透明或路由防火墙模式

本章介绍如何将防火墙模式设置为路由或透明模式，以及防火墙在各种防火墙模式下的工作方式。

可以在多情景模式下为每个情景独立设置防火墙模式。

关于防火墙模式

ASA支持两种防火墙模式：路由防火墙模式和透明防火墙模式。

关于路由防火墙模式

在路由模式中，ASA被视为网络中的路由器跃点。要在其间路由的每个接口都位于不同的子网上。您可以在情景之间共享第 3 层接口。

通过集成路由和桥接，您可以使用您用来对网络的多个接口进行分组的“网桥组”，ASA使用桥接技术在接口之间传递流量。每个桥接组包括一个网桥虚拟接口 (BVI)，供您为其分配一个网络 IP 地址。ASA在 BVI 与正规的路由接口之间进行路由。如果您不需要多情景模式或集群或 EtherChannel 或 VNI 成员接口，则可以考虑使用路由模式而非透明模式。在路由模式下，可以像在透明模式下一样具有一个或多个隔离的网桥组，但也可以使用正常的路由接口进行混合部署。

关于透明防火墙模式

通常情况下，防火墙是一个路由跃点，并充当与其中一个被屏蔽子网连接的主机的默认网关。另一方面，透明防火墙是一个第 2 层防火墙，充当“线缆中的块”或“隐蔽的防火墙”，不被视为是到所连接设备的路由器跃点。但是，与其他防火墙一样，接口之间的访问控制是受控制的，需要进行通常的所有防火墙检查。

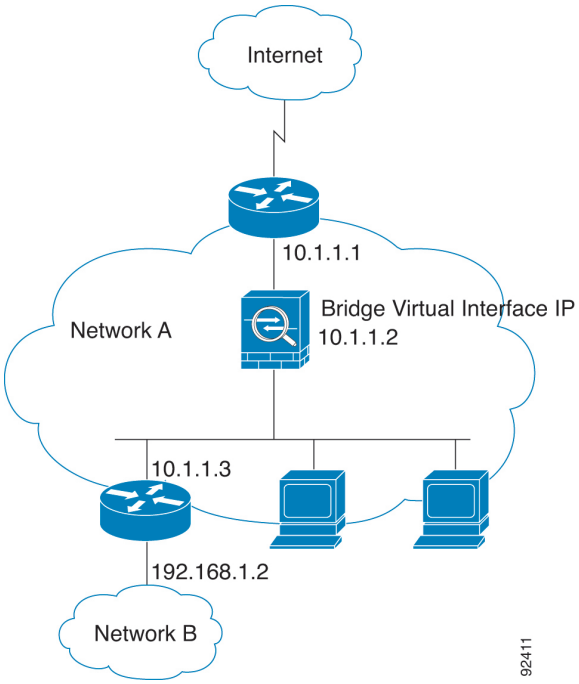
第 2 层连接使用您用来对网络的内部和外部接口进行分组的“网桥组”来实现，ASA使用桥接技术在接口之间传递流量。每个桥接组包括一个网桥虚拟接口 (BVI)，供您为其分配一个网络 IP 地址。多个网络可以有多个网桥组。在透明模式下，这些网桥组无法相互通信。

在网络中使用透明防火墙

ASA 在其接口之间连接同一个网络。由于防火墙不是路由跃点，因此可以将透明防火墙轻松引入到现有网络中。

下图显示典型的透明防火墙网络，其中的外部设备与内部设备在同一个子网上。内部路由器和主机显示为与外部路由器直接连接。

图 *1:* 透明防火墙网络



管理 接口

除了每个网桥虚拟接口 (BVI) IP 地址，您可以添加不属于任何网桥组的独立管理 插槽/端口接口，这样将仅允许管理流量通过 ASA。有关详细信息，请参阅管理接口。

允许路由模式功能通过流量

对于透明防火墙不直接支持的功能，您可以允许流量通过，以便上游和下游路由器能够支持这些功能。例如，通过使用访问规则，可以允许 DHCP 流量（而不是不受支持的 DHCP 中继功能）或组播流量（例如 IP/TV 产生的流量）。还可以通过透明防火墙建立路由协议邻接；可以根据扩访问规则允许 OSPF、RIP、EIGRP 或 BGP 流量通过。同样，诸如 HSRP 或 VRRP 之类的协议也可以通过 ASA。

关于网桥组

网桥组是指 ASA 网桥（而非路由）的接口组。 网桥组在透明和路由防火墙模式下受支持。与任何其他防火墙接口一样，接口之间的访问控制将受控制，并将部署所有普通防火墙检查。

网桥虚拟接口 (BVI)

每个网桥组包括一个网桥虚拟接口 (BVI)。ASA使用该 BVI IP 地址作为源自网桥组的数据包的源地址。BVI IP 地址必须与网桥组成员接口位于同一子网。BVI 不支持辅助网络上的流量；只有与 BVI IP 地址相同的网络上的流量才受支持。

在透明模式下：只有网桥组成员接口会被命名并可以与基于接口的功能配合使用。

在路由模式下：BVI 充当网桥组和其他路由接口之间的网关。要在网桥组/路由接口之间进行路由，必须为 BVI 命名。对于一些基于接口的功能，您可以单独使用 BVI：

- 访问规则 - 可以为网桥组成员接口和BVI配置访问规则；对于入站规则，会首先检查成员接口。对于出站规则，会首先检查 BVI。
- DHCPv4 服务器 - 只有 BVI 支持 DHCPv4 服务器配置。
- 静态路由 - 可以为 BVI 配置静态路由；不能为成员接口配置静态路由。
- 系统日志服务器和其他源自 ASA的流量 - 当指定系统日志服务器（或 SNMP 服务器，或流量源自 ASA的其他服务）时，可以指定 BVI 或成员接口。

如果您在路由模式下没有命名 BVI，则 ASA不会路由网桥组流量。此配置将为网桥组复制透明防火墙模式。如果您不需要多情景模式或集群或 EtherChannel 或 VNI 成员接口，则可以考虑改用路由模式。在路由模式下，可以像在透明模式下一样具有一个或多个隔离的网桥组，但也可以使用正常的路由接口进行混合部署。

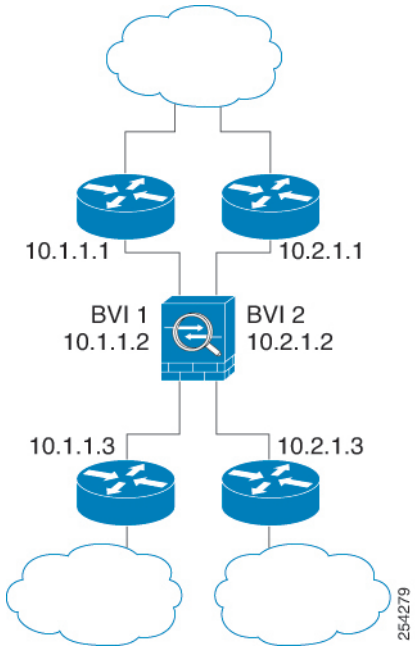
透明防火墙模式下的网桥组

网桥组的流量相互分离；流量不会路由至 ASA 中的另一个网桥组，并且流量必须退出 ASA 后才能通过外部路由器路由回ASA中的另一个网桥组。虽然每个网桥组的桥接功能是独立的，但所有网桥组之间可共享很多其他功能。例如，所有网桥组都共享系统日志服务器或AAA服务器的配置。为完全分离安全策略，请在每个情景中对一个网桥组使用安全情景。

可以在每个网桥组中包含多个接口。有关支持的网桥组和接口的确切数量，请参阅防火墙模式准则，第 9 页。如果您在每个网桥组中使用的接口数超过 2 个，则可以控制同一网络上多个网段之间的通信，而不只是在内部和外部之间的通信。例如，如果您有三个不需要彼此通信的内部网段，则可以将每个网段设置在单独的接口上，并且仅允许它们与外部接口通信。或者，您可以自定义接口之间的访问规则，以根据需要允许任意程度的访问。

下图显示连接到 ASA且具有两个网桥组的两个网络。

图 *2:* 具有两个网桥组的透明防火墙网络

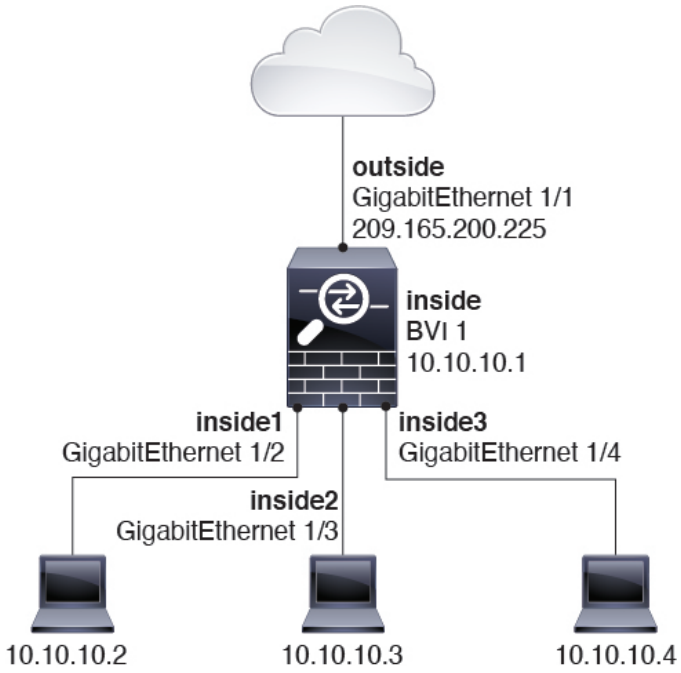


路由防火墙模式下的网桥组

网桥组流量可以路由到其他网桥组或路由接口。您可以选择通过不为网桥组的 BVI 接口分配名称来隔离网桥组流量。如果命名了 BVI，则 BVI 将像其他任何普通接口一样参与路由。

路由模式下网桥组的一种用途是在 ASA上而非外部交换机上使用额外接口。例如，某些设备的默认配置包括一个外部接口作为普通接口，还包括分配给内部网桥组的其他接口。由于此网桥组的目的是替换外部交换机，因此您需要配置访问策略，以便所有网桥组接口都可以自由通信。 例如，就像默认配置一样，将所有接口设置为同一安全级别，然后启用相同安全接口通信；无需访问规则。

图 *3:* 具有内部网桥组和外部路由接口的路由防火墙网络



传递路由模式下不允许的流量

在路由模式下，某些类型的流量无法通过 ASA，即使在访问规则中允许该流量也不行。但网桥组使用访问规则（对于 IP 流量）或 EtherType 规则（对于非 IP 流量）几乎可以允许所有流量通过。

- IP 流量 - 在路由防火墙模式下，即便访问规则（包括不支持的动态路由协议和 DHCP）中允许广播和组播流量，它们也会受到阻拦，除非配置了 DHCP 中继。在网桥组内，您可以通过访问规则（使用扩展 ACL）允许此流量。
- 非 IP 流量 - AppleTalk、IPX、BPDU 和 MPLS 等都可使用 EtherType 规则配置为通过。

注释 网桥组不传递 CDP 数据包，也不传递有效 EtherType 大于或等于 0x600 的任何数据包。BPDU 和 IS-IS 除外，它们受支持。

允许第 3 层流量

- 单播 IPv4 和 IPv6 流量可通过网桥组从安全性较高的接口自动流向安全性较低的接口，而无需访问规则。
- 对于从低安全性接口传播到高安全性接口的第3层流量，要求低安全性接口上有一个访问规则。
- 允许 ARP 双向通过网桥组，而无需访问规则。ARP 流量可通过 ARP 检测进行控制。
- IPv6 邻居发现和路由器请求数据包可以使用访问规则传递。

- 可使用访问规则允许广播和组播流量通过。

允许的 MAC 地址

如果得到您的访问策略的允许，将允许以下目标 MAC 地址通过网桥组（请参阅允许第 3 层流量，第 5 页）。系统会丢弃此列表中未列出的任何 MAC 地址。

- 实际广播目标 MAC 地址等于 FFFF.FFFF.FFFF
- IPv4 组播 MAC 地址的范围是 0100.5E00.0000 至 0100.5EFE.FFFF
- IPv6 组播 MAC 地址的范围是 3333.0000.0000 至 3333.FFFF.FFFF
- BPDU 组播地址等于 0100.0CCC.CCCD
- AppleTalk 组播 MAC 地址的范围是 0900.0700.0000 至 0900.07FF.FFFF

BPDU 处理

为防止环路使用生成树协议，默认情况下允许 BPDU 通过。要阻止 BPDU，需要将 EtherType 规则配置为拒绝 BPDU。您还可以阻止外部交换机上的 BPDU。例如，如果同一网桥组的成员连接到不同 VLAN 中的交换机端口，则可以阻止交换机上的 BPDU。在这种情况下，来自一个 VLAN 的 BPDU 将在另一个 VLAN 中可见，这可能会导致生成树根网桥选择过程问题。

如果使用故障转移功能，则可能要阻止 BPDU，以防止交换机端口在拓扑结构更改时进入阻止状态。有关详细信息，请参阅故障转移的网桥组要求。

MAC 地址与路由查找

对于网桥组中的流量，通过执行目标 MAC 地址查找而不是路由查找来确定数据包的传出接口。

但是，路由查找对于以下情况是必要的：

- 源自 ASA的流量 - 例如，在 ASA上为发往系统日志服务器所在的远程网络的流量添加一个默认/静态路由。
- 已启用检测的 IP 语音 (VoIP) 和 TFTP 流量，并且终端至少在一跳之外 - 在 ASA上为发往成功建立辅助连接的远程终端的流量添加静态路由。ASA会在访问控制策略中创建一个临时“针孔”以允许辅助连接；由于连接可能会使用一组不同于主连接的 IP 地址，所以 ASA需要执行路由查找以便在正确的接口上安装针孔。

  受影响的应用包括：

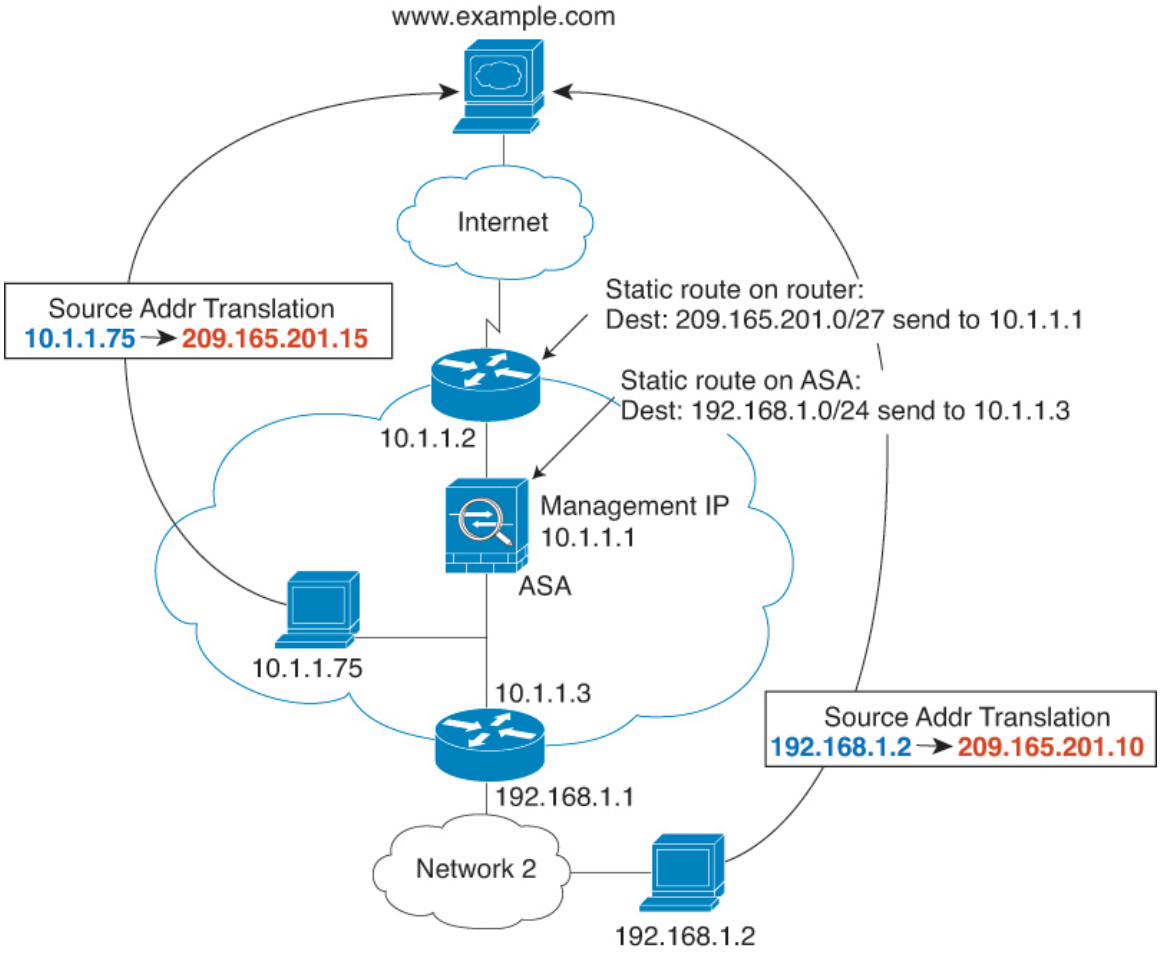
  - CTIQBE
  - GTP
  - H.323
  - MGCP
  - RTSP

- SIP
- Skinny (SCCP)
- SQL*Net
- SunRPC
- TFTP

- ASA对其执行 NAT 的至少一跳开外的流量 - 在 ASA上为发往远程网络的流量配置静态路由。您还需要在上游路由器上为要发送到 ASA的已映射地址的流量配置静态路由。

  此路由要求也适用已启用检测和 NAT 的 VoIP 和 DNS 的嵌入式 IP 地址，这些嵌入式 IP 地址都必须至少在一跳之外。ASA需要识别正确的出口接口，以便可以执行转换。

图 *4: NAT* 示例：网桥组中的 *NAT*



透明模式下网桥组不支持的功能

下表列出了在透明模式下网桥组中不受支持的功能。

表 *1:* 在透明模式下不支持的功能

功能	说明
动态 DNS	-
DHCPv6 无状态服务器	在网桥组成员接口上仅支持 DHCPv4 服务器。
DHCP 中继	透明防火墙可作为 DHCPv4 服务器，但它不支持 DHCP 中继。不需要使用 DHCP 中继，因为可使用两个访问规则来允许 DHCP 流量通过：一个规则用于允许从内部接口向外部发送 DCHP 请求；另一个用于允许来自另一个方向的服务器的应答。
动态路由协议	但是，对于网桥组成员接口，可以为 ASA上发起的流量添加静态路由。您还可以使用访问规则来允许动态路由协议通过 ASA。
组播 IP 路由	通过在访问规则中允许组播流量，可以允许组播流量通过 ASA。
QoS	-
针对直通流量终止 VPN	透明防火墙仅支持在网桥组成员接口上使用站点间的 VPN 隧道传输管理连接。它不会针对通过 ASA 的流量终止 VPN 连接。您可以使用访问规则允许 VPN 流量通过 ASA，但它不会终止非管理连接。无客户端 SSL VPN 也不受支持。
统一通信	—

路由模式下网桥组不支持的功能

下表列出了在路由模式下网桥组中不支持的功能。

表 *2:* 路由模式下不受支持的功能

功能	说明
EtherChannel 或 VNI 成员接口	仅支持物理接口和子接口作为网桥组成员接口。 管理 接口也不受支持。
集群	集群中不支持网桥组。
动态 DNS	-
DHCPv6 无状态服务器	只有 DHCPv4 服务器在 BVI 上受支持。
DHCP 中继	路由防火墙可以作为 DHCPv4 服务器，但它不支持在 BVI 或网桥组成员接口上使用 DHCP 中继。
动态路由协议	但您可以为 BVI 添加静态路由。您还可以使用访问规则来允许动态路由协议通过 ASA。非网桥组接口支持动态路由。

功能	说明
组播 IP 路由	通过在访问规则中允许组播流量，可以允许组播流量通过 ASA。非网桥组接口支持组播路由。
多情景模式	在多情景模式下，不支持网桥组。
QoS	非网桥组接口支持 QoS。
针对直通流量终止 VPN	您无法终止 BVI 上的 VPN 连接。非网桥组接口支持 VPN。 网桥组成员接口仅支持将站点间 VPN 隧道用于管理连接。它不会针对通过 ASA 的流量终止 VPN 连接。您可以使用访问规则通过网桥组传递 VPN 流量，但它不会终止非管理连接。无客户端 SSL VPN 也不受支持。
统一通信	非网桥组接口支持统一通信。

默认设置

默认模式

默认模式为路由模式。

网桥组默认设置

默认情况下，所有 ARP 数据包都在网桥组内通过。

防火墙模式准则

情景模式准则

根据情景设置防火墙模式。

桥接组准则（透明和路由模式）

- 您可以创建最多 250 个桥接组，每个桥接组 64 个接口。
- 各个直连网络必须在同一子网上。
- ASA不支持辅助网络上的流量；只有与 BVI IP 地址相同的网络上的流量才受支持。
- 每个桥接组都需要 BVI 的 IP 地址，以用于管理往返设备的流量和使流量通过 ASA。对于 IPv4 流量，请指定 IPv4 地址。对于 IPv6 流量，请指定 IPv6 地址。
- 您仅可手动配置 Ipv6 地址。

- BVI IP 地址必须与已连接网络位于同一子网上。您不能将该子网设置为主机子网 (255.255.255.255)。
- 不支持将管理接口作为桥接组成员。
- 对于具有桥接 ixgbevf 接口的 VMware 上的 ASAv50，透明模式不受支持，在路由模式中网桥组不受支持。
- 对于 Firepower 1010 和 Cisco Secure Firewall 1210/20，不能将逻辑 VLAN 接口和物理防火墙接口混合在同一个桥接组中。
- 在透明模式下，必须至少使用 1 个桥接组；数据接口必须属于桥接组。
- 在透明模式下，请勿将 BVI IP 地址指定为所连接设备的默认网关；设备需要将位于 ASA另一端的路由器指定为默认网关。
- 在透明模式下，默认路由（为管理流量提供返回路径所需的路由）仅适用于来自一个桥接组网络的管理流量。这是因为默认路由会指定网桥组中的接口以及网桥组网络上的路由器 IP 地址，而您只能定义一个默认路由。如果您具有来自多个桥接组网络的管理流量，则需要指定常规静态路由来确定预期会发出管理流量的网络。
- 在透明模式下，管理接口不支持 PPPoE。
- 在路由模式下，要在桥接组和其他路由接口之间路由，您必须指定 BVI。
- 在路由模式下，ASA - 不支持将 EtherChannel 和 VNI 接口定义为网桥组成员。 Firepower 4100/9300 上的 Etherchannel 可以是网桥组成员。
- 使用网桥组成员时，不允许双向转发检测 (BFD) 回应数据包通过 ASA。如果 ASA 的一端有两个邻居运行 BFD，则 ASA 会因二者具有相同的源 IP 地址和目标 IP 地址且疑似属于 LAND 攻击而丢弃 BFD 回应数据包。

其他准则和限制

- 在更改防火墙模式时，ASA 会清除正在运行的配置，因为许多命令不能同时支持两种模式。启动配置会保持不变。如果重新加载而不保存，则会加载启动配置，且模式会恢复为原始设置。有关备份配置文件的信息，请参阅设置防火墙模式，第 10 页。
- 如果将文本配置下载到 ASA 且使用 **firewall transparent** 命令来更改模式，请确保将该命令放在配置的顶部；ASA 会在读取命令后立即更改模式并继续读取下载的配置。如果此命令显示在配置的后面部分，则ASA会清除配置中在此命令前面的所有行。有关下载文本文件的信息，请参阅设置 ASA 映像、ASDM 和启动配置。

设置防火墙模式

本节介绍如何 更改防火墙模式。

注释 我们建议先设置防火墙模式再执行任何其他配置，因为更改防火墙模式会清除运行配置。

开始之前

在更改模式时，ASA 将清除运行的配置（有关详细信息，请参阅防火墙模式准则，第 9 页）。

- 如果您已经具有填充的配置，请务必在更改模式之前备份配置；在创建新配置时，可以使用此备份作为参考。请参阅备份和恢复配置或其他文件。
- 在控制台端口处使用 CLI 更改模式。如果使用任何其他类型的会话（包括 ASDM 命令行界面工具或 SSH），当清除配置时您将被断开，在任何情况下您必须使用控制台断开重新连接到 ASA。
- 在情景中设置模式。

注释 要将防火墙模式设置为透明模式，并要在清除配置后配置 ASDM 管理访问，请参阅配置 ASDM 访问。

过程

将防火墙模式设置为透明：

firewall transparent

示例：

```
ciscoasa(config)# firewall transparent
```

要将模式更改为路由模式，请输入 **no firewall transparent** 命令。

注释
系统不会提示您确认防火墙模式更改；更改会立即发生。

防火墙模式示例

本节包含流量如何通过处于路由和透明防火墙模式下的 ASA 的示例。

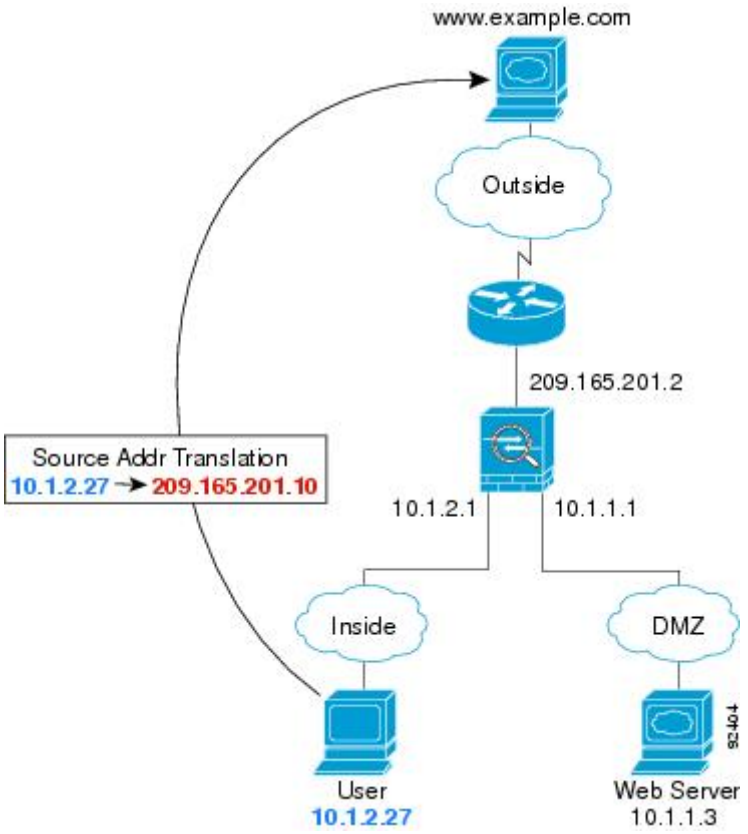
数据如何通过处于路由防火墙模式下的 ASA

以下各节介绍在多个情景中，数据如何通过处于路由防火墙模式下的 ASA。

内部用户访问 Web 服务器

下图显示了内部用户对外部 Web 服务器的访问。

图 *5:* 内部至外部



以下步骤介绍数据如何通过 ASA：

1. 内部网络中的用户从 www.example.com 请求访问网页。
2. ASA 接收数据包，由于是新会话，因此它会根据安全策略条款验证数据包是否获得允许。

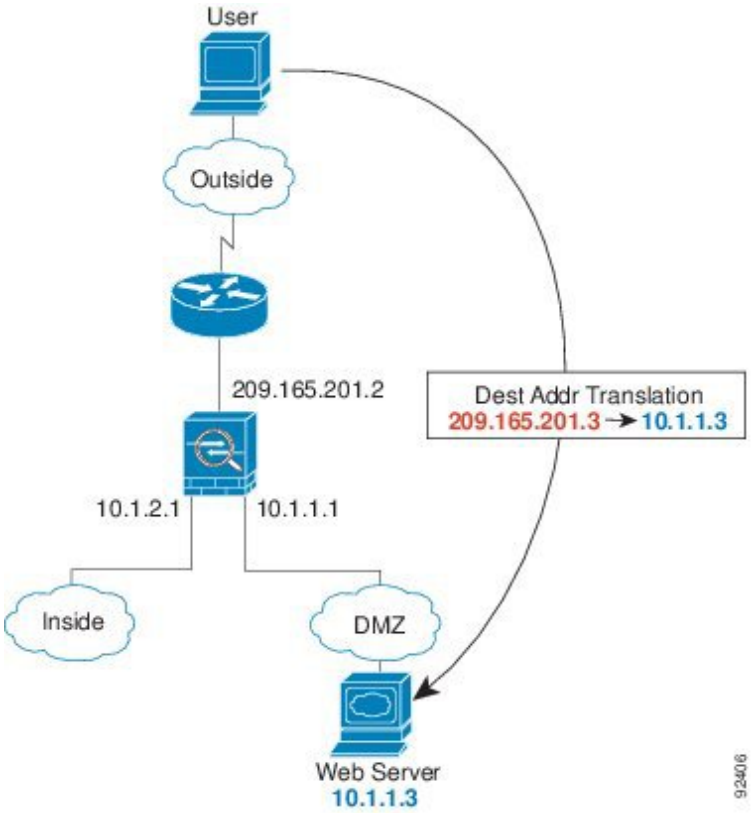
   对于多情景模式，ASA 会首先将数据包分类到一个情景中。
3. ASA 将实际地址 (10.1.2.27) 转换为映射的地址 209.165.201.10，后者位于外部接口子网上。

   映射的地址可能位于任意子网上，但当它位于外部接口子网上时，才会简化路由。
4. 然后，ASA 会记录有关会话已建立的信息，并从外部接口转发数据包。
5. 当 www.example.com 响应请求时，数据包会通过 ASA，由于已建立会话，因此数据包会绕过许多与新连接关联的查找。ASA 通过将全局目标地址逆向转换为本地用户地址 10.1.2.27 来执行 NAT。
6. ASA 将数据包转发给内部用户。

外部用户访问 DMZ 上的 Web 服务器

下图显示了访问 DMZ Web 服务器的外部用户。

图 *6:* 外部到 *DMZ*



以下步骤介绍数据如何通过 ASA：

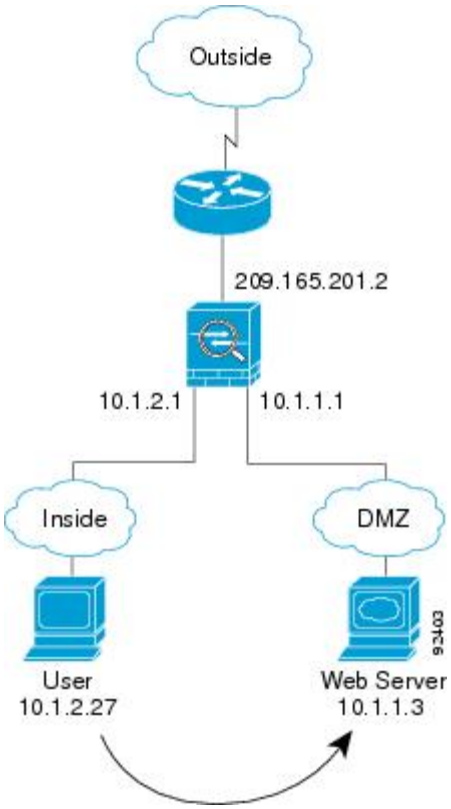
1. 外部网络上的用户使用映射地址 209.165.201.3（位于外部接口子网上）从 DMZ Web 服务器请求访问网页。
2. ASA 接收数据包并将映射的地址逆向转换为真实地址 10.1.1.3。
3. 由于是新会话，因此 ASA 会根据安全策略条款验证数据包是否获得允许。

   对于多情景模式，ASA 会首先将数据包分类到一个情景中。
4. 然后，ASA 将会话条目添加到快速路径，并从 DMZ 接口转发数据包。
5. 当 DMZ Web 服务器响应请求时，数据包会通过 ASA，由于已建立会话，因此数据包会绕过许多与新连接关联的查找。ASA 通过将真实地址转换为 209.165.201.3 来执行 NAT。
6. ASA 将数据包转发给外部用户。

内部用户访问 DMZ 上的 Web 服务器

下图显示了显示访问 DMZ Web 服务器的内部用户。

图 *7:* 从内部到 *DMZ*



以下步骤介绍数据如何通过 ASA：

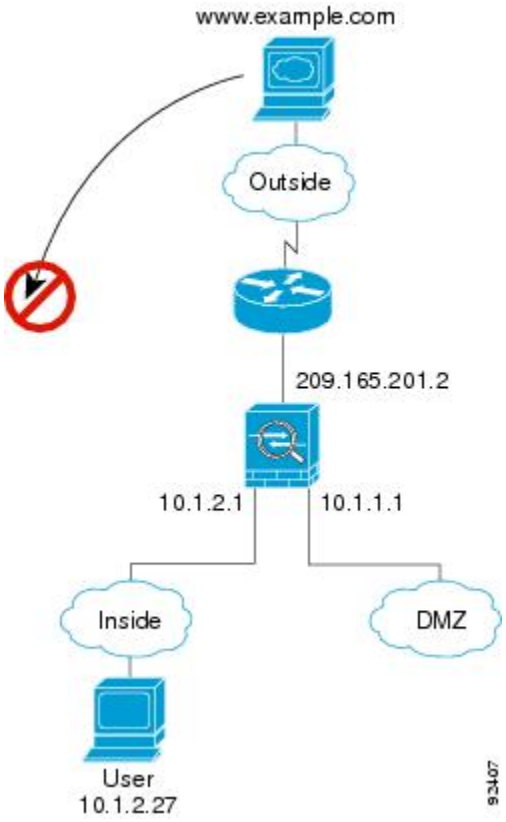
1. 内部网络上的用户使用目标地址 10.1.1.3 从 DMZ Web 服务器请求访问网页。
2. ASA 接收数据包，由于是新会话，因此 ASA 会根据安全策略条款验证数据包是否获得允许。

   对于多情景模式，ASA 会首先将数据包分类到一个情景中。
3. 然后，ASA 会记录有关会话已建立的信息，并从 DMZ 接口将数据包转发出去。
4. 当 DMZ Web 服务器响应请求时，数据包会通过快速路径，这样可使数据包绕过许多与新连接关联的查找。
5. ASA 将数据包转发给内部用户。

外部用户尝试访问内部主机

下图显示外部用户尝试访问内部网络。

图 *8:* 从外部到内部



以下步骤介绍数据如何通过 ASA：

1. 外部网络上的用户尝试访问内部主机（假设主机具有可路由的 IP 地址）。

   如果内部网络使用专用地址，则外部用户在没有执行 NAT 的情况下无法访问内部网络。外部用户可能会通过使用现有 NAT 会话尝试访问内部用户。

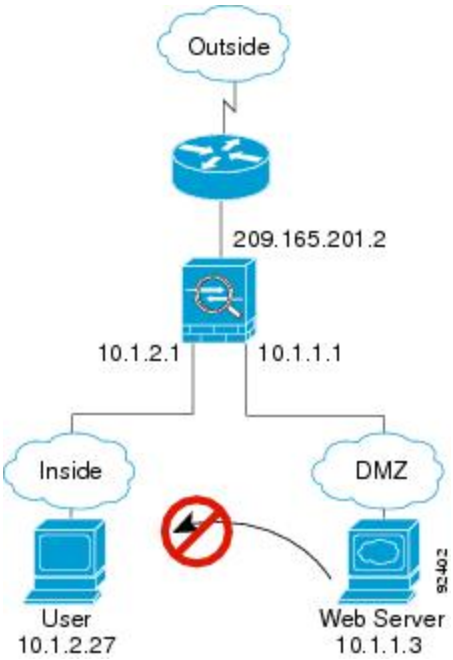
2. ASA 接收数据包；因为是新会话，因此它会根据安全策略验证是否允许该数据包。
3. 系统会拒绝数据包，而 ASA 则丢弃数据包并记录连接尝试情况。

   如果外部用户尝试攻击内部网络，则 ASA 会采用多种技术来确定数据包对于已建立的会话是否有效。

DMZ 用户尝试访问内部主机

下图显示了 DMZ 中的用户尝试访问内部网络。

图 *9:* 从 ***DMZ*** 到内部



以下步骤介绍数据如何通过 ASA：

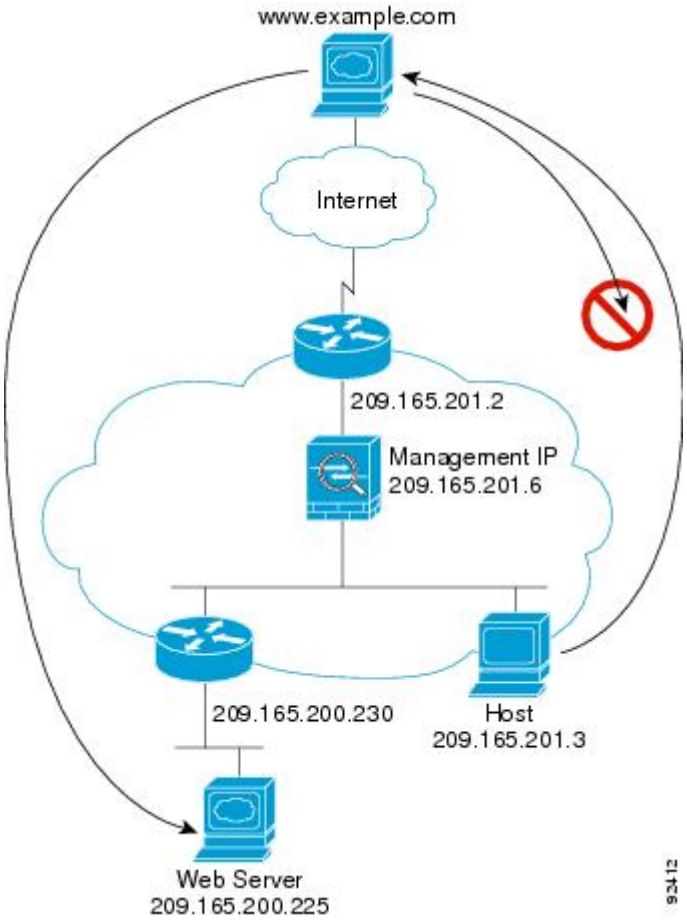
1. DMZ 网络上的用户尝试访问内部主机。由于 DMZ 不必路由互联网上的流量，因此专用寻址方案不会防止路由。
2. ASA 接收数据包；因为是新会话，因此它会根据安全策略验证是否允许该数据包。

   系统会拒绝数据包，而 ASA 则丢弃数据包并记录连接尝试情况。

数据如何通过透明防火墙

下图显示了包含公共Web服务器的内部网络上的典型透明防火墙实施。ASA具有访问规则以便内部用户可访问互联网资源。通过其他访问规则，外部用户只能访问内部网络上的 Web 服务器。

图 *10:* 典型透明防火墙数据路径

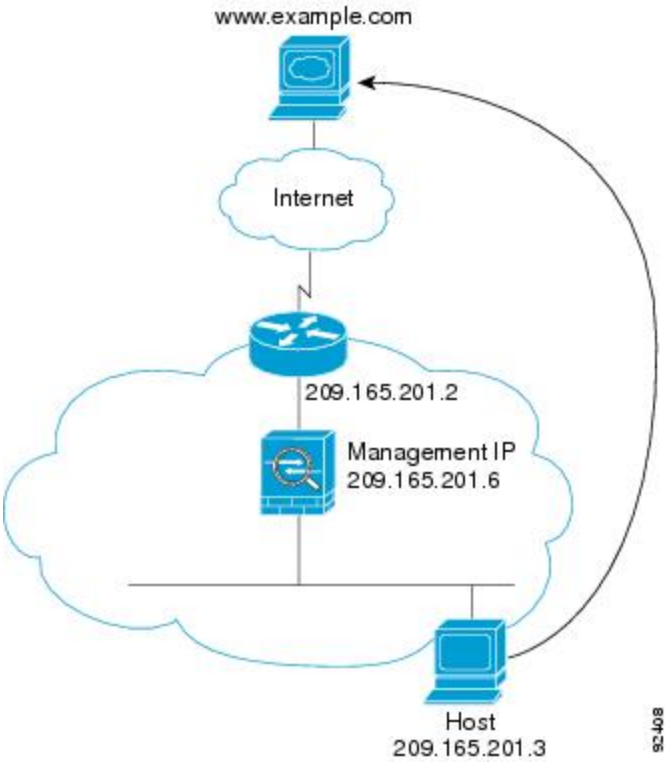


以下部分介绍数据如何通过 ASA。

内部用户访问 Web 服务器

下图显示了内部用户对外部 Web 服务器的访问。

图 *11:* 内部至外部



以下步骤介绍数据如何通过 ASA：

1. 内部网络中的用户从 www.example.com 请求访问网页。
2. ASA 接收数据包，并在需要时将源 MAC 地址添加到 MAC 地址表中。由于它是新会话，因此会根据安全策略条款验证数据包是否获得允许。

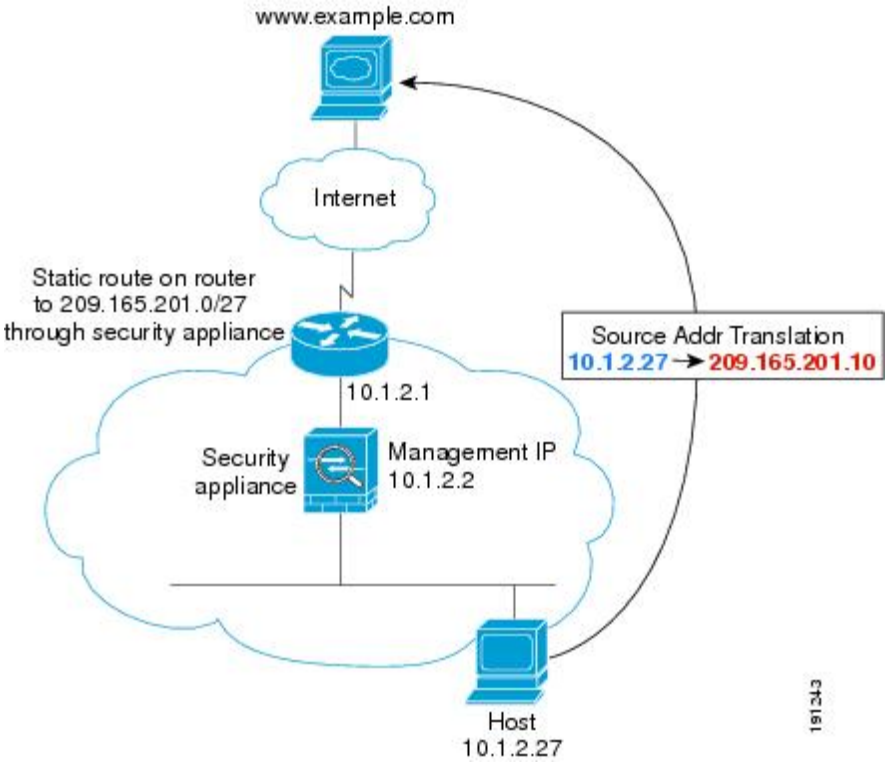
   对于多情景模式，ASA 会首先将数据包分类到一个情景中。
3. ASA 记录有关会话已建立的信息。
4. 如果目标 MAC 地址在其表中，则 ASA 会将数据包从外部接口转发出去。目标 MAC 地址是上游路由器的地址 (209.165.201.2)。

   如果目标 MAC 地址不在 ASA 表中，则它会通过发送 ARP 请求或 ping 来尝试发现 MAC 地址。系统会丢弃第一个数据包。
5. Web 服务器响应请求；由于已建立会话，因此数据包会绕过许多与新连接关联的查找。
6. ASA 将数据包转发给内部用户。

内部用户使用 NAT 访问 Web 服务器

下图显示了内部用户对外部 Web 服务器的访问。

图 *12:* 使用 *NAT* 从内部到外部



以下步骤介绍数据如何通过 ASA：

1. 内部网络中的用户从 www.example.com 请求访问网页。
2. ASA 接收数据包，并在需要时将源 MAC 地址添加到 MAC 地址表中。由于它是新会话，因此会根据安全策略条款验证数据包是否获得允许。

   对于多情景模式，ASA 会首先根据唯一接口对数据包进行分类。
3. ASA 会将真实地址 (10.1.2.27) 转换为映射地址 209.165.201.10。

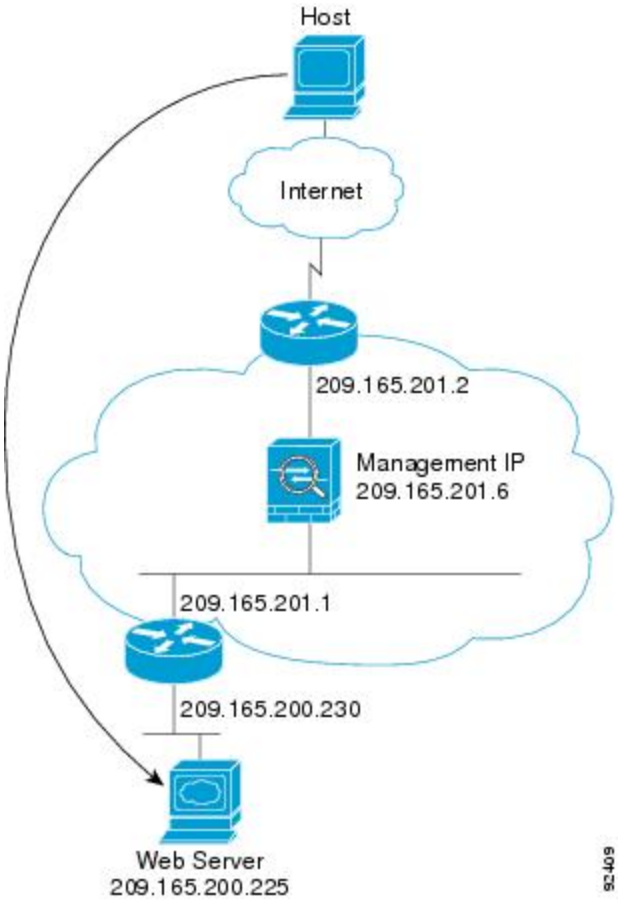
   由于映射地址与外部接口不在同一网络上，因此请确保上游路由器具有至映射网络（指向 ASA）的静态路由。
4. 然后，ASA 会记录有关会话已建立的信息，并从外部接口转发数据包。
5. 如果目标 MAC 地址在其表中，则 ASA 会将数据包从外部接口转发出去。目标 MAC 地址是上游路由器的地址 (10.1.2.1)。

   如果目标 MAC 地址不在 ASA 表中，则它会通过发送 ARP 请求和 ping 来尝试发现 MAC 地址。系统会丢弃第一个数据包。
6. Web 服务器响应请求；由于已建立会话，因此数据包会绕过许多与新连接关联的查找。
7. ASA 通过将映射地址逆向转换为真实地址 10.1.2.27 来执行 NAT。

外部用户访问内部网络上的 Web 服务器

下图显示了访问内部 Web 服务器的外部用户。

图 *13:* 从外部到内部



以下步骤介绍数据如何通过 ASA：

1. 外部网络上的用户从内部 Web 服务器请求访问网页。
2. ASA 接收数据包，并在需要时将源 MAC 地址添加到 MAC 地址表中。由于它是新会话，因此会根据安全策略条款验证数据包是否获得允许。

   对于多情景模式，ASA 会首先将数据包分类到一个情景中。
3. ASA 记录有关会话已建立的信息。
4. 如果目标 MAC 地址在其表中，则 ASA 会将数据包从内部接口转发出去。目标 MAC 地址是下游路由器的地址 (209.165.201.1)。

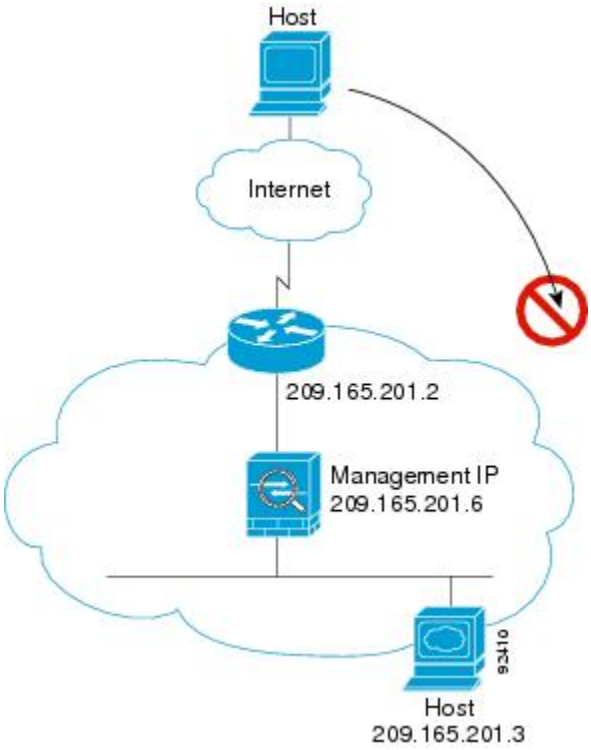
   如果目标 MAC 地址不在 ASA 表中，则它会通过发送 ARP 请求和 ping 来尝试发现 MAC 地址。系统会丢弃第一个数据包。
5. Web 服务器响应请求；由于已建立会话，因此数据包会绕过许多与新连接关联的查找。

6. ASA 将数据包转发给外部用户。

外部用户尝试访问内部主机

下图显示外部用户尝试访问内部网络上的主机。

图 *14:* 从外部到内部



以下步骤介绍数据如何通过 ASA：

1. 外部网络上的用户尝试访问内部主机。
2. ASA 接收数据包，并在需要时将源 MAC 地址添加到 MAC 地址表中。由于它是新会话，因此会根据安全策略条款验证数据包是否获得允许。

   对于多情景模式，ASA 会首先将数据包分类到一个情景中。
3. 由于没有允许外部主机的访问规则，因此会拒绝数据包，并且 ASA 会丢弃数据包。
4. 如果外部用户尝试攻击内部网络，则 ASA 会采用多种技术来确定数据包对于已建立的会话是否有效。

防火墙模式的历史记录

表 *3:* 防火墙模式的功能历史记录

功能名称	平台版本	功能信息
透明防火墙模式	7.0(1)	透明防火墙是 2 层防火墙，充当“嵌入式防火墙”或“隐藏防火墙”，并且不会被视为所连接设备的路由器跃点。 引入了以下命令：**firewall transparent** 和 **show firewall**。
透明防火墙网桥组	8.4(1)	如果您不希望产生安全情景开销，或者希望最大限度地利用安全情景，则可以将接口一起集合到网桥组中，然后配置多个网桥组，每个网络一个组。网桥组流量相互分隔。在单情景模式和多情景模式的每个情景中，最多可配置 8 个网桥组，每组最多 4 个接口。 注释 尽管您可以在 ASA 5505 上配置多个网桥组，但在 ASA 5505 上的透明模式下数据接口数限制为两个意味着只能有效地使用 1 个网桥组。 引入了以下命令：**interface bvi**、**bridge-group** 和 **show bridge-group**。
在多情景模式下支持混合防火墙模式	8.5(1)/9.0(1)	可以在多情景模式下为每个情景独立设置防火墙模式，因此某些情景可在透明模式下运行，而另一些情景则可在路由模式中运行。 修改了以下命令：**firewall transparent**。
透明模式的网桥组最大数量增加到 250	9.3(1)	网桥组最大数量从 8 个增加到 250 个网桥组。在单情景模式和多情景模式的每个情景中，最多可配置 250 个网桥组，每组最多 4 个接口。 修改了以下命令：**interface bvi** 和 **bridge-group**。
每个桥接组的透明模式最大接口数增加到 64	9.6(2)	每个网桥组的最大接口数量已从 4 增加到 64。 未修改任何命令。

功能名称	平台版本	功能信息
集成的路由与桥接	9.7(1)	集成路由和桥接提供了在网桥组和路由接口之间路由的功能。网桥组指 ASA 桥接（而非路由）的接口组。ASA 并非真正的网桥，因为 ASA 仍继续充当防火墙：控制接口之间的访问控制，并执行所有常规防火墙检查。以前，您只能在透明防火墙模式下配置网桥组，而无法在网桥组之间路由。通过此功能，可以在路由防火墙模式下配置网桥组，并在网桥组之间以及网桥组与路由接口之间进行路由。网桥组使用网桥虚拟接口 (BVI) 作为网桥组的网关，由此参与路由。如果 ASA 上还有额外接口可分配给网桥组，集成路由和桥接可提供替代使用外部第 2 层交换机的其他方案。在路由模式下，BVI 可以是已命名接口，并可独立于成员接口参与某些功能，例如访问规则和 DHCP 服务器。 路由模式不支持透明模式下支持的以下功能：多情景模式、ASA 集群。以下功能在 BVI 上也不受支持：动态路由和组播路由。 修改了以下命令：**access-group**、**access-list ethertype**、**arp-inspection**、**dhcpd**、**mac-address-table static**、**mac-address-table aging-time**、**mac-learn**、**route**、**show arp-inspection**、**show bridge-group**、**show mac-address-table**、**show mac-learn**
支持 Firepower 4100/9300 逻辑设备的透明模式部署	9.10(1)	您现在可以在 Firepower 4100/9300 上部署 ASA 时指定透明模式或路由模式。 新增/修改的 FXOS 命令：**enter bootstrap-key FIREWALL_MODE**、**set value routed** 和 **set value transparent**

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。