流量区域

可以向流量区域分配多个接口，流量区域允许现有数据流的流量在该区域内的任何接口上进出ASA。此功能允许 ASA 上的等价多路径 (ECMP) 路由以及对多个接口分担流向 ASA 的外部流量进行负载均衡。

关于流量区域

本节介绍应如何使用网络中的流量区域。

未分区行为

自适应安全算法在决定是允许还是拒绝流量时会考虑数据包的状态。流量的执行参数之一是流入和流出同一端口的流量。任何流入其他接口的现有流量都将被 ASA 丢弃。

通过流量区域，您可以将多个接口集合在一起，这样流入或流出区域的任意接口的流量都将执行自适应安全算法安全检查。

相关主题

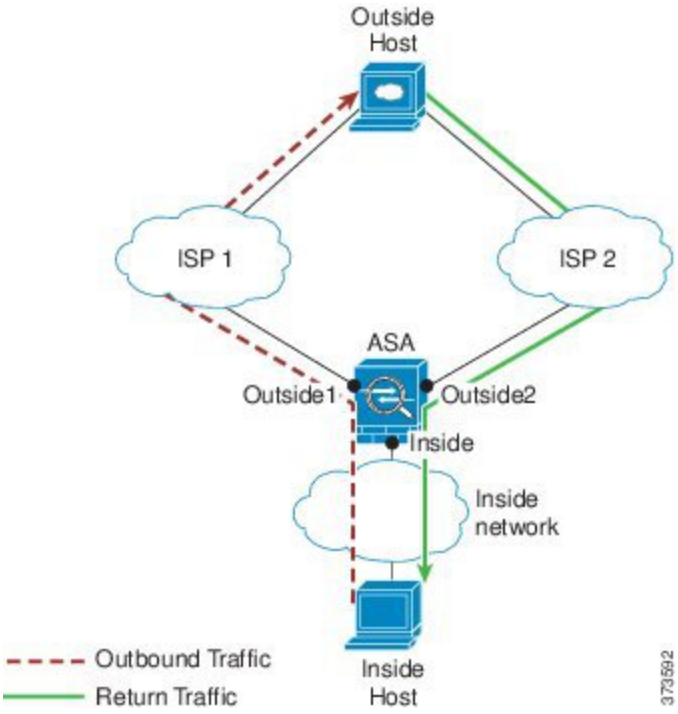
状态监测概览

为什么使用区域？

您可以使用区域来支持几种路由情景。

非对称路由

在以下场景中，通过 Outside1 接口上的 ISP 1 在内部主机和外部主机之间建立了连接。由于目标网络上的非对称路由，从 Outside2 接口上的 ISP 2 返回已到达的流量。

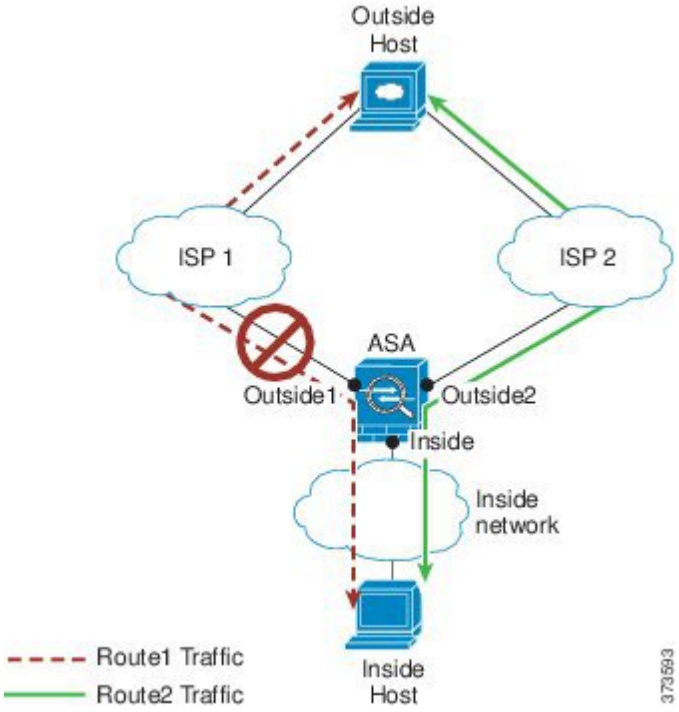


非区域问题：ASA 将为每个接口维护连接表。返回到达 Outside2 的流量时，它不会匹配连接表，并且将被丢弃。对于ASA集群，如果集群包含至同一路由器的多个邻接，则非对称路由可能会造成无法接受的流量损失。

通过划分区域解决问题：ASA 针对每个区域维护连接表。如果您将 Outside1 和 Outside2 集合到一个区域中，当返回到达 Outside2 的流量时，它将匹配每区域连接表，并且允许连接。

丢失的路由

在以下场景中，通过 Outside1 接口上的 ISP 1 在内部主机和外部主机之间建立了连接。由于 Outside1 和 ISP 1 之间的路由已丢失或移动，流量需要通过 ISP 2 采取不同的路由。

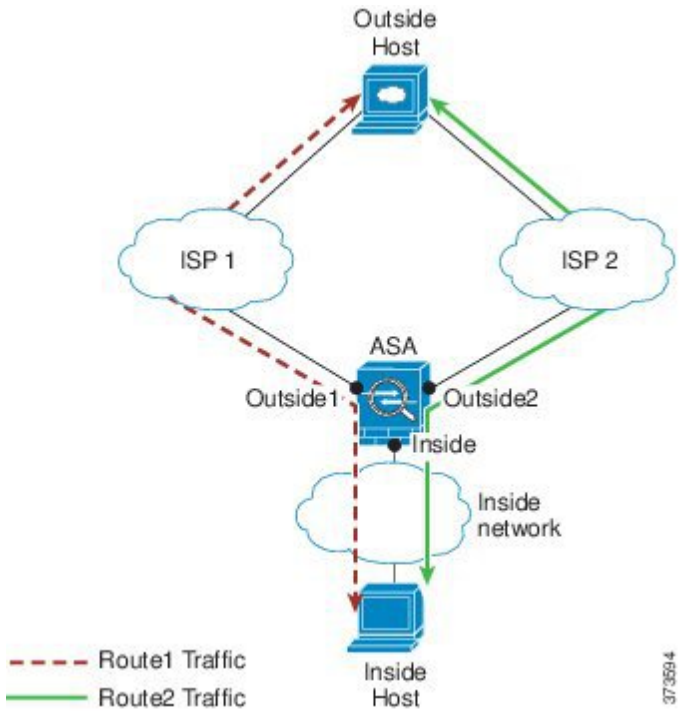


因未划分区域出现的问题：内部主机和外部主机之间的连接将被删除；您必须使用新的次优路由建立新连接。对于 UDP，新路由将在单次丢包之后使用；但对于 TCP，需要重新建立新连接。

区域解决方案：ASA 将检测丢失的路由并通过 ISP 2 切换至新路径的流量。流量将被无缝转发，无任何丢包现象。

负载均衡

在以下场景中，通过 Outside1 接口上的 ISP 1 在内部主机和外部主机之间建立了连接。借助通过 Outside2 上的 ISP 2 的等价路由建立了第二个连接。



因未划分区域出现的问题：无法进行跨接口负载均衡；您只能在一个接口上通过等价路由进行负载均衡。

区域解决方案：ASA 将跨区域内所有接口上的多达八个成本相同的路由实施连接负载均衡。

每区域连接和路由表

ASA维护每区域连接表，使流量能够到达任何一个区域接口。此外，ASA还维护每区域路由表，提供 ECMP 支持。

ECMP 路由

ASA 支持等开销多路径 (ECMP) 路由。

未划分区域的 ECMP 支持

如果没有区域，每个接口最多支持 8 个等价静态或动态路由。例如，您可以在外部接口上配置三个默认路由，指定不同的网关：

```
route outside 0 0 10.1.1.2
route outside 0 0 10.1.1.3
route outside 0 0 10.1.1.4
```

在这种情况下，流量在外部接口上的 10.1.1.2、10.1.1.3 和 10.1.1.4 之间进行负载均衡。流量基于散列源和目标 IP 地址的算法在指定网关之间进行分发。

不支持跨多个接口执行 ECMP，因此您不能在不同接口上定义到同一目标的路由。使用上述任一路由配置时，不允许使用以下路由：

```
route outside2 0 0 10.2.1.1
```

划分区域的 ECMP 支持

如果有区域，在一个区域中最多可以跨 8 个接口配置最多 8 个等价静态或动态路由。例如，您可以在区域中跨三个接口配置三个默认路由：

```
route outside1 0 0 10.1.1.2
route outside2 0 0 10.2.1.2
route outside3 0 0 10.3.1.2
```

同样，动态路由协议可以 自动配置等价路由。ASA 使用更稳健的负载均衡机制 跨接口对流量进行负载均衡。

当某条路由丢失时，ASA 将流量无缝 移至其他路由。

如何对连接进行负载均衡

ASA 可以使用数据包六元组（源和目标 IP 地址、源和目标端口、协议和入口接口）构成的散列跨等价路由对连接进行负载均衡。除非路由丢失，否则连接将在其持续时间内在所选接口上保持不中断的状态。

连接中的数据包不会跨路由进行负载均衡；连接只使用一个路由，除非此路由丢失。

ASA 执行负载均衡时，不考虑接口带宽或其他参数。您应确保同一区域中的所有接口都有相同的特性，例如 MTU、带宽等。

用户不能配置负载均衡算法。

回退到另一区域中的路由

当路由在某个接口上丢失时，如果区域中没有其他路由可用，则 ASA 将使用来自其他接口/区域的路由。如果使用此备用路由，可能会发生丢包现象，就像使用未划分区域的路由支持一样。

基于接口的安全策略

区域允许流量进出区域中的任何接口，但安全策略（访问规则、NAT 等）本身仍然应用于每个接口，而非每个区域。如果为区域中的所有接口配置相同的安全策略，则可对该流量成功实施 ECMP 和负载均衡。有关所需并行接口配置的详细信息，请参阅流量区域的前提条件，第 7 页。

流量区域支持的服务

区域支持以下服务：

- 访问规则

- NAT
- 服务规则，QoS 流量管制除外。
- 路由

虽然没有完整的划分区域支持，但您还可以配置流入流量和流出流量，第 6 页中列出的流向设备服务和流出设备服务。

请勿为流量区域中的接口配置其他服务（例如，VPN 或 Botnet 流量过滤器）；它们可能不会按预期运行或扩展。

注释 有关如何配置安全策略的详细信息，请参阅流量区域的前提条件，第 7 页。

安全级别

添加到区域的第一个接口决定区域的安全级别。所有其他接口必须具有相同的安全级别。要更改区域中接口的安全级别，除了一个接口之外，所有其他接口都必须删除，然后更改安全级别，再重新添加接口。

流量的主接口和当前接口

每个连接流都是在初始入口和出口接口的基础上构建的。这些接口是主接口。

如果由于路由更改或非对称路由而使用新的出口接口，则新接口为当前接口。

加入或离开区域

将接口分配到区域时，该接口上的所有连接都会删除。必须重新建立连接。

如果从区域删除某个接口，以该接口为主接口的连接都会删除。必须重新建立连接。如果该接口是当前接口，ASA 会将连接移回主接口。区域路由表也会刷新。

区域内流量

要允许流量进入一个接口，并且从同一区域内的另一接口退出，请启用 **same-security permit intra-interface** 命令（允许流量进出同一接口）以及 **same-security permit inter-interface** 命令（允许流量在同一安全级别的接口之间传送）。否则，流量不能在同一区域中的两个接口之间路由。

流入流量和流出流量

- 您不能向区域添加管理专用接口或管理访问接口。
- 对于区域中常规接口上的管理流量，仅支持对现有流量进行非对称路由；无 ECMP 支持。

- 您只能在一个区域接口上配置管理服务，但要利用非对称路由支持，需要在所有接口上配置管理服务。即使所有接口上的配置是并行的，也不支持 ECMP。
- ASA 在一个区域中支持以下流入服务和流出服务：
  - Telnet
  - SSH
  - HTTPS
  - SNMP
  - 系统日志

区域内重叠的 IP 地址

对于非区域接口，只要正确配置了 NAT，ASA 在接口上使用重叠的 IP 地址网络。但是，不支持同一区域中的接口上的重叠网络。

流量区域的前提条件

- 配置所有接口参数，包括名称、IP 地址和安全级别。注意，安全级别必须匹配区域中的所有接口。您应根据带宽和其他第 2 层属性计划同类接口的集合。
- 配置以下服务以便在所有区域接口上匹配：
  - 访问规则 - 将同一访问规则应用到所有区域成员接口，或者使用全局访问规则。

    例如：

    ```
    access-list ZONE1 extended permit tcp any host WEBSERVER1 eq 80
    access-group ZONE1 in interface outside1
    access-group ZONE1 in interface outside2
    access-group ZONE1 in interface outside3
    ```

  - NAT - 在区域的所有成员接口上配置相同的 NAT 策略，或者使用全局 NAT 规则（换句话说，使用“any”表示 NAT 规则中的区域接口）。

    不支持接口 PAT。

    例如：

    ```
    object network WEBSERVER1
      host 10.9.9.9 255.255.255.255
      nat (inside,any) static 209.165.201.9
    ```

注释 使用接口特定 NAT 和 PAT 池时，ASA 无法在原始接口发生故障的情况下切换连接。

如果使用的是接口特定 PAT 池，则来自同一主机的多个连接可能会对不同接口进行负载均衡，并使用不同的映射 IP 地址。在此情况下，使用多个并发连接的互联网服务或许无法正确工作。

- 服务规则 - 使用全局服务策略，或向区域中的每个接口分配相同策略。

  不支持 QoS 流量管制。

  例如：

```
service-policy outside_policy interface outside1
service-policy outside_policy interface outside2
service-policy outside_policy interface outside3
```

注释 对于 VoIP 检测，区域负载均衡会造成无序数据包增加。发生这种情况的原因是，后面的数据包可能先于前面的采用不同路径的数据包到达 ASA。无序数据包的特征包括：

- 中间节点（防火墙和 IDS）和接收端节点（如果使用查询）上的内存利用率更高。
- 视频或语音质量差。

为减少这些影响，我们建议 IP 地址仅用于 VoIP 流量的负载分配。

- 配置路由时着眼于 ECMP 区域功能。

流量区域指南

防火墙模式

仅支持路由防火墙模式。不支持透明防火墙模式或路由模式下的网桥组接口。

故障切换

- 您不能将故障切换或状态链路添加到区域。

- 在主用/主用故障切换模式下，您可以在每个情景中将接口分配给非对称路由 (ASR) 组。此服务允许在对等设备上的类似接口返回的流量恢复到原始设备。您无法在一个情景中同时配置 ASR 组和流量区域。如果在情景中配置一个区域，任何情景接口都不能属于 ASR 组。有关 ASR 组的详细信息，请参阅配置非对称路由数据包支持（主用/主用模式）。
- 仅将每个连接的主接口复制到备用设备；不复制当前接口。如果备用设备变为主用状态，它将根据需要分配一个新的当前接口。

集群

- 您不能将集群控制链路添加到区域。

型号指南

不能将 Firepower 1010 交换机端口和 VLAN 接口添加到区域。

其他准则

- 您最多可以创建 256 个区域。
- 您可以将以下类型的接口添加到区域：
  - 物理
  - VLAN
  - EtherChannel
  - 冗余
- 您不能添加以下类型的接口：
  - 管理专用
  - 管理访问
  - 故障切换或状态链路
  - 集群控制链路
  - EtherChannel 或冗余接口中的成员接口
  - VNI；此外，如果常规数据接口被标记为 nve-only，它不能成为区域的成员。
  - BVI，或网桥组成员接口。
- 接口只能是一个区域的成员。
- 每个区域最多可包含 8 个接口。
- 对于 ECMP，在所有区域接口上，每个区域最多可以添加 8 个等价路由。您也可以将单个接口上的多个路由配置为 8 路由限制的一部分。

- 在向区域添加接口时，将删除这些接口的所有静态路由。
- 不能在区域的接口上启用 DHCP 中继。
- 对于负载均衡到单独接口的片段，ASA 不支持分段的数据包重组；这些片段将被丢弃。
- 区域中的接口上不支持 PIM/IGMP 组播路由。

配置流量区域

配置已命名区域，并向该区域分配接口。

过程

步骤 1 添加区域：

zone *name*

示例：

```
zone outside
```

区域名称的最大长度为 48 个字符。

步骤 2 向区域添加接口：

interface *id* **zone-member** *zone_name*

示例：

```
interface gigabitethernet0/0
  zone-member outside
```

步骤 3 向区域添加更多接口；确保它们与您添加的第一个接口具有相同的安全级别。

示例：

```
interface gigabitethernet0/1
  zone-member outside
interface gigabitethernet0/2
  zone-member outside
interface gigabitethernet0/3
  zone-member outside
```

示例

以下示例配置具有 4 个成员接口的外部区域：

```
zone outside
interface gigabitethernet0/0
  zone-member outside
interface gigabitethernet0/1
  zone-member outside
interface gigabitethernet0/2
  zone-member outside
interface gigabitethernet0/3
  zone-member outside
```

监控流量区域

本节介绍如何监控流量区域。

区域信息

- **show zone** [*name*]

  显示区域 ID、情景、安全级别和成员。

  请参阅以下所示的 **show zone** 命令的输出：

```
ciscoasa# show zone outside-zone

Zone: zone-outside id: 2
Security-level: 0
Context: test-ctx
 Zone Member(s) : 2
  outside1       GigabitEthernet0/0
  outside2       GigabitEthernet0/1
```

- **show nameif zone**

  显示接口名称和区域名称。

  请参阅以下所示的 **show nameif zone** 命令的输出：

```
ciscoasa# show nameif zone
Interface               Name                    zone-name      Security
GigabitEthernet0/0      inside-1                inside-zone     100
GigabitEthernet0/1.21   inside                  inside-zone     100
GigabitEthernet0/1.31   4                                         0
GigabitEthernet0/2      outside                 outside-zone   0
Management0/0           lan                                       0
```

区域连接

- **show conn** [**long** | **detail**] [**zone** *zone_name* [**zone** *zone_name*] [...]]

show conn zone 命令可显示区域的连接。**long** 和 **detail** 关键字可显示用于构建连接的主接口和用于转发流量的当前接口。

请参阅以下所示的 **show conn long zone** 命令的输出：

```
ciscoasa# show conn long zone zone-inside zone zone-outside

TCP outside-zone:outside1(outside2): 10.122.122.1:1080
inside-zone:inside1(inside2): 10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

- **show asp table zone**

  显示用于调试的加速安全路径表。

- **show local-host** [**zone** *zone_name* [**zone** *zone_name*] [...]]

  显示区域内本地主机的网络状态。

  请参阅以下所示的 **show local-host zone** 命令的输出。首先列出的是主接口，当前接口用括号括起来。

```
ciscoasa# show local-host zone outside-zone

Zone:outside-zone: 4 active, 5 maximum active, 0 denied
local host: <10.122.122.1>,
    TCP flow count/limit = 3/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited

  Conn:
 TCP outside-zone:outside1(outside2): 10.122.122.1:1080
inside-zone:inside1(inside2): 10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

区域路由

- **show route zone**

  显示区域接口的路由。

  请参阅以下所示的 **show route zone** 命令的输出：

```
ciscoasa# show route zone

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

S    192.168.105.1 255.255.255.255 [1/0] via 172.16.1.1, outside-zone:outside1
C    192.168.212.0 255.255.255.0 is directly connected, lan-zone:inside,
```

```
C    172.16.1.0 255.255.255.0 is directly connected, wan-zone:outside2
S    10.5.5.0 255.255.255.0 [1/0] via 172.16.1.1, wan-zone:outside2
O    10.2.2.1 255.255.255.255 [110/11] via 192.168.212.3, 2:09:24, lan-zone:inside
O    10.1.1.1 255.255.255.255 [110/11] via 192.168.212.2, 2:09:24, lan-zone:inside
```

- **show asp table routing**

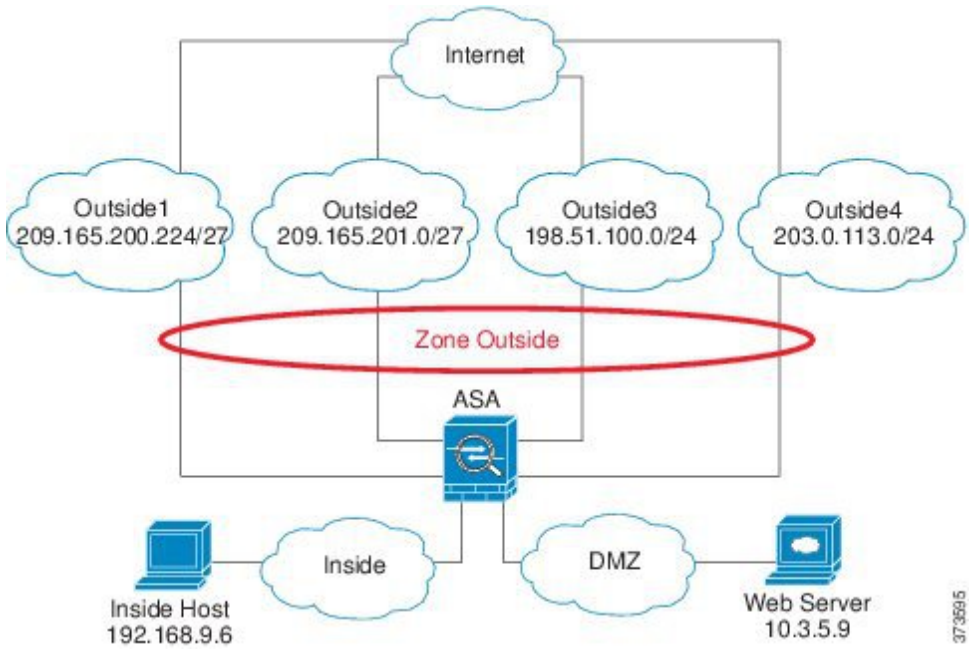
  显示用于调试的加速安全路径表，并显示与每个路由关联的区域。

  请参阅以下所示的 **show asp table routing** 命令的输出：

```
ciscoasa# show asp table routing
route table timestamp: 60
in   255.255.255.255 255.255.255.255 identity
in   10.1.0.1       255.255.255.255 identity
in   10.2.0.1       255.255.255.255 identity
in   10.6.6.4         255.255.255.255 identity
in   10.4.4.4         255.255.255.255 via 10.4.0.10 (unresolved, timestamp: 49)
in   172.0.0.67       255.255.255.255 identity
in   172.0.0.0       255.255.255.0   wan-zone:outside2
in   10.85.43.0      255.255.255.0   via 10.4.0.3 (unresolved, timestamp: 50)
in   10.85.45.0      255.255.255.0   via 10.4.0.20 (unresolved, timestamp: 51)
in   192.168.0.0        255.255.255.0   mgmt
in   192.168.1.0       255.255.0.0     lan-zone:inside
out  255.255.255.255 255.255.255.255 mgmt
out  172.0.0.67       255.255.255.255 mgmt
out  172.0.0.0        255.255.255.0   mgmt
out  10.4.0.0       240.0.0.0       mgmt
out  255.255.255.255 255.255.255.255 lan-zone:inside
out  10.1.0.1       255.255.255.255 lan-zone:inside
out  10.2.0.0       255.255.0.0     lan-zone:inside
out  10.4.0.0       240.0.0.0       lan-zone:inside
```

流量区域示例

以下示例将 4 个 VLAN 接口分配给了外部区域，并且配置了 4 个默认等价路由。为内部接口配置了 PAT，Web 服务器在使用静态 NAT 的 DMZ 接口上可用。




```
interface gigabitethernet0/0
  no shutdown
  description outside switch 1
interface gigabitethernet0/1
  no shutdown
  description outside switch 2

interface gigabitethernet0/2
  no shutdown
  description inside switch

zone outside

interface gigabitethernet0/0.101
  vlan 101
  nameif outside1
  security-level 0
  ip address 209.165.200.225 255.255.255.224
  zone-member outside
  no shutdown

interface gigabitethernet0/0.102
  vlan 102
  nameif outside2
  security-level 0
  ip address 209.165.201.1 255.255.255.224
  zone-member outside
  no shutdown

interface gigabitethernet0/1.201
  vlan 201
  nameif outside3
  security-level 0
  ip address 198.51.100.1 255.255.255.0
  zone-member outside
  no shutdown
```

```
interface gigabitethernet0/1.202
  vlan 202
  nameif outside4
  security-level 0
  ip address 203.0.113.1 255.255.255.0
  zone-member outside
  no shutdown

interface gigabitethernet0/2.301
  vlan 301
  nameif inside
  security-level 100
  ip address 192.168.9.1 255.255.255.0
  no shutdown

interface gigabitethernet0/2.302
  vlan 302
  nameif dmz
  security-level 50
  ip address 10.3.5.1 255.255.255.0
  no shutdown

# Static NAT for DMZ web server on any destination interface
object network WEBSERVER
  host 10.3.5.9 255.255.255.255
  nat (dmz,any) static 209.165.202.129 dns

# Dynamic PAT for inside network on any destination interface
object network INSIDE
  subnet 192.168.9.0 255.255.255.0
  nat (inside,any) dynamic 209.165.202.130

# Global access rule for DMZ web server
access-list WEB-SERVER extended permit tcp any host WEBSERVER eq 80
access-group WEB-SERVER global

# 4 equal cost default routes for outside interfaces
route outside1 0 0 209.165.200.230
route outside2 0 0 209.165.201.10
route outside3 0 0 198.51.100.99
route outside4 0 0 203.0.113.87
# Static routes for NAT addresses - see redistribute static command
route dmz 209.165.202.129 255.255.255.255 10.3.5.99
route inside 209.165.202.130 255.255.255.255 192.168.9.99

# The global service policy
class-map inspection_default
  match default-inspection-traffic
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
    dns-guard
    protocol-enforcement
    nat-rewrite
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225 _default_h323_map
    inspect h323 ras _default_h323_map
    inspect ip-options _default_ip_options_map
    inspect netbios
    inspect rsh
```

```
    inspect rtsp
    inspect skinny
    inspect esmtp _default_esmtp_map
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
service-policy global_policy global
```

流量区域的历史记录

功能名称	平台版本	说明
流量区域	9.3(2)	您可以将接口集合到一个流量区域以实现流量负载均衡（使用等价多路径 (ECMP) 路由）、路由冗余以及多个接口之间的非对称路由。 **注释** 您不能将安全策略应用于已命名的区域；安全策略是基于接口的策略。当区域中的接口配置了相同的访问规则、NAT 和服务策略时，负载均衡和非对称路由将能够正常工作。 引入或修改了以下命令：**zone**, **zone-member**、**show running-config zone**、**clear configure zone**、**show zone**、**show asp table zone**、**show nameif zone**、**show conn long**、**show local-host zone**、**show route zone**、**show asp table routing**、**clear conn zone**、**clear local-host zone**。
clear local-host 命令	9.14(1)	已弃用 **clear local-host** 命令及其所有属性和关键字。将会在未来的版本中删除。