配置Cisco IOS基于区域的防火墙与WAAS部署的互操作性

目录

简介

本文档介绍Cisco IOS®防火墙功能集的新配置模式。这种新型配置模型为多接口路由器提供了直观的策略，提高了防火墙策略应用的精细度，同时提供了一种默认的“全部拒绝”策略，这种策略将禁止防火墙安全区域之间往来的数据流，除非显式应用策略以允许所需数据流通过。

先决条件

要求

思科建议您了解Cisco IOS® CLI。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco 2900 系列路由器

- 思科IOS®软件版本15.2(4)M2

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

区域策略防火墙（也称为区域策略防火墙、ZFW或ZBF）将防火墙配置从较旧的基于接口的模型(CBAC)更改为更灵活、更易于理解的基于区域的模型。接口被分配到区域，并且检测策略应用于在区域之间移动的流量。区域间策略提供了极大的灵活性和精细度，因此您可以对连接到相同路由器接口的多个主机组应用不同的检查策略。防火墙策略配置了思科®策略语言(CPL)，该语言采用分层结构来定义网络协议的检查和应用检查的主机组。

Cisco IOS®防火墙支持WAAS

在Cisco IOS® 12.4(15)T版中引入了对Cisco IOS®防火墙的广域应用服务(WAAS)支持。它提供集成防火墙，通过以下优势优化符合安全标准的广域网和应用加速解决方案：

- 通过全状态检测功能优化广域网
- 简化支付卡行业(PCI)合规性
- 保护透明广域网加速流量
- 透明地集成WAAS网络
- 支持网络管理设备(NME)广域应用引擎(WAE)模块或独立WAAS设备部署

WAAS具有自动发现机制，在初始三次握手期间使用TCP选项，以透明地识别WAE设备。自动发现后，优化的流量（路径）会经历TCP序列号的更改，以便终端区分优化流量和非优化流量。

WAAS支持IOS®防火墙，可根据前面提到的序列号的变化调整用于第4层检测的内部TCP状态变量。如果Cisco IOS®防火墙发现流量已成功完成WAAS自动发现，它允许流量的初始序列号移动，并在优化流量上保持第4层状态。

WAAS流量优化部署方案

各节介绍分支机构部署的两种不同的WAAS流量优化方案。WAAS流量优化与思科集成多业务路由器(ISR)上的思科防火墙功能配合使用。

图中显示了使用思科防火墙进行端到端WAAS流量优化的示例。在此特定部署中，NME-WAE设备与思科防火墙位于同一设备上。使用Web缓存通信协议(WCCP)来重定向要拦截的流量。

- 带离路径设备的WAAS分支部署
- 带内联设备的WAAS分支部署

WAAS分支部署，带离路径设备

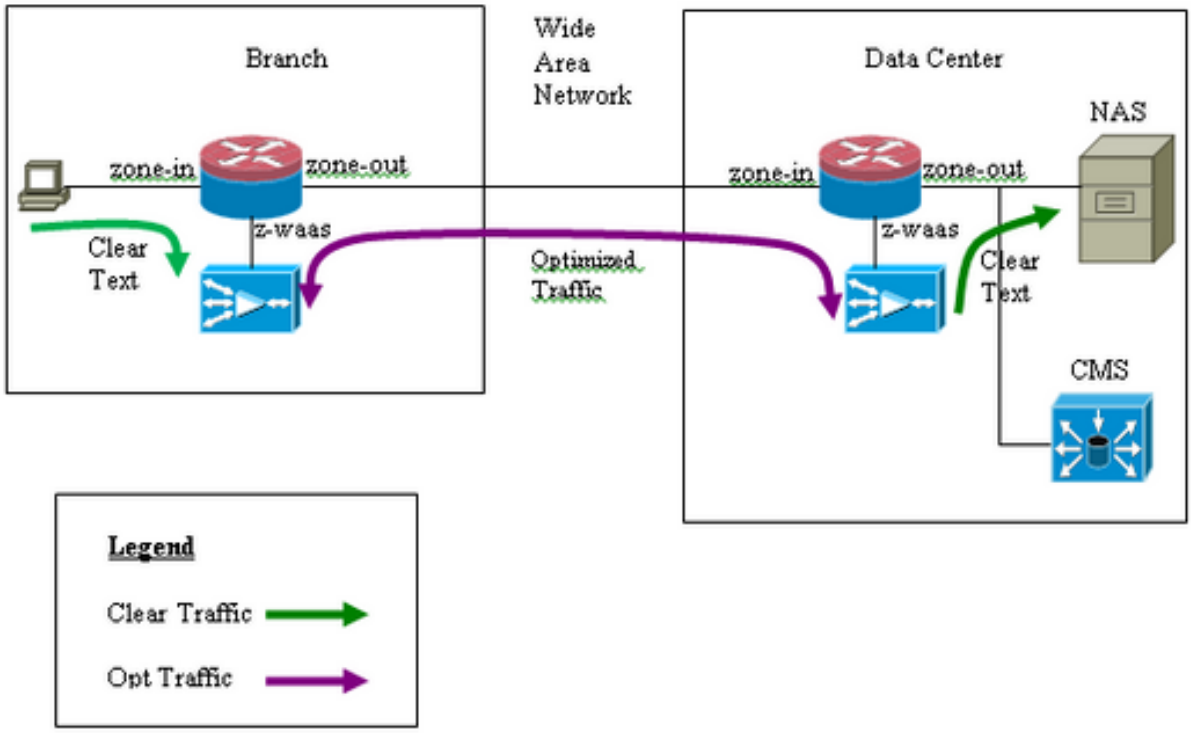
WAE设备可以是独立的思科广域网自动化引擎(WAE)设备，也可以是作为集成服务引擎安装在ISR上的思科WAAS网络模块(NME-WAE)。

图中显示了使用WCCP将流量重定向到离线独立WAE设备以进行流量拦截的WAAS分支部署。此选项的配置与使用NME-WAE的WAAS分支部署相同。

网络图

配置和数据包流

此图描述了一个为端到端流量和服务器端存在的集中管理系统(CMS)启用WAAS优化的示例设置。分支机构端和数据中心(DC)端的WAAS模块需要向CMS注册，以完成其操作。观察到CMS使用HTTPS与WAAS模块通信。



端到端WAAS流量

此示例为使用WCCP的Cisco IOS®防火墙提供端到端WAAS流量优化配置，以将流量重定向到WAE设备进行流量拦截。

第1节：IOS-FW WCCP相关配置：

```
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节：IOS-FW区域和区域对配置：

```
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部分：接口配置：

```
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
```

注意：Cisco IOS®版本12.4(20)T和12.4(22)T中的新配置将集成服务引擎置于其自己的区域中，无需成为任何区域对的一部分。区域对在区域输入和区域输出之间配置。

```
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
```

在集成 — 服务 — 引擎/0上未配置区域时，流量将被丢弃，并显示以下丢弃消息：

```
*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Central Manager注册的WAAS设备）

此处的示例为所列两种方案提供配置：

- 使用WCCP的Cisco IOS®防火墙的端到端WAAS流量优化配置，以将流量重定向到WAE设备进行流量拦截
- 允许CMS流量（流入/流出CMS设备/从CMS设备/流入WAAS设备的WAAS管理流量）

第1节：IOS-FW WCCP相关配置：

```
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节：与CMS流量相关的IOS-FW策略：

注意：要允许CMS流量通过，需要此处的类映射：

```
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节：IOS-FW区域和区域对配置：

```
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节：IOS-FW CMS相关区域和区域对配置：

注意：要应用之前为**CMS流量创**建的策**略，需要**区对**waas-out和out-waas。**

```
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部分：接口配置：

```
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节：CMS流量的访问列表。

注意：用于CMS流量的访问列表。由于CMS流量是HTTPS，因此它允许双向HTTPS流量。

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

ZBF会话信息

172.16.11.10（路由器R1后）的用户使用IP地址172.16.10.10访问远程端后托管的文件服务器，ZBF会话由输入区域对构建，然后路由器将数据包重定向到WAAS引擎进行优化。

```
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中从内部主机到远程服务器内建的会话。

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%
```

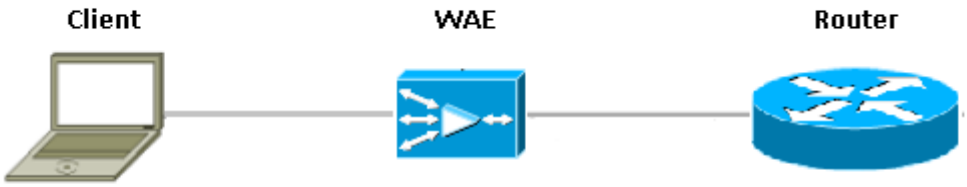
启用WAAS和ZBF的客户端路由器(R1)的工作配置

```
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
```

带内联设备的WAAS分支部署

图中显示了WAAS分支部署，该部署在ISR前面实际上有内联WAE设备。由于WAE设备在设备前面，Cisco防火墙会接收WAAS优化数据包，因此不支持客户端的第7层检测。



在WAAS设备之间运行Cisco IOS®防火墙的路由器只能看到优化的流量。ZBF功能会监控初始三次握手（TCP选项33和序列号偏移），并自动调整预期的TCP序列窗口（不更改数据包本身的序列号）。 它为WAAS优化会话应用完整的L4状态防火墙功能。WAAS透明解决方案可促进防火墙按会话状态防火墙和QoS策略实施。

详细信息

- 防火墙看到带0x21选项的普通TCP SYN数据包，并为其创建会话。由于不涉及WCCP，因此输入或输出接口没有问题。返回的SYN-ACK不是重定向的数据包，防火墙会注意它。
- 如果需要，防火墙会检查SYN-ACK中的0x21选项并执行序列号跳转。如果连接已优化，它还会关闭L7检查。
- 需要注意的是，将此区别于路由器1场景的唯一方面是返回流量不会重定向。此框上没有2个半连接。

配置

标准ZBF配置，无WAAS流量的任何特定区域。仅支持第7层检测。

ZBF与WAAS互操作性的限制

- Cisco IOS®防火墙不支持WCCP第2层重定向方法，它仅支持通用路由封装(GRE)重定向。
- Cisco IOS®防火墙仅支持WCCP重定向。如果WAAS使用基于策略的路由(PBR)来重定向数据包，则此解决方案无法确保互操作性，因此不受支持。
- Cisco IOS®防火墙不对WAAS优化TCP会话执行L7检测。
- Cisco IOS®防火墙要求**WCCP重定向使**用ip inspect waas enable**和ip wccp notify** CLI命令。
- 目前不支持具有NAT和WAAS-NM互操作性的Cisco IOS®防火墙。
- Cisco IOS®防火墙WAAS重定向仅应用于TCP数据包。
- Cisco IOS®防火墙不支持主用/主用拓扑。
- 属于会话的所有数据包都必须通过Cisco IOS®防火墙框。

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 安全配置指南：基于区域的策略防火墙，Cisco IOS版本15M&T
- 区域策略防火墙设计和应用指南
- 技术支持和文档 - Cisco Systems