Konfigurieren der Cisco IOS Zone-basierten Firewall-Interoperabilität mit WAAS-Bereitstellung

Inhalt

Einführung

Dieses Dokument beschreibt ein neues Konfigurationsmodell für die Cisco IOS® Firewall-Funktionen. Dieses neue Konfigurationsmodell bietet intuitive Richtlinien für Router mit mehreren Schnittstellen, eine größere Granularität der Anwendung von Firewall-Richtlinien und eine standardmäßige Richtlinie zur vollständigen Verweigerung (deny all), die den Datenverkehr zwischen Firewall-Sicherheitszonen untersagt, bis eine explizite Richtlinie angewendet wird, um den wünschenswerten Datenverkehr zu ermöglichen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse der Cisco IOS® CLI zu verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Router der Serie 2900
- Cisco IOS® Softwareversion 15.2(4) M2

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Zonenbasierte Richtlinien-Firewall (auch als Zone-Policy Firewall, ZFW oder ZBF bezeichnet) ändert die Firewall-Konfiguration vom älteren, schnittstellenbasierten Modell (CBAC) in ein flexibleres, besser verständliches zonenbasiertes Modell. Schnittstellen werden Zonen zugewiesen, und die Überprüfungsrichtlinie wird auf Datenverkehr angewendet, der zwischen den Zonen fließt. Zonenübergreifende Richtlinien bieten beträchtliche Flexibilität und Präzision, sodass unterschiedliche Inspektionsrichtlinien auf mehrere Hostgruppen angewendet werden können, die mit derselben Router-Schnittstelle verbunden sind. Firewall-Richtlinien werden mit der Cisco® Policy Language (CPL) konfiguriert, die eine hierarchische Struktur verwendet, um die Prüfung für Netzwerkprotokolle und die Hosts festzulegen, auf die die Überprüfung angewendet wird.

WAAS-Unterstützung mit Cisco IOS® Firewall

WAAS-Unterstützung (Wide Area Application Services) mit der Cisco IOS® Firewall wurde in Cisco IOS® Version 12.4(15)T eingeführt. Sie bietet eine integrierte Firewall, die sicherheitskonforme WANs und Lösungen zur Anwendungsbeschleunigung optimiert und dabei folgende Vorteile bietet:

- Optimierung eines WAN durch vollständige Stateful Inspection-Funktionen
- Vereinfacht die PCI-Konformität (Payment Card Industry)
- Schutz von transparentem WAN-beschleunigtem Datenverkehr
- Transparente Integration von WAAS-Netzwerken
- Unterstützt die Network Management Equipment (NME) Wide Area Application Engine (WAE)-Module oder die Standalone-Bereitstellung von WAAS-Geräten

WAAS verfügt über einen automatischen Erkennungsmechanismus, der während des ersten Drei-Wege-Handshakes TCP-Optionen verwendet, um WAE-Geräte transparent zu identifizieren. Nach der automatischen Erkennung verändern sich bei optimierten Datenverkehrsflüssen (Pfaden) die TCP-Sequenznummern, sodass die Endpunkte zwischen optimierten und nicht optimierten Datenverkehrsflüssen unterscheiden können.

Die WAAS-Unterstützung für die IOS®-Firewall ermöglicht die Anpassung interner TCP-Statusvariablen, die für die Layer-4-Überprüfung verwendet werden, basierend auf der Verschiebung in der zuvor erwähnten Sequenznummer. Wenn die Cisco IOS®-Firewall feststellt, dass ein Datenverkehrsfluss die automatische WAAS-Erkennung erfolgreich abgeschlossen hat, ermöglicht sie die Verschiebung der anfänglichen Sequenznummer für den Datenverkehrsfluss und erhält den Layer-4-Status im optimierten Datenverkehrsfluss aufrecht.

Bereitstellungsszenarien für die Optimierung des WAAS-Datenverkehrs

In den Abschnitten werden zwei verschiedene Szenarien zur Optimierung des WAAS-Datenverkehrsflusses bei Bereitstellungen in Zweigstellen beschrieben. Die Optimierung des WAAS-Datenverkehrsflusses funktioniert mit der Cisco Firewall-Funktion auf einem Cisco Integrated Services Router (ISR).

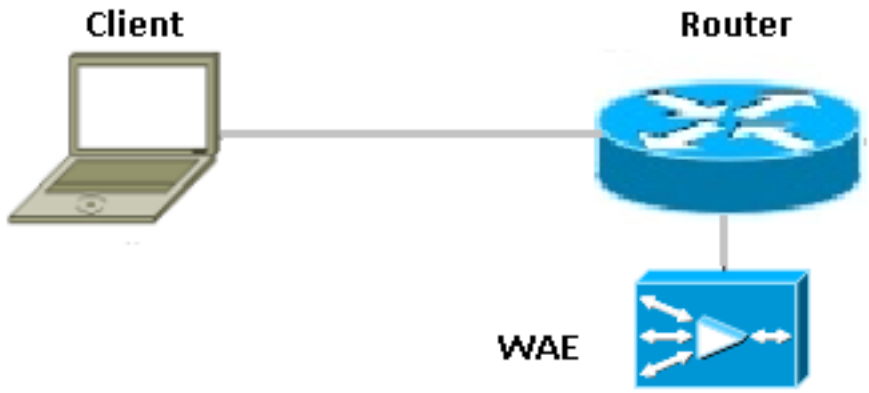
Die Abbildung zeigt ein Beispiel für eine End-to-End-Optimierung des WAAS-Datenverkehrsflusses mit der Cisco Firewall. In dieser speziellen Bereitstellung befindet sich ein NME-WAE-Gerät auf demselben Gerät wie die Cisco Firewall. Das Web Cache Communication Protocol (WCCP) wird verwendet, um den Datenverkehr zur Abhörung umzuleiten.

- WAAS-Zweigstellenbereitstellung mit einem Off-Path-Gerät
- WAAS-Zweigstellenbereitstellung mit einem Inline-Gerät

WAAS-Zweigstellenbereitstellung mit Off-Path-Gerät

Ein WAE-Gerät kann entweder ein eigenständiges Cisco WAN Automation Engine (WAE)-Gerät oder ein Cisco WAAS Network Module (NME-WAE) sein, das auf einem ISR als Integrated Service Engine installiert ist.

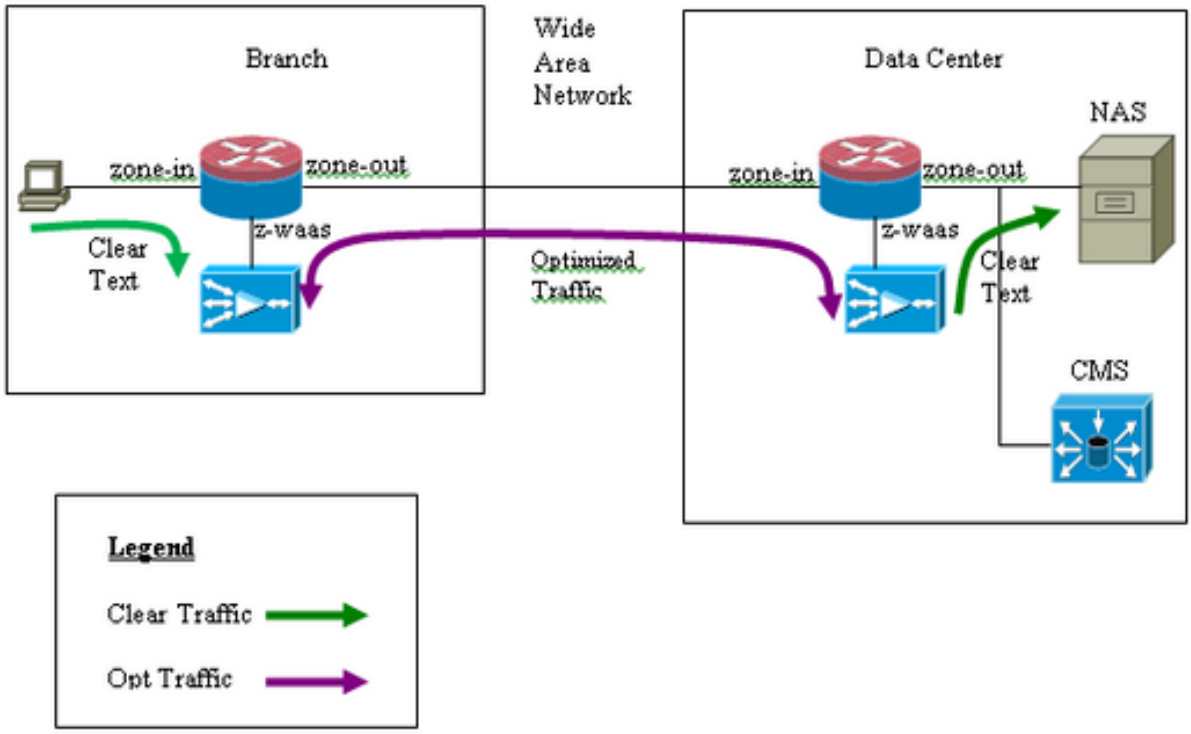
Die Abbildung zeigt eine WAAS-Zweigstellenbereitstellung, die WCCP verwendet, um den Datenverkehr an ein eigenständiges WAE-Gerät für das Abfangen des Datenverkehrs auf einem externen Pfad umzuleiten. Die Konfiguration für diese Option entspricht der Bereitstellung in der WAAS-Zweigstelle mit einer NME-WAE.



Netzwerkdiagramm

Konfiguration und Paketfluss

Dieses Diagramm zeigt eine Beispieleinrichtung mit aktivierter WAAS-Optimierung für End-to-End-Datenverkehr und zentralisiertes Management-System (CMS), das am Serverende vorhanden ist. Die WAAS-Module am Zweigstellen- und am Rechenzentrums-Ende müssen beim CMS registriert werden. Es wird beobachtet, dass das CMS HTTPS für die Kommunikation mit den WAAS-Modulen verwendet.



End-to-End-WAAS-Datenverkehrsfluss

Das Beispiel hier zeigt eine End-to-End-Konfiguration zur Optimierung des WAAS-Datenverkehrs für die Cisco IOS®-Firewall, die WCCP verwendet, um den Datenverkehr zur Überwachung des Datenverkehrs an ein WAE-Gerät umzuleiten.

Abschnitt 1: Konfiguration im Zusammenhang mit IOS-FW WCCP:

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

Abschnitt 2: IOS-FW-Richtlinienkonfiguration:

```
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
```

Abschnitt 3. IOS-FW Zone- und Zonenpaar-Konfiguration:

```
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
```

Abschnitt 4. Schnittstellenkonfiguration:

```
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
```

> **Hinweis**: Durch die neue Konfiguration in Cisco IOS® Version 12.4(20)T und 12.4(22)T befindet sich die Integrated-Service-Engine in einer eigenen Zone und muss nicht Teil eines Zonenpaars sein. Die Zonenpaare werden zwischen Zoneneingabe und Zonenausgang konfiguriert.

```
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
```

Wenn keine Zone für Integrated - Service - Enginel/0 konfiguriert ist, wird der Datenverkehr mit dieser Drop-Meldung verworfen:

```
*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-Datenverkehrsfluss (Registrierung von WAAS-Geräten beim Central Manager)

Das Beispiel hier zeigt die Konfiguration für die beiden folgenden Szenarien:

- End-to-End-Konfiguration zur Optimierung des WAAS-Datenverkehrs für die Cisco IOS® Firewall, die WCCP verwendet, um den Datenverkehr zur Überwachung des Datenverkehrs an ein WAE-Gerät umzuleiten
- Zulassen des CMS-Datenverkehrs (WAAS-Management-Datenverkehr, der von/zu WAAS-Geräten zum/vom CMS fließt)

Abschnitt 1: Konfiguration im Zusammenhang mit IOS-FW WCCP:

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

Abschnitt 2: IOS-FW-Richtlinienkonfiguration:

```
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
```

Abschnitt 2.1. IOS-FW-Richtlinie für CMS-Datenverkehr:

> **Hinweis**: Die Klassenzuordnung wird hier benötigt, damit der CMS-Datenverkehr durchlaufen kann:

```
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
```

Abschnitt 3. IOS-FW Zone- und Zonenpaar-Konfiguration:

```
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
```

Abschnitt 3.1. IOS-FW CMS-bezogene Zone- und Zonenpaar-Konfiguration:

> **Hinweis**: Die Zonenpaare **WAAS-Out** und **Out-WAAS** sind erforderlich, um die zuvor für den CMS-Datenverkehr erstellte Richtlinie anzuwenden.

```
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
```

Abschnitt 4. Schnittstellenkonfiguration:

```
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
```

Abschnitt 5. Zugriffsliste für CMS-Datenverkehr.

> **Hinweis**: Zugriffsliste für CMS-Datenverkehr. Es ermöglicht HTTPS-Datenverkehr in beide Richtungen, da der CMS-Datenverkehr HTTPS ist.

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

Informationen zu ZBF-Sitzungen

Benutzer mit der Nummer 172.16.11.10 hinter Router R1 greift auf den hinter dem Remote-Ende gehosteten Dateiserver mit der IP-Adresse 172.16.10.10 zu. Die ZBF-Sitzung wird aus dem In-Out-Zonenpaar aufgebaut. Anschließend leitet der Router das Paket zur Optimierung an die WAAS-Engine weiter.

```
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]
```

Integrierte Sitzung für R1-WAAS und R2-WAAS vom internen Host zum Remote-Server.

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%
```

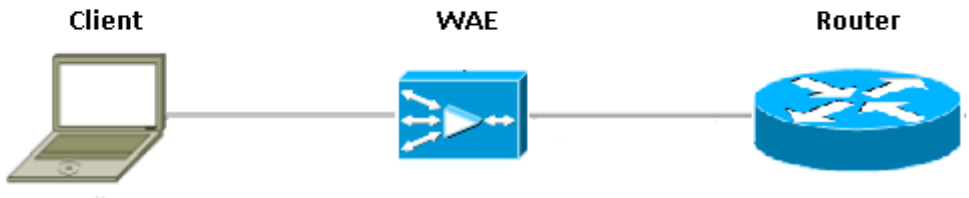
Konfiguration des Client Side Router (R1) mit aktivierter WAAS- und ZBF-Funktion

```
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
```

WAAS-Zweigstellenbereitstellung mit Inline-Gerät

Die Abbildung zeigt eine WAAS-Zweigstellenbereitstellung, bei der ein Inline-WAE-Gerät direkt vor dem ISR installiert ist. Da sich das WAE-Gerät vor dem Gerät befindet, erhält die Cisco Firewall für WAAS optimierte Pakete. Daher wird die Layer-7-Überprüfung auf Client-Seite nicht unterstützt.



Der Router, der die Cisco IOS® Firewall zwischen WAAS-Geräten ausführt, erkennt nur optimierten Datenverkehr. Die ZBF-Funktion überwacht den ersten Drei-Wege-Handshake (TCP-Option 33 und die Sequenznummer-Verschiebung) und passt automatisch das erwartete TCP-Sequenzfenster an (ändert nicht die Sequenznummer im Paket selbst). Es wendet vollständige L4 Stateful Firewall-Funktionen für WAAS-optimierte Sitzungen an. Die transparente WAAS-Lösung vereinfacht die Durchsetzung von Firewall- und QoS-Richtlinien pro Sitzung.

Details

- Die Firewall erkennt ein normales TCP-SYN-Paket mit der Option 0x21 und erstellt eine Sitzung für dieses Paket. Es gibt keine Probleme mit der Eingabe- oder Ausgabeschnittstelle, da WCCP nicht beteiligt ist. Die SYN-ACK-Rücksendung ist kein umgeleitetes Paket und die Firewall nimmt davon Kenntnis.
- Die Firewall sucht in der SYN-ACK nach der Option 0x21 und führt ggf. die Sequenznummern-Sprung aus. Wenn die Verbindung optimiert ist, wird auch die L7-Prüfung deaktiviert.
- Es ist zu beachten, dass der einzige Aspekt, der dies vom Router-1-Szenario unterscheidet,

darin besteht, dass der Rückverkehr nicht umgeleitet wird. Es sind keine zwei halben Anschlüsse auf diesem Gerät vorhanden.

Konfiguration

Standard-ZBF-Konfiguration ohne spezielle Zone für WAAS-Datenverkehr. Es wird keine Layer-7-Inspektion unterstützt.

Einschränkungen für die ZBF-Interoperabilität mit WAAS

- Die WCCP-Umleitungsmethode für Layer 2 wird von der Cisco IOS®-Firewall nicht unterstützt. Sie unterstützt nur die Umleitung über Generic Routing Encapsulation (GRE).
- Die Cisco IOS® Firewall unterstützt nur die WCCP-Umleitung. Wenn WAAS Policy Based Routing (PBR) verwendet, um die Pakete umzuleiten, gewährleistet diese Lösung NICHT die Interoperabilität und damit auch nicht die Unterstützung.
- Die Cisco IOS® Firewall führt keine L7-Prüfung für WAAS-optimierte TCP-Sitzungen durch.
- Die Cisco IOS®-Firewall erfordert **ip inspect waas enable** und **ip wccp notify-**CLI-Befehle für die WCCP-Umleitung.
- Die Cisco IOS®-Firewall mit NAT- und WAAS-NM-Interoperabilität wird derzeit nicht unterstützt.
- Die WAAS-Umleitung für die Cisco IOS® Firewall wird nur für TCP-Pakete angewendet.
- Die Cisco IOS®-Firewall unterstützt keine Aktiv/Aktiv-Topologien.
- Alle Pakete, die zu einer Sitzung gehören, MÜSSEN über die Cisco IOS® Firewall-Box geleitet werden.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Leitfaden zur Sicherheitskonfiguration: Zonenbasierte Firewall, Cisco IOS-Version 15M&T
- Firewall-Design und Anwendungshandbuch für zonenbasierte Richtlinien
- Technischer Support und Dokumentation - Cisco Systems