

# 区域策略防火墙设计和应用指南

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[区域策略概述](#)

[区域策略配置模型](#)

[应用区域策略防火墙的规则](#)

[设计区域策略网络安全](#)

[在 IPsec VPN 中使用区域策略防火墙](#)

[Cisco 策略语言 \(CPL\) 配置](#)

[配置区域策略防火墙的类映射](#)

[配置区域策略防火墙的策略映射](#)

[配置区域策略防火墙的参数映射](#)

[对区域策略防火墙策略应用日志](#)

[编辑区域策略防火墙的类映射和策略映射](#)

[配置示例](#)

[状态检查路由防火墙](#)

[状态检查透明防火墙](#)

[区域策略防火墙的速度策略](#)

[URL 过滤](#)

[控制对于路由器的访问](#)

[区域防火墙和广域应用程序服务](#)

[使用 show 和 debug 命令监控区域策略防火墙](#)

[调整区域策略防火墙的拒绝服务保护](#)

[附录](#)

[附录 A：基本配置](#)

[附录 B：最终（完整）配置](#)

[附录 C：两个区域的基本区域策略防火墙配置](#)

[相关信息](#)

## 简介

Cisco IOS 软件版本 12.4(6)T 引入了基于区域的策略防火墙 (ZFW)，这是针对 Cisco IOS 防火墙功能集的一种新配置模型。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。

新的区域策略检查接口支持几乎所有在早于 Cisco IOS 软件版本 12.4(6)T 中实现的传统 Cisco IOS 防火墙功能：

- 状态数据包检查
- VRF 感知 Cisco IOS 防火墙
- URL 过滤
- 拒绝服务 (DoS) 缓解

Cisco IOS 软件版本 12.4(9)T 增加了各类会话/连接以及吞吐量限制的 ZFW 支持，以及应用程序检查和控制：

- HTTP
- 邮局协议 (POP3)、Internet 邮件访问协议 (IMAP)、简单邮件传输协议/增强型简单邮件传输协议 (SMTP/ESMTP)
- Sun 远程过程调用 (RPC)
- 即时消息 (IM) 应用程序：Microsoft MessengerYahoo! MessengerAOL Instant Messenger
- 点对点 (P2P) 文件共享：BittorrentKazaaGnutellaeDonkey

Cisco IOS 软件版本 12.4(11)T 增加了针对早期 DoS 保护调整的统计数据。

在 Cisco IOS 软件版本 12.4(15)T 的 ZFW 中不支持的一些 Cisco IOS 传统防火墙特性和功能有：

- 身份验证代理
- 状态防火墙故障切换
- 统一防火墙 MIB
- IPv6 状态检查
- TCP 无序支持

ZFW 从总体上改进了大多数 Cisco IOS 防火墙检查活动的性能。

Cisco IOS ZFW 和传统防火墙均不提供多播数据流的状态检查支持。

## [先决条件](#)

### [要求](#)

本文档没有任何特定的要求。

### [使用的组件](#)

本文档不限于特定的软件和硬件版本。

### [规则](#)

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

## [区域策略概述](#)

Cisco IOS 传统防火墙状态检查（以前称为基于上下文的访问控制，简称 CBAC）使用了一种基于接口的配置模型，在这种模型中将对接口应用状态检查策略。所有通过此接口的数据流都将获得相

同的检查策略。这种配置模型限制了防火墙策略的精细度，并导致了防火墙策略应用的混乱，尤其当必须在多个接口间应用防火墙策略时。

区域策略防火墙（也称为区域-策略防火墙，简称 ZFW）弃用了传统的基于接口的防火墙配置模型，而改用更加灵活并且易于理解的区域模型。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。

## 区域策略配置模型

相对 Cisco IOS 传统防火墙而言，ZFW 完全改变了 Cisco IOS 防火墙检查的配置方式。

这种防火墙配置的第一个重大变化是引入了基于区域的配置。Cisco IOS 防火墙是首个实现区域配置模型的 Cisco IOS 软件威胁防御功能。随着时间推移，将来其他功能也可能采用这种区域模型。使用 **ip inspect** 命令集的 Cisco IOS 传统防火墙状态检查（或 CBAC）的基于接口的配置模型仍将在一段时间内继续使用。但是，只有少数新功能（如果有）可以通过传统的命令行界面 (CLI) 配置。ZFW 不使用状态检查或 CBAC 命令。这两种配置模型可以在路由器上同时使用，但不能在接口上混合使用。您不能将接口同时配置为安全区域成员以及配置用于 **ip inspect**。

区域建立了网络的安全边界。区域定义了数据流在流向网络中其他区域的过程中受策略限制的边界。ZFW 的默认区域间策略是“全部拒绝”。如果未明确配置任何策略，则将阻止所有数据流在区域间移动。这与状态检查模型明显不同，在状态检查模型中，除非通过访问控制表 (ACL) 明确阻止，否则将隐式允许数据流移动。

第二个重大变化是引入了一种称为 CPL 的新型配置策略语言。熟悉 Cisco IOS 软件模块化服务质量 (QoS) CLI (MQC) 的用户可能会发现，CPL 的格式类似于 QoS 在指定受策略映射中相应操作影响的数据流时所使用的类映射。

## 应用区域策略防火墙的规则

路由器网络接口的区域成员资格以及区域成员接口间的数据流移动均受以下规则影响，这些规则控制了接口的行为：

- 必须先配置区域，然后才能将接口指定给此区域。
- 一个接口只能指定给一个安全区域。
- 将接口指定给区域后，所有前往/来自给定接口的数据流将被隐式阻止，但前往/来自同一区域中的其他接口以及前往路由器上的任何接口的数据流除外。
- 默认情况下，隐式允许在属于相同区域成员的接口之间传送数据流。
- 要允许前往/来自某个区域成员接口的流量，必须配置一个策略以允许或检查此区域和任何其他区域之间往来的数据流。
- 对于默认的“全部拒绝”策略而言，自身区域是唯一的例外。除非显式拒绝，否则前往任何路由器接口的所有数据流都被允许。
- 不能在区域成员接口和任何非区域成员接口之间传送数据流。通过、检查和丢弃操作只能应用于两个区域之间。
- 未指定给区域的接口将作为传统路由器端口，并且仍然可以使用传统的状态检查/CBAC 配置。
- 如果要求机箱上的接口不能是区域或防火墙策略的一部分。您可能仍然需要将此接口放入区域

中，并在该区域以及数据流可以通过的任何其他区域之间配置“全部通过”策略（某种虚拟的策略）。

- 如前所述，如果数据流要在路由器的所有接口之间流动，则所有接口都必须是区域模型的组成部分（每个接口都必须是区域的成员）。
- 上述默认拒绝策略的唯一例外是前往/来自路由器的数据流，默认情况下将允许该数据流。您可以配置一个显式策略以限制此类数据流。

## [设计区域策略网络安全](#)

应该为网络中具有相关安全性的每个区域配置安全区域，这样指定给相同区域的所有接口都将得到相同安全级别的保护。例如，假定有一台具有三个接口的接入路由器：

- 一个接口连接到公共 Internet
- 一个接口连接到不能从公共 Internet 访问的专用 LAN
- 一个接口连接到 Internet 服务隔离区 (DMZ)，此区域中的 Web 服务器，域名系统 (DNS) 服务器和电子邮件服务器必须能够访问公共 Internet

在此网络中，每个接口都将被指定给其自己的区域，尽管您可能想要允许从公共 Internet 对 DMZ 中的特定主机进行各种访问，并允许对受保护 LAN 中的主机设置各种应用程序使用策略。（请参阅图 1。）

### **图 1：基本安全区域拓扑**

在本示例中，每个区域只有一个接口。如果有其他接口添加到专用区域，则连接到此区域中的新接口的主机将可以向位于相同区域中的所有主机的现有接口传送数据流。此外，从这些主机发送至其他区域中的主机的数据流也同样受现有策略的影响。

通常，示例网络将采用以下三种主要策略：

- 专用区域到 Internet 的连接
- 专用区域到 DMZ 主机的连接
- Internet 区域到 DMZ 主机的连接

由于 DMZ 暴露在公共 Internet 中，因此这些 DMZ 主机可能会受到成功攻陷一台或多台 DMZ 主机的恶意用户的影响。如果不为 DMZ 主机提供访问专用区域主机或 Internet 区域主机的策略，则攻陷 DMZ 主机的用户将无法利用这些 DMZ 主机对专用主机或 Internet 主机实施进一步的攻击。默认情况下，ZFW 将强制执行禁止访问的安全策略。因此，除非专门允许 DMZ 主机访问其他网络，否则 DMZ 主机将无法连接其他网络。同样地，Internet 主机也不能访问专用区域主机，因此专用区域主机也不会受到 Internet 主机的有害访问。

## [在 IPSec VPN 中使用区域策略防火墙](#)

最近对 IPSec VPN 所做的改进简化了 VPN 连接的防火墙策略配置。IPSec 虚拟隧道接口 (VTI) 和 GRE+IPsec 将隧道接口置于指定的安全区域中，从而可以将 VPN 站点到站点连接以及客户端连接限制在特定的安全区域。如果必须使用特定策略限制连接，可以将连接隔离在 VPN DMZ 中。或者，如果 VPN 连接被隐式信任，则可以将 VPN 连接作为受信任的内部网络置于相同的安全区域中。

如果使用了非 VTI IPSec，则 VPN 连接防火墙策略将要求进行严格审查以保持安全。如果安全主机所在的区域与 VPN Client 和路由器之间的加密连接所在的区域不同，则区域策略必须明确允许远程站点主机或 VPN 客户端的 IP 地址访问。如果未正确配置访问策略，则本应保护的主机最终可能暴露在可能有害的恶意主机控制下。有关详细的概念和配置细节的信息，请参阅[使用带有区域策略防火墙的 VPN](#)。

## Cisco 策略语言 (CPL) 配置

以下过程可用于配置 ZFW。这些步骤的顺序并不重要，但一些事件必须按顺序完成。例如，在将类映射指定给策略映射之前，您必须先配置类映射。同样地，在完成策略配置之前，您不能将策略映射指定给区域对。如果您尝试配置的某个部分依赖于另一个您尚未配置的配置部分，则路由器将显示一条错误消息。

1. 定义区域。
2. 定义区域对。
3. 定义用于描述数据流的类映射，以便在数据流跨越区域对时对其应用策略。
4. 定义策略映射以便对类映射的数据流应用操作。
5. 将策略映射应用于区域对。
6. 将接口指定给区域。

### 配置区域策略防火墙的类映射

类映射定义了防火墙选择要应用策略的数据流。第 4 层类映射将根据以下列出的条件对数据流进行排序。这些条件使用类映射中的 `match` 命令指定：

- Access-group — 标准、扩展或指定的 ACL，可以根据源 IP 地址/端口和目标 IP 地址/端口来过滤数据流。
- Protocol — 第 4 层协议 (TCP、UDP 和 ICMP) 和应用程序服务，例如 HTTP、SMTP 和 DNS 等等。任何已知的服务或端口-应用程序映射已知的用户定义服务都可以指定。
- Class-map — 提供可以嵌套在其他类映射中的附加匹配条件的次级类映射。
- Not — *not* 条件指定任何不匹配指定服务 (协议)、访问组或次级类映射的数据流都将被类映射选中。

#### 结合使用“匹配”条件：“Match-Any”与“Match-Any”

类映射可以应用 `match-any` 或 `match-all` 操作符，以确定如何应用匹配条件。如果指定 `match-any`，则数据流只能匹配类映射中的一个匹配条件。如果指定 `match-all`，则数据流必须匹配所有类映射条件才能属于此特定类。

如果数据流满足多个条件，则必须按从较为特定到较不特定的顺序应用匹配条件。例如，假定有以下类映射：

```
class-map type inspect match-any my-test-cmap
  match protocol http
  match protocol tcp
```

HTTP 数据流必须首先遇到匹配协议 `http` 才能确保此数据流由特定于此服务的 HTTP 检查功能进行处理。如果匹配过程颠倒，数据流在与匹配协议 `http` 比较之前遇到匹配协议 `tcp` 语句，那么数据流将被简单分类为 TCP 数据流，并根据防火墙的 TCP 检查组件功能进行检查。这对于某些服务来说会产生问题，例如 FTP、TFTP、一些多媒体和语音信号服务 (例如 H.323、SIP、Skinny、RTSP) 以及其他服务。这些服务需要使用其他检查功能才能识别其更为复杂的活动。

#### 应用 ACL 作为匹配条件

类映射可以将 ACL 作为应用策略时的一个匹配条件。如果 ACL 是类映射的唯一匹配条件，并且此类映射与某个应用检查操作的策略映射关联，则路由器将对 ACL 允许的所有数据流 (ZFW 对其提

供应用程序感知检查的数据流除外)应用基本的 TCP 或 UDP 检查。这包括(但不限于)FTP、SIP、Skinny(SCCP)、H.323、Sun RPC 和 TFTP。如果提供了特定于应用程序的检查,并且 ACL 允许主要信道或控制信道,则将允许所有与主要信道或控制信道关联的辅助信道或媒体信道,无论 ACL 是否允许此数据流。

如果类映射仅使用 ACL 101 作为匹配条件,ACL 101 类似如下所示:

```
access-list 101 permit ip any any
```

所有数据流都可以沿服务策略应用于给定区域对的方向流动,并允许相应的回程数据流沿相反方向流动。因此,ACL 必须应用限制以将数据流限制为所需的特定类型。请注意,PAM 列表包含一些应用程序服务,例如 HTTP、NetBIOS、H.323 和 DNS。然而,尽管 PAM 知道特定应用程序如何使用给定端口,但防火墙仅应用能够充分满足应用流量已知要求的特定于应用程序的功能。因此,简单的应用流量(例如 telnet 和 SSH)以及其他单信道应用程序将作为 TCP 进行检查,并且其统计数据将合并到 **show command output** 中。如果特定应用程序需要了解网络活动,则您需要根据应用程序名称配置服务检查策略(配置匹配协议 http、匹配协议 telnet 等)。

请将此配置的 **show policy-map type inspect zone-pair** 命令输出中提供的统计数据与显示在此页面下方的更为明确的防火墙策略进行比较。此配置用于检查来自 Cisco IP 电话以及使用各种数据流(包括 http、ftp、netbios、ssh 和 dns)的工作站的数据流:

```
class-map type inspect match-all all-private
  match access-group 101
!
policy-map type inspect priv-pub-pmap
  class type inspect all-private
    inspect
  class class-default
!
zone security private
zone security public
zone-pair security priv-pub source private destination public
  service-policy type inspect priv-pub-pmap
!
interface FastEthernet4
  ip address 172.16.108.44 255.255.255.0
  zone-member security public
!
interface Vlan1
  ip address 192.168.108.1 255.255.255.0
  zone-member security private
!
access-list 101 permit ip 192.168.108.0 0.0.0.255 any
```

尽管此配置易于定义,并且包含了从专用区域始发的所有数据流(只要数据流能够看到标准、PAM 可识别的目标端口),但通过此配置只能看到有限的服务活动,并且不能将 ZFW 的带宽和会话限制应用于特定类型数据流。以下 **show policy-map type inspect zone-pair priv-pub** 命令输出是早先简单配置的结果,此配置仅在区域对间使用 permit ip [subnet] any ACL。您可以看到,大多数工作站数据流都被计入基本 TCP 或 UDP 统计数据:

```
stg-871-L#show policy-map type insp zone-pair priv-pub Zone-pair: priv-pub Service-policy
inspect : priv-pub-pmap Class-map: all-private (match-all) Match: access-group 101 Inspect
Packet inspection statistics [process switch:fast switch] tcp packets: [413:51589] udp packets:
[74:28] icmp packets: [0:8] ftp packets: [23:0] tftp packets: [3:0] tftp-data packets: [6:28]
skinny packets: [238:0] Session creations since subsystem startup or last reset 39 Current
session counts (estab/half-open/terminating) [3:0:0] Maxever session counts (estab/half-
open/terminating) [3:4:1] Last session created 00:00:20 Last statistic reset never Last session
creation rate 2 Maxever session creation rate 7 Last half-open session total 0 Class-map: class-
default (match-any) Match: any Drop (default action) 0 packets, 0 bytes
```

相比而言,增加了特定应用程序类的相似配置则可提供更加精细的应用程序统计和控制,并且通过

在策略映射的最后定义最后一个类映射仅匹配 ACL，它仍然包含与前一个示例相同的带宽：

```
class-map type inspect match-all all-private
  match access-group 101
class-map type inspect match-all private-ftp
  match protocol ftp
  match access-group 101
class-map type inspect match-any netbios
  match protocol msrpc
  match protocol netbios-dgm
  match protocol netbios-ns
  match protocol netbios-ssn
class-map type inspect match-all private-netbios
  match class-map netbios
  match access-group 101
class-map type inspect match-all private-ssh
  match protocol ssh
  match access-group 101
class-map type inspect match-all private-http
  match protocol http
  match access-group 101
!
policy-map type inspect priv-pub-pmap
  class type inspect private-http
    inspect
  class type inspect private-ftp
    inspect
  class type inspect private-ssh
    inspect
  class type inspect private-netbios
    inspect
  class type inspect all-private
    inspect
  class class-default!
zone security private
zone security public
zone-pair security priv-pub source private destination public
  service-policy type inspect priv-pub-pmap
!
interface FastEthernet4
  ip address 172.16.108.44 255.255.255.0
  zone-member security public
!
interface Vlan1
  ip address 192.168.108.1 255.255.255.0
  zone-member security private
!
access-list 101 permit ip 192.168.108.0 0.0.0.255 any
```

更具体的配置提供了以下非常精细的 **show policy-map type inspect zone-pair priv-pub** 命令输出：

```
stg-871-L#sh policy-map type insp zone-pair priv-pub Zone-pair: priv-pub Service-policy inspect
: priv-pub-pmap Class-map: private-http (match-all) Match: protocol http Match: access-group 101
Inspect Packet inspection statistics [process switch:fast switch] tcp packets: [0:2193] Session
creations since subsystem startup or last reset 731 Current session counts (estab/half-
open/terminating) [0:0:0] Maxever session counts (estab/half-open/terminating) [0:3:0] Last
session created 00:29:25 Last statistic reset never Last session creation rate 0 Maxever session
creation rate 4 Last half-open session total 0 Class-map: private-ftp (match-all) Match:
protocol ftp Inspect Packet inspection statistics [process switch:fast switch] tcp packets:
[86:167400] ftp packets: [43:0] Session creations since subsystem startup or last reset 7
Current session counts (estab/half-open/terminating) [0:0:0] Maxever session counts (estab/half-
open/terminating) [2:1:1] Last session created 00:42:49 Last statistic reset never Last session
creation rate 0 Maxever session creation rate 4 Last half-open session total 0 Class-map:
private-ssh (match-all) Match: protocol ssh Inspect Packet inspection statistics [process
```



```
switch:fast switch] tcp packets: [0:62] Session creations since subsystem startup or last reset
4 Current session counts (estab/half-open/terminating) [0:0:0] Maxever session counts
(estab/half-open/terminating) [1:1:1] Last session created 00:34:18 Last statistic reset never
Last session creation rate 0 Maxever session creation rate 2 Last half-open session total 0
Class-map: private-netbios (match-all) Match: access-group 101 Match: class-map match-any
netbios Match: protocol msrpc 0 packets, 0 bytes 30 second rate 0 bps Match: protocol netbios-
dgm 0 packets, 0 bytes 30 second rate 0 bps Match: protocol netbios-ns 0 packets, 0 bytes 30
second rate 0 bps Match: protocol netbios-ssn 2 packets, 56 bytes 30 second rate 0 bps Inspect
Packet inspection statistics [process switch:fast switch] tcp packets: [0:236] Session creations
since subsystem startup or last reset 2 Current session counts (estab/half-open/terminating)
[0:0:0] Maxever session counts (estab/half-open/terminating) [1:1:1] Last session created
00:31:32 Last statistic reset never Last session creation rate 0 Maxever session creation rate 1
Last half-open session total 0 Class-map: all-private (match-all) Match: access-group 101
Inspect Packet inspection statistics [process switch:fast switch] tcp packets: [51725:158156]
udp packets: [8800:70] tftp packets: [8:0] tftp-data packets: [15:70] skinny packets: [33791:0]
Session creations since subsystem startup or last reset 2759 Current session counts (estab/half-
open/terminating) [2:0:0] Maxever session counts (estab/half-open/terminating) [2:6:1] Last
session created 00:22:21 Last statistic reset never Last session creation rate 0 Maxever session
creation rate 12 Last half-open session total 0 Class-map: class-default (match-any) Match: any
Drop (default action) 4 packets, 112 bytes
```

如前所述，使用更加精细的类映射和策略映射配置的另一个优点，是能够在会话和速度值上应用特定于类的限制，并且可以通过应用参数映射以调整每个类的检查行为，从而具体调整检查参数。

## 配置区域策略防火墙的策略映射

策略映射可以对一个或多个类映射应用防火墙策略操作，以定义将应用于安全区域对的服务策略。当创建检查类型策略映射时，在创建类后将会应用一个名为 `class class-default` 的默认类。`class class-default` 的默认策略操作是丢弃，但可以更改为通过。您可以在丢弃操作中添加日志选项。对于 `class class-default` 不能应用检查。

## 区域策略防火墙的操作

ZFW 针对区域间移动的数据流提供了三种操作：

- **丢弃** — 这是用于所有数据流的默认操作，它由终止所有检查类型策略映射的“`class class-default`”应用。您可以将策略映射中的其他类映射也配置为丢弃有害数据流。由丢弃操作处理的数据流将被 ZFW 静默丢弃（也就是说不会向相关终端主机发送丢弃通知），与之相反，ACL 行为则是向发出被拒绝数据流的主机发送 ICMP“host unreachable”消息。目前没有选项可以更改“静默丢弃”行为。您可以在丢弃操作中添加日志选项，以便显示 syslog 通知，指示防火墙已丢弃数据流。
- **通过** — 此操作允许路由器将来自一个区域的数据流转发到另一个区域。通过操作不会在数据流内跟踪连接或会话状态。它只允许一个方向的数据流通过。要允许相反方向的回程数据流通过，必须应用对应的策略。通过操作可以用于 IPsec ESP、IPsec AH、ISAKMP 等协议，以及其他具有可预测行为的内在安全协议。但是，大多数应用流量最好使用 ZFW 中的检查操作进行处理。
- **检查** — 检查操作提供了基于状态的数据流控制。例如，在上述示例网络中，如果检查了从专用区域到 Internet 区域的数据流，则路由器将维护 TCP 和用户数据报协议 (UDP) 数据流的连接或会话信息。因此，路由器将允许 Internet 区域主机响应专用区域连接请求而发送的回程数据流通过。此外，检查操作还可以对某些携带易受攻击或敏感应用流量的服务协议提供应用程序检查和控制。您可以通过参数映射应用审计追踪，以记录连接/会话的开始、终止、持续时间、传送的数据量以及源和目标地址。

操作与策略映射中的类映射关联：



```
conf t
policy-map type inspect z1-z2-pmap
class type inspect service-cmap
inspect|drop|allow [service-parameter-map]
```

参数映射提供了修改给定类映射的检查策略的连接参数的选项。

## [配置区域策略防火墙的参数映射](#)

参数映射指定了 ZFW 的检查行为参数，例如 DoS 保护、TCP 连接/UDP 会话计时器和审计追踪日志设置等。参数映射也应用于第 7 层类映射和策略映射，以定义特定于应用程序的行为，例如 HTTP 对象、POP3 和 IMAP 验证请求以及其他特定于应用程序的信息。

ZFW 的检查参数映射被配置为 **type inspect**，类似于其他 ZFW 类和策略对象：

```
stg-871-L(config)#parameter-map type inspect z1-z2-pmap stg-871-L(config-profile)#? parameter-
map commands: alert Turn on/off alert audit-trail Turn on/off audit trail dns-timeout Specify
timeout for DNS exit Exit from parameter-map icmp Config timeout values for icmp max-incomplete
Specify maximum number of incomplete connections before clamping no Negate or set default values
of a command one-minute Specify one-minute-sample watermarks for clamping sessions Maximum
number of inspect sessions tcp Config timeout values for tcp connections udp Config timeout
values for udp flows
```

特定类型的参数映射指定了第 7 层应用程序检查策略应用的参数。正则表达式类型参数映射定义了用于 HTTP 应用程序检查的正则表达式，以使用此正则表达式过滤数据流：

```
parameter-map type regex [parameter-map-name]
```

协议信息类型参数映射定义了用于即时消息应用程序检查的服务器名称：

```
parameter-map type protocol-info [parameter-map-name]
```

有关 HTTP 和 IM 应用程序检查的完整配置信息已在本文相应的应用程序检查部分提供。

调整 DoS 保护将在本文后面的章节中介绍。

配置应用程序检查将在本文后面的章节中介绍。

## [对区域策略防火墙策略应用日志](#)

ZFW 提供了用于记录由默认或配置的防火墙策略操作丢弃或检查的数据流的日志选项。审计追踪日志记录可以用于 ZFW 检查的数据流。通过在参数映射中定义审计追踪，然后在策略映射的检查操作中应用参数映射，可以应用审计追踪：

```
conf t
policy-map type inspect z1-z2-pmap
class type inspect service-cmap
inspect|drop|allow [parameter-map-name (optional)]
```

丢弃日志记录可以用于 ZFW 丢弃的数据流。通过对策略映射的丢弃操作添加日志可以配置丢弃日志记录：

```
conf t
policy-map type inspect z1-z2-pmap
class type inspect service-cmap
inspect|drop|allow [service-parameter-map]
```

## [编辑区域策略防火墙的类映射和策略映射](#)

ZFW 目前未集成可修改各种 ZFW 结构（例如策略映射、类映射和参数映射）的编辑器。要重新安

排策略映射的匹配语句或是应用于策略映射中包含的各种类映射的操作，您需要完成以下步骤：

1. 将现有结构复制到文本编辑器中，例如 Microsoft Windows Notepad 或 Linux/UNIX 平台中的 vi。
2. 从路由器配置中删除现有结构。
3. 在文本编辑器中编辑结构。
4. 将结构复制回路路由器的 CLI 中。

## 配置示例

此配置示例使用 Cisco 1811 集成服务路由器。有关基本 IP 连接配置、VLAN 配置以及在两个专用以太网 LAN 网段之间建立透明桥接等内容，请参阅[附录 A](#)。路由器分为 5 个区域：

- 公共 Internet 连接到 FastEthernet 0 ( Internet 区域 )
- 两台 Internet 服务器连接到 FastEthernet 1 ( DMZ 区域 )
- 以太网交换机配置有两个 VLAN：工作站连接到 VLAN1 ( 客户端区域 )。服务器连接到 VLAN2 ( 服务器区域 )。客户端区域和服务器区域位于相同子网。在这两个区域间将应用一个透明防火墙，因此这两个接口上的区域间策略将只影响客户端区域和服务器区域之间的数据流。
- VLAN1 接口和 VLAN2 接口通过网桥虚拟接口 (BVI1) 与其他网络通信。此接口被指定给专用区域。( 请参阅图 2。 ) **图 2：区域拓扑细节**

针对上面定义的网络区域应用了以下策略：

- Internet 区域主机可以访问一台 DMZ 服务器上的 DNS、SMTP 和 SSH 服务。另一台服务器将提供 SMTP、HTTP 和 HTTPS 服务。防火墙策略将限制对每台主机上的特定服务的访问。
- DMZ 主机不能连接到位于任何其他区域中的主机。
- 客户端区域主机可以连接到服务器区域主机的所有 TCP、UDP 和 ICMP 服务。
- 服务器区域主机不能连接到客户端区域主机，但基于 UNIX 的应用程序服务器可以在客户端区域的桌面 PC 上通过 6900 到 6910 端口打开 X Windows 服务器到 X Windows 客户端的会话。
- 位于专用区域中的所有主机 ( 客户端和服务器 ) 都可以使用 SSH、FTP、POP、IMAP、ESMTP 和 HTTP 服务访问 DMZ 中的主机，并且可以使用 HTTP、HTTPS 和 DNS 服务和 ICMP 访问 Internet 区域中的主机。此外，对于从专用区域到 Internet 区域的 HTTP 连接将使用应用程序检查，以确保受支持的即时消息应用程序和 P2P 应用程序未通过端口 80 传输。( 请参阅图 3。 ) **图 3：要在配置示例中应用的区域对服务权限**

按照复杂性顺序配置了以下防火墙策略：

1. 客户端-服务器 TCP/UDP/ICMP 检查
2. 专用-DMZ SSH/FTP/POP/IMAP/ESMTP/HTTP 检查
3. 通过主机地址限制的 Internet-DMZ SMTP/HTTP/DNS 检查
4. 利用端口-应用程序映射 (PAM) 指定的服务执行的服务器-客户端 X Windows 检查
5. 专用-Internet HTTP/HTTPS/DNS/ICMP 使用的 HTTP 应用程序检查

由于您将在不同时间对不同网段应用各个配置部分，因此请务必记住当您网段放入区域中时，该网段将丢失与其他网段的连接。例如，在配置专用区域后，如果不定义相应的策略，专用区域中的主机将丢失与 DMZ 区域和 Internet 区域的连接。

## 状态检查路由防火墙

### 配置专用 Internet 策略

图 4 介绍了专用 Internet 策略的配置。

#### 图 4：从专用区域到 Internet 区域的服务检查

专用 Internet 策略将对 HTTP、HTTPS 和 DNS 以及从专用区域到 Internet 区域的 ICMP 应用第 4 层检查。这允许从专用区域连接至 Internet 区域，并允许回程数据流。第 7 层检查的优点是应用程序控制更严格、安全性更高，并且支持需要修正功能的应用程序。但是如前所述，第 7 层检查要求对网络活动有更好的了解，因为未配置检查功能的第 7 层协议将不允许在区域间通过。

1. 根据上述策略，定义一些用于描述可在区域间通过的数据流的类映射：

```
conf t
class-map type inspect match-any internet-traffic-class
  match protocol http
  match protocol https
  match protocol dns
  match protocol icmp
```
2. 配置策略映射以检查刚刚在类映射中定义的数据流：

```
conf t
policy-map type inspect private-internet-policy
  class type inspect internet-traffic-class
  inspect
```
3. 配置专用区域和 Internet 区域，并为这些区域分别指定路由器接口：

```
conf t
zone security private
zone security internet
int bvil
zone-member security private
int fastethernet 0
zone-member security internet
```
4. 配置区域对并应用适当的策略映射。**注意：**要检查从专用区域到 Internet 区域的连接，目前您只需配置专用 Internet 区域对：

```
conf t
zone-pair security private-internet source private destination internet
  service-policy type inspect private-internet-policy
```

这样就完成了专用 Internet 区域对的第 7 层检查策略的配置，从而允许从客户端区域通过 HTTP、HTTPS、DNS 和 ICMP 连接到服务器区域，并对 HTTP 流量进行应用程序检查，以确保有害流量不能通过 HTTP 的服务端口 TCP 80 传输。

#### 配置专用 DMZ 策略

图 5 介绍了专用 DMZ 策略的配置。

#### 图 5：从专用区域到 DMZ 区域的服务检查

专用 DMZ 策略的配置增加了复杂性，因为它要求对区域间网络流量有更好的了解。此策略将对专用区域与 DMZ 之间的连接应用第 7 层检查。这允许从专用区域连接至 DMZ，并允许回程数据流。第 7 层检查的优点是应用程序控制更严格、安全性更高，并且支持需要修正功能的应用程序。但是如前所述，第 7 层检查要求对网络活动有更好的了解，因为未配置检查功能的第 7 层协议将不允许在区域间通过。

1. 根据上述策略，定义一些用于描述可在区域间通过的数据流的类映射：

```
conf t
class-map type inspect match-any L7-inspect-class
  match protocol ssh
  match protocol ftp
  match protocol pop
  match protocol imap
  match protocol esmtp
  match protocol http
```
2. 配置策略映射以检查刚刚在类映射中定义的数据流：

```
conf t
policy-map type inspect private-dmz-policy
  class type inspect L7-inspect-class
```

```
inspect
```

3. 配置专用区域和 DMZ 区域，并为这些区域分别指定路由器接口：conf t

```
zone security private
zone security dmz
int bv11
zone-member security private
int fastethernet 1
zone-member security dmz
```

4. 配置区域对并应用适当的策略映射。注意：要检查从专用区域到 DMZ 的连接，目前您只需配置专用 DMZ 区域对：conf t

```
zone-pair security private-dmz source private destination dmz
service-policy type inspect private-dmz-policy
```

这样就完成了专用 DMZ 的第 7 层检查策略的配置，从而允许从客户端区域到服务器区域的所有 TCP、UDP 和 ICMP 连接。该策略不对辅助信道应用修正，但提供了适用于大多数应用程序连接的简单策略示例。

## 配置 Internet DMZ 策略

图 6 介绍了 Internet DMZ 策略的配置。

### 图 6：从 Internet 区域到 DMZ 区域的服务检查

此策略将对 Internet 区域与 DMZ 之间的连接应用第 7 层检查。这将允许从 Internet 区域连接到 DMZ，并允许将数据量从 DMZ 主机返回至发起连接的 Internet 主机。Internet DMZ 策略结合使用了第 7 层检查与 ACL 定义的地址组，以限制访问特定主机、主机组或子网上的特定服务。这可以通过将用于指定服务的类映射嵌套在另一个用于引用 ACL 以指定 IP 地址的类映射中而实现。

1. 根据上述策略，定义一些用于描述可在区域间通过的数据流的类映射和 ACL。此时需要对服务使用多个类映射，因为访问两台不同的服务器时将应用不同的访问策略。将允许 Internet 主机通过 DNS 和 HTTP 连接到 172.16.2.2，以及通过 SMTP 连接到 172.16.2.3。请注意这些类映射的不同之处。用于指定服务的类映射使用 **match-any** 关键字以允许任何列出的服务。用于将 ACL 与服务类映射关联的类映射使用 **match-all** 关键字来要求必须同时满足类映射中的两个条件才允许数据流通过：conf t

```
access-list 110 permit ip any host 172.16.2.2
access-list 111 permit ip any host 172.16.2.3
class-map type inspect match-any dns-http-class
  match protocol dns
  match protocol http
class-map type inspect match-any smtp-class
  match protocol smtp
class-map type inspect match-all dns-http-acl-class
  match access-group 110
  match class-map dns-http-class
class-map type inspect match-all smtp-acl-class
  match access-group 111
  match class-map smtp-class
```

2. 配置策略映射以检查刚刚在类映射中定义的数据流：conf t

```
policy-map type inspect internet-dmz-policy
  class type inspect dns-http-acl-class
    inspect
  class type inspect smtp-acl-class
    inspect
```

3. 配置 Internet 区域和 Internet 区域，并为这些区域分别指定路由器接口：如果您已在前面设置了 DMZ 配置，请跳过此部分：conf t

```
zone security internet
zone security dmz
int fastethernet 0
zone-member security internet
```

```
int fastethernet 1
  zone-member security dmz
```

4. 配置区域对并应用适当的策略映射。**注意：**要检查从 Internet 区域到 DMZ 区域的连接，目前您只需配置 Internet DMZ 区域对：`conf t`

```
zone-pair security internet-dmz source internet destination dmz
```

`service-policy type inspect internet-dmz-policy`这样就完成了 Internet DMZ 区域对的特定地址第 7 层检查策略的配置。

## 状态检查透明防火墙

### 配置服务器-客户端策略

图 7 介绍了服务器-客户端策略的配置。

#### 图 7：从服务器区域到客户端区域的服务检查

服务器-客户端策略将使用用户定义的服务应用检查。将对从服务器区域到客户端区域的连接应用第 7 层检查。这将允许从服务器区域到客户端区域的特定端口范围的 X Windows 连接，并允许回程数据流。在 PAM 中，X Windows 不是本地支持的协议，因此必须在 PAM 中定义用户配置的服务，这样 ZFW 才能识别和检查相应的数据流。

在 IEEE 网桥组中配置了两个或多个路由器接口以提供集成的路由和桥接 (IRB)，从而可以桥接网桥组中的各个接口，并通过网桥虚拟接口 (BVI) 路由到其他子网。透明防火墙策略将对“跨越网桥”的数据流应用防火墙检查，但对于通过 BVI 离开网桥组的数据流不会应用此检查。该检查策略仅应用于跨越网桥组的数据流。因此在本示例中，将仅对嵌套在专用区域中的客户端区域和服务器区域之间移动的数据流应用检查。仅当数据流通过 BVI 离开网桥组时，才会应用专用区域与公共区域和 DMZ 区域之间的策略。当数据流通过 BVI 离开客户端区域或服务器区域时，将不会调用透明防火墙策略。

1. 使用用户定义的 X Windows 条目配置 PAM。X Windows 客户端 (应用程序的宿主) 通过从 6900 开始的端口范围向客户端 (用户工作的位置) 开放连接以显示信息。每个额外的连接都使用连续的端口，因此如果客户端要显示一台主机上的 10 次不同的会话，那么服务器将使用端口 6900-6909。因此，如果您要检查从 6900 到 6909 的端口范围，对编号 6909 以上的端口开放的连接将失败：`conf t`
2. 请参阅 PAM 文档以解决其他 PAM 问题，或参阅精度协议检测文档以了解有关 PAM 和 Cisco IOS 防火墙状态检查之间的互操作性的详细信息。
3. 根据上述策略，定义一些用于描述可在区域间通过的数据流的类映射：`conf t`
4. 配置策略映射以检查刚刚在类映射中定义的数据流：`conf t`
5. 配置客户端区域和服务器区域，并为这些区域分别指定路由器接口。如果您已配置了这些区域，并在“客户端-服务器策略配置”部分指定了接口，则可以跳到区域对定义。为了进行完整的说明，以下提供了桥接 IRB 的配置：`conf t`

```
bridge irb
bridge 1 protocol ieee
bridge 1 route ip
zone security clients
zone security servers
  int vlan 1
  bridge-group 1
```

```

zone-member security clients
int vlan 2
bridge-group 1
zone-member security servers

```

6. 配置区域对并应用适当的策略映射。**注意：**要检查从服务器区域到客户端区域的连接，目前您只需配置服务器-客户端区域对：`conf t`

```

zone-pair security servers-clients source servers destination clients

```

`service-policy type inspect servers-clients-policy`这样就完成了服务器-客户端区域对的用户定义检查策略的配置，从而允许通过 X Windows 从服务器区域连接到客户端区域。

## 配置服务器-客户端策略

图 8 介绍了服务器-客户端策略的配置。

### 图 8：从客户端区域到服务器区域的服务检查

与其他策略相比，客户端-服务器策略没那么复杂。对于从客户端区域到服务器区域的连接将应用第 4 层检查。这将允许从客户端区域连接到服务器区域，并允许回程数据流。第 4 层检查具备防火墙配置简单的优点，因为只需配置少数几个规则即可允许大多数应用流量。但是，第 4 层检查也具有两个主要缺点：

- 一些应用程序（例如 FTP 或流媒体服务）将频繁协商额外建立一条从服务器到客户端的辅助信道。这种功能通常在用于监控控制信道对话并允许辅助信道的服务修正中使用。第 4 层检查中并不提供此功能。
- 第 4 层检查将允许几乎所有应用程序层流量。如果必须控制网络使用，以便只允许少数应用程序通过防火墙，则必须对出站流量配置 ACL 以限制允许通过防火墙的服务。

由于两个路由器接口都在 IEEE 网桥组中配置，因此这种防火墙策略将应用透明防火墙检查。该策略将应用于 IEEE IP 网桥组中的两个接口。检查策略仅应用于跨越网桥组的数据流。这解释了客户端和服务器区域为什么嵌套在专用区域中。

1. 根据上述策略，定义一些用于描述可在区域间通过的数据流的类映射：`conf t`

```

class-map type inspect match-any L4-inspect-class
match protocol tcp
match protocol udp
match protocol icmp

```

2. 配置策略映射以检查刚刚在类映射中定义的数据流：`conf t`

```

policy-map type inspect clients-servers-policy
class type inspect L4-inspect-class
inspect

```

3. 配置客户端区域和服务器区域，并为这些区域分别指定路由器接口：`conf t`

```

zone security clients
zone security servers
int vlan 1
zone-member security clients
int vlan 2
zone-member security servers

```

4. 配置区域对并应用适当的策略映射。**注意：**要检查从客户端区域到服务器区域的连接，目前您只需配置客户端-服务器区域对：`conf t`

```

zone-pair security clients-servers source clients destination servers

```

`service-policy type inspect clients-servers-policy`这样就完成了客户端-服务器区域对的第 4 层检查策略的配置，从而允许从客户端区域到服务器区域的所有 TCP、UDP 和 ICMP 连接。该策略不对辅助信道应用修正，但提供了适用于大多数应用程序连接的简单策略示例。

## 区域策略防火墙的速度策略



限制特定类型网络流量的传输速率，以及限制低优先级流量对重要业务流量的影响等措施通常可为数据网络提供好处。Cisco IOS 软件通过流量策略提供了这种功能，使用流量策略可以限制数据流的标称速率和突发传输。Cisco IOS 软件从 Cisco IOS 版本 12.1(5)T 开始就已支持流量策略。

Cisco IOS 软件版本 12.4(9)T 增强了 ZFW 的速率限制功能，它增加了可以针对匹配特定类映射定义的数据流设置策略的功能，从而可以在其通过防火墙往来于各个安全区域时限制其流速。这使您可以通过一个配置点进行特定流量描述、防火墙策略应用以及数据流带宽消耗策略的设置。ZFW 策略与基于接口的策略不同，因为它只对符合策略的数据流提供传输操作，而对违反策略的数据流提供丢弃操作。ZFW 策略不能用 DSCP 标记数据流。

ZFW 策略只能以字节/秒或数据包/秒的形式指定带宽使用量，而不提供带宽百分比策略。无论是否存在基于接口的策略，都可以应用 ZFW 策略。因此，如果需要使用其他策略功能，您可以通过基于接口的策略应用这些功能。如果同时使用基于接口的策略与防火墙策略，请确保这两种策略不会相互冲突。

## 配置 ZFW 策略

ZFW 策略通过策略映射的类映射将数据流速度限制在用户定义的 8,000 到 2,000,000,000 比特/秒之间，可配置的突发流量值介于 1,000 到 512,000,000 字节之间。

ZFW 策略可以通过在策略映射中的策略操作之后增加配置行进行配置：

```
policy-map type inspect private-allowed-policy
  class type inspect http-class
    inspect
    police rate [bps rate value <8000-2000000000>] burst [value in bytes <1000-512000000>]
```

## 会话控制

ZFW 策略还引入了会话控制，它可以在匹配类映射的策略映射中限制数据流的会话数量。该功能将添加到现有功能中，以根据类映射应用 DoS 保护策略。此外，该功能还将允许对匹配任何给定类映射的跨越区域对的会话数量进行精细控制。如果相同类映射被用于多个策略映射或区域对，则可以在应用不同类映射时使用不同的会话限制。

通过配置包含所需会话数量的参数映射，然后在策略映射下将此参数映射附加到应用于类映射的检查操作中，可以应用会话控制：

```
parameter-map type inspect my-parameters
  sessions maximum [1-2147483647]

policy-map type inspect private-allowed-policy
  class type inspect http-class
    inspect my-parameters
```

参数映射只能应用于检查操作，而不能用于通过或丢弃操作。

使用以下命令可以查看 ZFW 的会话控制和策略活动

```
show policy-map type inspect zone-pair
```

## 应用程序检查

应用程序检查在 ZFW 中引入了附加功能。应用程序检查策略应用于 OSI 模型的第 7 层，用户应用程序将在这一层发送和接收用于允许该应用程序提供有用功能的消息。一些应用程序可能会提供不需要或易受攻击的功能，所以必须过滤掉与这些功能相关的消息，以限制这些应用程序服务的操作

。

Cisco IOS 软件 ZFW 提供了针对以下应用程序服务的应用程序检查和控制：

- HTTP
- SMTP
- POP3
- IMAP
- Sun RPC
- P2P 应用流量
- IM 应用程序

根据各种服务功能的不同，应用程序检查和控制 (AIC) 也有所不同。HTTP 检查可以对一些类型的应用程序活动进行精细过滤，它提供了用于限制传输大小、Web 地址长度和浏览器活动的功能，以强制符合应用程序行为标准，同时限制可以通过服务传输的内容类型。用于 SMTP 的 AIC 可以限制内容长度，并强制符合协议标准。POP3 和 IMAP 检查可帮助确保用户使用安全身份验证机制，以防用户凭证被窃取。

应用程序检查被配置为特定应用程序类映射和策略映射的附加功能集，然后通过检查策略映射中定义应用程序服务策略，应用于现有的检查类映射和策略映射。

## HTTP 应用程序检查

应用程序检查可以应用于 HTTP 流量，以控制将 HTTP 的服务端口不必要地用于其他应用程序，例如 IM、P2P 文件共享和隧道应用程序，这些应用程序可以进行重定向，否则将使用 TCP 80 通过防火墙应用程序。

配置应用程序检查类映射以描述违反允许的 HTTP 流量策略的流量：

```
! configure the actions that are not permitted
class-map type inspect http match-any http-aic-cmap
  match request port-misuse any
  match req-resp protocol-violation
! define actions to be applied to unwanted traffic
policy-map type inspect http http-aic-pmap
  class type insp http http-aic-cmap
    reset
    log
! define class-map for stateful http inspection
class-map type inspect match-any http-cmap
  match protocol http
! define class-map for stateful inspection for other traffic
class-map type inspect match-any other-traffic-cmap
  match protocol smtp
  match protocol dns
  match protocol ftp
! define policy-map, associate class-maps and actions
policy-map type inspect priv-pub-pmap
  class type inspect http-cmap
    inspect
  service-policy http http-aic-pmap
  class type inspect other-traffic-cmap
    inspect
```

## HTTP 应用程序检查改进功能

Cisco IOS 软件版本 12.4(9)T 改进了 ZFW 的 HTTP 检查功能。在 Cisco IOS 软件版本 12.3(14)T

中，Cisco IOS 防火墙引入了 HTTP 应用程序检查功能。Cisco IOS 软件版本 12.4(9)T 通过添加以下功能增强了现有功能：

- 能够根据报头名称和报头值允许、拒绝和监控请求和响应。此功能可用于阻止携带易受攻击的报头字段的请求和响应。
- 能够限制 HTTP 请求和响应报头中的不同元素的大小，例如最大 URL 长度、最大报头长度、最大报头数量，最大报头行长度等。此功能可用于防止缓冲区溢出。
- 能够阻止携带多个相同类型报头的请求和响应；例如，带有两个内容长度报头的请求。
- 能够阻止使用非 ASCII 报头的请求和响应。此功能可用于防止使用二进制和其他非 ASCII 字符向 Web 服务器提交蠕虫和其他恶意内容的各种攻击。
- 能够将各种 HTTP 方法划分到用户指定的类别中，并且能够灵活地阻止/允许/监控每一个组。HTTP RFC 允许使用有限的 HTTP 方法集。一些标准方法被认为不安全，因为它们可用于攻击 Web 服务器的漏洞。许多非标准方法具有不良的安全记录。
- 根据用户配置的正则表达式阻止特定 URI 的方法。此功能让用户可以阻止自定义 URI 和查询。
- 能够使用用户可自定义的字符串伪装报头类型（尤其是服务器报头类型）。此功能可用于防范攻击者通过分析 Web 服务器的响应了解大量信息，然后利用该特定 Web 服务器的漏洞发起攻击。
- 当一个或多个 HTTP 参数值匹配用户以正则表达式形式输入的值时，能够阻止 HTTP 连接或针对 HTTP 连接发出警告。一些可能的 HTTP 值上下文包括报头、正文、用户名、口令、用户代理、请求行、状态行和经过解码的 CGI 变量等。

用于 HTTP 应用程序检查改进功能的配置示例假定有一个简单网络：

防火墙将数据流划分为两类：

- HTTP 数据流
- 所有其他单信道 TCP、UDP 和 ICMP 数据流

HTTP 被分离出来，以允许对 Web 流量进行特定检查。这让您配置本文档第一部分中的策略以及第二部分中的 HTTP 应用程序检查。在本文的第三部分中，您将配置用于 P2P 和 IM 数据流的特定类映射和策略映射。允许从专用区域连接到公共区域。但无法从公共区域连接到专用区域。

有关用于实现初始策略的完整配置，请参阅[附录 C：两个区域的基本区域策略防火墙配置](#)。

## 配置 HTTP 应用程序检查增强功能

HTTP 应用程序检查（以及其他应用程序检查策略）需要比基本第 4 层配置更为复杂的配置。您必须配置第 7 层流量分类和策略以识别要控制的特定流量，然后对需要的流量和不需要的流量应用所需的操作。

HTTP 应用程序检查（类似于其他类型的应用程序检查）只能应用于 HTTP 流量。因此，您必须为特定 HTTP 流量定义第 7 层类映射和策略映射，然后专门为 HTTP 定义第 4 层类映射，并将第 7 层策略应用于第 4 层策略映射中的 HTTP 检查，如下所示：

```
!configure the layer-7 traffic characteristics:
class-map type inspect http match-any http-l7-cmap
  match req-resp protocol-violation
  match request body length gt 4096
!
!configure the action to be applied to the traffic
!matching the specific characteristics:
policy-map type inspect http http-l7-pmap
  class type inspect http http-l7-cmap
  reset
```

```

log
!
!define the layer-4 inspection policy
class-map type inspect match-all http-l4-cmap
  match protocol http
!
!associate layer-4 class and layer-7 policy-map
!in the layer-4 policy-map:
policy-map type inspect private-allowed-policy
  class type inspect http-l4-cmap
  inspect
  service-policy http http-l7-pmap

```

所有这些 HTTP 应用检查流量特性都在第 7 层类映射中定义：

- Header inspection** — 使用此命令可以允许/拒绝/监控其报头与已配置正则表达式匹配的请求或响应。您可以对匹配类映射条件的请求或响应应用允许或重置操作。增加日志操作将导致生成如下 syslog 消息：APPFW-6-HTTP\_HDR\_REGEX\_MATCHED **命令用法**：match {request|response|req-resp} header regex <parameter-map-name> **示例用例配置** http appfw 策略以阻止其报头中包含非 ASCII 字符的请求或响应。parameter-map type regex non\_ascii\_regex
 

```

pattern "[^\x00-\x80]"
class-map type inspect http non_ascii_cm
  match req-resp header regex non_ascii_regex
policy-map type inspect http non_ascii_pm
  class type inspect http non_ascii_cm
  reset

```
- Header length inspection** — 此命令将检查请求或响应报头的长度，并在报头长度超出配置的阈值时应用相应的操作。可以应用的操作有允许或重置。增加日志操作将导致生成如下 syslog 消息：APPFW-4- HTTP\_HEADER\_LENGTH **命令用法**：match {request|response|req-resp} header length gt <bytes> **示例用例配置** http appfw 策略以阻止报头长度超过 4096 字节的请求和响应。class-map type inspect http hdr\_len\_cm
 

```

match req-resp header length gt 4096

policy-map type inspect http hdr_len_pm
  class type inspect http hdr_len_cm
  reset

```
- Header count inspection** — 此命令将验证请求/响应中的报头行数（字段数），并在此数字超出配置的阈值时应用相应的操作。可以应用的操作有允许或重置。增加日志操作将导致生成如下 syslog 消息：APPFW-6- HTTP\_HEADER\_COUNT. **命令用法**：match {request|response|req-resp} header count gt <number> **示例用例配置** http appfw 策略以阻止报头字段数超过 16 个的请求。class-map type inspect http hdr\_cnt\_cm
 

```

match request header count gt 16

policy-map type inspect http hdr_cnt_pm
  class type inspect http hdr_cnt_cm
  reset

```
- Header field inspection** — 使用此命令可以允许/拒绝/监控包含特定 HTTP 报头字段和值的请求/响应。您可以对匹配类映射条件的请求或响应应用允许或重置操作。增加日志操作将导致生成如下 syslog 消息：APPFW-6- HTTP\_HDR\_FIELD\_REGEX\_MATCHED **命令用法**：match {request|response|req-resp} header <header-name> **示例用例配置** http 应用程序检查策略以阻止间谍软件/广告软件：parameter-map type regex ref\_regex
 

```

pattern "\.delfinproject\.com"
pattern "\.looksmart\.com"

parameter-map type regex host_regex
  pattern "secure\.keenvalue\.com"
  pattern "\.looksmart\.com"

```

```
parameter-map type regex usragnt_regex
  pattern "Peer Points Manager"
```

```
class-map type inspect http spy_adwr_cm
  match request header refer regex ref_regex
  match request header host regex host_regex
  match request header user-agent regex usragnt_regex
```

```
policy-map type inspect http spy_adwr_pm
  class type inspect http spy_adwr_cm
  reset
```

- **Header field length inspection** — 使用此命令可以限制报头字段行的长度。您可以对匹配类映射条件的请求或响应应用允许或重置操作。增加日志操作将导致生成如下 syslog 消息：APPFW-6- HTTP\_HDR\_FIELD\_LENGTH. **命令用法**：match {request|response|req-resp} header <header-name> length gt <bytes> **示例用例配置** http appfw 策略以阻止其 cookie 和用户代理字段长度分别超过 256 和 128 的请求。class-map type inspect http hdrline\_len\_cm

```
  match request header cookie length gt 256
  match request header user-agent length gt 128
```

```
policy-map type inspect http hdrline_len_pm
  class type inspect http hdrline_len_cm
  reset
```

- **Inspection of header field repetition** — 此命令将检查请求或响应是否具有重复的报头字段。您可以对匹配类映射条件的请求或响应应用允许或重置操作。当启用日志操作时，它将生成如下 syslog 消息：APPFW-6- HTTP\_REPEATED\_HDR\_FIELDS. **命令用法**：match {request|response|req-resp} header <header-name> **示例用例配置** http appfw 策略以阻止带有多个内容长度报头行的请求或响应。这是常用于防止会话走私的功能之一。class-map type inspect http multi\_occrns\_cm

```
  match req-resp header content-length count gt 1
```

```
policy-map type inspect http multi_occrns_pm
  class type inspect http multi_occrns_cm
  reset
```

- **Method inspection** — HTTP RFC 允许使用有限的 HTTP 方法集。然而，即使一些标准方法也被认为不安全，因为它们可以被用于攻击 Web 服务器的漏洞。许多非标准方法经常被用于恶意活动。因此有必要将方法划分到各种类别中，然后让用户选择要对每个类别执行的操作。此命令为用户提供了一种将各个方法划分到不同类别的灵活方式，例如安全方法、非安全方法、rfc 方法和扩展方法等类别。您可以对匹配类映射条件的请求或响应应用允许或重置操作。增加日志操作将导致生成如下 syslog 消息：APPFW-6-HTTP\_METHOD. **命令用法**：match request method <method> **示例用例配置** http appfw 策略以将各种 HTTP 方法划分到以下三个类别中：安全、不安全和 webdav。下表显示了这些类别。配置操作，以便：允许所有安全方法而不记录到日志中允许所有非安全方法，但记录到日志中阻止所有 webdav 方法并记录到日志中。http policy:

```
class-map type inspect http safe_methods_cm
  match request method get
  match request method head
  match request method option
```

```
class-map type inspect http unsafe_methods_cm
  match request method post
  match request method put
  match request method connect
  match request method trace
```

```
class-map type inspect http webdav_methods_cm
  match request method bcopy
  match request method bdelete
  match request method bmove
```

```

policy-map type inspect http methods_pm
  class inspect http safe_methods_cm
    allow
  class type inspect http unsafe_methods_cm
    allow log
  class type inspect http webdav_methods_cm
    reset log

```

- **URI inspection** — 使用此命令可以允许/拒绝/监控 URI 匹配已配置常规检查的请求。此功能让用户可以阻止自定义 URI 和查询。您可以对匹配类映射条件的请求或响应应用允许或重置操作。增加日志操作将导致生成如下 syslog 消息：APPFW-6- HTTP\_URI\_REGEX\_MATCHED **命令用法**：match

```

request uri regex <parameter-map-name> 示例用例配置 http appfw 策略以阻止其 URI 匹配以下任何一个正则表达式的请求：.。 *cmd.exe。 *sex。 *gambling
parameter-map type regex uri_regex_cm
  pattern ".*cmd.exe"
  pattern ".*sex"
  pattern ".*gambling"

```

```

class-map type inspect http uri_check_cm
  match request uri regex uri_regex_cm

```

```

policy-map type inspect http uri_check_pm
  class type inspect http uri_check_cm
    reset

```

- **URI length inspection** — 此命令将验证在请求中发送的 URI 的长度，并在其长度超出配置的阈值时应用配置的操作。您可以对匹配类映射条件的请求或响应应用允许或重置操作。增加日志操作将导致生成如下 syslog 消息：APPFW-6- HTTP\_URI\_LENGTH. **命令用法**：match request uri

```

length gt <bytes> 示例用例配置 http appfw 策略以便在请求的 URI 长度超出 3076 字节时发出警报。
class-map type inspect http uri_len_cm
  match request uri length gt 3076

```

```

policy-map type inspect http uri_len_pm
  class type inspect http uri_len_cm
    log

```

- **参数检查** — 使用此命令可以允许、拒绝或监控其参数与已配置的常规检查匹配的请求。您可以对匹配类映射条件的请求或响应应用允许或重置操作。增加日志操作将导致生成如下 syslog 消息：APPFW-6- HTTP\_ARG\_REGEX\_MATCHED **命令用法**：match request arg regex <parameter-map-name> **示例用例配置** http appfw 策略以阻止其参数匹配以下任何一个正则表达式的请求：.。

```

*codered。 *attack
parameter-map type regex arg_regex_cm
  pattern ".*codered"
  pattern ".*attack"

```

```

class-map type inspect http arg_check_cm
  match request arg regex arg_regex_cm

```

```

policy-map type inspect http arg_check_pm
  class type inspect http arg_check_cm
    reset

```

- **Argument length inspection** — 此命令将验证在请求中发送的参数的长度，并在其长度超出配置的阈值时应用配置的操作。您可以对匹配类映射条件的请求或响应应用允许或重置操作。增加日志操作将导致生成如下 syslog 消息：APPFW-6- HTTP\_ARG\_LENGTH. **命令用法**：match request arg

```

length gt <bytes> 示例用例配置 http appfw 策略以便在请求的参数长度超出 512 字节时发出警报。
class-map type inspect http arg_len_cm
  match request arg length gt 512

```

```

policy-map type inspect http arg_len_pm
  class type inspect http arg_len_cm

```



log

- **Body inspection** — 使用此 CLI，用户可以指定要与请求或响应正文匹配的正则表达式的列表。您可以对匹配类映射条件的请求或响应应用允许或重置操作。增加日志操作将导致生成如下 **syslog 消息**：APPFW-6- HTTP\_BODY\_REGEX\_MATCHED **命令用法**：match {request|response|req-resp} body regex <parameter-map-name> **示例用例配置** http appfw 以阻止其正文包含模式 `*[Aa][Tt][Tt][Aa][Cc][Kk] parameter-map type regex body_regex pattern ".*[Aa][Tt][Tt][Aa][Cc][Kk]"`  

```
class-map type inspect http body_match_cm
  match response body regex body_regex

policy-map type inspect http body_match_pm
  class type inspect http body_match_cm
  reset
```
- **Body (Content) length inspection** — 此命令将验证通过请求或回应发送的消息的大小。您可以对匹配类映射条件的请求或响应应用允许或重置操作。增加日志操作将导致生成如下 **syslog 消息**：APPFW-4- HTTP\_CONTENT\_LENGTH **命令用法**：match {request|response|req-resp} body length lt <bytes> gt <bytes> **示例用例配置** http appfw 策略以阻止请求或响应中携带的消息大小超过 10K 字节的 http 会话。`class-map type inspect http cont_len_cm match req-resp header content-length gt 10240`  

```
policy-map type inspect http cont_len_pm
  class type inspect http cont_len_cm
  reset
```
- **Status line inspection** — 使用此命令，用户可以指定要与响应的状态行匹配的正则表达式的列表。您可以对匹配类映射条件的请求或响应应用允许或重置操作。增加日志操作将导致生成如下 **syslog 消息**：APPFW-6-HTTP\_STLINE\_REGEX\_MATCHED. **命令用法**：match response status-line regex <class-map-name> **示例用例配置** http appfw 以便在有人试图访问禁止页时记录警报。禁止页通常包含 403 状态代码和状态行，例如 HTTP/1.0 403 page forbidden\r\n。`parameter-map type regex status_line_regex pattern "[Hh][Tt][Tt][Pp][/][0-9][.][0-9][ \t]+403"`  

```
class-map type inspect http status_line_cm
  match response status-line regex status_line_regex

policy-map type inspect http status_line_pm
  class type inspect http status_line_cm
  log
```
- **Content-type inspection** — 此命令将验证消息报头的内容类型是否在支持的内容类型列表中。它还将验证此报头的内容类型是否与消息数据或正文部分的内容匹配。如果配置了关键字 **mismatch**，此命令将验证响应消息的内容类型与已接收请求消息的字段值是否匹配。您可以对匹配类映射条件的请求或响应应用允许或重置操作。增加日志操作将导致生成相应的 **syslog 消息**：APPFW-4- HTTP\_CONT\_TYPE\_VIOLATION, APPFW-4- HTTP\_CONT\_TYPE\_MISMATCH, APPFW-4- HTTP\_CONT\_TYPE\_UNKNOWN **命令用法**：match {request|response|req-resp} header content-type [mismatch|unknown|violation] **示例用例配置** http appfw 策略以阻止携带具有未知内容类型的请求和响应的 http 会话。`class-map type inspect http cont_type_cm match req-resp header content-type unknown`  

```
policy-map type inspect http cont_type_pm
  class type inspect http cont_type_cm
  reset
```
- **Port-misuse inspection** — 此命令用于防止其他应用程序误用 HTTP 端口 (80)，例如 IM、P2P、隧道应用程序等。您可以对匹配类映射条件的请求或响应应用允许或重置操作。增加日志操作将导致生成相应的 **syslog 消息**：APPFW-4- HTTP\_PORT\_MISUSE\_TYPE\_IM

```
APPFW-4-HTTP_PORT_MISUSE_TYPE_P2P
```

```
APPFW-4-HTTP_PORT_MISUSE_TYPE_TUNNEL 命令用法 : match request port-misuse
```

```
{im|p2p|tunneling|any} 示例用例配置 http appfw 策略以阻止被 IM 应用程序误用的 HTTP 会话
```

```
o class-map type inspect http port_misuse_cm  
  match request port-misuse im
```

```
policy-map type inspect http port_misuse_pm  
  class type inspect http port_misuse_cm  
  reset
```

- **Strict-http inspection** — 此命令将对 HTTP 请求和响应启用严格的协议一致性检查。您可以对匹配类映射条件的请求或响应应用允许或重置操作。增加日志操作将导致生成如下 syslog 消息 : APPFW-4- HTTP\_PROTOCOL\_VIOLATION 命令用法 : match req-resp protocol-violation 示例用例配置 http appfw 策略以阻止违反 RFC 2616 的请求或响应 : class-map type inspect http proto-viol\_cm

```
  match req-resp protocol-violation
```

```
policy-map type inspect http proto-viol_pm  
  class type inspect http proto-viol_cm  
  reset
```

- **Transfer-Encoding inspection** — 使用此命令可以允许、拒绝或监控其传输编码类型与已配置的类型匹配的请求/响应。您可以对匹配类映射条件的请求或响应应用允许或重置操作。增加日志操作将导致生成如下 syslog 消息 : APPFW-6- HTTP\_TRANSFER\_ENCODING 命令用法 : match

```
{request|response|req-resp} header transfer-encoding
```

```
{regex <parameter-map-name> |gzip|deflate|chunked|identity|all} 示例用例配置 http appfw 策略
```

```
以阻止使用压缩类型编码的请求或响应。 class-map type inspect http trans_encoding_cm  
  match req-resp header transfer-encoding type compress
```

```
policy-map type inspect http trans_encoding_pm  
  class type inspect http trans_encoding_cm  
  reset
```

- **Java Applet inspection** — 此命令将检查响应中是否包含 Java 小程序，并在检测到小程序时应用已配置的操作。您可以对匹配类映射条件的请求或响应应用允许或重置操作。增加日志操作将导致生成如下 syslog 消息 : APPFW-4- HTTP\_JAVA\_APPLET 命令用法 : match response body java-applet 示例用例配置 http appfw 策略以阻止 Java 小程序。 class-map type inspect http java\_applet\_cm

```
  match response body java-applet
```

```
policy-map type inspect http java_applet_pm  
  class type inspect http java_applet_cm  
  reset
```

## 为即时消息和对等应用程序控制提供 ZFW 支持

Cisco IOS 软件版本 12.4(9)T 为 IM 和 P2P 应用程序提供了 ZFW 支持。

Cisco IOS 软件首先在 Cisco IOS 软件版本 12.4(4)T 中为 IM 应用程序控制提供支持。ZFW 的最初版本并不能在 ZFW 接口中支持 IM 应用程序。因此如果需要控制 IM 应用程序，用户将无法迁移到 ZFW 配置接口。Cisco IOS 软件版本 12.4(9)T 为 IM 检查提供了 ZFW 支持，从而可以支持 Yahoo! Messenger (YM)、MSN Messenger (MSN) 和 AOL Instant Messenger (AIM)。

Cisco IOS 软件版本 12.4(9)T 是首个针对 P2P 文件共享应用程序提供本地 IOS 防火墙支持的 Cisco IOS 软件版本。

IM 和 P2P 检查均提供了用于应用流量的第 4 层和第 7 层策略。这意味着 ZFW 可以提供基本的状态检查以允许或拒绝数据流，同时能够针对各种协议的特定活动提供精细的第 7 层控制，从而可以

允许某些应用程序活动，而拒绝其他应用程序活动。

## P2P 应用程序检查和控制

SDM 2.2 在其防火墙配置部分引入了 P2P 应用程序控制。SDM 使用基于网络的应用程序识别 (NBAR) 和 QoS 策略来检测 P2P 应用程序活动，并将其线路速率设置为零，从而阻止所有 P2P 流量。这样做会产生相应的问题，即那些希望在 IOS 防火墙 CLI 中提供 P2P 支持的 CLI 用户将无法在 CLI 中配置 P2P 阻止，除非他们知道必要的 NBAR/QoS 配置。Cisco IOS 软件版本 12.4(9)T 在 ZFW CLI 中引入了本地 P2P 控制，从而可以利用 NBAR 来检测 P2P 应用程序活动。此软件版本支持以下几种 P2P 应用程序协议：

- BitTorrent
- eDonkey
- Fasttrack
- Gnutella
- KaZaA/KaZaA2
- Winmx

P2P 应用程序很难检测到，这是因为它们采用了“端口跳变”以及其他一些技巧以避免检测，同时 P2P 应用程序的频繁更改和更新也引入了一些问题，因为它们会修改协议的行为。ZFW 集成了本地防火墙状态检查与 NBAR 的数据流识别功能，从而可以在 ZFW 的 CPL 配置接口中提供 P2P 应用程序控制。NBAR 提供了两个出色的功能：

- 可选的启发式应用程序识别，无论其行为多复杂、多难以检测都可以识别应用程序
- 可扩展基础架构提供了更新机制，从而可以保持与协议的更新和修改同步

## 配置 P2P 检查

如前所述，P2P 检查和控制提供了第 4 层状态检查和第 7 层应用程序控制。

如果只需检查本地应用程序服务端口即可，那么第 4 层检查的配置与其他应用程序服务类似：

```
class-map type inspect match-any my-p2p-class
match protocol [bittorrent | edonkey | fasttrack | gnutella | kazaa | kazaa2 | winmx ]
[signature (optional)]
!
policy-map type inspect private-allowed-policy
 class type inspect my-p2p-class
  [drop | inspect | pass]
```

请注意 match protocol [service-name] 中的其他签名选项。通过在 match protocol 语句结尾添加签名选项，可以使用 NBAR 启发式功能在数据流中搜索特定 P2P 应用程序活动的迹象。这包括为避免数据流检测而使用的端口跳变和其他应用程序行为的更改。这种级别的数据流检查将会增加 CPU 使用率，并减小网络吞吐量。如果不应用签名选项，则不会应用 NBAR 启发式分析来检测端口跳变行为，CPU 使用率也不会受到同样程度的影响。

本地服务检查的缺点是，在 P2P 应用程序“跳跃”到非标准的源端口和目标端口，或者 P2P 应用程序经过更新并开始使用无法识别的端口号时，无法保持对 P2P 应用程序的控制：

应用程序	本地端口 ( 通过 12.4(15)T PAM 列表识别 )
bittorrent	TCP 6881-6889
edonkey	TCP 4662

fasttrack	TCP 1214
gnutella	TCP 6346-6349 TCP 6355,5634 UDP 6346-6348
kazaa2	取决于 PAM
winmx	TCP 6699

如果您希望允许 ( 检查 ) P2P 数据流，则可能需要提供其他配置。一些应用程序可能使用多个 P2P 网络，或者实现了一些特定行为，您可能需要在防火墙配置中包含这些行为，这样防火墙应用程序才能正确工作：

- Bittorrent 客户端通常通过 http 与在某个非标准端口上运行的“tracker” ( 对等目录服务器 ) 通信。此端口一般是 TCP 6969，但您可能需要检查 torrent 专用的 tracker 端口。如果您希望允许 Bittorrent，则添加此附加端口的最好方法是将 HTTP 配置为匹配协议之一，并使用 `ip port-map` 命令将 TCP 6969 添加到 HTTP：
- eDonkey 发起的连接似乎会被同时检测为 eDonkey 和 Gnutella。
- Kazaa 检查完全依靠 NBAR 签名检测。

第 7 层 ( 应用程序 ) 检查通过可识别和应用特定于服务的操作 ( 例如有选择地阻止或允许文件搜索、文件传输和文本聊天功能 ) 增强了第 4 层检查。特定于服务的功能将根据服务的不同而不同。

P2P 应用程序检查类似于 HTTP 应用程序检查：

```
!configure the layer-7 traffic characteristics:
class-map type inspect [p2p protocol] match-any p2p-l7-cmap
  match action
!
!configure the action to be applied to the traffic
!matching the specific characteristics:
policy-map type inspect [p2p protocol] p2p-l7-pmap
  class type inspect p2p p2p-l7-cmap
    [ reset | allow ]
  log
!
!define the layer-4 inspection policy
class-map type inspect match-all p2p-l4-cmap
  match protocol [p2p protocol]
!
!associate layer-4 class and layer-7 policy-map
!in the layer-4 policy-map:
policy-map type inspect private-allowed-policy
  class type inspect p2p-l4-cmap
    [ inspect | drop | pass ]
  service-policy p2p p2p-l7-pmap
```

P2P 应用程序检查为第 4 层检查支持的部分应用程序提供了特定于应用程序的功能：

- edonkey
- fasttrack
- gnutella
- kazaa2

每一种应用程序都提供了特定于应用程序的不同匹配条件选项：

*edonkey*

```
router(config)#class-map type inspect edonkey match-any edonkey-l7-cmap router(config-
```

```
router(config)#class-map type inspect fasttrack match-any ftrak-17-cmap router(config-cmap)#match ? file-transfer Match file transfer stream flow Flow based QoS parameters search-file-name Match file name text-chat Match text-chat
```

### **fasttrack**

```
router(config)#class-map type inspect fasttrack match-any ftrak-17-cmap router(config-cmap)#match ? file-transfer File transfer stream flow Flow based QoS parameters
```

### **gnutella**

```
router(config)#class-map type inspect gnutella match-any gtella-17-cmap router(config-cmap)#match ? file-transfer Match file transfer stream flow Flow based QoS parameters
```

### **kazaa2**

```
router(config)#class-map type inspect kazaa2 match-any kazaa2-17-cmap router(config-cmap)#match ? file-transfer Match file transfer stream flow Flow based QoS parameters
```

新的 P2P 协议定义或对于现有 P2P 协议的更新可以使用 NBAR 的动态 pdlm 更新功能进行加载。以下是用于加载新 PDLM 的配置命令：

```
ip nbar pdlm <file-location>
```

新的协议可以在 class type inspect 的 match protocol ... 命令中提供。如果新 P2P 协议具有服务（子协议），则可以使用新的第 7 层检查类映射类型以及第 7 层匹配条件。

## **IM 应用程序检查和控制**

Cisco IOS 软件版本 12.4(4)T 引入了 IM 应用程序检查和控制。12.4(6)T 的 ZFW 中未提供 IM 支持，因此用户不能在相同防火墙策略中同时应用 IM 控制和 ZFW，因为 ZFW 和传统防火墙功能无法在给定接口上共存。

Cisco IOS 软件版本 12.4(9)T 支持以下 IM 服务的状态检查和应用程序控制：

- AOL Instant Messenger
- MSN Messenger
- Yahoo! Messenger

由于 IM 检查依赖于控制每项给定服务对于特定主机组的访问，因此对于大多数服务来说 IM 检查会稍有不同。IM 服务通常依赖于相对恒定的目录服务器组，客户端必须能够与这些目录服务器组通信才能访问 IM 服务。从协议或服务的角度来看，IM 应用程序通常非常难以控制。控制这些应用程序的最有效方式是限制对指定 IM 服务器的访问。

## **配置 IM 检查**

IM 检查和控制提供了第 4 层状态检查和第 7 层应用程序控制。

第 4 层检查的配置与其他应用程序服务类似：

```
class-map type inspect match-any my-im-class
match protocol [aol | msnmsgr | ymsgr ]
!
policy-map type inspect private-allowed-policy
class type inspect my-im-class
[drop | inspect | pass
```

IM 应用程序能够通过多个端口与服务器通信以保持其功能。如果您希望通过应用检查操作以允许给定 IM 服务，则可能不需要使用服务器列表以定义允许访问的 IM 服务服务器。然而，如果您配置了一个指定给定 IM 服务（例如 AOL Instant Messenger）的类映射，并在相关的策略映射中应用了丢

弃操作，则可能导致 IM 客户端尝试使用和查找其他允许连接 Internet 的端口。如果您不想允许连接到给定服务，或者要将 IM 服务功能限制为文本聊天，则您必须定义服务器列表，这样 ZFW 才能识别与 IM 应用程序关联的数据流：

```
!configure the server-list parameter-map:
parameter-map type protocol-info <name>
  server name <name>
  server ip a.b.c.d
  server ip range a.b.c.d a.b.c.d
```

例如，可以按照如下方式定义 Yahoo IM 服务器列表：

```
parameter-map type protocol-info ymsgr-pmap
  server name scs.msg.yahoo.com
  server name scsd.msg.yahoo.com
  server ip 66.77.88.99
  server ip range 103.24.5.67 103.24.5.99
```

您需要将此服务器列表应用到协议定义中：

```
class-map type inspect match-any ym-l4-cmap
  match protocol ymsgr ymsgr-pmap
```

您必须配置 **ip domain lookup** 和 **ip name-server ip.ad.re.ss** 命令才能启用名称解析。

IM 服务器名称很容易变化。您需要定期检查所配置的 IM 服务器列表是否完整和正确。

第 7 层（应用程序）检查通过可识别和应用特定于服务的操作（例如有选择地阻止或允许文本聊天功能，同时拒绝其他服务功能）增强了第 4 层检查。

IM 应用程序检查目前提供了可区分文本聊天活动与其他应用程序服务的功能。要将 IM 活动限制为文本聊天，请配置一个第 7 层策略：

```
class-map type inspect ymsgr match-any ymsgr-text-cmap
  match service text-chat

class-map type inspect ymsgr match-any ymsgr-default-cmap
  match service any

policy-map type inspect im ymsgr-l7-pmap
  class type inspect im ymsgr-text-cmap
    allow
    [log]
  class type inspect im ymsgr-default-cmap
    reset
    [log]
```

将此第 7 层策略应用于之前配置的 Yahoo! Messenger 策略：

```
class-map type inspect match-any my-im-class
  match protocol ymsgr
!
policy-map type inspect private-allowed-policy
  class type inspect my-im-class
    inspect
  service-policy im ymsgr-l7-pmap
```

## [URL 过滤](#)

ZFW 提供了 URL 过滤功能，它通过在路由器上定义白名单或黑名单，或通过将域名转发到 URL 过滤服务器以验证是否可以访问特定域，从而限制只有指定 URL 可以访问 Web 内容。在 Cisco IOS 软件版本 12.4(6)T 到 12.4(15)T 中，ZFW URL 过滤将作为附加策略操作应用，类似于应用程序检



查。

对于基于服务器的 URL 过滤，您必须定义用于描述 `urlfilter` 服务器配置的参数映射：

```
parameter-map type urlfilter websense-parmap
  server vendor [n2h2 | websense] 10.1.1.1
```

如果使用静态白名单或黑名单，您可以定义要具体允许或拒绝的域或子域列表，同时对不匹配列表的数据流应用相反操作：

```
parameter-map type urlfilter websense-parmap
  exclusive-domain deny .disallowed.com
  exclusive-domain permit .cisco.com
```

如果定义 URL 黑名单时在 `exclusive-domain` 定义中使用了 `deny` 选项，则所有其他域将被允许。如果定义了任何“`permit`”定义，则必须显式指定所有要允许的域，类似于 IP 访问控制列表的功能。

设置匹配 HTTP 数据流的类映射：

```
class-map type inspect match-any http-cmap
  match protocol http
```

定义用于将类映射与检查和 `urlfilter` 操作关联的策略映射：

```
policy-map type inspect http-filter-pmap
  class type inspect http-cmap
    inspect
  urlfilter websense-parmap
```

这将配置与 URL 过滤服务器通信的最低要求。有一些选项可以用于定义其他 URL 过滤行为。

某些网络部署可能希望对一些主机或子网应用 URL 过滤，而对其他主机不应用 URL 过滤。例如，在图 9 中，除了特定主机 192.168.1.101 外，所有专用区域主机的 HTTP 数据流都必须经过 URL 过滤服务器的检查。

## 图 9：URL 过滤示例拓扑

这可以通过定义两个不同的类映射实现：

- 一个类映射只用于匹配大型主机组的 HTTP 数据流，此主机组将接受 URL 过滤。
- 一个类映射则用于小型主机组，此主机组不接受 URL 过滤。第二个类映射将匹配 HTTP 数据流，以及不应用 URL 过滤策略的主机列表。

这两个类映射都配置在一个策略映射中，但只有一个类映射将接收 `urlfilter` 操作：

```
class-map type inspect match-any http-cmap
  match protocol http
class-map type inspect match-all http-no-urlf-cmap
  match protocol http
  match access-group 101
!
policy-map type inspect http-filter-pmap
  class type inspect http-no-urlf-cmap
    inspect
  class type inspect http-cmap
    inspect
    urlfilter websense-parmap
!
access-list 101 permit ip 192.168.1.101 any
```

## [控制对于路由器的访问](#)

多数网络安全工程师不会容许将路由器的管理接口（例如 SSH、Telnet、HTTP、HTTPS 和 SNMP 等）暴露在公共 Internet 中，并且在一些情况下，也可能需要控制 LAN 访问路由器。Cisco IOS 软件提供了一些用于限制访问各种接口的选项，包括网络基础保护 (NFP) 功能系列，各种管理接口访问控制机制，以及 ZFW 的自身区域等。您应了解其他功能（例如 VTY 访问控制、管理平面保护和 SNMP 访问控制），以确定哪些路由器控制功能组合最适合您的特定应用程序。

通常，NFP 功能系列最适合用于控制流向路由器本身的数据流。有关使用 NFP 功能保护路由器的信息，请参阅 [Cisco IOS 软件的控制层面安全概述](#)。

如果您决定应用 ZFW 以控制前往/来自路由器自身 IP 地址的数据流，您必须了解此防火墙的默认策略和功能与其他用于中转流量的防火墙不同。中转流量被定义为源和目标 IP 地址与应用于任何路由器接口的任何 IP 地址都不匹配的网络流量，并且路由器不会传送这种流量，例如 ICMP TTL 到期或网络/主机不可访问等网络控制消息。

ZFW 将对区域间移动的数据流应用默认的“全部拒绝”策略，但根据通用规则，从任何区域中直接流向路由器接口地址的流量将被隐式允许。这保证了在对路由器应用区域防火墙配置时，可以保持与路由器管理接口的连接。如果相同的“全部拒绝”策略影响了到路由器的直接连接，则在路由器上配置区域之前，必须应用一种全面的管理策略配置。如果此策略实现不正确或应用顺序错误，这可能会造成管理连接中断。

当将接口配置为某个区域成员时，会将连接到此接口的主机包含在此区域中。但是，前往/来自路由器接口 IP 地址的数据流将不受区域策略的控制（除非使用下图 10 中介绍的环境）。相反，在配置 ZFW 时，路由器上的所有 IP 接口将自动成为自身区域的成员。为了控制从路由器上的各个区域流向路由器接口的 IP 数据流，必须应用策略以阻止或允许/检查区域与路由器自身区域之间的数据流。（请参阅图 10。）

#### 图 10：在网络区域和路由器自身区域之间应用策略

尽管路由器在所有区域与自身区域之间提供了默认允许策略，但如果只配置了从任何区域到自身区域的策略，而未配置从自身区域到与路由器的用户可配置接口连接的各个区域的策略，则所有从路由器发出的数据流在返回路由器时，将遇到从连接区域到自身区域的策略而被阻止。因此，必须检查路由器发出的数据流以允许其返回到自身区域。

**注意：**对于 syslog、tftp、telnet 以及其他控制层面服务等数据流，Cisco IOS 软件总是使用与“最接近”目标主机的接口关联的 IP 地址，并对此数据流应用自身区域防火墙策略。然而，如果服务定义了一个特定接口作为源接口使用包括的命令，但是对 `logging source-interface [type number]`、`ip tftp source-interface [type number]` 和 `ip telnet source-interface [type number]` 没有限制，流量对自身区域被服从。

**注意：**不能将一些使用临时或非可配置接口的服务（尤其是路由器的 voice-over-IP 服务）指定给安全区域。如果这些服务的数据流不能与已配置的安全区域关联，它们将可能无法正常运行。

#### 自身区域策略限制

与中转流量区域对的策略相比，自身区域策略的功能有限：

- 类似于传统状态检查，路由器生成的数据流受限于 TCP、UDP、ICMP 以及用于 H.323 的复杂协议检查。
- 应用程序检查不能用于自身区域策略。
- 不能在自身区域策略中配置会话和速率限制。

#### 自身区域策略配置

在多数情况下，以下访问策略可以用于路由器管理服务：

- 拒绝所有 Telnet 连接，因为 Telnet 的明文协议容易暴露用户凭证和其他敏感信息。
- 允许来自任何区域的任何用户的 SSH 连接。SSH 将加密用户凭证和会话数据，从而防范恶意用户利用数据包捕捉工具监听用户活动，并窃取用户凭证或敏感信息（例如路由器配置）。SSH 第 2 版提供了更加强大的保护功能，它解决了 SSH 第 1 版所固有的一些特定漏洞。
- 如果专用区域是可信赖的，则允许从专用区域到路由器的 HTTP 连接。否则，恶意用户有可能利用专用区域来窃取信息，因为 HTTP 不会通过加密来保护管理流量，并且可能会泄露一些敏感信息，例如用户凭据或配置。
- 允许来自任何区域的 HTTPS 连接。与 SSH 类似，HTTPS 将会加密会话数据和用户凭证。
- 限制对特定主机或子网的 SNMP 访问。SNMP 可以用于修改路由器配置和获取配置信息。应在各种社区上使用配置 SNMP 访问控制。
- 阻止从公共 Internet 到专用区域地址的 ICMP 请求（假设专用区域地址可路由）。必要时，可以对 ICMP 数据流暴露一个或多个公共地址，以用于排除网络故障。一些 ICMP 攻击可以用于耗尽路由器资源或窥探网络拓扑和体系结构。

路由器可以应用这种类型的策略，并针对每个必须受控的区域增加两个区域对。除非数据流不会从相反方向发出，否则在各自的相反方向策略中，接收/发出流量的每个区域对以及路由器自身区域都必须匹配。可以对入站和出站区域对分别应用一个用于描述所有流量的策略映射，或是对每个区域对应用一个特定的策略映射。每个策略映射的特定区域对配置提供了用于查看匹配每个策略映射的活动的精细度。

假设示例网络使用位于 172.17.100.11 的 SNMP 管理站，以及位于 172.17.100.17 的 TFTP 服务器，则以下输出提供了整个管理接口访问策略的示例：

```
class-map type inspect match-any self-service-cmap
  match protocol tcp
  match protocol udp
  match protocol icmp
  match protocol h323
!
class-map type inspect match-all to-self-cmap
  match class-map self-service-cmap
  match access-group 120
!
class-map type inspect match-all from-self-cmap
  match class-map self-service-cmap
!
class-map type inspect match-all tftp-in-cmap
  match access-group 121
!
class-map type inspect match-all tftp-out-cmap
  match access-group 122
!
policy-map type inspect to-self-pmap
  class type inspect to-self-cmap
    inspect
  class type inspect tftp-in-cmap
    pass
!
policy-map type inspect from-self-pmap
  class type inspect from-self-cmap
    inspect
  class type inspect tftp-out-cmap
    pass
!
zone security private
zone security internet
```

```

zone-pair security priv-self source private destination self
  service-policy type inspect to-self-pmap
zone-pair security net-self source internet destination self
  service-policy type inspect to-self-pmap
zone-pair security self-priv source self destination private
  service-policy type inspect from-self-pmap
zone-pair security self-net source self destination internet
  service-policy type inspect from-self-pmap

!
interface FastEthernet 0/0
  ip address 172.16.100.10
  zone-member security internet
!
interface FastEthernet 0/1
  ip address 172.17.100.10
  zone-member security private
!
access-list 120 permit icmp 172.17.100.0 0.0.0.255 any
access-list 120 permit icmp any host 172.17.100.10 echo
access-list 120 deny icmp any any
access-list 120 permit tcp 172.17.100.0 0.0.0.255 host 172.17.100.10 eq www
access-list 120 permit tcp any any eq 443
access-list 120 permit tcp any any eq 22
access-list 120 permit udp any host 172.17.100.10 eq snmp
access-list 121 permit udp host 172.17.100.17 host 172.17.100.10
access-list 122 permit udp host 172.17.100.10 host 172.17.100.17

```

很遗憾，自身区域策略不提供检查 TFTP 传输的功能。因此，如果 TFTP 必须通过防火墙，则防火墙必须允许前往/来自 TFTP 服务器的所有数据流。

如果路由器将终止 IPsec VPN 连接，您还应定义策略以允许 IPsec ESP、IPsec AH、ISAKMP 和 NAT-T IPsec (UDP 4500) 通过。这取决于要使用的服务所需的协议。除了上述策略之外，还可以使用以下策略。请注意对于策略映射的更改，在此更改中插入了一个对 VPN 流量使用通过操作的类映射。通常情况下，加密流量都是可信赖的，除非您的安全策略规定您必须允许前往/来自指定终端的加密流量。

```

class-map type inspect match-all crypto-cmap
  match access-group 123
!
policy-map type inspect to-self-pmap
  class type inspect crypto-cmap
    pass
  class type inspect to-self-cmap
    inspect
  class type inspect tftp-in-cmap
    pass
!
policy-map type inspect from-self-pmap
  class type inspect crypto-cmap
    pass
  class type inspect from-self-cmap
    inspect
  class type inspect tftp-out-cmap
    pass
!
access-list 123 permit esp any any
access-list 123 permit udp any any eq 4500
access-list 123 permit ah any any
access-list 123 permit udp any any eq 500

```

## 区域防火墙和广域应用程序服务

有关提供配置示例和使用指导的应用程序说明，请参阅 [Cisco 广域应用程序服务 \(软件版本 4.0.13\) - 软件版本 4.0.13 的新功能](#)

## 使用 show 和 debug 命令监控区域策略防火墙

ZFW 引入了一些用于查看策略配置和监控防火墙活动的新命令。

显示区域说明和指定区域中包含的接口：

```
show zone security [<zone-name>]
```

如果不提供区域名称，此命令将显示所有已配置区域的信息。

```
Router#show zone security z1 zone z1 Description: this is test zone1 Member Interfaces:  
Ethernet0/0
```

显示源区域、目标区域以及应用于此区域对的策略：

```
show zone-pair security [source <source-zone-name>] [destination <destination-zone-name>]
```

如果不指定源区域或目标区域，则将显示所有具有源区域、目标区域和相关策略的区域对。如果仅提供源区域/目标区域，则将显示所有包含此区域作为源区域/目标区域的区域对。

```
Router#show zone-pair security zone-pair name zp Source-Zone z1 Destination-Zone z2 service-  
policy p1
```

显示指定的策略映射：

```
show policy-map type inspect [<policy-map-name>] [class <class-map-name>]
```

如果不指定策略映射名称，则将显示所有检查类型的策略映射（包括含有子类型的第 7 层策略映射）。

```
Router#show policy-map type inspect p1 Policy Map type inspect p1 Class c1 Inspect
```

显示指定区域对上现有的运行时检查类型策略映射的统计数据。

```
show policy-map type inspect zone-pair [zone-pair-name] [sessions]
```

如果不指定区域对名称，则将显示所有区域对的策略映射。

**sessions** 选项用于显示指定区域对的策略映射应用程序创建的检查会话。

```
Router#show policy-map type inspect zone-pair zp Zone-pair: zp Service-policy : p1 Class-map: c1  
(match-all) Match: protocol tcp Inspect Session creations since subsystem startup or last reset  
0 Current session counts (estab/half-open/terminating) [0:0:0] Maxever session counts  
(estab/half-open/terminating) [0:0:0] Last session created never Last statistic reset never Last  
session creation rate 0 Last half-open session total 0 Class-map: c2 (match-all) Match: protocol  
udp Pass 0 packets, 0 bytes Class-map: class-default (match-any) Match: any Drop 0 packets, 0  
bytes
```

**urlfilter** 关键字用于显示与指定策略映射（如果未指定区域对名称，则指所有目标的策略映射）的 **urlfilter** 相关的统计数据：

```
show policy-map type inspect zone-pair [zone-pair-name] [urlfilter [cache]]
```

如果同时指定了 **cache** 和 **urlfilter** 关键字，则将显示 IP 地址的 **urlfilter** 缓存。

检查策略映射的 **show policy-map** 命令总结：

```
show policy-map type inspect inspect { <policy name> [class <class name>] | zone-pair [<zone-pair name>] [sessions | urlfilter cache] }
```

## [调整区域策略防火墙的拒绝服务保护](#)

ZFW 提供了 DoS 保护以便在网络活动发生巨大变化时警告网络工程师，同时缓解有害活动以减少网络活动变化的影响。ZFW 对每个策略映射的类映射单独维护一个计数器。因此，如果一个类映射用于两个不同区域对的策略映射，则将应用两套不同的 DoS 保护计数器。

在 12.4(11)T 之前的 Cisco IOS 软件版本中，ZFW 默认会提供 DOS 攻击缓解。Cisco IOS 软件版本 12.4(11)T 更改了默认的 DoS 保护行为。有关进一步的讨论以及调整 ZFW DoS 保护的过程，请参阅[调整 Cisco IOS 防火墙的拒绝服务保护](#)。

有关 TCP SYN DOS 攻击的详细信息，请参阅[定义用于防范 TCP SYN 拒绝服务攻击的策略](#)。

## [附录](#)

### [附录 A：基本配置](#)

```
ip subnet-zero
ip cef
!
bridge irb
!
interface FastEthernet0
 ip address 172.16.1.88 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1
 ip address 172.16.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet2
 switchport access vlan 2
!
interface FastEthernet3
 switchport access vlan 2
!
interface FastEthernet4
 switchport access vlan 1
!
interface FastEthernet5
 switchport access vlan 1
!
interface FastEthernet6
 switchport access vlan 1
!
interface FastEthernet7
 switchport access vlan 1
!
interface Vlan1
 no ip address
 bridge-group 1
!
interface Vlan2
```

```

no ip address
bridge-group 1
!
interface BVI1
 ip address 192.168.1.254 255.255.255.0
 ip route-cache flow
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.1.1
!
bridge 1 protocol ieee
bridge 1 route ip
!
end

```

## 附录 B : 最终 ( 完整 ) 配置

```

ip subnet-zero
ip cef
!
ip port-map user-Xwindows port tcp from 6900 to 6910
!
class-map type inspect match-any L4-inspect-class
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-any L7-inspect-class
 match protocol ssh
 match protocol ftp
 match protocol pop
 match protocol imap
 match protocol esmtp
 match protocol http
class-map type inspect match-any dns-http-class
 match protocol dns
 match protocol http
class-map type inspect match-any smtp-class
 match protocol smtp
class-map type inspect match-all dns-http-acl-class
 match access-group 110
 match class-map dns-http-class
class-map type inspect match-all smtp-acl-class
 match access-group 111
 match class-map smtp-class
class-map type inspect match-any Xwindows-class
 match protocol user-Xwindows
class-map type inspect match-any internet-traffic-class
 match protocol http
 match protocol https
 match protocol dns
 match protocol icmp
class-map type inspect http match-any bad-http-class
 match port-misuse all
 match strict-http
!
policy-map type inspect clients-servers-policy
 class type inspect L4-inspect-class
 inspect
policy-map type inspect private-dmz-policy
 class type inspect L7-inspect-class
 inspect
policy-map type inspect internet-dmz-policy
 class type inspect dns-http-acl-class
 inspect

```

```
class type inspect smtp-acl-class
inspect
policy-map type inspect servers-clients-policy
class type inspect Xwindows-class
inspect
policy-map type inspect private-internet-policy
class type inspect internet-traffic-class
inspect
class type inspect bad-http-class
drop
!
zone security clients
zone security servers
zone security private
zone security internet
zone security dmz
zone-pair security private-internet source private destination internet
service-policy type inspect private-internet-policy
zone-pair security servers-clients source servers destination clients
service-policy type inspect servers-clients-policy
zone-pair security clients-servers source clients destination servers
service-policy type inspect clients-servers-policy
zone-pair security private-dmz source private destination dmz
service-policy type inspect private-dmz-policy
zone-pair security internet-dmz source internet destination dmz
service-policy type inspect internet-dmz-policy
!
bridge irb
!
interface FastEthernet0
ip address 172.16.1.88 255.255.255.0
zone-member internet
!
interface FastEthernet1
ip address 172.16.2.1 255.255.255.0
zone-member dmz
!
interface FastEthernet2
switchport access vlan 2
!
interface FastEthernet3
switchport access vlan 2
!
interface FastEthernet4
switchport access vlan 1
!
interface FastEthernet5
switchport access vlan 1
!
interface FastEthernet6
switchport access vlan 1
!
interface FastEthernet7
switchport access vlan 1
!
interface Vlan1
no ip address
zone-member clients
bridge-group 1
!
interface Vlan2
no ip address
zone-member servers
bridge-group 1
```



```
!  
interface BVII1  
 ip address 192.168.1.254 255.255.255.0  
 zone-member private  
!  
ip classless  
ip route 0.0.0.0 0.0.0.0 172.16.1.1  
!  
access-list 110 permit ip any host 172.16.2.2 access-list 111 permit ip any host 172.16.2.3 !  
bridge 1 protocol ieee bridge 1 route ip ! End
```

## [附录 C : 两个区域的基本区域策略防火墙配置](#)

本示例提供了一个基础的简单配置，用于测试 Cisco IOS 软件 ZFW 的增强功能。此配置是用于两个区域的模式配置，这两个区域配置在 1811 路由器上。专用区域应用于路由器的固定交换机端口，因此该交换机端口上的所有主机都连接到 VLAN1。公共区域应用于 FastEthernet 0。

```
class-map type inspect match-any private-allowed-class  
 match protocol tcp  
 match protocol udp  
 match protocol icmp  
class-map type inspect match-all http-class  
 match protocol http  
!  
policy-map type inspect private-allowed-policy  
 class type inspect http-class  
 inspect my-parameters class type inspect private-allowed-class inspect ! zone security private  
zone security public zone-pair security priv-pub source private destination public service-  
policy type inspect private-allowed-policy ! interface fastethernet 0 zone-member security  
public ! Interface VLAN 1 zone-member security private
```

## [相关信息](#)

- [技术支持和文档 - Cisco Systems](#)