

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の基本的なサポートを提供します。ただし、12.4(15)T4/T5および12.4(20)Tで実装されたトラフィックへのログメッセージ相関が改善された変更は、CS MARSでです。

キャパシティ プラン

インドのファイアウォールコールインスペクションパフォーマンステスト結果は未定です。

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

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、監視、およびトラブルシュートするためのshowコマンドとdebugコマンドが用意されています。このセクションでは、基本的なファイアウォールの動作を監視するためのshowコマンドの使用と、設定のトラブルシューティングやテクニカルサポートとのディスカッションで詳細情報が必要な場合のZone Firewallのdebugコマンドの概要について説明します。

トラブルシューティングのためのコマンド

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。これらのコマンドの多くは、aliasコマンドを使用することで、より短いコマンドに置き換えることができます。

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。

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またはその他の製品のテクニカルサポートサービスと連携して相互運用性の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対してdebugコマンドを適用すると、非常に多く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。デバッグが必要な場合でも、端末ダイアログをモニタしないTelnetウィンドウなどの代替コマンドラインインターフェイス(CLI)アクセスを提供できます。デバッグはルータのパフォーマンスに大きく影響する可能性があるため、デバッグはオフライン（ラボ環境）機器または計画されたメンテナンス期間内でのみ有効にしてください。

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 CallManager Express Securityのベストプラクティス(CME SRND)
- 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
- Cisco IOS Firewall：SIP の機能強化：ALG と AIC
- ソフトウェアCisco IOS Firewall H.323のサポート
- Skinny Local Traffic および CME 向けの Cisco IOS Firewall に関するサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems