ASA/PIX 7.x 及更高版本：缓解网络攻击

目录

简介

本文档介绍如何使用 Cisco 安全设备 (ASA/PIX) 防范各种网络攻击，例如拒绝服务 (DoS)。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据Cisco ASA 5500系列自适应安全设备(ASA)该运行软件版本7.0及以后。

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。

相关产品

本文档也可以用于运行软件版本 7.0 及更高版本的 Cisco 500 系列 PIX。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

防御 SYN 攻击

如何减轻传输控制协议(TCP)同步/在ASA/PIX的启动(SYN)攻击？

TCP SYN 攻击

TCP SYN 攻击是一种发送方发送大量无法完成的连接的 DOS 攻击。这将造成连接队列填满的情况，从而拒绝合法 TCP 用户的服务。

当启动正常的 TCP 连接时，目标主机将收到源主机发出的 SYN 数据包，并返回同步确认 (SYN ACK)。然后，目标主机必须监听到 SYN ACK 的确认，才会建立连接。这个过程被称为 TCP 三次握手。

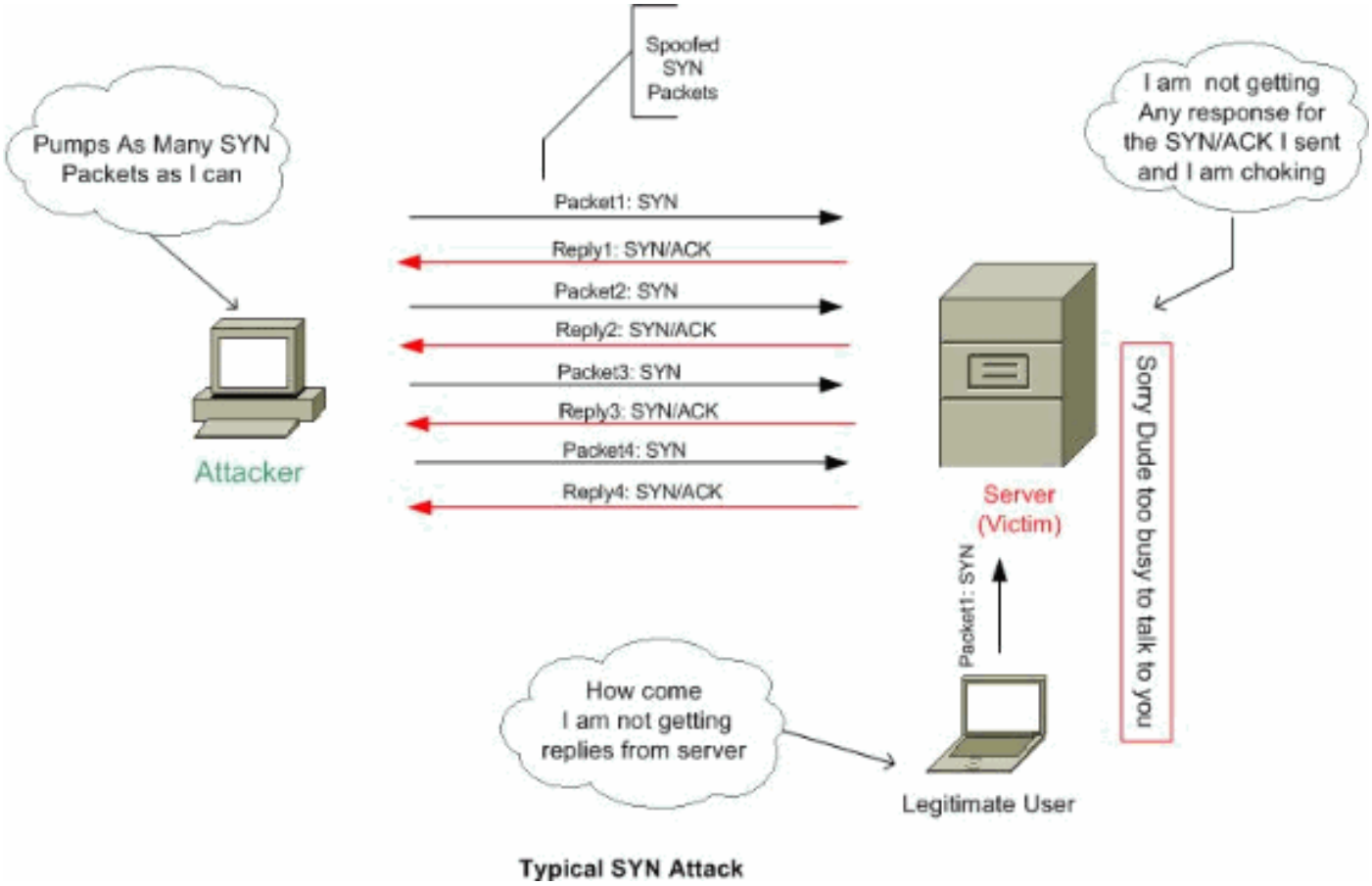
等待同步应答（SYN ACK）的确认（ACK）时，目的地主机上的大小有限的连接队列将记录等待完成的连接。由于在发出同步确认后的几毫秒内，确认即会到达，因此该队列通常迅速清空。

TCP SYN 攻击利用了此设计，由攻击源主机（相对于受害主机）生成带有随机源地址的 TCP 同步数据包。受害目标主机向随机源地址发送同步确认，并且在连接队列中添加新条目。由于同步确认指向不正确或不存在的主机，因此“三次握手”的最后一部分永远不会完成，并且条目将一直保留在连接队列中，直到计时器超时，保留时间通常为一分钟。通过从随机 IP 地址快速生成欺骗性 TCP 同步数据包，有可能将连接队列填满，从而拒绝合法用户请求的 TCP 服务（例如电子邮件、文件传输或 WWW）。

由于来源 IP 地址是伪造的，因此很难追踪到攻击者。

问题的外部表现包括：无法获得电子邮件、无法收到 WWW 的或 FTP 服务连接，或者主机上存在大量处于 SYN_RCVD 状态的 TCP 连接。

有关 TCP SYN 攻击的详细信息，请参阅防御 TCP SYN 泛洪攻击。



Typical SYN Attack

缓解

此部分描述如何通过设置最大数量减轻SYN攻击TCP和用户数据报协议(UDP)连接，最大初期连接，连接超时和如何禁用TCP序列随机化。

如果达到初期连接限制，则安全设备将使用“SYN+ACK”来响应每个被发送到服务器的 SYN 数据包，并且不会将此 SYN 数据包传递到内部服务器。如果外部设备用 ACK 数据包做出响应，则安全设备将知道它是一个有效的请求（而不是潜在 SYN 攻击的一部分）。然后安全设备将与该服务器建立连接，并将这些连接收集在一起。如果安全设备未从该服务器处获得确认，它将主动让该初期连接超时。

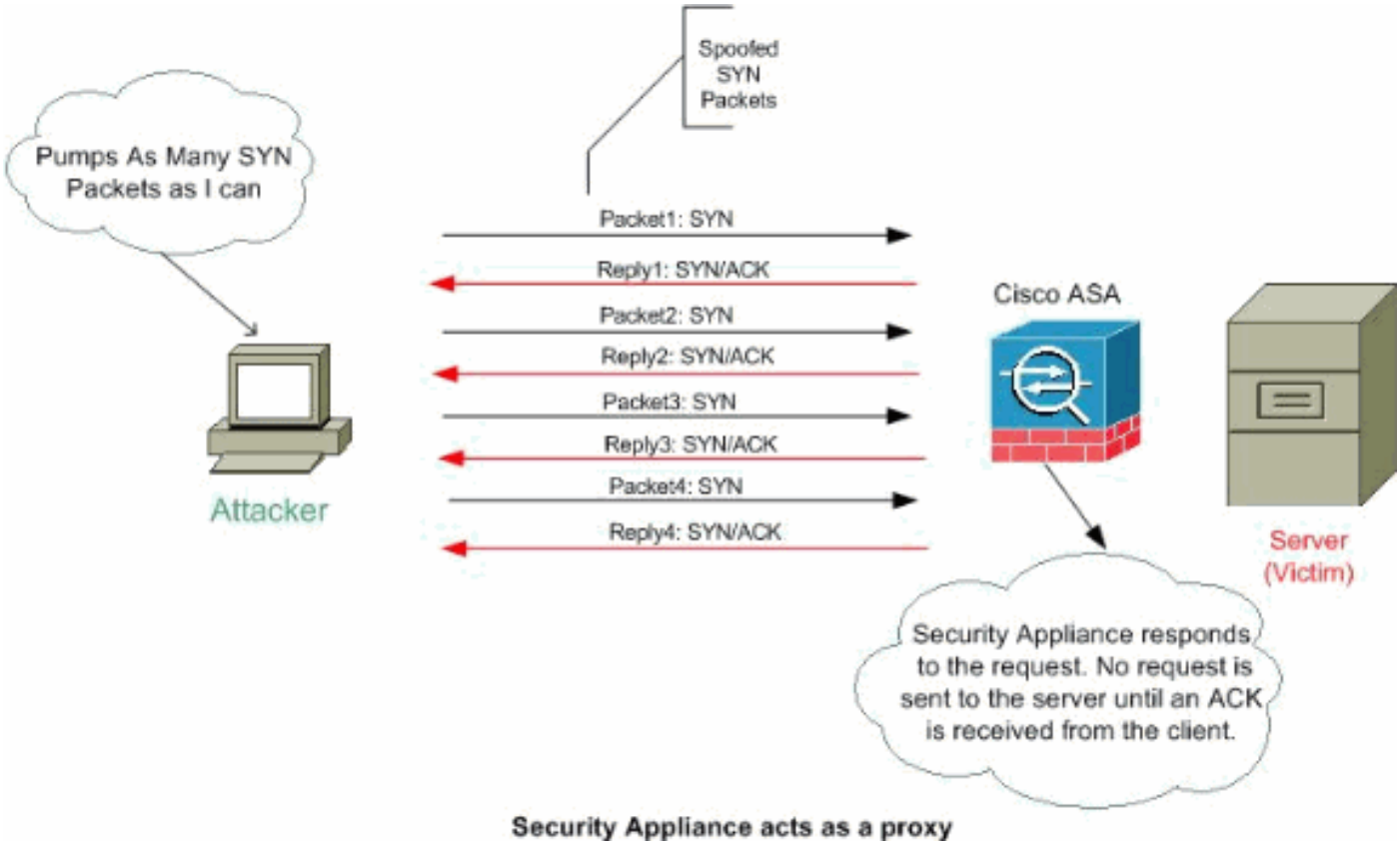
每TCP连接有两个初始序号(ISNs) ：一个由客户端生成，另一个由服务器生成。安全设备将随机设置沿入站和出站方向传送的 TCP SYN 的 ISN。

随机设置受保护主机的 ISN 可以防止攻击者预测用于新连接的下一个 ISN，从而防止攻击者劫持新会话。

您可以根据需要禁用 TCP 初始序列号随机化。例如：

- 如果另一个在线防火墙也执行初始序列号随机化，则这两个防火墙不必都执行此操作，尽管此操作不影响数据流。
- 如果您通过安全设备使用外部 BGP (EBGP) 多跃点，并且 eBGP 对等体使用 MD5，则随机化将中断 MD5 校验和。
- 您使用要求安全工具不随机化连接序号的一个广域应用服务(WAAS)设备。

注意： 您还可以在 NAT 配置中设置最大连接数、最大初期连接数以及 TCP 序列随机化。如果您对相同数据流同时使用这两种方法配置这些设置，则安全设备将使用下限。对于 TCP 序列随机化，如果使用任何一种方法将其禁用，则安全设备将禁用 TCP 序列随机化。



Security Appliance acts as a proxy

要设置连接限制，请执行以下步骤：

1. 要指定数据流，请按照使用模块化策略框架的说明使用 **class-map** 命令添加一个类映射。
2. 要添加或编辑用于对类映射数据流设置操作的**策略映射**，请输入以下命令：`hostname(config)#`**`policy-map name`**
3. 要指定对其分配操作的类映射（从第 1 步），请输入以下命令：`hostname(config-pmap)#`**`class class_map_name`**
4. 要设置最大连接数（TCP 和 UDP）、最大初期连接数、每客户端初期最大值、每客户端最大值或是否禁用 TCP 序列随机化，请输入以下命令：`hostname(config-pmap-c)#`**`set connection`** `{[`**`conn-max`** `number] [`**`embryonic-conn-max`** `number] [`**`per-client-embryonic-max`** `number] [`**`per-client-max`** `number][`**`random-sequence-number`** `{`**`enable`** `|` **`disable`**`}}` 其中的 number 是一个介于 0 到 65535 之间的整数。默认值是 0，这意味着连接数不受限制。您可以在一行中输入此命令（按任何顺序），或者以单独命令的形式分别输入每个属性。在上述运行配置中，此命令被合并到一行。
5. 要设置连接超时、初期连接数（半开放）和半封闭连接数，请输入以下命令：`hostname(config-pmap-c)#`**`set connection`** `{[`**`embryonic`** `hh[:mm[:ss]]] [`**`half-closed`** `hh[:mm[:ss]]] [`**`tcp`** `hh[:mm[:ss]]]}` 其中的 **embryonic** hh[:分[：ss]是0:0:5和1192:59:59之间的时期。默认是 0:0:30。您也可以将此值设置为 0，这表示连接永不会超时。**half-closed** hh[:分[：ss] 和 **tcp** hh[:分[：ss]值是0:5:0和1192:59:59之间的时期。**半闭的**默认是0:10:0，并且**tcp的**默认是 1:0:0。您也可以将这些值设置为 0，这表示连接永不会超时。您可以在一行中输入此命令（按任何顺序），或者以单独命令的形式分别输入每个属性。在上述运行配置中，此命令被合并到一行。**初期（半开放）连接** — 初期连接指的是源和目标之间尚未完成必要的握手的 TCP 连接请求。**半封闭连接** — 半封闭连接指的是通过发送 FIN 仅在一个方向封闭的连接。但是，连接对方仍在维护 TCP 会话。每客户端初期最大值 — 每个客户端允许的最大初期并发连接数，介于 0 到 65535 之间。默认值是 0，表示不限连接数。每客户端最大值 — 每个客户端允许的最大并发连接数，介于 0 到 65535 之间。默认值是 0，表示不限连接数。
6. 要在一个或多个接口上激活策略映射，请输入以下命令：`hostname(config)#`**`service-policy policymap_name`** *`{global | interface interface_name}`* 此处如果使用 **global**，则会将策略映射应

用于所有接口，而如果使用 interface 则会将策略应用于一个接口。仅允许有一个全局策略。您可以通过对接口应用服务策略以覆盖此接口的全局策略。您只能对每个接口应用一个策略映射。

示例：

```
ciscoasa(config)#class-map tcp_syn ciscoasa(config-cmap)#match port tcp eq 80 ciscoasa(config-cmap)#exit ciscoasa(config)#policy-map tcpmap ciscoasa(config-pmap)#class tcp_syn ciscoasa(config-pmap-c)#set connection conn-max 100 ciscoasa(config-pmap-c)#set connection embryonic-conn-max 200 ciscoasa(config-pmap-c)#set connection per-client-embryonic-max 10 ciscoasa(config-pmap-c)#set connection per-client-max 5 ciscoasa(config-pmap-c)#set connection random-sequence-number enable ciscoasa(config-pmap-c)#set connection timeout embryonic 0:0:45 ciscoasa(config-pmap-c)#set connection timeout half-closed 0:25:0 ciscoasa(config-pmap-c)#set connection timeout tcp 2:0:0 ciscoasa(config-pmap-c)#exit ciscoasa(config-pmap)#exit ciscoasa(config)#service-policy tcpmap global
```

注意： 为了验证半打开会话总数所有特定主机的，请使用此命令：

```
ASA-5510-8x# show local-host all Interface dmz: 0 active, 0 maximum active, 0 denied Interface management: 0 active, 0 maximum active, 0 denied Interface xx: 0 active, 0 maximum active, 0 denied Interface inside: 7 active, 18 maximum active, 0 denied local host: <10.78.167.69>, TCP flow count/limit = 2/unlimited TCP embryonic count to host = 0 TCP intercept watermark = unlimited UDP flow count/limit = 0/unlimited
```

注意： 线路，TCP，显示半打开会话数量。

防御 IP 伪装攻击

PIX/ASA 能否拦截 IP 伪装攻击？

IP 伪装

为了获得访问权限，入侵者使用伪装的源 IP 地址创建了数据包。这种攻击利用了应用程序根据 IP 地址进行身份验证的漏洞，并可能导致未经授权的用户获得目标系统的根访问权限。其示例有 rsh 和 rlogin 服务。

如果未将防火墙配置为过滤源地址位于本地域中的传入数据包，则数据包将有可能通过过滤路由防火墙。请务必注意，即使攻击者无法收到响应数据包，所描述的攻击也是可能发生的。

可能易受攻击的配置示例包括：

- 代理防火墙，在这种环境中代理应用程序使用源 IP 地址进行身份验证
- 连接外部网络的路由器支持多个内部接口
- 路由器中有两个接口支持在内部网络中划分子网

缓解

单播逆向路径转发(URPF)防护装置防御IP伪装(数据包使用一不正确源IP地址遮暗其真正的源)通过根据路由表匹配正确源接口的保证所有信息包有一源IP地址。

通常，仅当在确定要将数据包转发到何处时，安全设备才会查看其目标地址。单播 RPF 指示安全设备同时查看源地址。这就是为什么将其称为**反向路径转发**的原因。对于要允许通过安全设备的所有数据流，安全设备路由表中必须包含其回程源地址的路由。有关详细信息，请参阅 RFC 2267 。

注意： - %PIX-1-106021 当反向路径检查启用时，请src_addrdest_addrint_name日志消息能被看到。

禁用与**没有ip的**反向路径检查**验证reverse-path接口(接口名称)**命令为了解决此问题：

no ip verify reverse-path interface (interface name)
例如，对于外部数据流，安全设备可以使用默认路由进行单播 RPF 保护。如果数据流从外部接口进入，并且路由表中不存在其源地址，安全设备将使用默认路由将源接口正确识别为外部接口。

如果数据流从路由表中已知的地址进入外部接口，但与内部接口关联，安全设备将丢弃此数据包。同样地，如果数据流从未知的源地址进入内部接口，安全设备将丢弃数据包，因为匹配路由（默认路由）表明了外部接口。

单播 RPF 的实现如下所示：

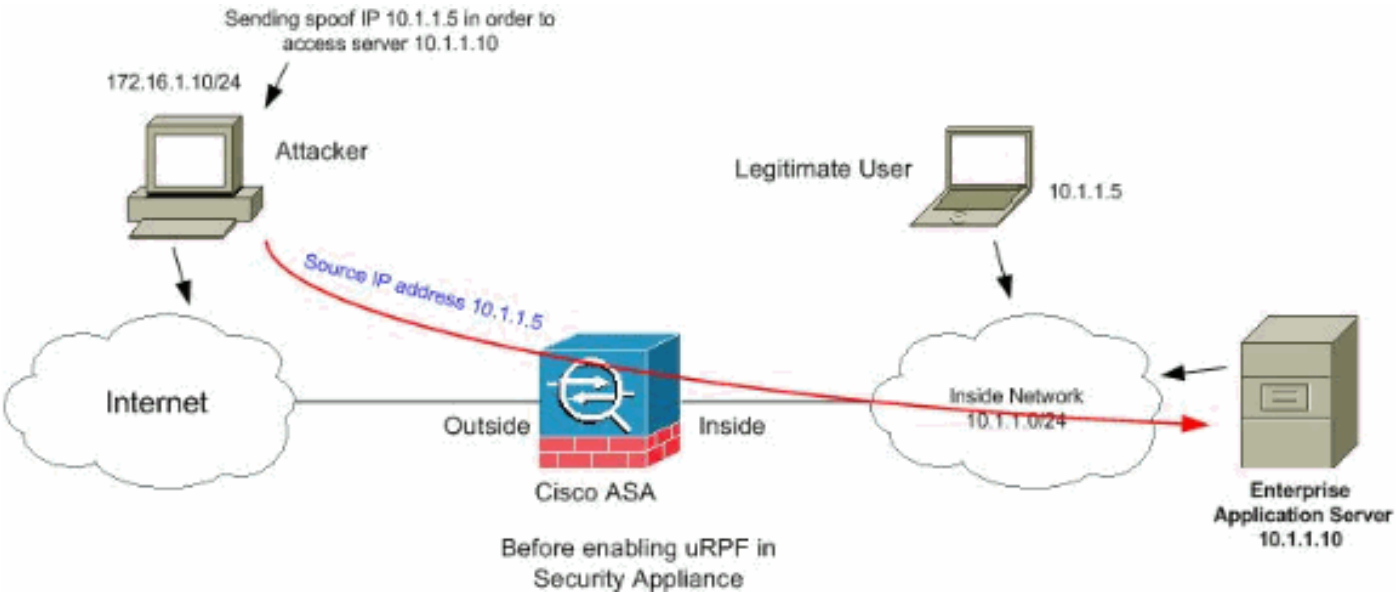
- ICMP 数据包不存在会话，因此每个数据包都将被检查。
- UDP 和 TCP 具有会话，因此初始数据包要求反向路由查找。作为会话一部分，系统将使用现有状态对会话期间到达的后续数据包进行检查。同时会检查非初始数据包，以确保它们到达与初始数据包相同的接口。

要启用单播 RPF，请输入以下命令：

```
hostname(config)#ip verify reverse-path interface interface_name
```

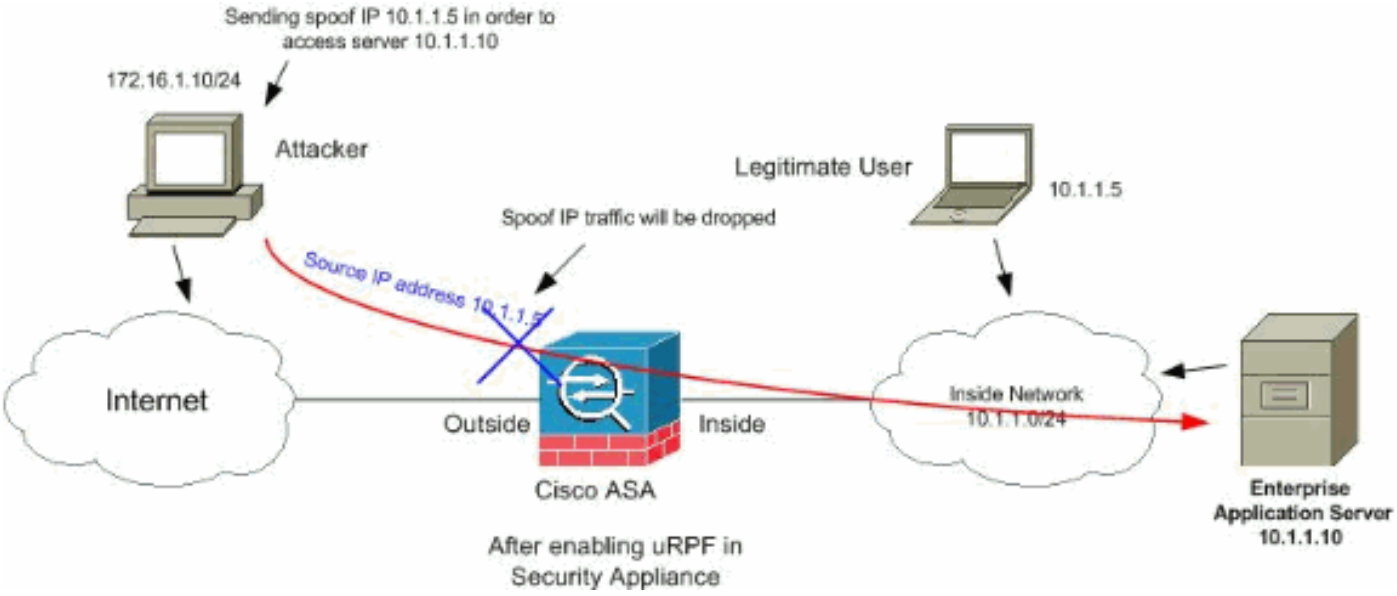
示例：

如图所示，攻击者 PC 通过伪造的源 IP 地址 10.1.1.5 /24 发送数据包，从而产生一个针对应用服务器 10.1.1.10 的请求，而服务器则发送一个数据包到实际 IP 地址 10.1.1.5 /24 以响应请求。这种非法数据包将攻击网络内部的应用服务器和合法用户。



单播 RPF 可以根据源地址伪装防御攻击。您需要在 ASA 的外部接口配置单播 RPF，如下所示：

```
ciscoasa(config)#ip verify reverse-path interface outside
```



使用系统日志消息识别伪装

安全设备持续收到系统日志错误消息，如下显示。这表明存在使用伪装数据包的潜在攻击，或可能由于非对称路由而触发潜在攻击。

1. **%PIX|ASA-2-106001: Inbound TCP connection denied from IP_address/port to IP_address/port flags tcp_flags on interface interface_name** **说明**这是一条与连接相关的消息。当针对特定数据流类型定义的安全策略拒绝了对于内部地址的连接尝试时，将会出现此消息。可能的 *tcp_flags* 值对应于连接被拒绝时 TCP 报头的标志位。例如，如果安全设备中不存在已到达 TCP 数据包的连接状态，则此数据包将被丢弃。此数据包中的 *tcp_flags* 是 FIN 和 ACK。其 *tcp_flags* 如下所示：ACK —确认号接收。FIN —数据发送。PSH —对应用程序的接收方合格数据。RST —连接重置。SYN —序号同步开始连接。URG —紧急指示器宣称的有效。在 PIX/ASA 上，静态转换失效有许多原因。但是，常见原因是，如果非敏感区域(DMZ)接口配置与同一个安全等级(0)象外部接口。要解决此问题，请对所有接口指定一个不同的安全级别。有关详细信息，请参阅配置接口参数。如果外部设备向内部客户端发送一个 IDENT 数据包，而此数据包被 PIX 防火墙丢弃，也会出现此错误消息。有关详细信息，请参阅由 IDENT 协议引起的 PIX 性能问题
2. **%PIX|ASA-2-106007: Deny inbound UDP from outside_address/outside_port to inside_address/inside_port due to DNS {Response|Query}** **说明**这是一条与连接相关的消息。如果指定连接由于 **outbound deny** 命令而失败，则将出现此消息。协议变量可以是 ICMP、TCP 或者 UDP。**建议操作：**请使用 **show outbound** 命令检查出站列表。
3. %PIX|ASA-3-106014: Deny inbound icmp src interface_name: IP_address dst interface_name: IP_address (type dec, code dec)**说明**安全设备拒绝了所有入站 ICMP 数据包访问。默认情况下，除非特别允许，否则将拒绝所有 ICMP 数据包访问。
4. %PIX|ASA-2-106016: Deny IP spoof from (IP_address) to IP_address on interface interface_name.**说明**当目标 IP 地址为 0.0.0.0 并且目标 MAC 地址为安全设备接口的数据包到达安全设备接口时，将会生成此消息。另外，当安全设备丢弃了源地址无效的数据包时，也会出现此消息；无效源地址可能包含以下一个或其他无效地址：环回网络 (127.0.0.0)广播（有限、网络定向、子网定向和全子网定向）目标主机 (land.c)为进一步改善伪装数据包检测功能，请使用 **icmp** 命令配置安全设备以丢弃源地址属于内部网络的数据包。这是因为 **access-list command** 已被废弃，不保证能够正确工作。**建议操作：**确定外部用户是否尝试危害受保护网络。检查配置错误的客户端。

5. `%PIX|ASA-2-106017: Deny IP due to Land Attack from IP_address to IP_address`**说明**安全设备收到了 IP 源地址与 IP 目标地址相同的数据包，并且目标端口等于源端口。此消息表明收到了旨在攻击系统的伪装数据包。这种攻击被称为着陆攻击。**建议操作**：如果此消息一直存在，则表明攻击可能正在进行。数据包无法提供足够的信息以确定发出攻击的位置。
6. `%PIX|ASA-1-106021: Deny protocol reverse path check from source_address to dest_address on interface interface_name`**说明**攻击正在进行。有人企图在入站连接上伪装 IP 地址。单播 RPF（也称为反向路由查找）检测到没有源路由地址的数据包，并认为它是对安全设备的一次攻击的一部分。当您使用 **ip verify reverse-path** 命令启用单播 RPF 时，此消息将会出现。此功能将作用于输入到接口的数据包。如果在外部配置此功能，则安全设备将检查从外部到达的数据包。安全设备将根据源地址查找路由。如果未找到相关条目，并且未定义路由，则将显示此系统日志消息，并中断连接。如果发现路由，安全设备将检查其对应的接口。如果数据包到达另一个接口，则它可能是一种伪装，或者存在可以通过多条路径到达一个目标的非对称路由环境。安全设备不支持非对称路由。如果在内部接口中配置了安全设备，则它将检查静态路由命令语句或 RIP。如果未找到源地址，则是内部用户伪装了其地址。**建议操作**：即使攻击正在进行，如果启用此功能，则不需要用户执行任何操作。安全设备将会防御攻击。**注意： drop命令显示的asp**表示加速的安全路径或连接丢弃的数据包 (asp)，也许帮助您排除故障问题。它还指出了上一次清除 asp 丢包计数器的时间。使用 **show asp drop rpf-violated** 命令时，当接口上配置了 ip 验证反向路由，并且安全设备的源 IP 路由查询表明，查询得到的接口与已接收数据包的接口不同时，此计数器将会增加。`ciscoasa#`**`show asp drop frame rpf-violated`** `Reverse-path verify failed 2` **注意： 建议：**根据以下一条系统消息中显示的源 IP 跟踪数据流的来源，并调查它为什么发送伪装数据流。**注意： 系统日志消息**：106021
7. `%PIX|ASA-1-106022: Deny protocol connection spoof from source_address to dest_address on interface interface_name`**说明**匹配连接的数据包到达的接口与开始连接的接口不同。例如，如果用户在内部接口启动连接，但安全设备检测到相同连接到达了周边接口，则安全设备具有多条路径可以到达目标。这称为非对称路由，安全设备不支持此功能。作为进入安全设备的一种方式，攻击者也可能尝试将一个连接的数据包附加到另一个连接中。无论如何，安全设备都将显示此消息并中断连接。**建议操作**：如果未配置 **ip verify reverse-path** 命令，也会出现此消息。请检查路由是否不是非对称的。
8. `%PIX|ASA-4-106023: Deny protocol src [interface_name:source_address/source_port] dst interface_name:dest_address/dest_port [type {string}, code {code}] by access_group acl_ID`**说明**IP 数据包被 ACL 拒绝。即使您没有为 ACL 启用**日志**选项，也会显示此消息。**建议操作**：如果相同源地址持续发出消息，则这些消息可能表示存在脚印拓取或端口扫描尝试。请与远程主机管理员联系。
9. `%PIX|ASA-3-210011: Connection limit exceeded cnt/limit for dir packet from sip/sport to dip/dport on interface if_name.`
10. `%ASA-4-419002: Received duplicate TCP SYN from in_interface:src_address/src_port to out_interface:dest_address/dest_port with different initial sequence number.`**说明**此系统日志消息表示通过防火墙设备建立新连接将导致超出至少一个已配置的连接限制最大值。此系统日志消息适用于使用静态命令配置的连接限制，或使用 Cisco 模块化策略框架配置的连接限制。除非其中一个现有连接中断，从而使当前连接计数低于已配置的最大值，否则系统将不会允许新连接通过防火墙设备。*cnt* — 当前连接计数*limit* — 配置的连接限制*dir* — 流量的方向，即入站或出站*sip* — 源 IP 地址*sport* — 源端口*dip* — 目标 IP 地址*dport* — 目标端口if_name — 收到数据流单元的接口名称，可能是主接口或辅助接口。**建议操作**：如果出于安全考虑配置了连接限制，则此系统日志消息可以指出可能的 DOS 攻击，在这种情况下，数据流的来源可能是一个伪装的 IP 地址。如果源 IP 地址不是完全随机的，则可以确定来源并使用访问列表拦截它。在其他情况下，使用嗅探器跟踪和分析数据流的来源可能有助于分离合法数据流和恶意数据流。

ASA 8.x 的基本威胁检测功能

Cisco 安全设备 ASA/PIX 软件版本 8.0 及更高版本均支持被称为威胁检测的功能。使用基本威胁检测，安全设备将监视数据包丢弃率以及由于以下原因产生的安全事件：

- 被访问列表拒绝
- 数据包格式损坏（例如 ip 报头无效或 tcp 报头长度无效）
- 超过连接限制（系统资源限制以及在配置中设置的限制）
- 检测到 DOS 攻击（例如 SPI 无效，状态防火墙检查故障等）
- 基本防火墙检查失败（此选项是一个组合率，它包括在此清单列表中列出的所有防火墙相关丢包。它不包括非防火墙相关丢包，例如接口超载、数据包未通过应用检查以及检测到扫描攻击等。）
- 检测到可疑 ICMP 数据包
- 数据包未通过应用检查
- 接口超载
- 检测到扫描攻击（此选项监视扫描攻击；例如，第一个 TCP 数据包不是 SYN 数据包，或者 TCP 连接的三次握手失败。全面扫描威胁检测（有关详细信息，请参阅配置扫描威胁检测）将获取此扫描攻击率信息，并针对攻击执行相关操作，例如将主机划分为攻击者并自动避开它们。）
- 会话检测未完成，例如检测到 TCP SYN 攻击或未检测到数据 UDP 会话攻击。

当安全设备检测到威胁时，它将立即发送一条系统日志消息 (730100)。

仅当存在丢包或潜在威胁时，基本威胁检测才会影响性能。即使在这种情况下，其性能影响也是微不足道的。

当您登录安全设备时，可使用 **show threat-detection rate** 命令以识别潜在的攻击。

```
ciscoasa#show threat-detection rate Average(eps) Current(eps) Trigger Total events 10-min ACL drop: 0 0 0 16 1-hour ACL drop: 0 0 0 112 1-hour SYN attck: 5 0 2 21438 10-min Scanning: 0 0 29 193 1-hour Scanning: 106 0 10 384776 1-hour Bad pkts: 76 0 2 274690 10-min Firewall: 0 0 3 22 1-hour Firewall: 76 0 2 274844 10-min DoS attck: 0 0 0 6 1-hour DoS attck: 0 0 0 42 10-min Interface: 0 0 0 204 1-hour Interface: 88 0 0 318225
```

有关配置部分的详细信息，请参阅《ASA 8.0 配置指南》的配置基本威胁检测部分。

系统日志消息 733100

错误消息：

```
%ASA-4-733100: Object drop rate rate_ID exceeded. Current burst rate is rate_val per second, max configured rate is rate_val; Current average rate is rate_val per second, max configured rate is rate_val; Cumulative total count is total_cnt
```

系统日志消息中的指定对象超出了指定的突发阈值率或平均阈值率。此对象可以是主机、TCP/UDP 端口、IP 协议的丢包行为或由于潜在攻击而导致的各种丢包。它表明系统受到潜在攻击。

注意： 这些错误消息与解决方法仅适用于 ASA 8.0 及更高版本。

1. 对象 — 丢包率计数的常规或特定来源，可能包括以下对象：防火墙数据包损坏丢包率限制 DoS 攻击ACL 丢包连接限制ICMP 攻击扫描SYN 攻击Inspect接口
2. rate_ID — 被超出的已配置丢包率。多数对象可以对不同时间间隔配置最多三种不同的丢包率
3. rate_val — 特定丢包率值。

4. total_cnt — 自从创建或清除对象后的总体计数。

以下三个示例显示了这些变量如何发生：

- 由于 CPU 或总线限制产生的接口丢包：`%ASA-4-733100: [Interface] drop rate 1 exceeded. Current burst rate is 1 per second, max configured rate is 8000; Current average rate is 2030 per second, max configured rate is 2000; Cumulative total count is 3930654`
- 由于潜在攻击产生的扫描丢包：`ASA-4-733100: [Scanning] drop rate-1 exceeded. Current burst rate is 10 per second_ max configured rate is 10; Current average rate is 245 per second_ max configured rate is 5; Cumulative total count is 147409 (35 instances received)`
- 由于潜在攻击产生的损坏数据包数量：`%ASA-4-733100: [Bad pkts] drop rate 1 exceeded. Current burst rate is 0 per second, max configured rate is 400; Current average rate is 760 per second, max configured rate is 100; Cumulative total count is 1938933`

建议操作：

根据在消息中出现的指定对象类型，执行以下步骤：

1. 如果系统日志消息中的对象属于以下一种：防火墙数据包损坏丢包率限制DoS 攻击ACL 丢包连接限制ICMP 攻击扫描SYN 攻击Inspect接口检查丢包率是否是当前运行环境可接受的。
2. 通过运行 **threat-detection rate xxx** 命令将特定丢包的阈值率调整为合适的值，其中 *xxx* 是以下一种类型：ACL 丢包数据包损坏丢包连接限制丢包DOS 丢包防火墙丢包ICMP 丢包检查丢包接口丢包扫描威胁SYN 攻击
3. 如果系统消息中的对象是 TCP 或 UDP 端口、IP 协议或主机丢包，请检查丢包率对当前运行环境来说是否是可接受的。
4. 通过运行 **threat-detection rate bad-packet-drop** 命令将特定丢包的阈值率调整为合适的值。有关详细信息，请参阅《ASA 8.0 配置指南》的配置基本威胁检测部分。

注意： 如果您不希望看到丢包率超出警告，可以通过运行 **no threat-detection basic-threat** 命令禁用它。

相关信息

- Cisco 5500 系列自适应安全设备支持页
- Cisco 500 系列 PIX 支持页
- 防御 TCP SYN 泛洪攻击
- Cisco 应用缓解公告：识别和缓解利用内容交换模块中的拒绝服务漏洞造成的威胁
- Cisco 应用缓解公告：识别和缓解利用 Cisco PIX 和 ASA 设备以及防火墙服务模块中的多个漏洞造成的威胁
- IP 伪装
- 技术支持和文档 - Cisco Systems