ASA 8.3：通过Cisco安全设备的连通性建立和故障排除

目录

简介

当初始配置思科自适应安全设备 (ASA) 时，它有一个内部所有人都能出去而外部没有人能进入的默认安全策略。如果您的站点需要一个不同的安全策略，您可允许外部用户通过 ASA 连接至您的 Web 服务器。

建立通过 Cisco ASA 的基本连接后，您可对防火墙进行配置更改。确保您对 ASA 做出的任何配置更改都符合您的站点安全策略。

请参阅 PIX/ASA：有关在 8.2 及更低版本的 Cisco ASA 上进行相同配置的信息，请参阅建立通过思科安全设备的连接并进行故障排除。

先决条件

要求

本文档假设一些基本配置已在 Cisco ASA 上完成。请参阅以下文档以获取初始 ASA 配置的示例：

- ASA 8.3(x) ：将一个内部网络连接至互联网
- 在思科自适应安全设备 (ASA) 上配置 PPPoE 客户端

使用的组件

本文档中的信息基于运行 8.3 及以上版本的 Cisco 自适应安全设备 (ASA).

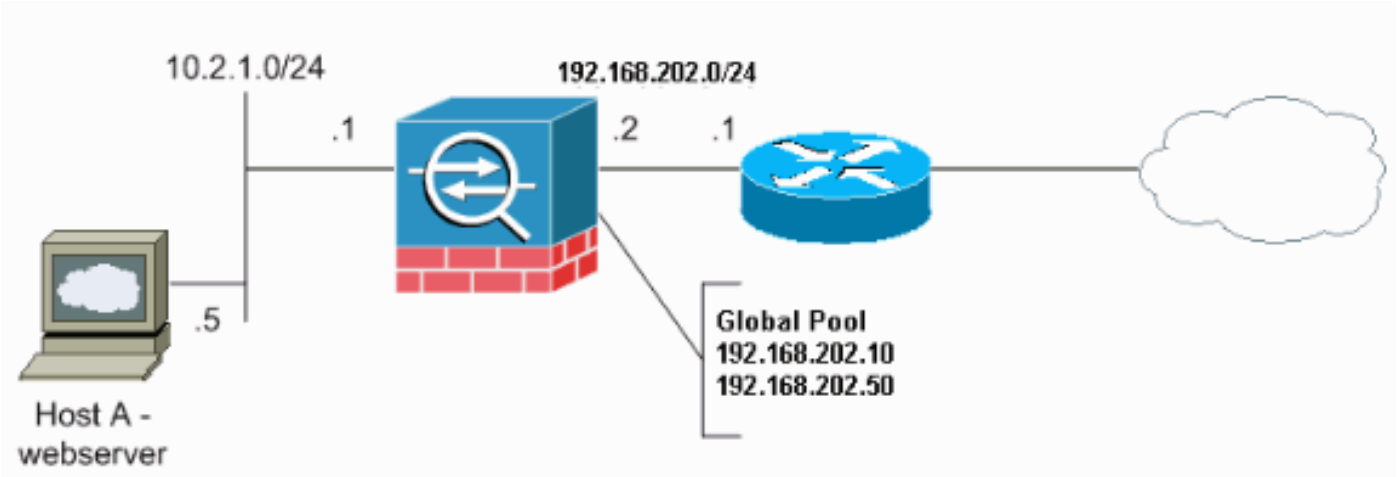
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

通过 ASA 的连接如何工作

在此网络中，主机 A 是内部地址为 10.2.1.5 的 Web 服务器。为 Web 服务器分配了外部（转换）地址 192.168.202.5。Internet 用户必须指向 192.168.202.5，才能访问 Web 服务器。用于 Web 服务器的 DNS 条目必须为该地址。不允许来自 Internet 的其他连接。



注意： 此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

配置通过 Cisco ASA 的连接

完成以下步骤以配置通过 ASA 的连接：

1. 创建一个定义内部子网的网络对象，并为 IP 池范围定义另一个网络对象。使用以下网络对象配置 NAT：
   ```
   object network inside-net subnet 0.0.0.0 0.0.0.0 object network outside-pat-pool range
   192.168.202.10 192.168.202.50 nat (inside,outside) source dynamic inside-net outside-pat-
   pool
   ```
2. 为 Internet 用户有权访问的内部主机分配静态转换地址。
   ```
   object network obj-10.2.1.5 host 10.2.1.5 nat (inside,outside) static 192.168.202.5
   ```
3. 使用 **access-list 命令**以允许外部用户通过 Cisco ASA。请始终在 **access-list 命令**中使用转换的地址。
   ```
   access-list 101 permit tcp any host 192.168.202.5 eq www access-group 101 in interface
   outside
   ```

允许 ARP 广播流量

安全设备在其内部接口和外部接口上连接相同的网络。由于防火墙不是一个路由跳，您可轻松地向

现有网络引入一个透明防火墙。无需进行 IP 再寻址。自动允许 IPv4 流量通过透明防火墙从较高的安全接口到达较低的安全接口，无需访问列表。允许地址解析协议 (ARP) 在两个方向通过透明防火墙，无需访问列表。ARP 流量可以由 ARP 检查功能控制。对于从低安全接口传输到高安全接口的第 3 层流量，需要使用扩展的访问列表。

注意： 透明模式安全设备不传递 Cisco 设备发现协议 (CDP) 数据包或 IPv6 数据包，也不传递不大于或等于 0x600 的有效 EtherType 的任何数据包。例如，您不能传递 IS-IS 数据包。网桥协议数据单元 (BPDU) 受支持，这是个例外。

允许的 MAC 地址

以下目标 MAC 地址允许通过透明防火墙。不在此列表中的 MAC 地址会被丢弃：

- 等于 FFFF.FFFF.FFFF 的 TRUE 广播目标 MAC 地址
- 范围从 0100.5E00.0000 到 0100.5EFE.FFFF 的 IPv4 多播 MAC 地址
- 范围从 3333.0000.0000 到 3333.FFFF.FFFF 的 IPv6 多播 MAC 地址
- 等于 0100.0CCC.CCCD 的 BPDU 多播地址
- 范围从 0900.0700.0000 到 0900.07FF.FFFF 的 AppleTalk 组播 MAC 地址

在路由器模式下不允许通过的流量

在路由器模式下，即使您在访问列表中允许某些类型的流量，它们也无法通过安全设备。但是，透明防火墙也可以使用扩展访问列表（用于 IP 流量）或 EtherType 访问列表（用于非 IP 流量）允许几乎任何流量通过。

例如，可以通过透明防火墙建立路由协议邻接。您可以根据扩展的访问列表，允许开放最短路径优先 (OSPF)、Routing Information Protocol (RIP)、Enhanced Interior Gateway Routing Protocol (EIGRP) 或边界网关协议 (BGP) 流量通过。同样地，热备份路由协议 (HSRP) 或虚拟路由冗余协议 (VRRP) 等协议可通过安全设备。

可使用 EtherType 访问列表配置非 IP 流量（例如 AppleTalk、IPX、BPDU 和 MPLS）通过安全设备。

对于透明防火墙上没有直接支持的功能，您可以允许流量通过，以便上游路由器和下游路由器能够支持该功能。例如，通过使用扩展访问列表，您可允许动态主机配置协议 (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 创建的组播流量）通过安全设备。

解决连接问题

如果互联网用户无法访问您的网站，请完成以下步骤：

1. 确保您正确地输入了配置地址：有效的外部地址正确的内部地址外部 DNS 具有转换的地址
2. 检查外部接口是否有错误。Cisco 安全设备已预先配置为自动检测接口上的速度及双工设置。但是，有几种情况可能会导致自动协商过程失败。这会导致速度或双工不匹配（并产生性能问题）。对于任务关键型网络基础架构，Cisco 对于每个接口的速度和双工采用手动硬编码，这样就避免了发生错误的机会。这些设备通常不移动。因此，如果正确配置这些设备，则应该不需要更改它们。**示例：**`asa(config)#interface ethernet 0/0 asa(config-if)#duplex full asa(config-if)#speed 100 asa(config-if)#exit` 在某些情况下，对速度和双工设置进行硬编码会导致生成错误。所以，如本例所示，您需要将该接口配置为自动检测模式的默认设置：**示例**

：asa(config)#**interface ethernet 0/0** asa(config-if)#**duplex auto** asa(config-if)#**speed auto** asa(config-if)#**exit**

3. 如果流量不通过 ASA 的接口或头端路由器发送或接收，请尝试清除 ARP 统计信息。asa#**clear arp**
4. 使用 **show run object** 和 **show run static** 命令来确保静态转换已启用。**示例：**
   object service www service tcp source eq www object network 192.168.202.2 host 192.168.202.2 object network 10.2.1.5 host 10.2.1.5 object service 1025 service tcp source eq 1025 nat (inside,outside) source static 10.2.1.5 192.168.202.2 service 1025 www 在此方案中，外部 IP 地址用作 Web 服务器的映射 IP 地址。
   nat (inside,outside) source dynamic 10.2.1.5 interface service 1025 www
5. 检查 Web 服务器上的默认路由是否指向 ASA 的内部接口。
6. 使用 show xlate 命令检查转换表，以确定是否创建了转换。
7. 使用 logging buffered 命令来检查日志文件，看看是否发生拒绝。（查找转换地址并确定是否看到任何拒绝。）
8. 使用 capture 命令：
   access-list webtraffic permit tcp any host 192.168.202.5 capture capture1 access-list webtraffic interface outside **注意：** 此命令会生成大量输出。它会在流量负载较大时导致路由器挂起或重新加载。
9. 如果数据包到达 ASA，则确保从 ASA 到 Web 服务器的路由正确。（请检查 ASA 配置中的路由命令。）
10. 检查代理 ARP 是否已禁用。在 ASA 8.3 中发出 show running-config sysopt 命令。在这里，代理 ARP 会被 **sysopt noproxyarp outside** 命令禁用：ciscoasa#**show running-config sysopt** no sysopt connection timewait sysopt connection tcpmss 1380 sysopt connection tcpmss minimum 0 no sysopt nodnsalias inbound no sysopt nodnsalias outbound no sysopt radius ignore-secret **sysopt noproxyarp outside** sysopt connection permit-vpn 为了重新启用代理 ARP，请在全局配置模式下输入此命令：ciscoasa(config)#**no sysopt noproxyarp outside** 当主机向同一以太网上的其他设备发送 IP 流量时，主机需要知道该设备的 MAC 地址。ARP 是可将 IP 地址解析为 MAC 地址的第 2 层协议。主机发送 ARP 请求并询问“Who is this IP address?”。拥有该 IP 地址的设备将回复“I own that IP address;here is my MAC address.”代理 ARP 允许安全设备代表它后面的主机回复 ARP 请求。它执行此操作的方法是为这些主机的静态映射地址答复 ARP 请求。安全设备会使用自己的 MAC 地址响应请求，然后将 IP 数据包转发给相应的内部主机。例如，在本文的图表中，当对 Web 服务器的全局 IP 地址 192.168.202.5 发出 ARP 请求时，安全设备将用自己的 MAC 地址来响应。在此情况下，如果未启用代理 ARP，则安全设备的外部网络上的主机就无法通过为地址 192.168.202.5 发出请求来到达 Web 服务器。有关 sysopt 命令的详细信息，请参阅命令参考。
11. 如果一切设置似乎都正确，但用户仍然不能访问网络服务器，则应请求Cisco 技术支持打开一个案例。

错误消息 - %ASA-4-407001：

一些主机无法连接至互联网，错误消息 - %ASA-4-407001：Deny traffic for local-host interface_name:系统日志中收到 inside_address，超出许可证数量限制错误消息。如何解决此问题？

当用户数量超过所用许可证的用户限制时会收到此错误消息。为了解决此错误，请将许可证升级到更高的用户数量。根据需要，这可以是 50、100 或者无限制用户的许可证。

相关信息

- Cisco ASA 5500 系列自适应安全设备
- 安全产品现场通告（包括思科自适应安全设备 (ASA)）
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems