目次

Cisco IOSÂ® ソフトウェア リリース 12.4(6)T はゾーン ベースのポリシー ファイアウォール（ZBPFW）を、Cisco IOS ファイアウォール機能セットのための新しい設定 モデル導入しました。 この新しい設定モデルでは、複数インターフェイスのルータで直感的に使用できるポリシー、ファイアウォール ポリシー適用の精度の増加、および望ましいトラフィックを許可する明示的なポリシーが適用されるまでファイアウォールのセキュリティ ゾーン間のトラフィックを禁止するデフォルトの deny-all ポリシーが提供されます。

ゾーン ベースのポリシー ファイアウォール（別名ゾーン ポリシー ファイアウォール、か ZFW より古いインターフェース ベース モデル（CBAC）からより適用範囲が広い、より簡単により理解されたゾーン ベースのモデルに）ファイアウォール構成を変更します。 インターフェイスはゾーンに割り当てられ、検査ポリシーはゾーン間を移動するトラフィックに適用されます。 ゾーン間ポリシーでは十分な柔軟性と精度が提供されるので、同一のルータ インターフェイスに接続された複数のホスト グループにさまざまな検査ポリシーを適用できます。

ファイアウォール ポリシーはホストのネットワークプロトコルおよびインスペクションが適用するグループのためのインスペクションを定義するために階層構造を用いる CiscoÂ® ポリシー言語で（完全な）設定されます。

前提条件

要件

Cisco は Cisco IOS$^{Â®}$ CLI の基本的な知識があることを推奨します。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco 2900 シリーズ ルータ
- IOSソフトウェアリリース 15.2(4) M2

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

Cisco IOS ファイアウォールとの WAAS サポート

Cisco IOS ファイアウォールとの WAAS （Wide Area Application Services）サポートは Cisco IOS Release 12.4(15)T で導入されました。 それは次の利点が付いているセキュリティ対応 WAN およびアプリケーション アクセラレータ ソリューションを最適化する統合ファイアウォールを提供します:

- 完全なステートフル 点検機能によって WAN を最適化します。
- 支払いカード企業（PCI）準拠性を簡素化します。
- 透過的な WAN によって加速されるトラフィックを保護します。
- WAAS ネットワークを透過的に統合。
- ネットワーク管理 機器（NME） WAE （ワイドエリア アプリケーション エンジン）モジュールかスタンドアロン WAAS デバイス配備をサポートします。

WAAS に WAE デバイスを透過的に識別するのに使用される最初の 3方向ハンドシェイクの間に TCP オプションを使用する自動ディスカバリ メカニズムがあります。 自動ディスカバリの後で、最適化されたトラフィックフロー（パス）はエンドポイントが最適化され、nonoptimized トラフィックフローの間で区別するように TCP シーケンス番号の変更を経験します。

IOSファイアウォールのための WAAS サポートは上記されるシーケンス番号でシフトに基づいてレイヤ4 インスペクションに、使用する内部 TCP 状態 変数の調整を可能にします。 トラフィックフローは正常に WAAS 自動ディスカバリを完了したことに Cisco IOS ファイアウォールが注意すれば、割り当てトラフィックフローのための最初のシーケンス番号シフト最適化されたトラフィックフローのレイヤ4 状態を維持し。

WAAS トラフィックフロー 最適化 デプロイメントシナリオ

以降のセクションはブランチ オフィス配備のための 2 つの異なる WAAS トラフィックフロー 最適化シナリオを解説しています。 WAAS トラフィックフロー 最適化は Cisco 統合サービス ルータ（ISR）の Cisco Firewall 機能を使用します。

図は下記の Cisco Firewall のエンドツーエンド WAAS トラフィックフロー 最適化の例を示します。 この特定の配備では、ネットワーク管理 機器（NME）は Cisco Firewall と同じデバイスに-WAE デバイスあります。 Web Cache Communication Protocol （WCCP）が途中受信のためのトラフィックをリダイレクトするのに使用されています。

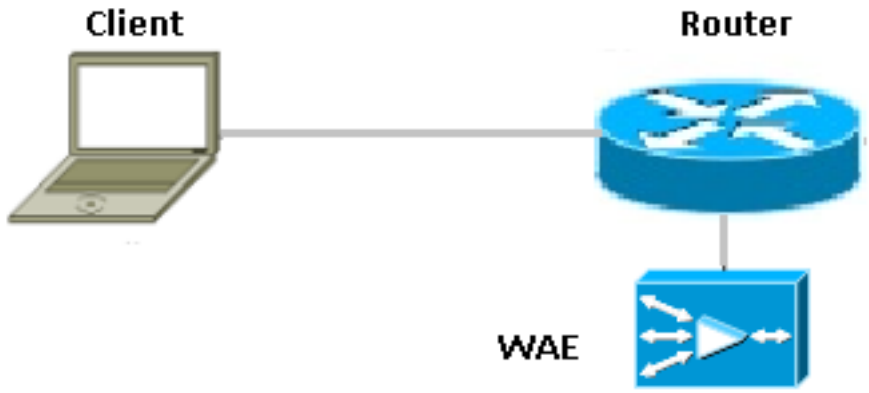
- **以外パス デバイスとの WAAS ブランチ配備**
- **インライン デバイスとの WAAS ブランチ配備**

以外パス デバイスとの WAAS ブランチ配備

ワイドエリア アプリケーション エンジン（WAE）デバイスはスタンドアロン Cisco WAN オートメーション エンジン（WAE）デバイスまたは統合サービス ルータ（ISR）でように統合サービス エンジン インストールされている Cisco WAAS ネットワークモジュール（NME-WAE）のどれで

ある場合もあります（図 ワイドエリア アプリケーションサービス[WAAS]ブランチ配備に示すように）。

図は下記の以外パスにトラフィックをリダイレクトするのに Web Cache Communication Protocol（WCCP）を使用する WAAS ブランチ配備をトラフィック途中受信のためのスタンドアロン WAE デバイス示します。 このオプションのための設定は NME-WAE の WAAS ブランチ配備同じです。

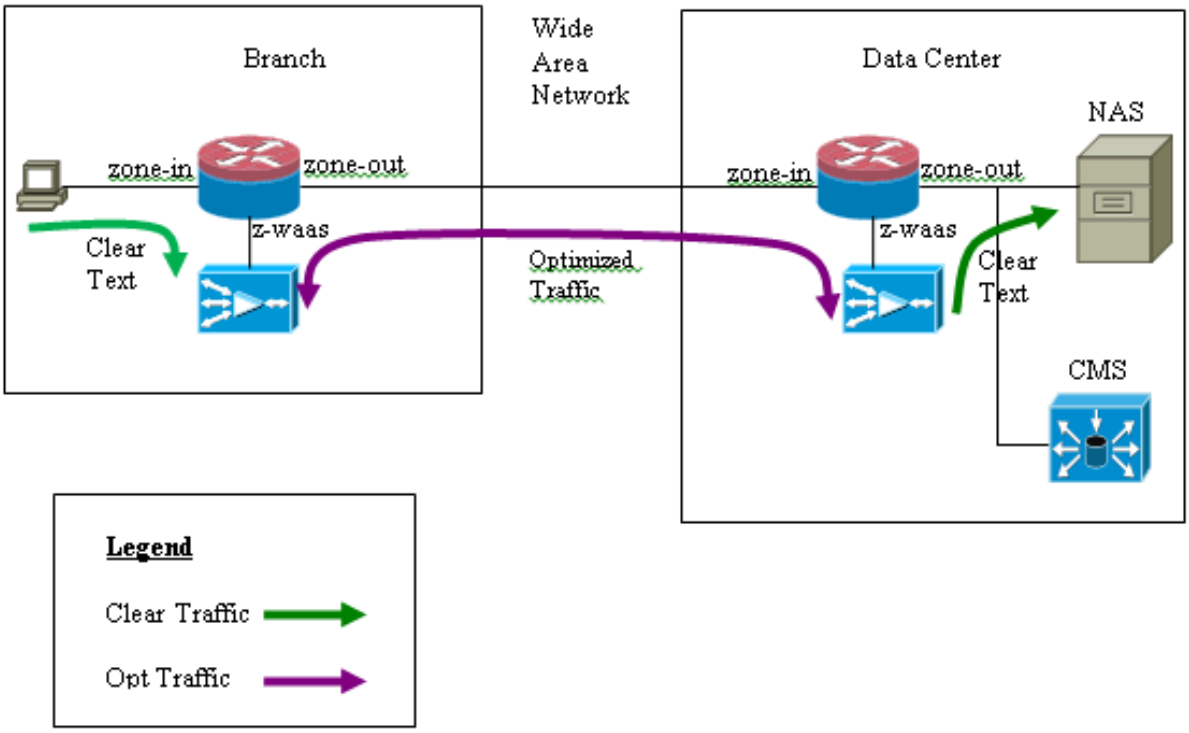


ネットワークダイアグラム例

設定およびパケットフロー

以下はエンド ツー エンド トラフィックおよび CMS のためにつく WAAS 最適化のセットアップ例を描写するダイアグラムです

（中央集中型管理 システム）サーバ端に現在です。 ブランチ端およびデータセンタ端に現在の waas モジュールはオペレーションのための CMS と登録する必要があります。 CMS がそれのために HTTPS を使用することが観察されますか。WAAS モジュールが付いている s 通信。



エンドツーエンド WAAS トラフィックフロー

次の例はトラフィック途中受信のための WAE デバイスにトラフィックをリダイレクトするのに WCCP を使用する Cisco IOS ファイアウォールにエンドツーエンド WAAS トラフィックフロー最適化 設定を提供したものです

セクション 1： IOS-FW WCCP 関連構成

```
ip wccp 61ip wccp 62ip inspect waas enable
```

セクション 2: IOS-FW ポリシー構成

```
class-map type inspect most-traffic match protocol icmp match protocol ftp match protocol tcp
match protocol udp!policy?map type inspect p1 class type inspect most?traffic  inspect class
class?default  drop
```

セクション 3: IOS-FW ゾーンおよびゾーン ペア構成

```
zone security zone-inzone security zone-outzone security z-waas zone?pair security in?out source
zone-in destination zone-outservice?policy type inspect p1zone?pair security out-in source zone-
out destination zone-inservice?policy type inspect p1
```

セクション 4: インターフェイス設定

```
interface GigabitEthernet0/0 description Trusted interface ip address 172.16.11.1 255.255.255.0
ip wccp 61 redirect in zone?member security zone-in

!interface GigabitEthernet0/1 description Untrusted interface ip address 203.0.113.1
255.255.255.0 ip wccp 62 redirect in zone?member security zone-out
```

Cisco IOS Release 12.4(20)T および 12.4(22)T の新しい設定に置き、統合されサービス エンジンを自身のゾーンにあらゆるゾーン ペアの一部である必要はありません**注意して下さい。** ゾーンペアはその間ゾーンでゾーン設定され。

```
interface Integrated?Service?Enginel/0 ip address 192.168.10.1 255.255.255.0 ip wccp redirect
exclude in zone?member security z-waas
```

Integrated?Service?Enginel/0 トラフィックで設定されるゾーン無しで次の通信筒とドロップされます:

```
*Mar 9 11:52:30.647: %FW-6-DROP_PKT: Dropping tcp session 172.16.11.59:44191 172.16.10.10:80 due
to One of the interfaces not being cfged for zoning with ip ident 0
```

CMS トラフィックフロー (中央マネージャと登録する WAAS デバイス)

次の例は下記に記載されている両方のシナリオに構成を提供したものです:

- トラフィック途中受信のための WAE デバイスにトラフィックをリダイレクトするのに WCCP を使用する Cisco IOS ファイアウォールのためのエンドツーエンド WAAS トラフィックフロー 最適化 設定
- CMS トラフィック (WAAS デバイス from/to CMS に出入して WAAS マネジメントトラフィック フロー) の許可。

セクション 1： IOS-FW WCCP 関連構成

```
ip wccp 61ip wccp 62ip inspect waas enable
```

セクション 2: IOS-FW ポリシー構成

```
class-map type inspect most-traffic match protocol icmp match protocol ftp match protocol tcp
match protocol udppolicy?map type inspect p1 class type inspect most?traffic  inspect class
class?default  drop
```

セクション 2.1: CMS トラフィックに関する IOS-FW ポリシー

クラスマップに下記の CMS トラフィックが行くようにです必要**注意して下さい。**

```
class-map type inspect waas-special match access-group 123policy-map type inspect p-waas-man
class type inspect waas-special   pass class class-default  drop
```

セクション 3: IOS-FW ゾーンおよびゾーン ペア構成

```
zone security zone-inzone security zone-outzone security z-waas zone?pair security in?out source
zone-in destination zone-outservice?policy type inspect p1zone?pair security out?in source zone-
out destination zone-inservice?policy type inspect p1
```

セクション 3.1: IOS-FW CMS 関連ゾーンおよびゾーン ペア構成

ゾーン ペア ***waas-out*** **に注意すれば waas** CMS トラフィックのために上で作成されるポリシーを適用するために必要とされます。

```
zone-pair security waas-out source z-waas destination zone-outservice-policy type inspect p-
waas-manzone-pair security out-waas source zone-out destination z-waasservice-policy type
inspect p-waas-man
```

セクション 4: インターフェイス設定

```
interface GigabitEthernet0/0
description Trusted interface
ipaddress 172.16.11.1 255.255.255.0
ip wccp 61 redirect in
zone?member security zone-in
!
interface GigabitEthernet0/1
description Untrusted interface
ip address 203.0.113.1 255.255.255.0
ip wccp 62 redirect in
zone?member security zone-out! interface Integrated?Service?Enginel/0
ip address 192.168.10.1 255.255.255.0
ip wccp redirect exclude in
```

```
zone?member security z-waas
```

セクション 5: CMS トラフィックのための Access-list

注 Access-list CMS トラフィックのために使用される。 それは CMS トラフィックが HTTPS であるので両方の方向の HTTPS トラフィックを可能にしています。

```
access-list 123 permit tcp any eq 443 anyaccess-list 123 permit tcp any any eq 443
```

ZBF セッション情報

ルータ R1 の背後にある 172.16.11.10 のユーザは 172.16.10.10 の IP アドレスのリモート エンドの後ろでホストされるファイルサーバにアクセスしています ZBF セッションは内部ゾーン ペアから構築され、その後ルータは最適化のための WAAS エンジンにパケットをリダイレクトします。

```
R1#sh policy-map type inspect zone-pair in-out sesspolicy exists on zp in-out  Zone-pair: in-out
Service-policy inspect : p1    Class-map: most-traffic (match-any)      Match: protocol icmp
0 packets, 0 bytes        30 second rate 0 bps      Match: protocol ftp        0 packets, 0
bytes        30 second rate 0 bps      Match: protocol tcp        2 packets, 64 bytes        30
second rate 0 bps      Match: protocol udp        0 packets, 0 bytes        30 second rate 0 bps
Inspect      Number of Established Sessions = 1      Established Sessions        Session
3D4A32A0 (172.16.11.10:49300)=>(172.16.10.10:445) tcp SIS_OPEN/TCP_ESTAB          Created
00:00:40, Last heard 00:00:10          Bytes sent (initiator:responder) [0:0]
```

リモートサーバにホストの中から R1-WAAS および R2-WAAS で構築されるセッション。

R1-WAAS

```
R1-WAAS#show statistics connectionCurrent Active Optimized Flows:                       1
Current Active Optimized TCP Plus Flows:          1   Current Active Optimized TCP Only Flows:
0   Current Active Optimized Single Sided Flows:      0   Current Active Optimized TCP
Preposition Flows:   0Current Active Auto-Discovery Flows:                 1Current Reserved
Flows:                              10Current Active Pass-Through Flows:
0Historical Flows:                                    13D:DRE,L:LZ,T:TCP Optimization RR:Total
Reduction RatioA:AOIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,I:ICA,M:MAPI,N:NFS,S:SSL,W:WAN
SECURE,V:VIDEO, X: SMB Signed ConnectionConnID        Source IP:Port          Dest IP:Port
PeerID Accel RR    14    172.16.11.10:49185   172.16.10.10:445 c8:9c:1d:6a:10:61 TCDL  00.0%
```

R2-WAAS

```
R2-WAAS#show statistics connectionCurrent Active Optimized Flows:                       1
Current Active Optimized TCP Plus Flows:          1   Current Active Optimized TCP Only Flows:
0   Current Active Optimized TCP Preposition Flows:   0Current Active Auto-Discovery Flows:
0Current Reserved Flows:                              10Current Active Pass-Through Flows:
0Historical Flows:                                    9D:DRE,L:LZ,T:TCP Optimization RR:Total
Reduction RatioA:AOIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,M:MAPI,N:NFS,S:SSL,V:VIDEOConnID
Source IP:Port          Dest IP:Port            PeerID Accel RR    10    172.16.11.10:49185
172.16.10.10:445 c8:9c:1d:6a:10:81 TCDL  00.0%
```

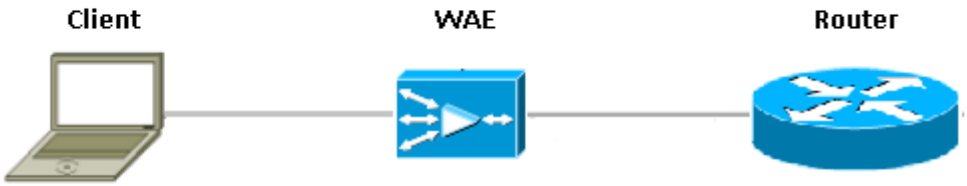
有効に なる WAAS および ZBF のクライアント側ルータ（R1）の運用コンフィギュレーション。

```
R1#sh runBuilding configuration...Current configuration : 3373 bytes!hostname R1!boot-start-
markerboot bootstrap tftp c2900-universalk9-mz.SPA.153-3.M4.bin 255.255.255.255boot system flash
c2900-universalk9-mz.SPA.153-3.M4.binboot-end-marker!ip wccp 61ip wccp 62no ipv6 cef!parameter-
map type inspect global WAAS enable log dropped-packets enable max-incomplete low 18000 max-
incomplete high 20000multilink bundle-name authenticated!license udi pid CISCO2911/K9 sn
FGL171410K8license boot module c2900 technology-package securityk9license boot module c2900
technology-package uck9license boot module c2900 technology-package datak9hw-module pvdm 0/1!hw-
module sm 1!class-map type inspect match-any most-traffic match protocol icmp match protocol ftp
match protocol tcp match protocol udp!policy-map type inspect p1 class type inspect most-traffic
inspect class class-default  drop!zone security in-zonezone security out-zonezone security waas-
```

```
zonezone-pair security in-out source in-zone destination out-zone service-policy type inspect
p1zone-pair security out-in source out-zone destination in-zone service-policy type inspect
p1!interface GigabitEthernet0/0 description Connection to IPMAN FNN N6006654R bandwidth 6000 ip
address 203.0.113.1 255.255.255.0 ip wccp 62 redirect in ip flow ingress ip flow egress zone-
member security out-zone duplex auto speed auto!interface GigabitEthernet0/1 ip address
172.16.11.1 255.255.255.0 no ip redirects no ip proxy-arp ip wccp 61 redirect in zone-member
security in-zone duplex auto speed auto!interface SM1/0 description WAAS Network Module Device
Name dciacbra01c07 ip address 192.168.10.1 255.255.255.0 ip wccp redirect exclude in service-
module ip address 192.168.183.46 255.255.255.252 !Application: Restarted at Sat Jan  5 04:47:14
2008 service-module ip default-gateway 192.168.183.45 hold-queue 60 out!end
```

インライン デバイスとの WAAS ブランチ配備

図は下記の統合サービス ルータ (ISR) の前に物理的にあるインライン ワイドエリア アプリケーション エンジン (WAE) デバイスがあるワイドエリア アプリケーションサービス (WAAS) ブランチ配備を示します。 WAE デバイスがデバイスの前にあるので、Cisco Firewall は WAAS によって最適化されるパケットを受信し、その結果、クライアント側のレイヤ7 インスペクションはサポートされません。



WAAS デバイスの間で IOSファイアウォールを実行するルータは最適化されたトラフィックだけ見ます。 最初の三方ハンドシェイク (TCP オプション 33 およびシーケンス番号シフト) およびそれのための ZBF 機能視聴は自動的に期待された TCP Sequence ウィンドウ (doesn を調節しますか。t はパケットのシーケンス番号自体を変えます)。 それは WAAS によって最適化されるセッションのための完全な L4 ステートフル ファイアウォール 機能を加えます。 WAAS 透過的なソリューションはセッション ステートフル ファイアウォールおよび QoS ポリシーごとにファイアウォールを実施します促進します。

詳細

- ファイアウォールは 0x21 オプションの正常な TCP 同期信号 パケットを見、それのためのセッションを作成します。 WCCP が複雑ではないので入力または出力インターフェイスにおいての問題がありません。帰り SYN ACK はリダイレクトされたパケットではないし、ファイアウォールはそれを書き留めます。
- ファイアウォールは SYN ACK の 0x21 オプションがあるように確認し、シーケンス番号ジャンプを必要ならば行います。 それはまた接続が最適化される場合 L7 インスペクションを消します。
- それは Router-1 シナリオとこれを区別する唯一の側面がリターントラフィックはリダイレクトされないことであること観察されるべきです。2 がありませんか。半分か。 このボックスの接続。

設定

WAAS トラフィックのための特定のゾーンのない標準 ZBF 設定。 レイヤ7 インスペクションだけサポートされません。

WAAS の ZBF インターオペラビリティのための制限

- WCCP レイヤ2 リダイレクト 方式は総称ルーティング カプセル化 (GRE) リダイレクションだけをサポートする IOSファイアウォールでサポートされません。
- IOSファイアウォールは WCCP リダイレクションだけをサポートします。 パケットをリダイ

レクトされて取得すればのに WAAS が Policy Based Routing（PBR）を使用する場合このソリューションはインターオペラビリティをそれ故にサポートされていない確保しないし。
- IOSファイアウォールは WAAS によって最適化された TCP セッションの L7 インスペクションを行いません。
- IOSファイアウォールは必要となりますか。**ip inspect waas イネーブルか。** およびか。**IP wccp は知らせますか。** WCCP リダイレクションのための CLI コマンド。
- NAT および WAAS-NM インターオペラビリティの IOSファイアウォールは現在サポートされません。
- IOSファイアウォール WAAS リダイレクションは TCP パケットにだけ適用します。
- IOSファイアウォールはアクティブ/アクティブ接続形態をサポートしません。 セッションに属するすべてのパケットは IOSファイアウォール ボックスをフローする必要があります。

関連情報

セキュリティ構成ガイド: ゾーン ベースのポリシー ファイアウォール、Cisco IOS リリース 15M&T

ゾーンベース ポリシー ファイアウォールの設計とアプリケーション ガイド