IOS ：区域根据与WAAS部署的防火墙互通性

目录

[先决条件](#)
[要求](#)
[使用的组件](#)
[与Cisco IOS防火墙的WAAS支持](#)
[WAAS分组部署用PATH设备](#)
[网络图示例](#)
[配置和数据包流](#)
[ZBF会话信息](#)
[工作配置客户端路由器(R1)有启用的WAAS和ZBF的。](#)
[WAAS分组部署用一个轴向设备](#)
[详细信息](#)
[配置](#)
[ZBF互通性的限制与WAAS](#)
[相关信息](#)
[相关的思科支持社区讨论](#)

Cisco IOS软件版本12.4(6)T介绍的基于区域的策略防火墙(ZBPFW)， Cisco IOS防火墙特性集的一个新的配置型号。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。

基于区域的策略防火墙(亦称区域政策防火墙或者ZFW)更改从更旧的基于接口的型号(CBAC)的防火墙配置对一个更加灵活，更加容易地了解基本模型。这种模型首先将接口指定给区域，然后对区域之间往来的数据流应用检查策略。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。

防火墙策略使用 Cisco® 策略语言 (CPL) 配置，这种语言使用分层结构来定义要应用于网络协议的检查策略以及要应用此检查策略的主机组。

先决条件

要求

思科建议您有Cisco IOS CLI基本的了解。

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
- 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。

与Cisco IOS防火墙的WAAS支持

与Cisco IOS防火墙的WAAS (广域应用服务)支持在Cisco IOS版本12.4(15)T介绍。它提供优化安全兼容WAN和应用程序加速度解决方案与以下好处的一个集成化防火墙：

- 通过全双工状态检测功能优化广域网。
- 简化付款卡德行业(PCI)标准。
- 保护透明广域网加速的流量。
- 集成WAAS网络透明地。
- 支持网络管理设备(NME) WAE (广域应用引擎)模块或独立WAAS设备部署。

WAAS有使用TCP选项在被使用最初的三方握手期间识别WAE设备透明地的自动发现机制。在自动发现以后，优化通信流(路径)体验在TCP序列号上的一个变化允许终端区分在优化和nonoptimized通信流之间。

IOS防火墙的WAAS支持允许用于第4层检查的内部TCP状态变量的调整，根据班次在以上提到的序号。如果Cisco IOS防火墙注意通信流顺利地完成WAAS自动发现，允许通信流的初始序号班次并且保持优化通信流的Layer4状态。

WAAS通信流优化部署方案

以下部分描述分支机构部署的两个不同的WAAS通信流优化方案。WAAS通信流优化与Cisco防火墙功能一起使用在思科集成业务路由器(ISR)。

下面的图显示一端到端WAAS通信流优化的示例与Cisco防火墙的。在此特定的部署，网络管理设备(NME) - WAE设备在设备和Cisco防火墙一样。WEB缓存通信协议(WCCP)用于重定向拦截的流量。

- **WAAS分组部署用PATH设备**
- **WAAS分组部署用一个轴向设备**

WAAS分组部署用PATH设备

广域应用引擎(WAE)设备可以是一个独立Cisco广域网自动化引擎(WAE)设备或在集成业务路由器的Cisco WAAS网络模块(NME-WAE) (ISR)安装作为集成服务引擎(如图广域应用服务[WAAS]分组部署所显示)。

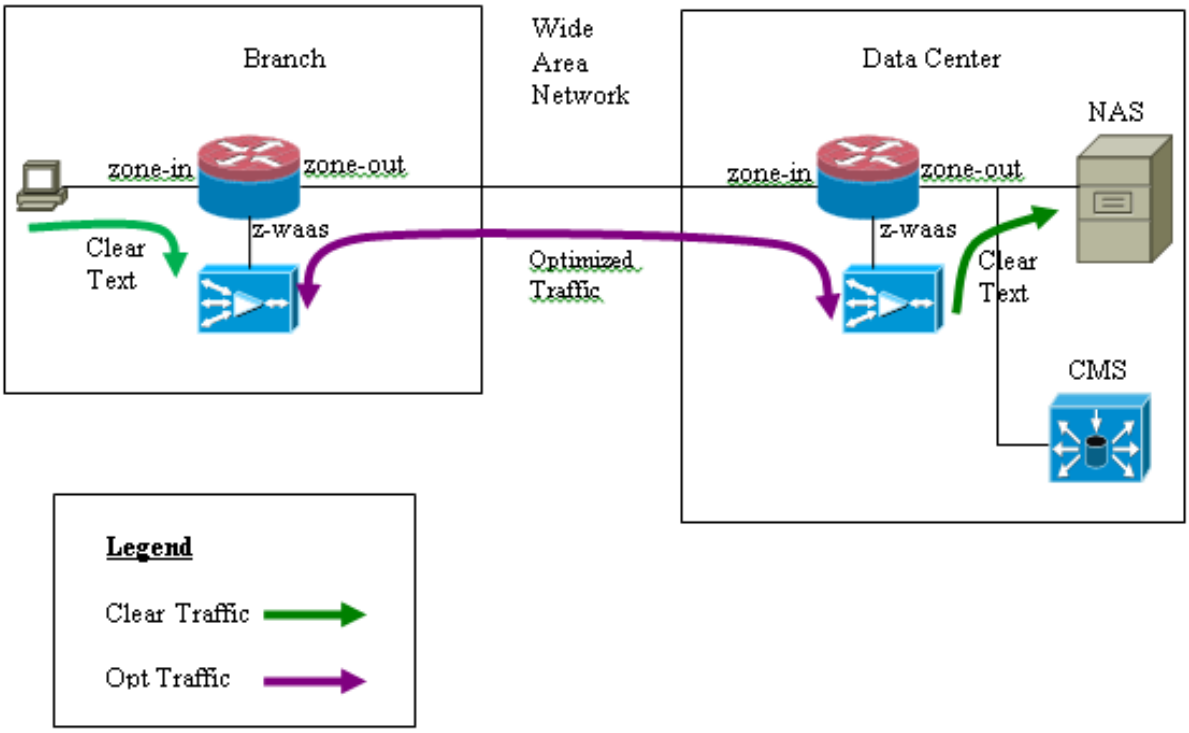
下面的图显示使用WEB缓存通信协议(WCCP)重定向流量到PATH的WAAS分组部署，流量拦截的独立WAE设备。此选项的配置是相同的象与NME-WAE的WAAS分组部署。

网络图示例

配置和数据包流

下列是表示与WAAS优化的图表一个示例设置打开为端到端数据流和CMS

(集中管理系统)是存在服务器末端。waas模块现在分组末端和数据中心末端需要向他们的操作的CMS登记。注意到它的CMS用途HTTPS是通信用WAAS模块。



端到端WAAS通信流

以下示例为使用WCCP重定向流量到流量拦截的一个WAE设备的Cisco IOS防火墙提供一端到端WAAS通信流优化配置

第 1 部分：IOS-FW WCCP涉及的设置

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

第 2 部分：IOS-FW策略设置

```
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区域和区域对设置

```
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：接口设置

```
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
```

注释在Cisco IOS版本12.4(20)T和12.4(22)T的新的配置在其自己的区域安置集成服务引擎并且不需要是任何区域对的一部分。区域对配置之间区域在和区域。

```
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
```

没有在集成服务配置的区域— Enginel/0流量被撤销与以下投下通信：

```
*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通信流(注册与中央管理器)的WAAS设备

以下示例为如下所示的两个方案提供设置：

- 使用WCCP重定向流量到流量拦截的一个WAE设备的Cisco IOS防火墙的端到端WAAS通信流优化配置
- 允许CMS流量(流到/从CMS的WAAS管理数据流从/至WAAS设备)。

第 1 部分：IOS-FW WCCP涉及的设置

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

第 2 部分：IOS-FW策略设置

```
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
```

部分2.1 ：与CMS流量涉及的IOS-FW策略

注释下面的类映射是需要的允许CMS流量经历。

```
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区域和区域对设置

```
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
```

部分3.1 ：IOS-FW CMS涉及区域和区域对设置

注释区域对***WAAS***，并且外***WAAS***要求申请创建的策略以上CMS流量。

```
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：接口设置

```
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：access-list CMS流量

注释得access-list使用CMS流量。因为CMS流量是HTTPS，它允许在两个方向的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的用户在路由器R1背后访问在远程终端后主机的文件服务器用172.16.10.10的IP地址，ZBF会话从区域对被建立，并且路由器尔后重定向数据包到优化的WAAS引擎。

```
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]
```

在R1-WAAS和R2-WAAS建立的会话从主机里边对远程服务器。

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%
```

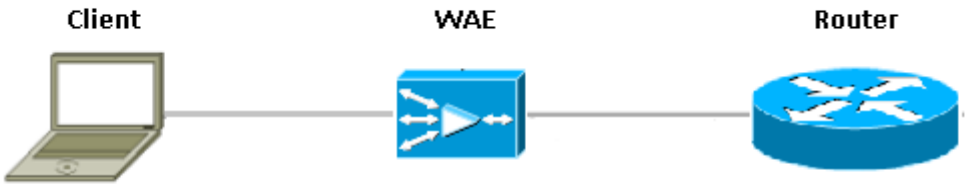
工作配置客户端路由器(R1)有启用的WAAS和ZBF的。

```
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分组部署用轴向设备

下面的图显示有一个轴向广域应用引擎的广域应用服务(WAAS)分组部署(WAE)设备物理的是在集成业务路由器(ISR)前面。由于WAE设备是在设备前面，Cisco防火墙收到WAAS优化的数据包，结果，并且，不支持在客户端的第七层检查。



运行IOS防火墙的路由器在WAAS设备之间，看到仅优化流量。ZBF功能注意最初的三通的握手(TCP选项33和序号班次)和它自动调整预计TCP序列窗口(不修改在数据包的序号)。它申请全双工

L4状态防火墙功能WAAS优化的会话。 WAAS透明解决方案实现防火墙每会话状态防火墙和QoS策略强制执行。

详细信息

- 防火墙看到与0x21选项的一个正常TCP Syn信息包并且创建它的一会话。因为WCCP不是包含的，没有与输入或输出接口的问题。回归SYN-ACK不是一重定向的数据包，并且防火墙注意到它。
- 防火墙检查在SYN-ACK的0x21选项并且如果需要，执行序号跃迁。如果连接优化，它也关闭L7检查。
- 将注意到与Router-1方案区分此的唯一的方面是回程数据流没有重定向。没有2"在此方框的半"连接。

配置

没有任何特定区域的标准的ZBF配置WAAS流量的。不会支持仅第七层检查。

ZBF互通性的限制与WAAS

- WCCP Layer2只支持通用路由封装(GRE)重定向IOS防火墙不支持的重定向方法。
- IOS防火墙只支持WCCP重定向。如果WAAS使用基于策略的路由(PBR)得到数据包重定向，此解决方案不会保证互通性并且不支持的。
- IOS防火墙不会执行L7在WAAS优化的TCP会话的检查。
- IOS防火墙要求**"IP inspect waas enable (event)"**，并且**"ip WCCP通知"** WCCP重定向的CLI命令。
- 当前不支持与NAT和WAAS-NM互通性的IOS防火墙。
- IOS防火墙WAAS重定向为TCP信息包只应用。
- IOS防火墙不支持激活/活动拓扑。属于会话的所有数据包必须流经IOS防火墙方框。

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