配置與WAAS部署的Cisco IOS基於區域的防火牆互操作性

目錄

簡介

本檔案介紹Cisco IOS®防火牆功能集的新組態模式。此新配置模型為多介面路由器提供了直觀的策略，提高了防火牆策略應用的粒度，並提供了預設的deny-all策略，該策略在應用顯式策略以允許所需流量之前禁止防火牆安全區域之間的流量。

必要條件

需求

Cisco建議您瞭解Cisco IOS® CLI。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco 2900系列路由器

- Cisco IOS®軟體版本15.2(4)M2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

基於區域的策略防火牆（也稱為區域策略防火牆、ZFW或ZBF）將防火牆配置從舊的基於介面的模型(CBAC)更改為更靈活、更易於理解的基於區域的模型。介面分配給區域，檢查策略應用於在區域之間移動的流量。區域間策略提供了相當大的靈活性和精細度，因此可以將不同的檢查策略應用於連線到同一路由器介面的多個主機組。防火牆策略使用Cisco®策略語言(CPL)進行配置，該語言採用分層結構，以定義對網路協定以及應用檢查的主機組的檢查。

Cisco IOS®防火牆的WAAS支援

Cisco IOS®防火牆的廣域應用程式服務(WAAS)支援是在Cisco IOS®版本12.4(15)T中匯入。它提供整合防火牆，可最佳化符合安全要求的廣域網和應用加速解決方案，並具有以下優勢：

- 通過全面的狀態檢測功能最佳化WAN
- 簡化支付卡行業(PCI)合規性
- 保護透明的WAN加速流量
- 透明整合WAAS網路
- 支援網路管理裝置(NME)廣域應用引擎(WAE)模組或獨立WAAS裝置部署

WAAS具有自動發現機制，在初始三次握手期間使用TCP選項來透明地識別WAE裝置。自動發現後，最佳化流量流（路徑）會遇到TCP序列號的變化，以便使端點能夠區分最佳化流量和非最佳化流量。

IOS®防火牆的WAAS支援允許根據前面提到的序列號變化調整用於第4層檢測的內部TCP狀態變數。如果Cisco IOS®防火牆注意到流量已成功完成WAAS自動發現，它允許流量流的初始序列號偏移，並保持最佳化流量流的第4層狀態。

WAAS流量最佳化部署方案

本節介紹兩種不同的WAAS流量最佳化方案，用於分支機構部署。WAAS流量最佳化與Cisco整合多業務路由器(ISR)上的Cisco防火牆功能配合使用。

圖中顯示了使用Cisco防火牆進行端到端WAAS流量最佳化的示例。在此特定部署中，NME-WAE裝置與思科防火牆位於同一裝置上。網路快取通訊協定(WCCP)用於重新導向流量以進行偵聽。

- 帶脫離路徑裝置的WAAS分支部署
- 帶內聯裝置的WAAS分支部署

帶脫離路徑裝置的WAAS分支部署

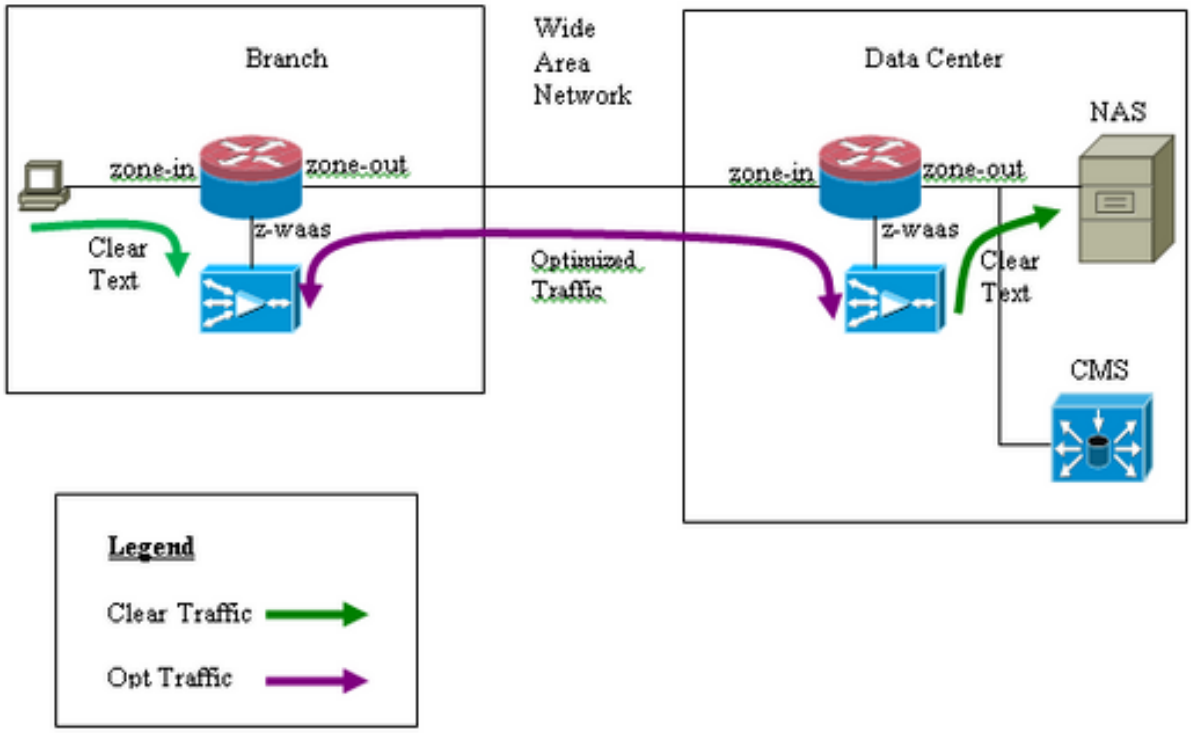
WAE裝置可以是獨立的Cisco WAN自動化引擎(WAE)裝置，也可以是作為整合服務引擎安裝在ISR上的Cisco WAAS網路模組(NME-WAE)。

圖中所示為WAAS分支機構部署，它使用WCCP將流量重定向到偏離路徑的獨立WAE裝置以進行流量攔截。此選項的配置與使用NME-WAE的WAAS分支部署相同。

網路圖表

配置和資料包流

此圖說明一個為端到端流量啟用WAAS最佳化和伺服器端存在集中管理系統(CMS)的示例設定。分支機構端和資料中心(DC)端的WAAS模組需要註冊到CMS才能運行。據觀察，CMS使用HTTPS與WAAS模組進行通訊。



端到端WAAS流量

此處的示例為使用WCCP將流量重定向到WAE裝置以進行流量攔截的Cisco IOS®防火牆提供端到端WAAS流量最佳化配置。

第1部分。 IOS-FW WCCP相關配置：

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

第2部分。 IOS-FW策略配置：

```
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
```

第3部分。 IOS-FW區域和區域對配置：

```
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
```

第4節：介面配置：

```
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
```

> **附註**：Cisco IOS®版本12.4(20)T和12.4(22)T中的新配置將整合服務引擎置於其自己的區域中，無需成為任何區域對的一部分。區域對配置在區域內和區域外之間。

```
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
```

在Integrated - Service - Engine/0上未配置任何區域時，流量會隨以下丟棄消息被丟棄：

```
*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流量（向中央管理器註冊的WAAS裝置）

以下範例提供所列兩種情況的組態：

- 使用WCCP將流量重定向到WAE裝置以進行流量攔截的Cisco IOS®防火牆的端到端WAAS流量最佳化配置
- 允許CMS流量（從CMS裝置流入/流出CMS的WAAS管理流量）

第1部分。 IOS-FW WCCP相關配置：

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

第2部分。 IOS-FW策略配置：

```
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
```

第2.1節：與CMS流量相關的IOS-FW策略：

附註：若要允許CMS流量通過，此處需要類對映：

```
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
```

第3部分。 IOS-FW區域和區域對配置：

```
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
```

第3.1節：IOS-FW CMS相關區域和區域對配置：

附註：區域對**為**out**和**out-waas**是應用先前為CMS流量建立的策略所必需的。

```
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
```

第4節：介面配置：

```
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
```

第5部分。 CMS流量的訪問清單。

附註：用於CMS流量的訪問清單。它允許兩個方向的HTTPS流量，因為CMS流量是HTTPS。

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

ZBF會話資訊

路由器R1後172.16.11.10的使用者訪問IP地址為172.16.10.10的遠端終端後託管的檔案伺服器，ZBF會話由內出區域對構建，然後路由器將資料包重定向到WAAS引擎進行最佳化。

```
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和R2-WAAS中構建的從內部主機到遠端伺服器的會話。

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%
```

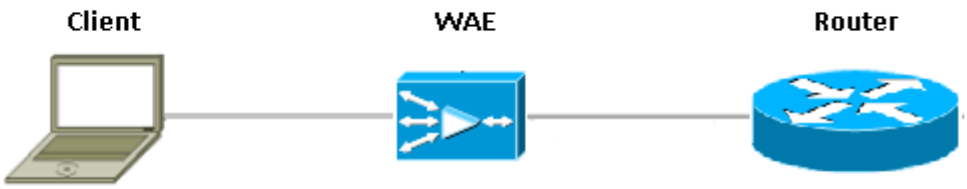
啟用WAAS和ZBF的客戶端路由器(R1)的工作配置

```
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
```

帶內聯裝置的WAAS分支部署

圖中顯示了WAAS分支部署，該部署在ISR前面有一個內聯WAE裝置。由於WAE裝置位於裝置前面，因此Cisco防火牆接收WAAS最佳化資料包，因此客戶端不支援第7層檢測。



在WAAS裝置之間運行Cisco IOS®防火牆的路由器只能看到最佳化的流量。ZBF功能監視初始三次握手（TCP選項33和序列號偏移），並自動調整預期的TCP序列視窗（不更改資料包本身的序列號）。 它為WAAS最佳化會話應用完整的L4狀態防火牆功能。WAAS透明解決方案便於防火牆按會話實施狀態防火牆和QoS策略。

詳細資料

- Firewall會看到帶有0x21選項的普通TCP SYN資料包，並為它建立會話。由於不涉及WCCP，因此輸入或輸出介面沒有問題。傳回SYN-ACK不是重新導向封包，因此防火牆已注意到該封包。
- Firewall會檢查SYN-ACK中的0x21選項，並在必要時執行序列號跳轉。如果連線已最佳化，也會關閉L7檢查。
- 可以觀察到，將此方案與Router-1方案區分開的唯一方面是返回流量沒有重新導向。此機箱上沒有2個半連線。

組態

標準ZBF配置，無針對WAAS流量的任何特定區域。僅不支援第7層檢測。

ZBF與WAAS互操作性的限制

- Cisco IOS®防火牆不支援WCCP第2層重新導向方法，它僅支援通用路由封裝(GRE)重新導向。
- Cisco IOS®防火牆僅支援WCCP重定向。如果WAAS使用基於策略的路由(PBR)來重定向資料包，則此解決方案不能確保互操作性，因此不受支援。
- Cisco IOS®防火牆不會對WAAS最佳化的TCP會話執行L7檢測。
- Cisco IOS®防火牆要求**ip inspect waas enable** 和**ip wccp notify** CLI命令才能進行WCCP重定向。
- 目前不支援具備NAT和WAAS-NM互操作性的Cisco IOS®防火牆。
- Cisco IOS®防火牆WAAS重定向僅適用於TCP資料包。
- Cisco IOS®防火牆不支援主動/主動拓撲。
- 所有屬於會話的資料包都必須通過Cisco IOS®防火牆盒。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- 安全配置指南：基於區域的策略防火牆，Cisco IOS版本15M&T
- 基於區域的策略防火牆設計和應用指南
- 技術支援與文件 - Cisco Systems