WAAS導入によるCisco IOSゾーンベースファイアウォールの相互運用性の設定

内容

概要

このドキュメントでは、Cisco IOS® Firewallフィーチャセットの新しい設定モデルについて説明します。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。

前提条件

要件

Cisco IOS® CLIに関する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いています。

- Cisco 2900 シリーズ ルータ
- Cisco 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ました。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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

ゾーンベースポリシーファイアウォール（ゾーンポリシーファイアウォール、ZFW、またはZBFとも呼ばれる）は、ファイアウォール設定を古いインターフェイスベースモデル(CBAC)から、より柔軟で理解しやすいゾーンベースモデルに変更します。インターフェイスはゾーンに割り当てられ、インスペクション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)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の検査とホストのグループを定義します。

Cisco IOS®ファイアウォールによるWAASサポート

Cisco IOS®ファイアウォールでのWide Area Application Services(WAAS)のサポートは、Cisco IOS®リリース12.4(15)Tで導入されました。セキュリティに準拠したWANおよびアプリケーション高速化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、次のメリットを提供します。

- 完全なステートフルインスペクション機能によりWANを最適化
- Payment Card Industry(PCI)コンプライアンスの簡素化
- 透過的なWAN高速化トラフィックを保護
- WAASネットワークを透過的に統合
- Network Management Equipment(NME)Wide Area Application Engine(WAE)モジュールまたはスタンドアロンのWAASデバイス導入をサポート

WAASには、WAEデバイスを透過的に識別するために使用される最初の3ウェイハンドシェイク中に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、エンドポイントが最適化されたトラフィックフローと非最適化のトラフィックフローを区別できるように、TCPシーケンス番号が変更されます。

IOS®ファイアウォールに対するWAASのサポートにより、前述のシーケンス番号の変化に基づいて、レイヤ4検査に使用される内部TCP状態変数を調整できます。Cisco IOS®ファイアウォールは、トラフィックフローがWAAS自動検出を正常に完了したことを検出すると、トラフィックフロー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でレイヤ4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

このセクションでは、ブランチオフィスの導入に関する2つの異なる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。

この図は、シスコ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、NME-WAEデバイスはシスコファイアウォールと同じデバイス上にあります。Web Cache Communication Protocol(WCCP)は、トラフィックを代行受信にリダイレクトするために使用されます。

- 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

オフパスデバイスによるWAASブランチ導入

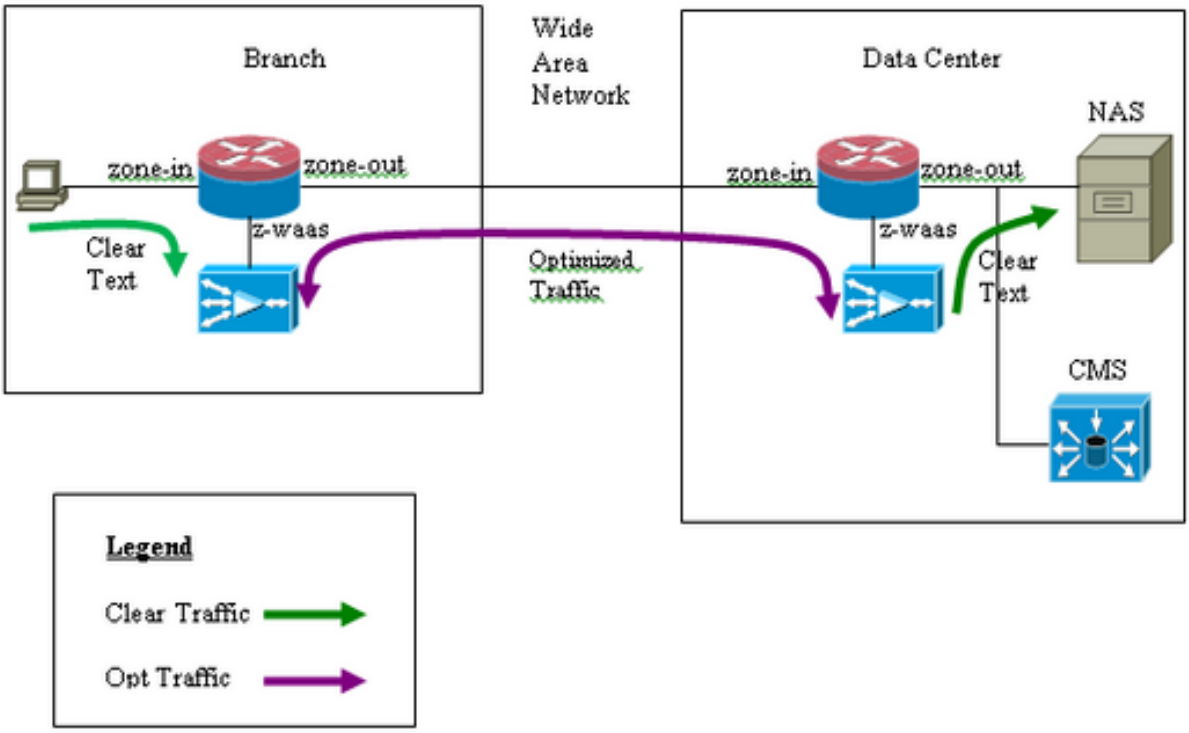
WAEデバイスは、スタンドアロンのCisco WAN Automation Engine(WAE)デバイスか、統合サービスエンジンとしてISRにインストールされるCisco WAAS Network Module(NME-WAE)のいずれかになります。

図は、トラフィックを代行受信のためにオフパスのスタンドアロンWAEデバイスにトラフィックをリダイレクトするためにWCCPを使用するWAASブランチ展開を示しています。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。

ネットワーク図

構成およびパケット フロー

次の図は、サーバの終端にあるエンドツーエンドのトラフィックと中央集中型の管理システム(CMS)のWAAS最適化をオンにした設定例を示しています。ブランチ側とデータセンター(DC)側にあるWAASモジュールは、CMSに登録して運用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

この例では、トラフィックを代行受信のためにWAEデバイスにトラフィックをリダイレクトするためにWCCPを使用する、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設定を示します。

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ポリシーの設定：

```
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ゾーンとゾーンペアの設定：

```
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：**Cisco IOS®リリース12.4(20)Tおよび12.4(22)Tの新しい設定では、統合サービスエンジンが独自のゾーンに配置されるため、ゾーンペアの一部であ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
```

Integrated—Service—Engine/0にゾーンが設定されていない場合、トラフィックは次のドロップメッセージでドロップされます。

```
*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、リストされている両方のシナリオの設定を示しています。

- トラフィックを代行受信のためにWAEデバイスにトラフィックをリダイレクトするためにWCCPを使用する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設定
- CMSトラフィックの許可（CMSデバイスとの間で送受信される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ポリシーの設定：

```
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トラフィックに関連するIOS-FWポリシー：

注：CMSトラフィックが通過できるようにするには、次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ゾーンとゾーンペアの設定：

```
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の設定：

注：ゾーンペアのwaas-out**とout-waasは、CMSトラフィック用に**作成されたポリシーを適用するために必要です。

```
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：**CMSトラフィックに使用されるアクセスリスト。CMSトラフィックがHTTPSであるため、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172.16.11.10のユーザは、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IPアドレス172.16.10.10でアクセスし、ZBFセッションはインアウトゾーンペアから構築された後、ルータは最適化のために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%
```

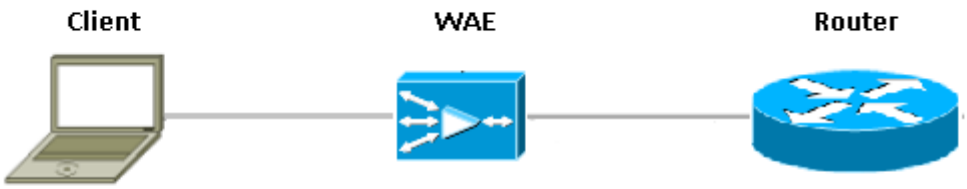
WAASおよびZBFが有効なクライアント側ルータ(R1)の動作設定

```
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を使用したWAASブランチ導入

図は、ISRの前に物理的にインラインWAEデバイスがあるWAASブランチの展開を示しています。WAEデバイスは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Cisco 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のみを認識します。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とシーケンス番号シフト）を監視し、予想されるTCPシーケンスウィンドウを自動的に調整します（パケット自体のシーケンス番号は変更しません）。 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。
- ファイアウォールは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つのハーフコネクションはありません。

コンフィギュレーション

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検査だけがサポートされていません。

WAAS との ZBF の相互運用性に関する制約事項

- WCCPレイヤ2リダイレクト方式は、Cisco IOS®ファイアウォールではサポートされておらず、Generic Routing Encapsulation(GRE)リダイレクションのみをサポートしています。
- Cisco IOS®ファイアウォールは、WCCPリダイレクションのみをサポートします。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のリダイレクトを取得する場合、このソリューションでは相互運用性が保証されないため、サポートされていません。
- Cisco IOS®ファイアウォールは、WAAS最適化TCPセッションでL7検査を実行しません。
- Cisco IOS®ファイアウォールでは、WCCPリダイレクションに**ip inspect waas enable**コマンドと**ip wccp notify** CLIコマンドが必要です。
- NATおよびWAAS-NMの相互運用性を備えたCisco IOS®ファイアウォールは、現在サポートされていません。

- Cisco IOS®ファイアウォールWAASリダイレクションは、TCPパケットにのみ適用されます。
- Cisco 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ていません。
- セッションに属するすべてのパケットは、Cisco IOS®ファイアウォールボックスを通過する必要があります。

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

現在、この設定に関する特定のトラブルシューティング情報はありません。

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
- テクニカル サポートとドキュメント – Cisco Systems