IOS： WAAS 導入によるゾーンベース ファイアウォールの相互運用性

目次

Cisco IOS® ソフトウェア リリース 12.4(6)T では、Cisco IOS Firewall フィーチャ セットの新しい設定モデルである Zone-Based Policy Firewall（ZBPFW）が導入されました。 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 ポリシー ファイアウォール（または Zone-Policy Firewall（ZFW））は、以前のインターフェイスベースのモデル（CBAC）から、より柔軟性があり、簡単に理解できるゾーンベースのモデルへとファイアウォールの設定を変更しました。 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 Cisco® Policy Language（CPL; シスコ ポリシー言語）で設定されます。CPL は、階層構造を採用して、検査が適用されるネットワーク プロトコルとホストのグループに検査を定義します。

前提条件

要件

Cisco IOS® CLI に関する基本的な知識があることが推奨されます。

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 リース 15.2(4) M2

本書の情報は、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、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

Cisco IOS ファイアウォールによる WAAS のサポート

Cisco IOS ファイアウォールによる WAAS（Wide Area Application Services）のサポートが、Cisco IOS リリース 12.4(15)T で導入されています。 これは、セキュリティ準拠 WAN とアプリケーション アクセラレーション 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、次の利点を備えています。

- フル ステートフル インスペクション機能により WAN を最適化します。
- Payment Card Industry（PCI）コンプライアンスを簡略化します。
- 透過的な WAN アクセラレーション 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します。
- ネットワーク管理機器（MME）WAE（Wide Area Application Engine）モジュールまたはスタンドアロンの WAAS デバイスの導入をサポートします。

WAAS には、初期の 3 方向ハンドシェイク中に WAE デバイスをトランスペアレントに識別するための TCP オプションを使用する自動検出メカニズムがあります。 自動検出後、最適化されたトラフィック フロー（パス）では TCP シーケンス番号が変化し、エンドポイントは最適化されたトラフィック フローと最適化されてないトラフィック フローを区別できます。

Cisco IOS ファイアウォールに関する WAAS のサポートは、上記ようなシーケンス番号のシフトに基づいて、レイヤ 4 検査に使用される内部 TCP 状態変数を調整できるようにします。 Cisco IOS ファイアウォールは、トラフィック フローが正常に WAAS 自動検出を完了したことを認識すると、トラフィック フロー用の初期シーケンス番号のシフトを許可し、最適化されたトラフィック フローのレイヤ 4 の状態を維持します。

WAAS トラフィック フロー最適化導入シナリオ

次の各項では、支店オフィス展開における 2 種類の WAAS トラフィック フロー最適化シナリオについて説明します。 WAAS トラフィック フローの最適化は、Cisco サービス統合型ルータ（ISR）の Cisco ファイアウォール機能と連動します。

下の図は、Cisco ファイアウォールを使用したエンドツーエンドの WAAS トラフィック フロー最適化の例を示しています。 この特定の導入では、ネットワーク管理機器（NME）WAE デバイスが Cisco IOS ファイアウォールと同じルータ上にあります。 Web Cache Communication Protocol（WCCP）は、傍受のためにトラフィックをリダイレクトする目的で使用されます。

- **Off-Path デバイスによる WAAS 支店の導入**
- **インライン デバイスによる WAAS 支店の導入**

Off-Path デバイスによる WAAS 支店の導入

Wide Area Application Engine（WAE）デバイスは、サービス統合型エンジンとしてサービス統合型ルータ（ISR）にインストールされているスタンドアロンの Cisco WAN Automation Engine（WAE）デバイスか、Cisco WAAS Network Module（NME-WAE）のいずれかを使用できます（Wide Area Application Service [WAAS] 支店の導入の図を参照）。

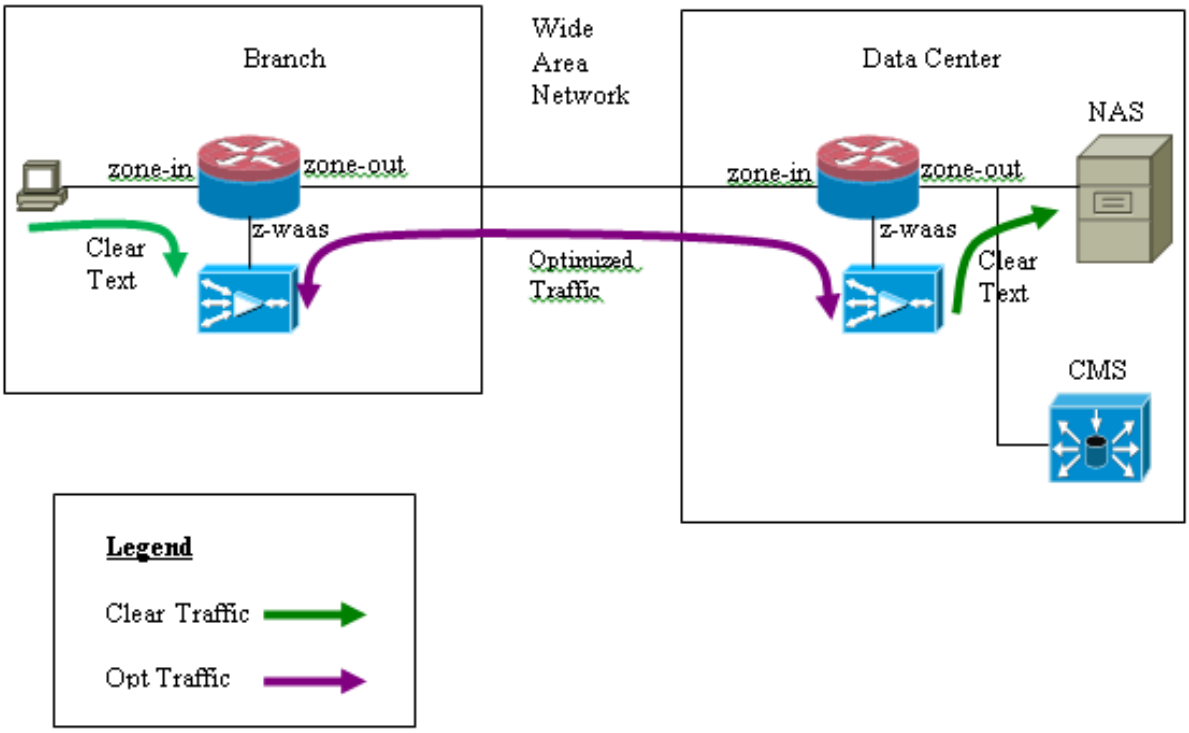
下の図は、トラフィックの代行受信のために、Web Cache Communication Protocol（WCCP）を使用してトラフィックを Off-Path スタンドアロン WAE デバイスにリダイレクトする WAAS 支店の導入例です。 このオプションの設定は、NME-WAE を使用した WAAS 支店の展開と同じです。

ネットワーク構成図のサンプル

構成およびパケット フロー

次の図は、エンドツーエンドのトラフィックとサーバ側に存在する CMS（Centralized Management System）用に

WAAS 最適化を有効にしたセットアップ例です。 支店側とデータセンター側に存在する WAAS モジュールが動作するには、CMS に登録する必要があります。 CMS は WAAS モジュールと通信するために HTTPS を使用していることがわかります。



エンドツーエンドの WAAS トラフィック フロー

次の例は、トラフィックをインターセプトするために WCCP を使用してトラフィックを WAE デバイスにリダイレクトする、Cisco IOS ファイアウォールのエンドツーエンド WAAS トラフィック フロー最適化コンフィギュレーションを示します。

セクション 1： IOS-FW WCCP 関連の設定

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

セクション 2： IOS-FW ポリシー設定

```
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の設定

```
zone security zone-in
zone security zone-out
zone security z-waas
```

```
zone—pair security in—out source zone-in destination zone-out
service—policy type inspect p1

zone—pair security out-in source zone-out destination zone-in
service—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
```

注意：この Cisco IOS Release 12.4(20)T および 12.4(22)T の新しいコンフィギュレーションは、統合サービス エンジンをその固有のゾーンに配置します。このゾーンをゾーン ペアの一部にする必要はありません。 ゾーンペアはゾーンインとゾーンアウトの間に設定されます。

```
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
```

統合サービス エンジンでゾーンが設定されていないと、I/0 トラフィックは次のドロップ メッセージとともにドロップされます。

```
*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 (Central Manager に登録する WAAS デバイス)

次の例は、以下に記載されている両方のシナリオに設定を提供します。

- トラフィックをインターセプトするために WCCP を使用してトラフィックを WAE デバイスにリダイレクトする、Cisco IOS ファイアウォールのエンドツーエンド WAAS トラフィック フロー最適化構成
- CMS トラフィックを許可 (CMS と WAAS デバイスとの間を相互に流れる WAAS 管理トラフィック) 。

セクション 1： IOS-FW WCCP 関連の設定

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

セクション 2： IOS-FW ポリシー設定

```
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 2.1： CMS のトラフィックに関連する IOS-FW ポリシー

注意：CMS トラフィックが通過できるようにするには、以下のクラスマップが必要です。

```
class-map type inspect waas-special
 match access-group 123

policy-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の設定

```
zone security zone-in
zone security zone-out
zone security z-waas

zone—pair security in—out source zone-in destination zone-out
service—policy type inspect p1

zone—pair security out—in source zone-out destination zone-in
service—policy type inspect p1
```

セクション 3.1： IOS-FW CMS 関連のゾーンおよびゾーンペア設定

注意：CMS トラフィック用に上記で作成されたポリシーを適用するには、ゾーンペア ***waas-out*** および ***out-waas*** が必要です。

```
zone-pair security waas-out source z-waas destination zone-out
service-policy type inspect p-waas-man

zone-pair security out-waas source zone-out destination z-waas
service-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 トラフィックのアクセス リスト

注意：CMS トラフィックに使用されるアクセス リスト。 CMS トラフィックは HTTPS なので、両方向の HTTPS トラフィックが許可されます。

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

ZBF セッション情報

ルータ R1 の背後にいる 172.16.11.10 のユーザは、172.16.10.10 の IP アドレスを持つリモート エンドの背後でホストされているファイル サーバにアクセスしており、ZBF セッションが in-out ゾーンペアから構築され、その後、ルータが最適化のために 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 sess

policy 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]
```

R1-WAAS および R2-WAAS で内部ホストからリモート サーバ宛てに作成されたセッション

R1-WAAS

```
R1-WAAS#show statistics connection

Current 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: 0
Current Active Auto-Discovery Flows:               1
Current Reserved Flows:                            10
Current Active Pass-Through Flows:                 0
Historical Flows:                                  13
```

```
D:DRE,L:LZ,T:TCP Optimization RR:Total Reduction Ratio
A:AOIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,I:ICA,M:MAPI,N:NFS,S:SSL,W:WAN SECURE,V:VID
EO, X: SMB Signed Connection

ConnID        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 connection

Current Active Optimized Flows:                       1
   Current Active Optimized TCP Plus Flows:           1
   Current Active Optimized TCP Only Flows:           0
   Current Active Optimized TCP Preposition Flows:    0
Current Active Auto-Discovery Flows:                  0
Current Reserved Flows:                               10
Current Active Pass-Through Flows:                    0
Historical Flows:                                     9


D:DRE,L:LZ,T:TCP Optimization RR:Total Reduction Ratio
A:AOIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,M:MAPI,N:NFS,S:SSL,V:VIDEO

ConnID        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%
```

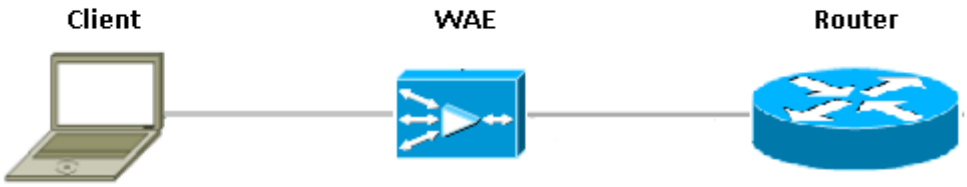
WAAS と ZBF が有効な状態のクライアント側ルータ（R1）が動作するための設定

```
R1#sh run
Building configuration...
Current configuration : 3373 bytes
!
hostname R1
!
boot-start-marker
boot bootstrap tftp c2900-universalk9-mz.SPA.153-3.M4.bin 255.255.255.255
boot system flash c2900-universalk9-mz.SPA.153-3.M4.bin
boot-end-marker
!
ip wccp 61
ip wccp 62
no ipv6 cef
!
parameter-map type inspect global
 WAAS enable
 log dropped-packets enable
 max-incomplete low 18000
 max-incomplete high 20000
multilink bundle-name authenticated
!
license udi pid CISCO2911/K9 sn FGL171410K8
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
license boot module c2900 technology-package datak9
hw-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-zone
zone security out-zone
zone security waas-zone
zone-pair security in-out source in-zone destination out-zone
 service-policy type inspect p1
zone-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 デバイスによる WAAS 支店の導入

下の図は、サービス統合型ルータ（ISR）の前に物理的に設置されるインライン Wide Area Application Engine（WAE）デバイスを使用する Wide Area Application Service（WAAS）支店の展開例です。 WAE デバイスがデバイスの前にあるため、Cisco ファイアウォールは WAAS 最適化パケットを受信し、その結果、クライアント側のレイヤ 7 検査はサポートされません。



WAAS デバイス間で IOS ファイアウォールを実行しているルータは、最適化されたトラフィックのみを感知します。 ZBF 機能は最初の 3 ウェイ ハンドシェイク（TCP オプション 33 およびシーケンス番号のシフト）を監視し、予想される TCP シーケンス ウィンドウを自動調整します（パケット自体内のシーケンス番号を変更しません）。 これにより、WAAS 最適化セッションにフル L4 ステートフル ファイアウォール機能が適用されます。 WAAS の透過的ソリューションは、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強制を促進します。

詳細

- ファイアウォールは、通常の 0x21 オプション付きの TCP SYN パケットを感知し、そのセッションを作成します。 WCCP が関与していないので、入力または出力インターフェイスの問題は存在しません。リターン SYN-ACK は、リダイレクトされたパケットではなく、ファイアウォールはそのことに留意します。
- ファイアウォールが SYN-ACK で 0x21 オプションをチェックし、必要に応じて、シーケンス番号のジャンプを実行します。 また、接続が最適化されている場合、L7 検査もオフにします。
- ルータ 1 のシナリオと、このシナリオを区別する唯一の側面は、リターン トラフィックがリダイレクトされないことが認められます。このボックスには 2 つの「ハーフ」接続は存在しません。

設定

WAAS トラフィック用の特定のゾーンがない標準 ZBF 構成。 レイヤ 7 検査のみサポートされません。

WAAS との ZBF の相互運用性に関する制約事項

- IOS ファイアウォールでは、WCCP レイヤ 2 リダイレクト方式はサポートされていません。Generic Routing Encapsulation（GRE）のみサポートされています。
- IOS ファイアウォールは WCCP リダイレクションのみサポートします。 WAAS がポリシーベース ルーティング（PBR）を使用してパケットをリダイレクトさせる場合、このソリューションでは相互運用性は保証されず、したがって、サポートされません。
- IOS ファイアウォールは、WAAS 最適化 TCP セッションでは L7 検査を実行しません。
- IOS ファイアウォールは、WCCP リダイレクションに「**ip inspect waas enable**」および「**ip wccp notify**」CLI コマンドを必要とします。
- NAT と WAAS-NM の相互運用性を持つ IOS ファイアウォールは、現時点ではサポートされていません。
- IOS ファイアウォール WAAS リダイレクトは、TCP パケットのみに適用されます。
- IOS ファイアウォールは、アクティブ/アクティブ トポロジをサポートしません。 ある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 ボックスを通って流れる必要があります。

関連情報

セキュリティの設定ガイド： ゾーンベース 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適用ガイド