NetScreen 概念与范例

ScreenOS 参考指南

第 4 卷：攻击检测和防御机制

ScreenOS 5.1.0

编号 093-1369-000-SC

修订本 B

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with NetScreen's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR NETSCREEN REPRESENTATIVE FOR A COPY.

目录

前言

第 4 卷，“攻击检测和防御机制”介绍 ScreenOS 中可用的 Juniper Networks NetScreen 网络安全选项。这些选项中很多都是可在安全区段级启用的 SCREEN 选项。 SCREEN 选项适用于通过绑定到区段 (已为其启用了这些选项) 的任一接口而到达 NetScreen 设备的信息流。 SCREEN 选项提供对 IP 地址和端口扫描、拒绝服务 (DoS) 攻击以及其它类型的恶意活动的保护。您可以在策略级应用其它网络安全选项，如 URL 过滤、防病毒检查以及入侵检测和预防 (IDP)。这些选项只适用于在启用它们的策略管辖范围内的信息流。

注意：*在本卷中，仅当有关策略的主题适用于可在策略级启用的网络安全选项时，才会进行简要介绍。有关策略的详细阐述，请参阅第* ***2*** *-293 页上的 “策略”。*

本卷中的资料编排如下：

- 第 1 章，“保护网络”概述攻击的基本阶段，以及在每个阶段可用于对抗攻击的防火墙选项。
- 第 2 章，“侦查威慑”介绍可用于封锁 IP 地址扫描、端口扫描以及发现目标系统的操作系统 (OS) 类型的尝试的选项。
- 第 3 章，“拒绝服务攻击防御”解释防火墙、网络和与操作系统相关的 DoS 攻击，并说明 NetScreen 如何减轻这类攻击。
- 第 4 章，“内容监控和过滤”介绍如何保护 “超文本传输协议” (HTTP) 和 “文件传输协议” (FTP) 用户不受恶意 “统一资源定位器” (URL) 的影响，并说明如何配置 NetScreen 设备以便与第三方产品配合提供防病毒扫描和 URL 过滤。
- 第 5 章，“深入检查”说明如何配置 NetScreen 设备以获得 IDP 攻击对象更新、如何创建用户定义的攻击对象和攻击对象组、以及如何在策略级应用 IDP。
- 第 6 章，“可疑数据包属性”介绍保护网络资源的几个 SCREEN 选项，防止网络资源受到由异常 IP 和 ICMP 数据包属性所指示的潜在攻击。
- 第 7 章，“GPRS 超额计费攻击防护”介绍 GPRS 超额计费攻击并阐述解决方案。
- 附录 A，“用户定义签名的环境”提供对定义状态式签名攻击对象时可指定的环境的说明。

约定

本文档包含几种类型的约定，以下各节将对其加以介绍：

CLI 约定

当出现命令行界面 (CLI) 命令的语法时，使用以下约定：

- 在中括号 [ ] 中的任何内容都是可选的。
- 在大括号 { } 中的任何内容都是必需的。
- 如果选项不止一个，则使用管道 (|) 分隔每个选项。例如，

  ```
  set interface { ethernet1 | ethernet2 | ethernet3 } manage
  ```

  意味着 “设置 ethernet1、 ethernet2 或 ethernet3 接口的管理选项”。
- 变量以*斜体*方式出现。例如：

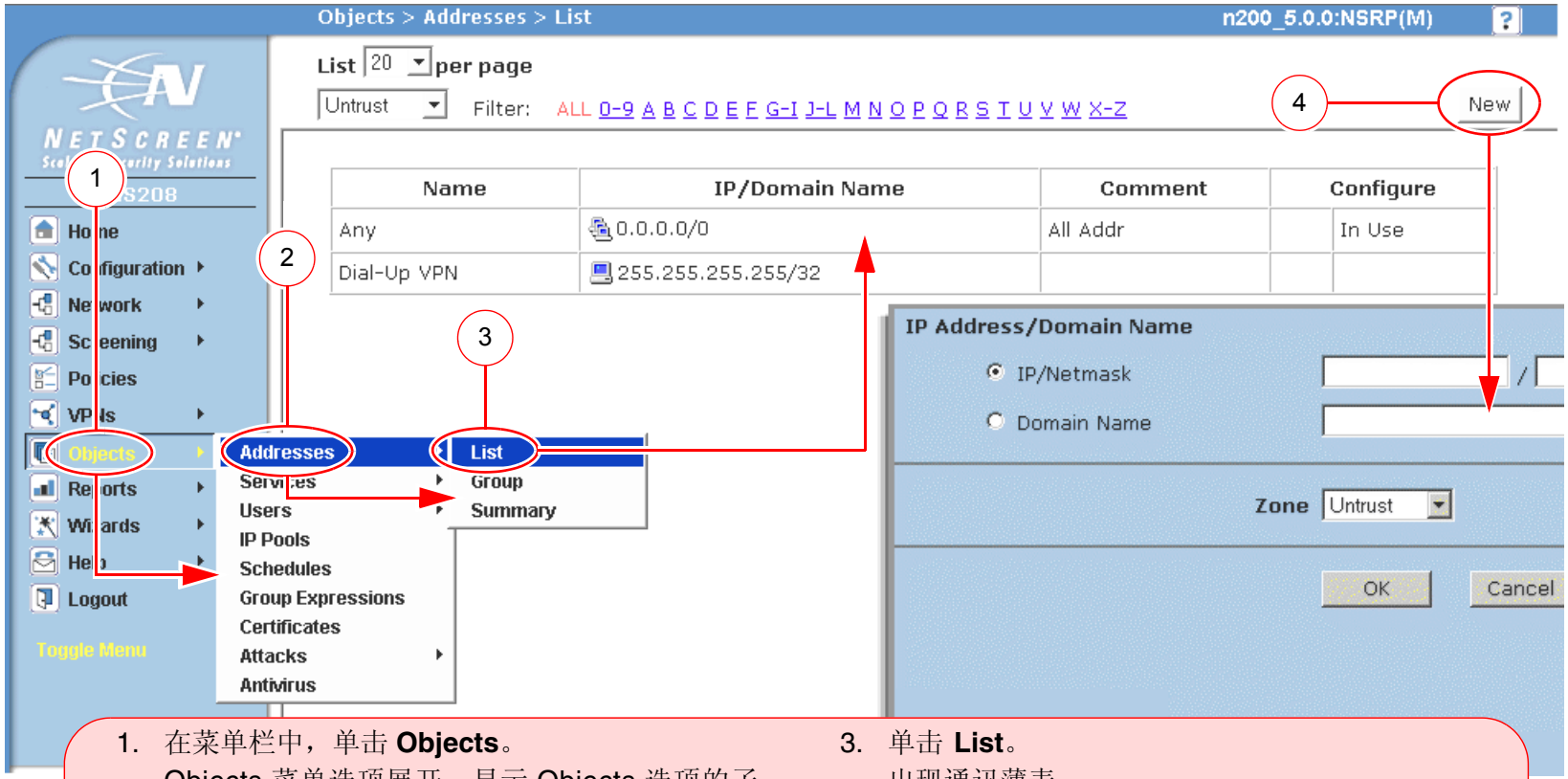
  ```
  set admin user name password
  ```

当 CLI 命令在句子的上下文中出现时，应为**粗体** (除了始终为*斜体*的变量之外)。例如：“使用 **get system** 命令显示 NetScreen 设备的序列号”。

> ***注意：****当键入关键字时，只需键入足够的字母就可以唯一地标识单词。例如，要输入命令* ***set admin user joe j12fmt54****，键入* ***set adm u joe j12fmt54*** *就足够了。尽管输入命令时可以使用此捷径，但本文所述的所有命令都以完整的方式提供。*

WebUI 约定

贯穿本书的全部篇章，用一个 V 形符号 (>) 来指示在 WebUI 中导航，其方法是单击菜单选项和链接。例如，指向地址配置对话框的路径显示为 **Objects > Addresses > List > New**。此导航序列如下所示。



1. 在菜单栏中，单击 **Objects**。
   Objects 菜单选项展开，显示 Objects 选项的子菜单。
2. (Applet 菜单) 将鼠标光标悬停在 **Addresses** 上。
   (DHTML 菜单) 单击 **Addresses**。
   Addresses 选项展开，显示 Addresses 选项的子菜单。
3. 单击 **List**。
   出现通讯薄表。
4. 单击 **New** 链接。
   出现新地址配置对话框。

如要用 WebUI 执行任务，必须首先导航到相应的对话框，然后可在该对话框中定义对象和设置参数。每个任务的指令集划分为两部分：导航路径和配置详细信息。例如，下列指令集包含指向地址配置对话框的路径和要配置的设置：

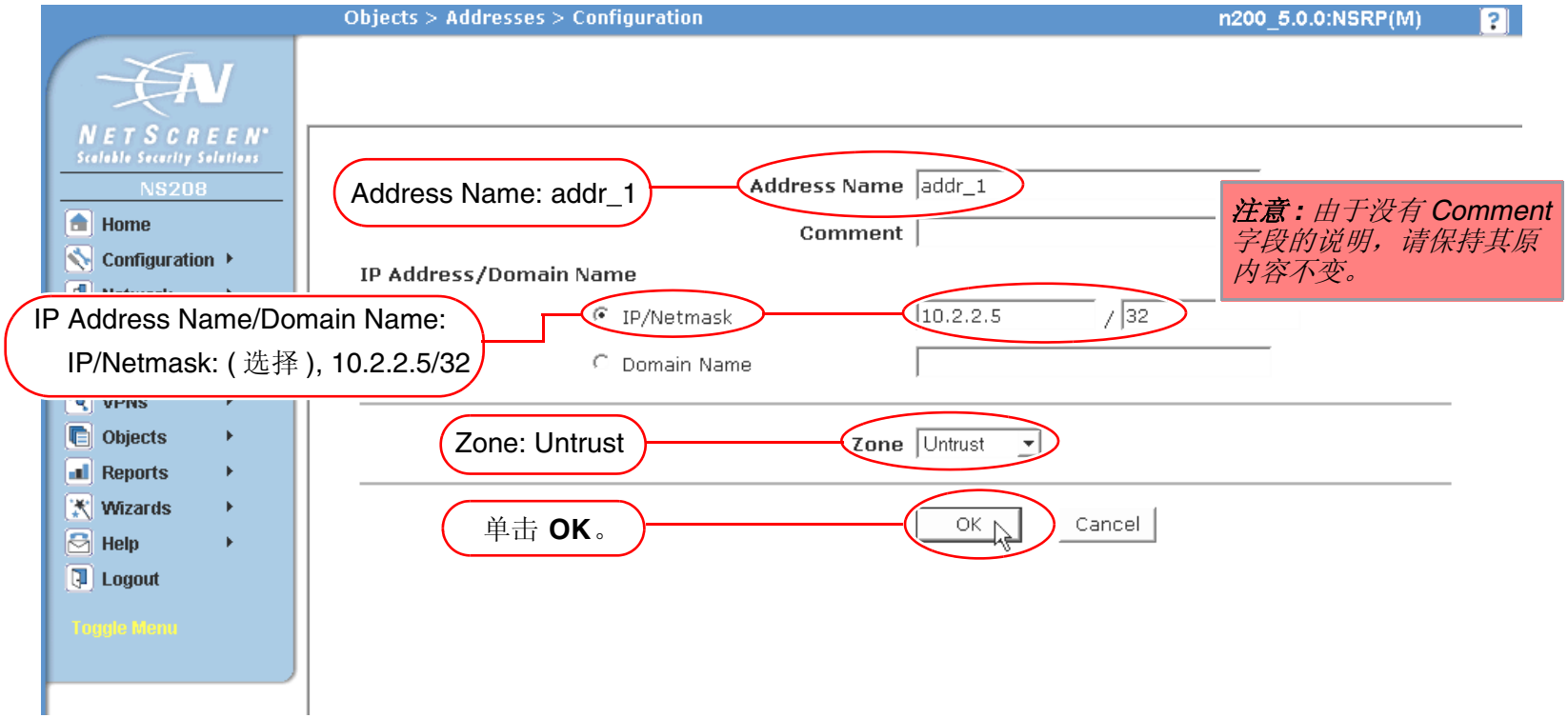
Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

Address Name: addr_1

IP Address/Domain Name:

IP/Netmask: (选择), 10.2.2.5/32

Zone: Untrust

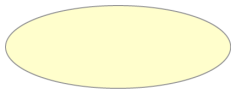


插图约定

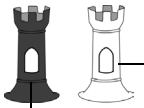
下列图形构成了贯穿本书的插图所用的基本图像集：

通用 NetScreen 设备

虚拟路由选择域



安全区段



安全区段接口

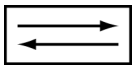
白色 = 受保护区段接口
（例如：Trust 区段）

黑色 = 区段外接口
（例如：Untrust 区段）

通道接口

VPN 通道

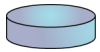
路由器图标



交换机图标

包含单个子网的局域网 (LAN)
（例如：10.1.1.0/24）

互联网



动态 IP (DIP) 池

台式计算机

便携式计算机

通用网络设备
（例如：NAT 服务器，
接入集中器）

服务器

命名约定和字符类型

关于 ScreenOS 配置中定义的对象 (如地址、 admin 用户、 auth 服务器、 IKE 网关、虚拟系统、 VPN 通道和区段) 的名称， ScreenOS 采用下列约定。

- 如果名称字符串包含一个或多个空格，则必须将该整个名称字符串用双引号 (") 括起来；例如，**set address trust "local LAN" 10.1.1.0/24**。
- NetScreen 会删除一组双引号内文本的前导或结尾空格，例如，**" local LAN "** 将变为 **"local LAN"**。
- NetScreen 将多个连续的空格视为单个空格。
- 尽管许多 CLI 关键字不区分大小写，但名称字符串是区分大小写的。例如，**"local LAN"** 不同于 **"local lan"**。

ScreenOS 支持以下字符类型 :

- 单字节字符集 (SBCS) 和多字节字符集 (MBCS)。SBCS 的例子是 ASCII、欧洲语和希伯莱语。MBCS (也称为双字节字符集， DBCS) 的例子是中文、韩文和日文。

  注意 : *控制台连接只支持 SBCS。WebUI 对 SBCS 和 MBCS 都支持，取决于 Web 浏览器所支持的字符集。*

- 从 32 (十六进制 0x20) 到 255 (0xff) 的 ASCII 字符，双引号 (") 除外，该字符有特殊的意义，它用作包含空格的名称字符串的开始或结尾指示符。

JUNIPER NETWORKS NETSCREEN 文档

要获取任何 Juniper Networks NetScreen 产品的技术文档，请访问 www.juniper.net/techpubs/。

要获取技术支持，请使用 http://www.juniper.net/support/ 下的 Case Manager 链接打开支持个例，还可拨打电话 1-888-314-JTAC (美国国内) 或 1-408-745-9500 (美国以外的地区)。

如果在以下内容中发现任何错误或遗漏，请用下面的电子邮件地址与我们联系：

techpubs-comments@juniper.net

1

保护网络

入侵受保护网络的动机可能有很多。下表包含一些常见的目的：

- 收集有关受保护网络的下列各类信息：
  - 网络的拓扑
  - 活动主机的 IP 地址
  - 活动主机上的活动端口数
  - 活动主机的操作系统
- 用虚假信息流耗尽受保护网络上主机的资源，诱发拒绝服务 (DoS)
- 用虚假信息流耗尽受保护网络的资源，诱发网络级 DoS
- 用虚假信息流耗尽防火墙的资源，并因此诱发其保护的网络发生 DoS
- 导致受保护网络上主机的数据破坏以及窃取该主机的数据
- 获得受保护网络上主机的访问权限以获取信息
- 获得主机的控制权以发起其它攻击
- 获得防火墙的控制权以控制对其保护的网络的访问

ScreenOS 提供了检测性和防御性的工具，以使当攻击者试图攻击受 NetScreen 设备保护的网络时，能查明和阻挡其达到上述目的的企图。

本章先概述攻击的主要阶段，并说明在每个阶段可用以阻挡攻击的各种防御机制：

- 第 2 页上的 “攻击阶段”
- 第 3 页上的 “检测和防御机制”
- 第 5 页上的 “攻击监视”

攻击阶段

每次攻击通常都分两个主要阶段进行。第一阶段攻击者收集信息，第二阶段攻击者发起攻击。

1. 执行侦查。
    1. 映射网络并确定哪些主机是活动的 (IP 地址扫描)。
    2. 在通过 IP 地址扫描而发现的主机上，识别哪些端口是活动的 (端口扫描)。
    3. 确定操作系统，从而暴露出操作系统中的弱点，或者提出一个易影响该特定操作系统的攻击。
2. 发动攻击。
    1. 隐藏攻击的发起点。
    2. 执行攻击。
    3. 删除或隐藏证据。

检测和防御机制

攻击过程可以是收集信息的探查，也可以是破坏、停用或损害网络或网络资源的攻击。在某些情况下，两种攻击目的之间的区别不太清楚。例如，TCP SYN 段的阻塞可能是旨在触发活动主机的响应的 IP 地址扫描，也可能是以耗尽网络资源使之不能正常工作为目的的 SYN 泛滥攻击。此外，由于攻击者通常在攻击之前先对目标执行侦查，因而我们可以将收集信息的尝试视为即将来临的攻击的先兆 — 也就是说，它们构成了攻击的第一阶段。因此，术语 “攻击” 既包括侦查活动，也包括攻击活动，有时不太好区分这两者之间的差别。

Juniper Networks 提供了各种区段级和策略级的检测方法和防御机制，以便在所有阶段对抗攻击行为 :

- 区段级的 SCREEN 选项[1]
- 区段间、区段内和超区段的策略级的防火墙策略。 (“超区段” 表示全局策略，不涉及任何安全区段)

为保护所有连接尝试的安全， NetScreen 设备使用了一种动态数据包过滤方法，即通常所说的状态式检查。使用此方法， NetScreen 设备在 IP 数据包和 TCP 片段包头中记入各种不同的信息单元 — 源和目标 IP 地址、源和目标端口号，以及数据包序列号 — 并保持穿越防火墙的每个 TCP 会话和伪 UDP 会话的状态。 (NetScreen 也会根据变化的元素，如动态端口变化或会话终止，来修改会话状态。) 当响应的 TCP 数据包到达时， NetScreen 设备会将其包头中包含的信息与检查表中储存的相关会话的状态进行比较。如果相符，允许响应数据包通过防火墙。如果不相符，则丢弃该数据包。

NetScreen SCREEN 选项用于保护区段的安全，具体做法是先检查要求经过绑定到该区段的某一接口的所有连接尝试，然后予以准许或拒绝。然后 NetScreen 设备应用防火墙策略，在这些策略中，可能包含针对通过 SCREEN 过滤器的信息流的内容过滤和入侵检测及防护 (IDP) 组件。

1. 尽管 VLAN 和 MGT 区段都是功能区段而非安全区段，但仍可为这些区段设置 SCREEN 选项。 VLAN 区段支持与第 3 层安全区段相同的一组 SCREEN 选项。(第 2 层安全区段支持第 3 层安全区段中不支持的一个附加 SYN 泛滥选项 : Drop Unknown MAC。) 由于下列 SCREEN 选项不适用于 MGT 区段，因此不能用于该区段 : SYN 泛滥保护、 SYN-ACK-ACK 代理泛滥保护、 HTTP 组件封锁、以及 WinNuke 攻击保护。

下面概述 NetScreen 防火墙为网络保护提供的各组防御机制：

如前所述， NetScreen 网络保护设置工作有两个级别 : 安全区段和策略。 NetScreen 设备在安全区段级执行侦查威慑和 DoS 攻击防御。在内容监视和过滤区段中， NetScreen 设备在区段级应用碎片重组，在策略级执行防病毒 (AV) 扫描和“统一资源定位器”(URL) 过滤。NetScreen 设备在策略级应用 IDP，但对 HTTP 组件的检测和封锁除外，这些活动在区段级发生。区段级防火墙设置是 SCREEN 选项。在策略中设置的网络保护选项是该策略的一个组成部分。

攻击监视

虽然您通常希望 NetScreen 设备封锁攻击，有时也可能希望收集有关这些攻击的信息。您可能希望具体了解某个特定的攻击 — 发现其意图、技巧和可能的来源 (如果攻击者不小心或不够老练)。

如果您希望收集有关攻击的信息，可以让它发生、监视它、分析它、执行辩论练习，然后按照先前准备好的事件响应计划的描述做出响应。您可以指示 NetScreen 设备将攻击的情况通知您，但 NetScreen 不采取应对措施，而是允许该攻击发生。然后可以研究所发生的现象，并尝试了解攻击者的方法、策略和目的。增加了对网络威胁的了解之后，就能让您更好地加强防御。虽然精明的攻击者会隐藏其位置和身份，但您或许能通过收集足够的信息来识别攻击的始发点。您也许还能估计攻击者的能力。这种信息使您能评估一些响应。

范例 : 监视来自 Untrust 区段的攻击

在本例中，来自 Untrust 区段的 IP 欺骗攻击每日都发生，通常是在 21:00 点与 0:00 之间。当含有欺骗性源 IP 地址的数据包到来时，您希望让 NetScreen 设备发出通知，但不丢弃它们，而是让其通过，或者将其引导到您已在 DMZ 接口连接上连接的某个“蜜罐”(honeypot)[2] 上。20:55 时，您更改防火墙的行为，从通知并拒绝属于已检测到的攻击的数据包，变为通知并接受。攻击发生时，即可使用“蜜罐”监视攻击者越过防火墙后的活动。您也可以与上游 ISP (互联网服务提供商) 合作，开始跟踪数据包来源以找出其源头。

WebUI

Screening > Screen (Zone: Untrust): 输入以下内容，然后单击 **Apply**:

Generate Alarms without Dropping Packet: (选择)

IP Address Spoof Protection: (选择)

CLI

```
set zone untrust screen alarm-without-drop
set zone untrust screen ip-spoofing
save
```

2. “蜜罐”是一个假网络服务器，用来引诱攻击者，然后记录他们在攻击期间的行为。

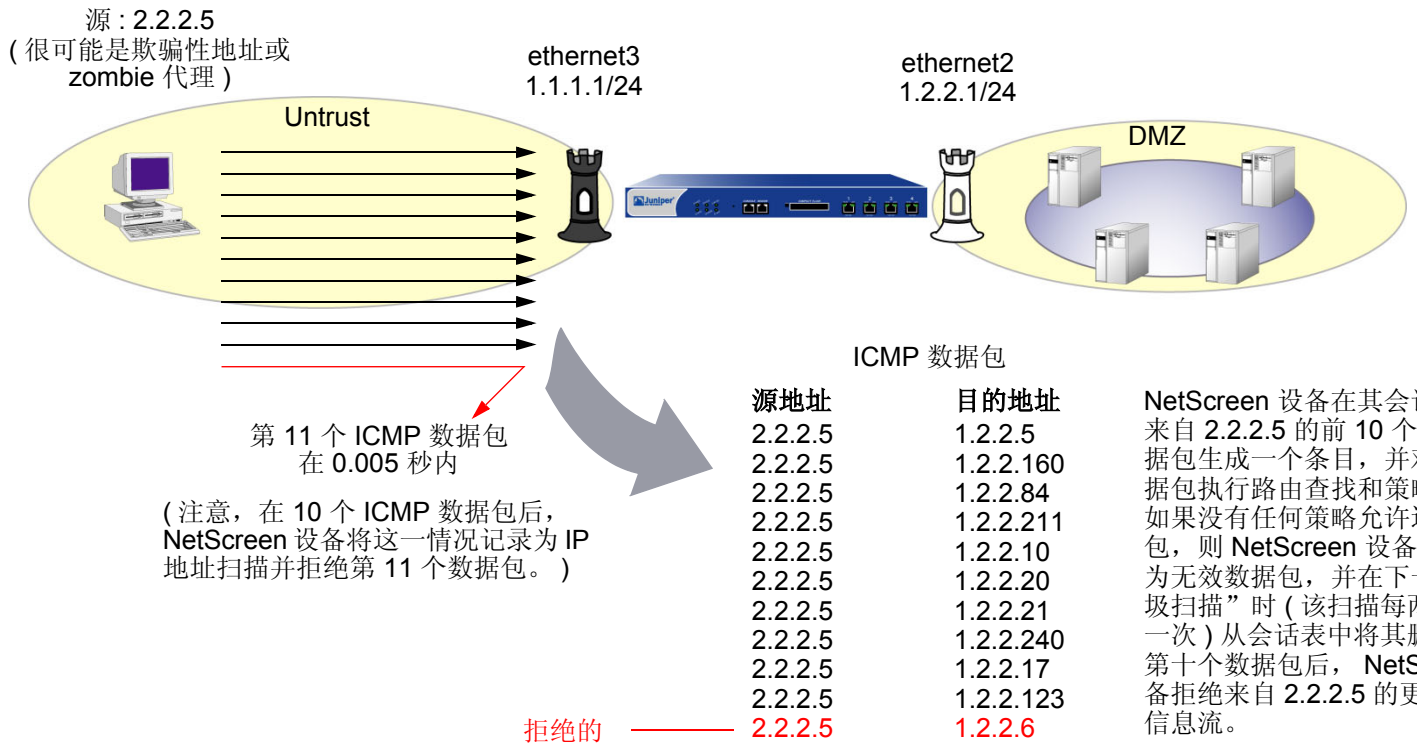
2

侦查威慑

当攻击者先知道了目标网络的布局 (哪些 IP 地址有活动主机)、可能的入口点 (在活动主机上哪些端口号是活动的) 和其受害者的结构 (活动主机在运行哪些操作系统) 后，他们就能更好地计划其攻击。为了获得这些信息，攻击者必须执行侦查。 Juniper Networks 提供了几个 SCREEN 选项以防止攻击者的侦查尝试，从而可阻碍其获得有关受保护网络和网络资源的重要信息。

IP 地址扫描

当一个源 IP 地址在规定的时间间隔 (缺省值为 5000 微秒) 内将 10 个 ICMP 数据包发送给不同的主机时，即进行了一次地址扫描。此方案的目的是将 ICMP 数据包 (通常是应答请求) 发送给各个主机，以期获得至少一个回复，从而查明目标的地址。 NetScreen 设备在内部记录从某一远程源地点发往不同地址的 ICMP 数据包数目。使用缺省设置时，如果某个远程主机在 0.005 秒 (5000 微秒) 内将 ICMP 信息流发送给 10 个地址，则 NetScreen 将其标记为地址扫描攻击，并且在这一秒的剩余时间内拒绝来自该主机的第 11 个及其它更多 ICMP 数据包。



注意 : zombie 代理*是在攻击者的隐秘控制下的受损主机。*

如果有一个策略允许来自某个安全区段的信息流，请考虑为该区段启用此 SCREEN 选项。否则不需要启用它。如果不存在这样的策略，则会拒绝来自该区段的所有 ICMP 信息流，以阻止攻击者成功地执行 IP 地址扫描。

要封锁在特定的安全区段内始发的 IP 地址扫描，请执行以下操作之一：

WebUI

Screening > Screen (Zone: 选择区段名称): 输入以下内容，然后单击 **Apply**:

IP Address Sweep Protection: (选择)

Threshold: (输入触发 IP 地址扫描防护的值[1])

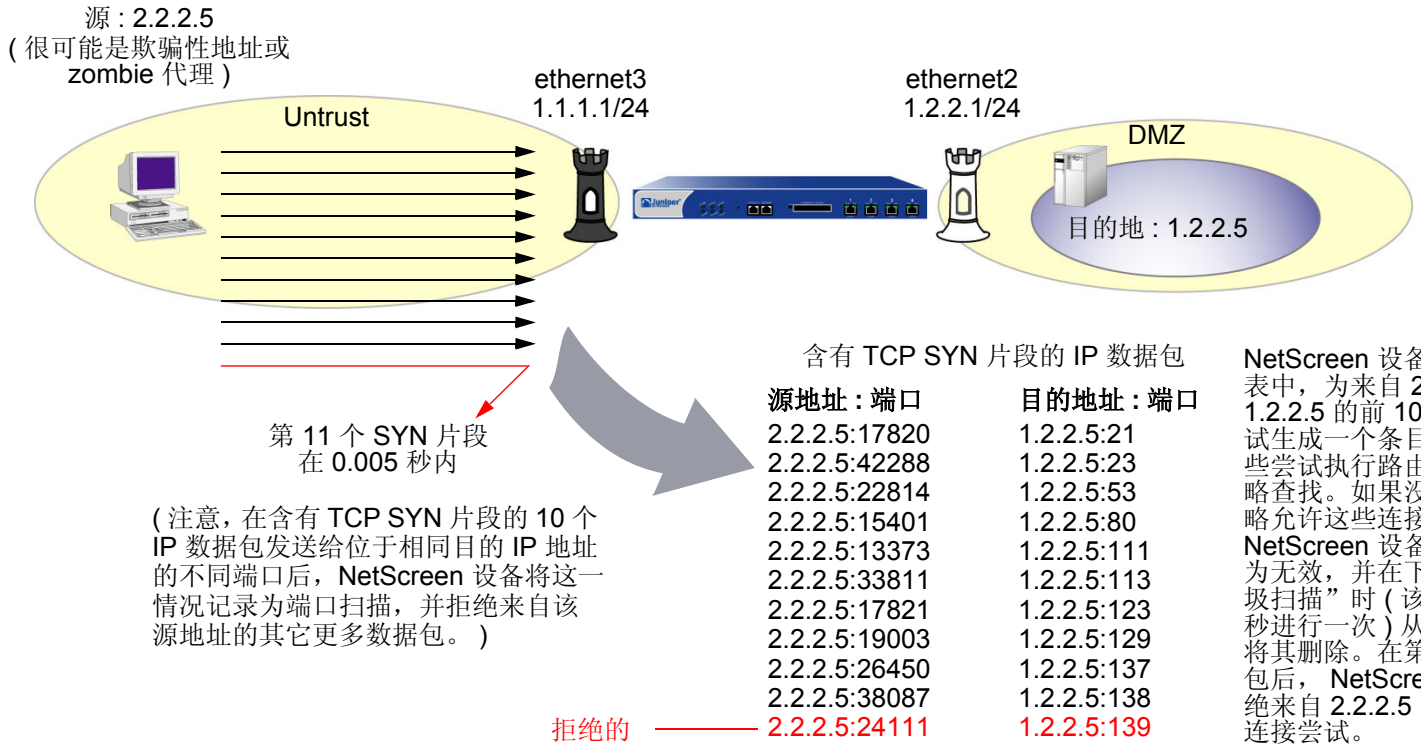
CLI

```
set zone zone screen ip-sweep threshold number
set zone zone screen ip-sweep
```

1. 值的单位为微秒。缺省值是 5000 微秒。

端口扫描

当一个源 IP 地址在规定的时间间隔内 (缺省值为 5000 微秒) 将含有 TCP SYN 片段的 IP 数据包发送给位于相同目标 IP 地址的 10 个不同端口时，即进行了一次端口扫描。此方案的目的是扫描可用的服务，希望至少会有一个端口响应，从而识别目标的服务。 NetScreen 设备在内部记录从某一远程源地点扫描的不同端口的数目。使用缺省设置时，如果某个远程主机在 0.005 秒 (5000 微秒) 内扫描了 10 个端口，则 NetScreen 将其标记为端口扫描攻击，并在这一秒的剩余时间内拒绝来自该远程源地点的其它数据包 (不论目标 IP 地址为何)。



要封锁在特定的安全区段内始发的端口扫描，请执行以下操作之一：

WebUI

Screening > Screen (Zone: 选择区段名称): 输入以下内容，然后单击 **Apply**:

Port Scan Protection: (选择)

Threshold: (输入触发端口扫描防护的值[2])

CLI

```
set zone zone screen port-scan threshold number
set zone zone screen port-scan
```

2. 值的单位为微秒。缺省值是 5000 微秒。

使用 IP 选项的网络侦查

互联网协议标准 “RFC 791, Internet Protocol” 指定了一组选项以提供特殊路由控制、诊断工具和安全性。这些选项出现在 IP 数据包包头中的目的地址后。

IP 包头

RFC 791 承认这些选项 “对于最常用的通信而言是不必要的”，而且，实际上它们很少出现在 IP 数据包包头中。当这些选项确实出现时，则经常被用于某些罪恶用途。下面是所有 IP 选项及其相应的属性的列表 :

类型	类	编号	长度	预期用途	罪恶用途
选项结尾	0*	0	0	表示一个或多个 IP 选项的结尾。	无
无选项	0	1	0	表示包头中没有 IP 选项。	无

类型	类	编号	长度	预期用途	罪恶用途
安全	0	2	11 位	为主机提供一种手段，以发送符合“国防部” (DoD) 要求安全性、分隔、TCC (非公开用户组) 参数以及“处理限制代码”。(此选项在 RFC 791, Internet Protocol 和 RFC 1038, Revised IP Security Option 中说明，目前已废弃。)	未知，但由于此选项已不用，故若在 IP 包头出现时应引起怀疑。
松散源路由	0	3	变化	指定一个部分路由列表，供数据包在从源到目标的行程中选择。数据包必须按照所指定的地址顺序前进，但允许其通过所指定的地址之间的其它路由器。	逃避。攻击者可以使用所指定的路由来隐藏数据包的真实来源，或者获得对受保护网络的访问权限。 (请参阅第 35 页上的 “IP 源路由选项”。)
记录路由	0	7	变化	记录沿 IP 数据包的前进路径的网络设备 IP 地址。然后目标机器可以提取和处理路由信息。 (由于选项和存储空间均受限于 40 字节大小，因此最多只能记录 9 个 IP 地址。)	侦查。如果目标主机是在攻击者控制下的受害机器，攻击者就能收集关于数据包所通过的网络拓扑和编址方案的信息。
流 ID	0	8	4 位	(已废弃) 此选项提供了一种方法，用于在不支持流概念的网络中输送 16 位 SATNET 流标识符。	未知，但由于此选项已不用，故若在 IP 包头出现时应引起怀疑。

类型	类	编号	长度	预期用途	罪恶用途
严格源路由	0	9	变化	指定完整路由列表，供数据包在从源到目标的行程中选择。此列表中的最后一个地址将取代目标字段中的地址。	逃避。攻击者可以使用所指定的路由来隐藏数据包的真实来源，或者获得对受保护网络的访问权限。(请参阅第 35 页上的 “IP 源路由选项”。)
时戳	2†	4		在数据包从起始点到目的地的前进过程中，记录每个网络设备接收到该数据包的时间 (采用世界时‡)。网络设备用 IP 编号加以标识。 此选项建立沿数据包前进路径的路由器 IP 地址列表，并列出每个路由器之间的传输持续时间。	侦查。如果目标主机是在攻击者控制下的受害机器，攻击者就能收集关于数据包所通过的网络的拓扑和寻址方案的信息。

* 标识为 “0” 的选项类旨在用于提供额外的数据包或网络控制。

† 标识为 “2” 的选项类设计用于诊断、调试和度量。

‡ 时戳使用从世界时 (UT) 午夜开始的微秒数。世界时也通常称为 “格林威治时间” (GMT)，这是国际时间标准的基础。

下列 SCREEN 选项检测攻击者用于侦查或某些未知而可疑目的的 IP 选项 :

- **Record Route:** NetScreen 设备检测 IP 选项为 7 (记录路由) 的数据包，并在入口接口的 SCREEN 计数器列表中记录事件。
- **Timestamp:** NetScreen 设备检测 IP 选项列表包含选项 4 (互联网时戳) 的数据包，并在入口接口的 SCREEN 计数器列表中记录事件。
- **Security:** NetScreen 设备检测 IP 选项为 2 (安全) 的数据包，并在入口接口的 SCREEN 计数器列表中记录事件。
- **Stream ID:** NetScreen 设备检测 IP 选项为 8 (流 ID) 的数据包，并在入口接口的 SCREEN 计数器列表中记录事件。

要检测设置了上述 IP 选项的数据包，请执行以下任一操作，其中指定的安全区段是数据包始发的区段：

WebUI

Screening > Screen (Zone: 选择区段名称): 输入以下内容，然后单击 **Apply**:

IP Record Route Option Detection: (选择)

IP Timestamp Option Detection: (选择)

IP Security Option Detection: (选择)

IP Stream Option Detection: (选择)

CLI

```
set zone zone screen ip-record-route
set zone zone screen ip-timestamp-opt
set zone zone screen ip-security-opt
set zone zone screen ip-stream-opt
```

操作系统探查

在发起攻击之前，攻击者可能会尝试探查目标主机，以了解其操作系统 (OS)。有了操作系统信息，攻击者便能更好地决定发起哪种攻击和利用哪些漏洞。 NetScreen 设备可以封锁常用于收集关于操作系统类型信息的侦察性探查。

设置 SYN 和 FIN 标志

通常不会在同一 TCP 片段包头中同时设置 SYN 和 FIN 控制标志。SYN 标志同步化发起 TCP 连接的序列号。FIN 标志表示完成 TCP 连接的数据传输的结束。两种标志的用途是互相排斥的。同时设置了 SYN 和 FIN 标志的 TCP 包头是异常的 TCP 行为，会导致来自接收者的不同响应 (具体取决于操作系统)。

TCP 包头

攻击者可以通过发送同时设置了两个标志的片段，来查看将返回何种系统应答，从而确定出接收端上的系统的种类。接着，攻击者可以利用已知的系统漏洞来实施进一步的攻击。

当启用了此 SCREEN 选项时，NetScreen 设备将检查 TCP 包头中是否设置了 SYN 和 FIN 标志。如果发现了这样的包头，则会丢弃相应的数据包。

要封锁同时设置了 SYN 和 FIN 标志的数据包，请执行以下任一操作，其中指定的安全区段是数据包始发的区段：

WebUI

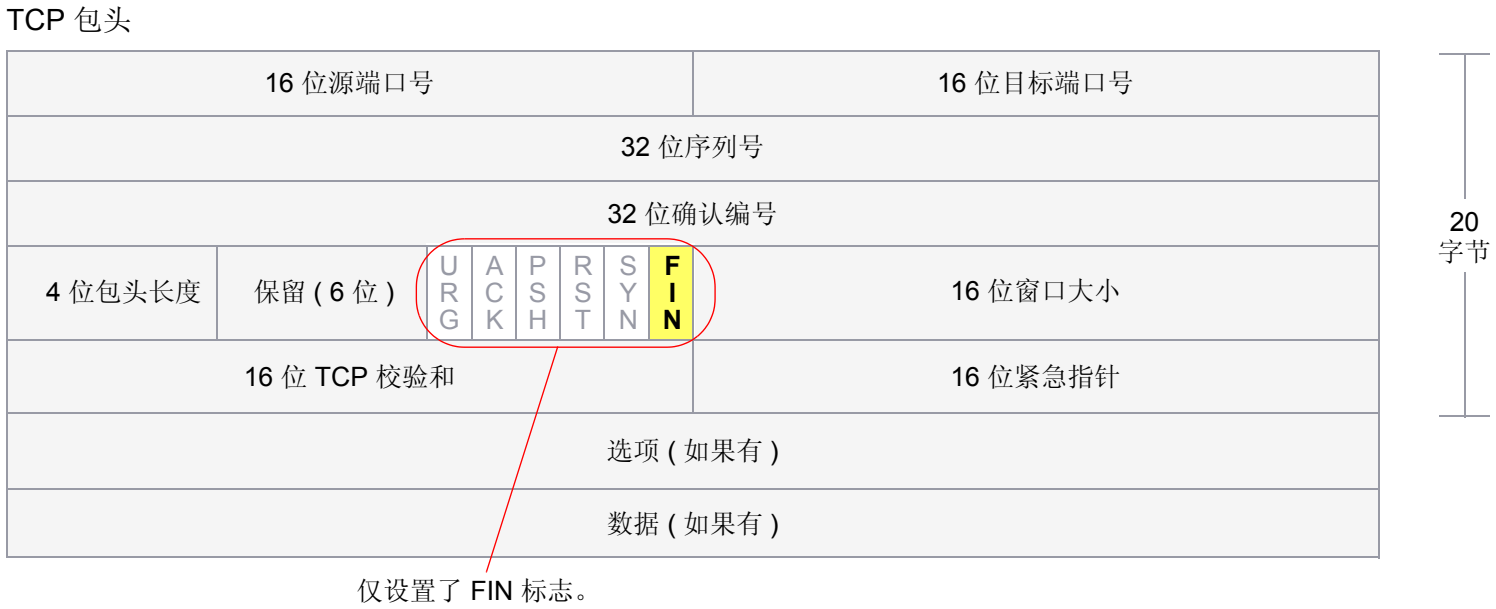
Screening > Screen (Zone: 选择区段名称): 选择 **SYN and FIN Bits Set Protection**，然后单击 **Apply**。

CLI

```
set zone zone screen syn-fin
```

有 FIN 标志但无 ACK 标志

设置了 FIN 控制标志 (以发送会话结束信号并终止连接) 的 TCP 片段通常也设置了 ACK 标志 (以确认接收到的前一个数据包)。由于设置了 FIN 标志但未设置 ACK 标志的 TCP 包头是异常的 TCP 行为，因而对此没有统一的响应[3]。有的操作系统可能会通过发送设置了 RST 标志的 TCP 片段来做出响应。另一些操作系统则可能会完全忽略这种数据包。受害者的响应会给攻击者提供有关其操作系统的线索。(发送设置了 FIN 标志的 TCP 片段的另外一个目的是 : 在执行地址和端口扫描时躲避检测，以及通过执行 FIN 泛滥攻击来躲避对 SYN 泛滥攻击的防御。有关 FIN 扫描的信息，请参阅第 22 页上的 “FIN 扫描”。)



当启用了此 SCREEN 选项时，NetScreen 设备将检查 TCP 包头中是否设置了 FIN 标志而未设置 ACK 标志。如果发现含这种包头的数据包，则会丢弃该数据包。

3. 在设计 TCP/IP 实现方案时，各供货商以不同的方式解释 RFC 793, “Transmission Control Protocol”。当设置了 FIN 标志而未设置 ACK 标志的 TCP 片段到达时，有些实现方案会发送 RST 片段。有些则丢弃数据包而不发送 RST。

要封锁设置了 FIN 标志而未设置 ACK 标志的数据包，请执行以下任一操作，其中指定的安全区段是数据包始发的区段：

WebUI

Screening > Screen (Zone: 选择区段名称): 选择 **FIN Bit with No ACK Bit in Flags Protection**，然后单击 **Apply**。

CLI

```
set zone zone screen fin-no-ack
```

未设置标志的 TCP 包头

常规的 TCP 片段包头至少设置了一个标志控制。未设置任何控制标志的 TCP 片段是一个异常事件。由于不同的操作系统对这种异常情况的响应方式不同，目标设备的响应 (或不响应) 会提供有关其正在运行的操作系统类型的线索。

TCP 包头

当启用了 NetScreen 设备以检测未设置标志的 TCP 片段时， NetScreen 设备将丢弃缺失标志字段或含有残缺标志字段的所有 TCP 数据包。

要封锁未设置标志的数据包，请执行以下任一操作，其中指定的安全区段是数据包始发的区段：

WebUI

Screening > Screen (Zone: 选择区段名称): 选择 **TCP Packet without Flag Protection**，然后单击 **Apply**。

CLI

```
set zone zone screen tcp-no-flag
```

逃避技术

无论是收集信息还是发起攻击，攻击者通常都必须逃避检测。尽管有些 IP 地址和端口扫描是明显和易检测的，但是更狡猾的攻击者会使用各种手段来隐藏其活动。像使用 FIN 扫描来代替 SYN 扫描 (攻击者知道大多数防火墙和入侵检测程序都会检测它) 这类技巧，表明用于躲避检测并成功完成任务的侦查和攻击技术有了较大的发展。

FIN 扫描

FIN 扫描发送设置了 FIN 标志的 TCP 片段，以尝试引发响应 (设置了 RST 标志的 TCP 片段)，并因此而发现活动主机或主机上的活动端口。攻击者可能会使用这种方法，以代替执行含 ICMP 回应请求的地址扫描或含 SYN 片段的地址扫描，因为攻击者知道很多防火墙通常会防御后两种手段 — 但不一定会防御 FIN 片段。使用设置了 FIN 标志的 TCP 片段可能能够躲避检测，因而可帮助攻击者成功实现其侦查尝试。

要阻止 FIN 扫描，可执行以下两种操作之一或两者 :

- 启用相应的 SCREEN 选项，以便专门封锁设置了 FIN 标志但未设置 ACK 标志 (该标志对 TCP 片段而言是异常的) 的 TCP 片段 :

  WebUI: Screening > Screen: 从 Zone 下拉列表中选择要应用此 SCREEN 选项的区段，然后选择 **FIN Bit With No ACK Bit in Flags Protection**

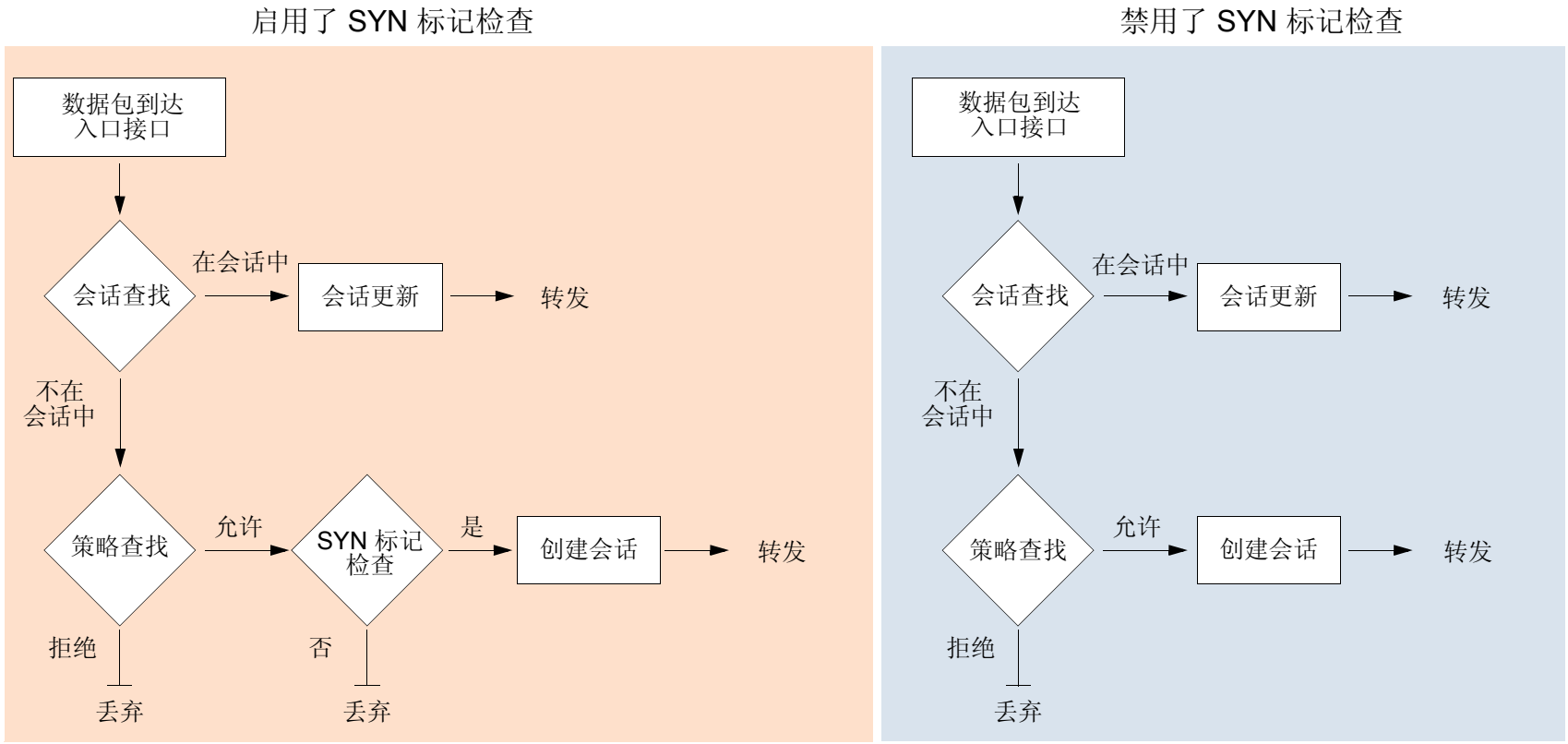
  CLI: 输入 **set zone** *name* **screen fin-no-ack**，其中 *name* 是您要对其应用 SCREEN 选项的区段名

- 通过输入以下 CLI 命令来更改数据包处理行为，以丢弃不属于现有会话的所有无 SYN 的数据包 : **set flow tcp-syn-check**。 (有关 SYN 标记检查的详细信息，请参阅以下小节，第 23 页上的 “非 SYN 标记”。)

注意 : *更改数据包流以检查不属于现有会话的数据包是否设置了 SYN 标记还会阻止其它类型的非 SYN 扫描，例如无标志扫描 (未设置 TCP 标记时)。*

非 SYN 标记

在缺省情况下[4]，NetScreen 设备在会话的第一个数据包检查 SYN 标记并拒绝试图发起会话的不含 SYN 标记的任何 TCP 片段。可以不管此数据包流，或者更改它使得创建会话之前 NetScreen 设备不执行 SYN 标记检查。以下说明了启用和禁用 SYN 标记检查时的数据包流序列[5]:



4. 在缺省情况下，如果安装了运行 ScreenOS 5.1.0 的 NetScreen 设备，将启用检查会话初始数据包中 TCP SYN 标记的功能。如果是从早于 ScreenOS 5.1.0 的版本进行的升级，则在缺省情况下 SYN 检查功能保持禁用状态 — 除非先前已更改了缺省行为。

5. 不论入口接口是运行在第 3 层 (“路由” 或 NAT 模式) 还是第 2 层 (“透明” 模式)，这些数据包流均相同。

当启用了 SYN 标记检查的 NetScreen 设备接收到不属于现有会话的不含 SYN 标记的 TCP 片段时，它将丢弃相应的数据包并向源主机发送 TCP RST — 除非初始的不含 SYN 标记的 TCP 数据包的代码位也是 RST。如果出现这种情况， NetScreen 设备将仅丢弃相应的数据包。

可以使用以下 CLI 命令启用和禁用 SYN 检查：

```
set flow tcp-syn-check
unset flow tcp-syn-check
```

不在第一个数据包检查 SYN 标记具有以下优点：

- **使用非对称路由的 NSRP:** 在动态路由环境的双主动 NSRP 配置中，主机可能向一个 NetScreen 设备 (NetScreen-A) 发送设置了 SYN 标记的初始 TCP 片段，但 SYN/ACK 可能被路由到集群中的其它 NetScreen 设备 (NetScreen-B)。如果这种非对称路由发生在 NetScreen-A 与 NetScreen-B 同步了其会话之后，将不会有任何问题。另一方面，如果 SYN/ACK 响应在 NetScreen-A 同步会话之前到达 NetScreen-B，并且启用了 SYN 检查，则 NetScreen-B 会拒绝 SYN/ACK，从而不能建立会话。如果禁用 SYN 检查，则 NetScreen-B 将接受 SYN/ACK 响应并为其创建一个新会话表条目，即使没有该响应所属的现有会话也是如此。
- **不间断的会话：**如果启用 SYN 检查并向工作网络添加一台以 “透明” 模式运行的 NetScreen 设备，它将中断所有的现有会话，然后必须重新启动这些会话[6]。对于超长的会话来说 (例如大量数据传输或数据库备份)，这种中断将很是麻烦。同样，如果是重置 NetScreen 设备，或者即便是更改策略[7] 核心部分的一个组件，并且启用 SYN 检查，则会中断所有现有会话或应用策略变更的那些会话，并且必须重新启动这些会话。禁用 SYN 检查可以避免这类网络信息流的中断。

6. 对于这种情况，可以在安装 NetScreen 设备时先禁用 SYN 检查。然后，在几小时后 (当建立的会话通过 NetScreen 设备运行时) 启用 SYN 检查。
7. 策略的核心部分包含以下主要组件：源和目标区段、源和目标地址、一项或更多服务以及一项操作。

但是，上述优点的取得将牺牲以下安全性：

- **侦查漏洞：**当一个带有非 SYN 标记 (例如 ACK、URG、RST、FIN) 的初始 TCP 片段到达一个关闭的端口时，多数操作系统 (例如 Windows) 将用设置了 RST 标记的一个 TCP 片段来响应。如果端口是开放的，那么接收方将不进行任何响应。

  通过分析这些响应或无响应，聪明的信息收集者能够侦查受保护的网络以及 NetScreen 策略集。如果侦查者发送设置了非 SYN 标记的 TCP 片段并且策略允许片段通过，接收这类片段的目标主机可能会丢弃片段并用设置了 RST 标记的 TCP 片段来响应。这样的响应将告知犯罪者在特定地址存在活动主机并且目标端口号被关闭。聪明的信息收集者还将知道防火墙策略允许访问相应主机的该端口号。

  通过启用 SYN 标记检查， NetScreen 设备将丢弃不属于现有会话的不含 SYN 标记的 TCP 片段。并且设备不返回 TCP RST 片段。结果，无论策略集是否存在或目标主机上的端口是开放的还是关闭的，扫描者将得不到任何回复。

- **会话表泛滥：**如果禁用 SYN 检查，攻击者可以通过发送大量设置了非 SYN 标记的 TCP 片段来泛滥受保护的网络，以此绕过 NetScreen SYN 泛滥防护功能。尽管目标主机会丢弃数据包，并可能发送 TCP RST 片段来应答，此类泛滥会填满 NetScreen 设备的会话表。会话表填满后， NetScreen 设备将无法处理合法信息流的新会话。

  通过启用 SYN 检查和 SYN 泛滥防护，可以阻止这类攻击。检查在会话的初始数据包上是否设置了 SYN 标记将会强制所有新会话的建立必须从设置了 SYN 标记的 TCP 片段开始。 SYN 泛滥防护即可限制每秒的 TCP SYN 片段数，从而使会话表不致被泛滥。

  ***注意：**有关会话表泛滥的信息，请参阅第 40 页上的 “会话表泛滥”。有关 SYN 泛滥的信息，请参阅第 49 页上的 “SYN 泛滥”。*

如果您不必要禁用 SYN 检查， Juniper Networks 强烈推荐启用 SYN 检查 (ScreenOS 5.1.0 初始安装的缺省状态)。可以使用以下命令来启用该功能 : **set flow tcp-syn-check**。启用 SYN 检查后，除非设置了非 SYN 标记的 TCP 片段属于一个已建立的会话，否则 NetScreen 设备会拒绝这类片段。

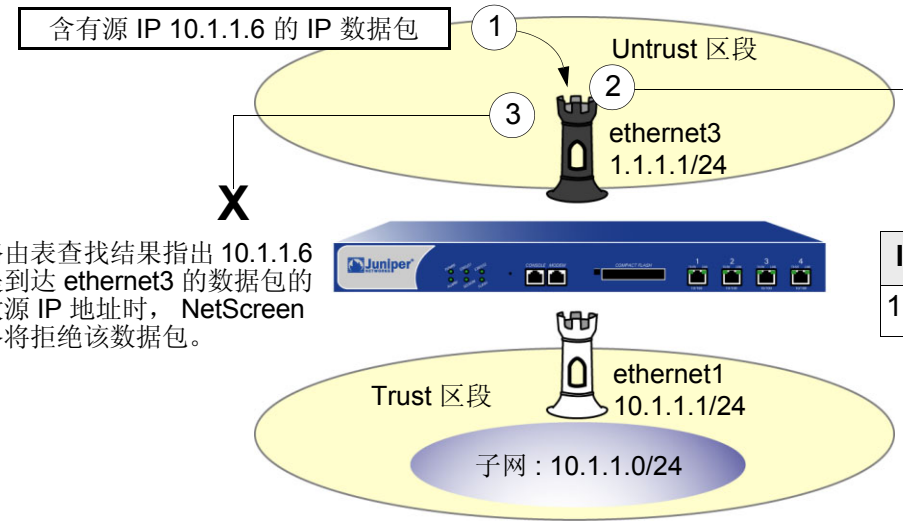
IP 欺骗

尝试获得网络中受限区域的访问权限的一个方法是，在数据包包头中插入虚假源地址，以使该数据包看似发自受信源。这种技术称为 IP 欺骗。 NetScreen 具有两种 IP 欺骗检测方法，均用于完成同样的任务：即确定数据包并非来自其包头所指示的位置。 NetScreen 设备使用何种方法取决于它是运行在 OSI 模型的第 3 层还是第 2 层。

- **第 3 层** – 当 NetScreen 设备上的接口在路由或 NAT 模式下工作时，检测 IP 欺骗的机制依赖于路由表条目。例如，如果含有源 IP 地址 10.1.1.6 的数据包到达 ethernet3，但 NetScreen 设备拥有通过 ethernet1 到 10.1.1.0/24 的路由，那么 IP 欺骗检查会指出该地址到达无效的接口 — 根据路由表中的定义，来自 10.1.1.6 的有效数据包只能通过 ethernet1 到达，而不能通过 ethernet3 到达。因此，设备断定该数据包含有欺骗性源 IP 地址并将其丢弃。

1. IP 数据包到达 ethernet3。其源 IP 地址是 10.1.1.6。

2. 由于在 Untrust 区段中启用了 IP 欺骗防护，因此 NetScreen 设备将检查 10.1.1.6 是否是到达 ethernet3 的数据包的有效源 IP 地址。



路由表

ID	IP 前缀	接口	网关	P
1	10.1.10/24	eth1	0.0.0.0	C

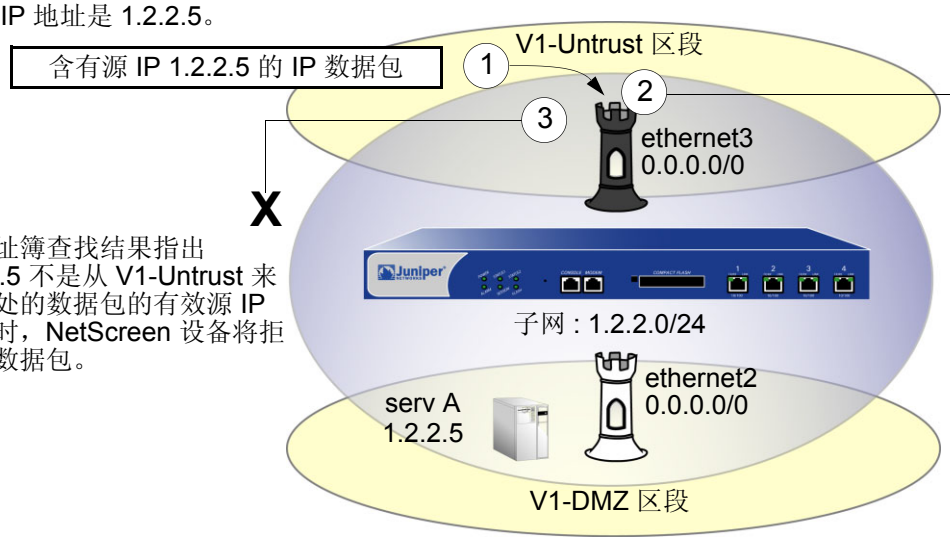
3. 当路由表查找结果指出 10.1.1.6 不是到达 ethernet3 的数据包的有效源 IP 地址时， NetScreen 设备将拒绝该数据包。

如果数据包中的源 IP 地址不在路由表中，则在缺省情况下 NetScreen 设备允许该数据包通过 (假定有一个策略允许它)。使用下列 CLI 命令 (其中指定的安全区段是数据包始发的区段)，可以指示 NetScreen 设备丢弃源 IP 地址不在路由表中的任何数据包 :

set zone *zone* screen ip-spoofing drop-no-rpf-route

- **第 2 层** – 当 NetScreen 设备上的接口在 “透明”模式下工作时， IP 欺骗检查机制将利用地址簿条目。例如，将 “serv A”的地址定义为 V1-DMZ 区段中的 1.2.2.5/32。如果含有源 IP 地址 1.2.2.5 的数据包到达 V1-Untrust 区段接口 (ethernet3)，则 IP 欺骗检查会指出该地址到达了无效的接口。该地址属于 V1-DMZ 区段，但不属于 V1-Untrust 区段，并且只能在绑定到 V1-DMZ 的 ethernet2 处被接受。设备断定该数据包含有欺骗性源 IP 地址并将其丢弃。

1. IP 数据包从 V1-Untrust 区段来到此处。其源 IP 地址是 1.2.2.5。



2. 由于在 V1-Untrust 区段中启用了 IP 欺骗防护，因此 NetScreen 设备将检查 1.2.2.5 是否是从 V1-Untrust 来到此处的数据包的有效源 IP 地址。

地址区段名称 : V1-DMZ

名称	地址	网络掩码
serv A	1.2.2.5	255.255.255.255

3. 当地址簿查找结果指出 1.2.2.5 不是从 V1-Untrust 来到此处的数据包的有效源 IP 地址时，NetScreen 设备将拒绝该数据包。

为跨越多个安全区段的子网定义地址时请多加小心。在上图中， 1.2.2.0/24 同时属于 V1-Untrust 和 V1-DMZ 区段。如果按照如下方式配置 NetScreen 设备，则设备将封锁来自 V1-DMZ 区段的信息流，在该区段中您希望允许：

- 定义 V1-Untrust 区段中的一个地址 1.2.2.0/24。
- 建立一个策略，允许从 V1-DMZ 区段中任一地址到 V1-Untrust 区段中任一地址的信息流 (**set policy from v1-dmz to v1-untrust any any any permit**)。
- 启用 IP 欺骗检查。

由于 V1-DMZ 区段中的地址也在 1.2.2.0/24 子网中，因而当来自这些地址的信息流到达 ethernet2 时， IP 欺骗检查将参考地址簿找出 V1-Untrust 区段中的 1.2.2.0/24。因此， NetScreen 设备封锁该信息流。

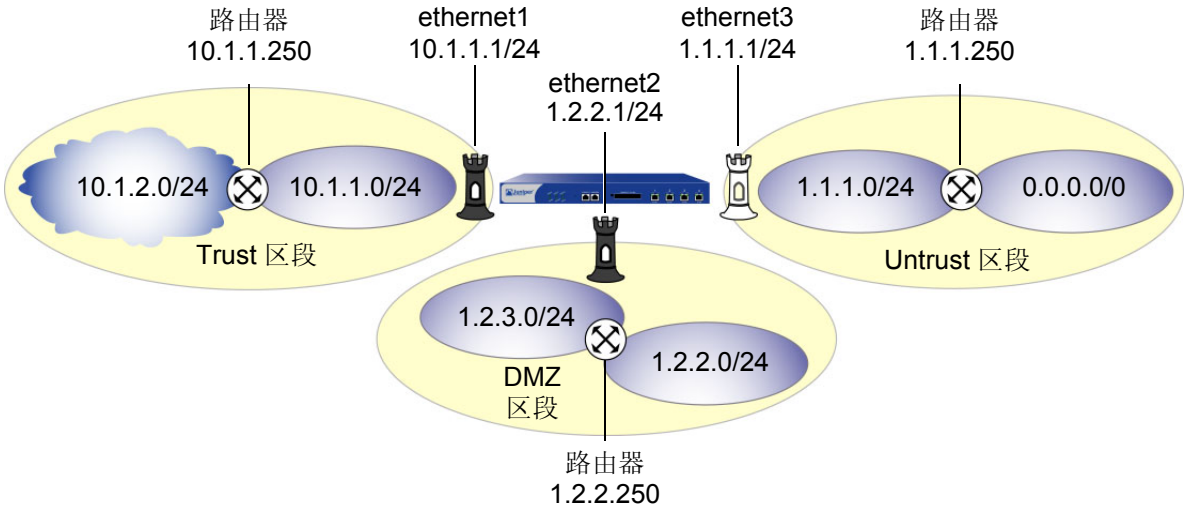
范例：L3 IP 欺骗防护

在本例中，为在第 3 层工作的 NetScreen 设备的 Trust、 DMZ 和 Untrust 区段启用 IP 欺骗防护。在缺省情况下，NetScreen 设备在路由表中自动为接口 IP 地址中指定的子网生成条目。除了这些自动路由表条目外，请手动输入以下三个路由：

目的地：	出口接口：	下一网关：
10.1.2.0/24	ethernet1	10.1.1.250
1.2.3.0/24	ethernet2	1.2.2.250
0.0.0.0/0	ethernet3	1.1.1.250

如果启用了 IP 欺骗防护 SCREEN 选项但没有输入上述三个路由，则 NetScreen 设备将丢弃来自 “目的地”栏中地址的所有信息流，并在事件日志中输入警报信息。例如，如果含有源地址 10.1.2.5 的数据包到达 ethernet1，并且没有通过 ethernet1 到 10.1.2.0/24 子网的路由，则 NetScreen 设备将确定该数据包已到达无效的接口，并将其丢弃。

本例中的所有安全区域都在 trust-vr 路由域中。



WebUI

1. 接口

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容，然后单击 **Apply**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

输入以下内容，然后单击 **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (对于 ethernet2): 输入以下内容，然后单击 **OK**:

Zone Name: DMZ

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.2.2.1/24

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容，然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. 路由

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 10.1.2.0/24

Gateway: (选择)

Interface: ethernet1

Gateway IP Address: 10.1.1.250

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 1.2.3.0/24

Gateway: (选择)

Interface: ethernet2

Gateway IP Address: 1.2.2.250

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

3. IP 欺骗防护

Screening > Screen (Zone: Trust): 选择 **IP Address Spoof Protection**，然后单击 **Apply**。

Screening > Screen (Zone: DMZ): 选择 **IP Address Spoof Protection**，然后单击 **Apply**。

Screening > Screen (Zone: Untrust): 选择 **IP Address Spoof Protection**，然后单击 **Apply**。

CLI

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat

set interface ethernet2 zone dmz
set interface ethernet2 ip 1.2.2.1/24

set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. 路由

```
set vrouter trust-vr route 10.1.2.0/24 interface ethernet1 gateway 10.1.1.250
set vrouter trust-vr route 1.2.3.0/24 interface ethernet2 gateway 1.2.2.250
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

3. IP 欺骗防护

```
set zone trust screen ip-spoofing
set zone dmz screen ip-spoofing
set zone untrust screen ip-spoofing
save
```

范例 : L2 IP 欺骗防护

在本例中，您保护 V1-DMZ 区段，以防止始发自 V1-Untrust 区段中的信息流上的 IP 欺骗。首先，为 V1-DMZ 区段中的三个 Web 服务器定义下列地址 :

- servA: 1.2.2.10
- servB: 1.2.2.20
- servC: 1.2.2.30

然后启用 V1-Untrust 区段中的 IP 欺骗防护。

如果 V1-Untrust 区段中的攻击者试图用 V1-DMZ 区段中的三个地址之一来欺骗源 IP 地址，则 NetScreen 设备会将该地址与地址簿中的地址进行核对。当发现来自 V1-Untrust 区段的数据包中的源 IP 地址属于 V1-DMZ 区段的地址时， NetScreen 设备将拒绝该数据包。

WebUI

1. 地址

   Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

   Address Name: servA

   IP Address/Domain Name:

   IP/Netmask: (选择), 1.2.2.10/32

   Zone: V1-DMZ

   Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

   Address Name: servB

   IP Address/Domain Name:

   IP/Netmask: (选择), 1.2.2.20/32

   Zone: V1-DMZ

Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

Address Name: servC

IP Address/Domain Name:

IP/Netmask: (选择), 1.2.2.30/32

Zone: V1-DMZ

2. IP 欺骗防护

Screening > Screen (Zone: V1-Trust): 选择 **IP Address Spoof Protection**，然后单击 **Apply**。

CLI

1. 地址

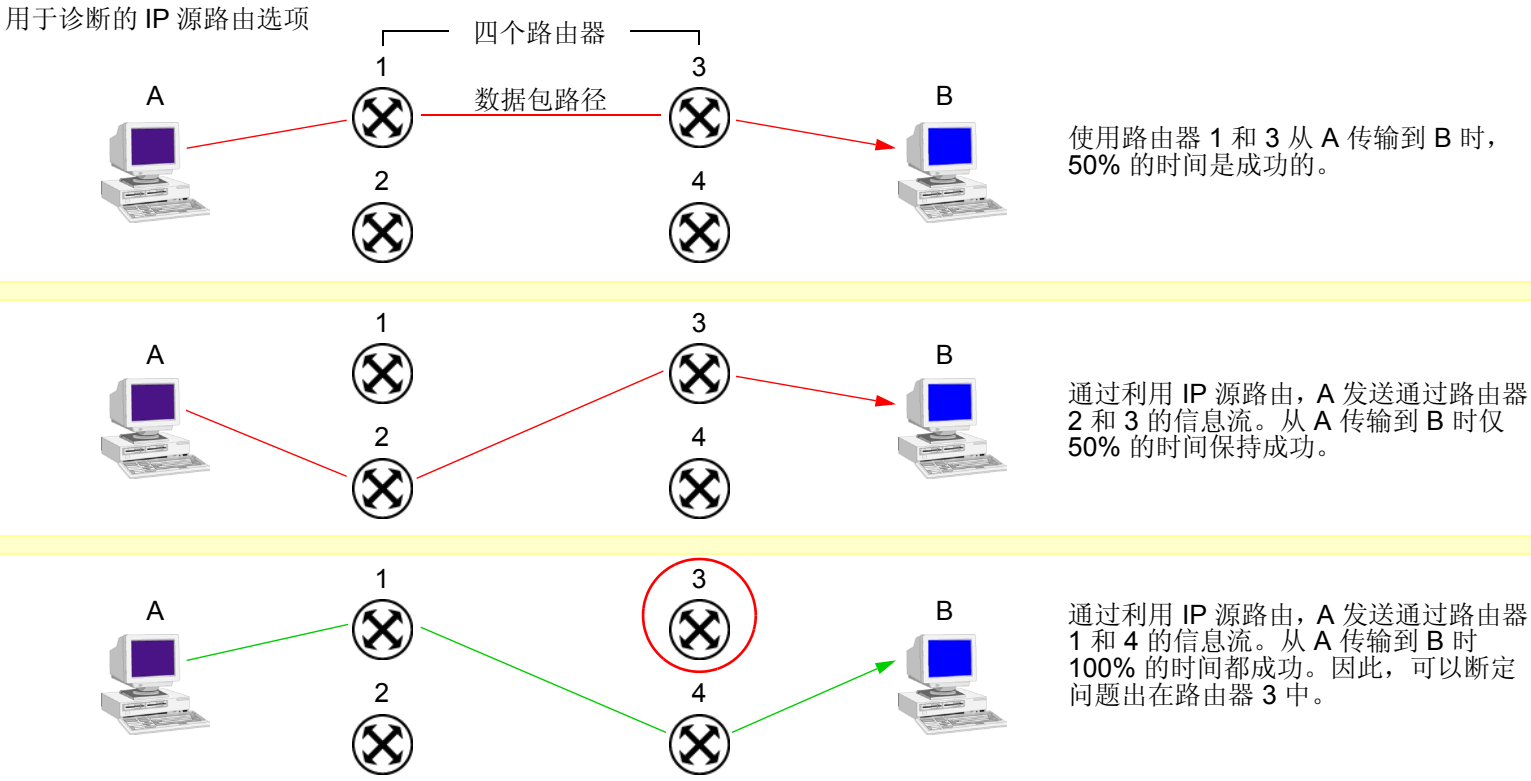
```
set address v1-dmz servA 1.2.2.10/32
set address v1-dmz servB 1.2.2.20/32
set address v1-dmz servC 1.2.2.30/32
```

2. IP 欺骗防护

```
set zone v1-untrust screen ip-spoofing
save
```

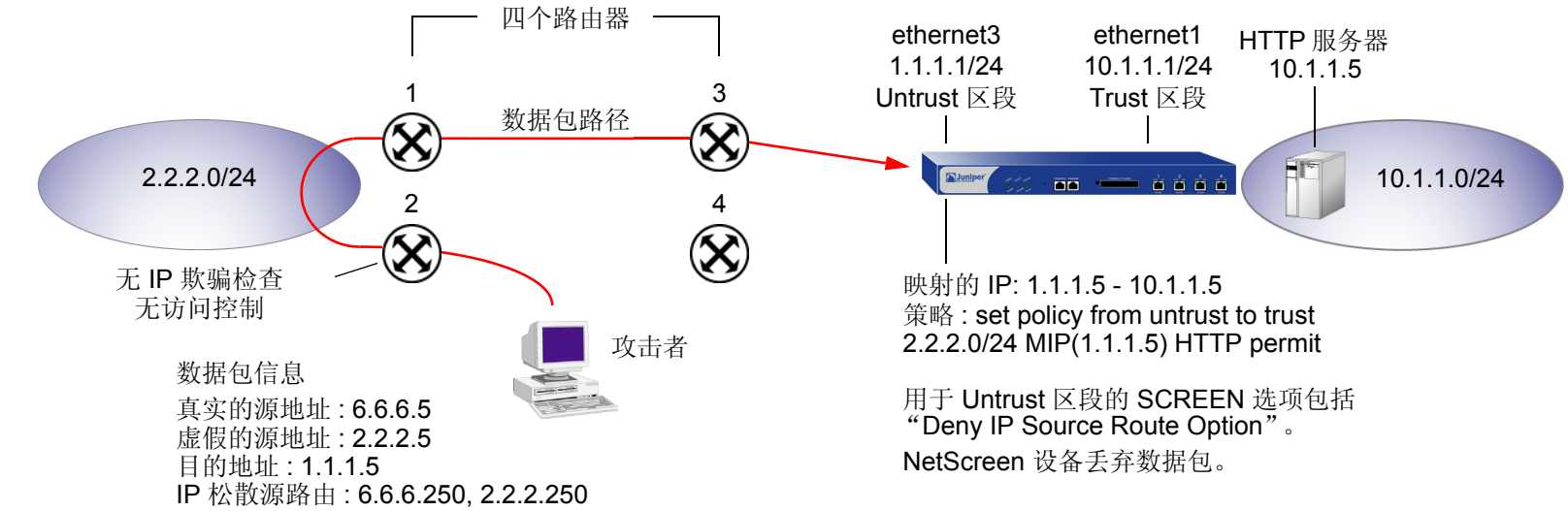
IP 源路由选项

源路由的设计旨在允许位于 IP 数据包传输来源的用户指定沿着某一路径的路由器的 IP 地址 (也称为 “跳”)，用户希望 IP 数据包在通往目的地的行程中采用该路径。 IP 源路由选项最初是为了提供路由控制工具，以协助进行诊断分析。例如，如果向特定目的地成功传输数据包并不规则，您可以首先使用记录路由或时戳 IP 选项，来发现沿着该数据包所采取的路径的路由器地址。然后可以使用松散或严格源路由选项，通过从记录路由或时戳选项产生的结果中所了解的地址，沿特定的路径传送信息流。通过更改路由器地址以改变路径，并沿不同的路径发送几个数据包，您可以注意到提高或降低成功率的变化。通过分析和排除过程，您也许能推断出问题所在的位置。



尽管使用 IP 源路由选项的最初意图是良好的，但攻击者已学会将其用于更多不正当的用途。他们可以使用 IP 源路由选项来隐藏真实地址，并通过指定不同路径来访问网络的受限制区域。为了用范例说明攻击者如何能使用两种欺骗手段，请考虑以下情形。

用于欺骗的松散 IP 源路由选项



NetScreen 防火墙仅允许来自 2.2.2.0/24 并通过 ethernet1 (绑定到 Untrust 区段的接口) 的信息流。路由器 3 和 4 实施访问控制，但路由器 1 和 2 不实施。而且，路由器 2 不检查 IP 欺骗。攻击者伪造源地址，并且通过使用松散源路由选项，将数据包引导通过路由器 2 而到达 2.2.2.0/24 网络，并在此处转发到路由器 1。然后路由器 1 将其转发到路由器 3，而后者将其转发到 NetScreen 设备。由于该数据包来自 2.2.2.0/24 子网，并且含有来自该子网的源地址，因此该数据包看似有效。但是，仍存在早期欺骗的一个残留项 : 松散源路由选项。在本例中，已为 Untrust 区段启用了“Deny IP Source Route Option” SCREEN 选项。当数据包到达 ethernet3 时， NetScreen 设备会将其拒绝。

您可以启用 NetScreen 设备，使之封锁设置了松散或严格源路由选项的任何数据包，或者检测这些数据包，然后在入口接口的计数器列表中记录事件。 SCREEN 选项如下：

- **Deny IP Source Route Option:** 启用此选项可封锁使用松散或严格源路由选项的所有 IP 信息流。源路由选项可以允许攻击者用假的 IP 地址进入网络。
- **Detect IP Loose Source Route Option:** NetScreen 设备检测 IP 选项为 3 (松散源路由) 的数据包，并在入口接口的 SCREEN 计数器列表中记录事件。此选项指定一个部分路由列表，供数据包在从源到目标的行程中选择。数据包必须按照所指定的地址顺序前进，但允许其通过所指定的地址之间的其它路由器。
- **Detect IP Strict Source Route Option:** NetScreen 设备检测 IP 选项为 9 (严格源路由) 的数据包，并在入口接口的 SCREEN 计数器列表中记录事件。此选项指定完整路由列表，供数据包在从源到目标的行程中选择。此列表中的最后一个地址将取代目的地字段中的地址。

  (有关所有 IP 选项的详细信息，请参阅第 12 页上的 “使用 IP 选项的网络侦查”。)

要封锁设置了松散或严格源路由选项的数据包，请执行以下任一操作，其中指定的安全区段是数据包始发的区段：

WebUI

Screening > Screen (Zone: 选择区段名称): 选择 **IP Source Route Option Filter**，然后单击 **Apply**。

CLI

```
set zone zone screen ip-filter-src
```

要检测并记录 (但不封锁) 设置了松散或严格源路由选项的数据包，请执行以下任一操作，其中指定的安全区段是数据包始发的区段 :

WebUI

Screening > Screen (Zone: 选择区段名称): 输入以下内容，然后单击 **Apply**:

IP Loose Source Route Option Detection: (选择)

IP Strict Source Route Option Detection: (选择)

CLI

```
set zone zone screen ip-loose-src-route
set zone zone screen ip-strict-src-route
```

3

拒绝服务攻击防御

拒绝服务 (DoS) 攻击的目的是用极大量的虚假信息流耗尽目标受害者的资源，使受害者被迫全力处理虚假信息流，而无法处理合法信息流。攻击的目标可以是 NetScreen 防火墙、防火墙所控制访问的网络资源、或者个别主机的特定硬件平台或操作系统 (OS)。

如果 DoS 攻击始发自多个源地址，则称为分布式拒绝服务 (DDoS) 攻击。通常， DoS 攻击中的源地址是欺骗性的。DDoS 攻击中的源地址可以是欺骗性地址，也可以是攻击者以前损害过的主机的实际地址，以及攻击者目前正用作“zombie 代理”且从中发起攻击的主机的实际地址。

NetScreen 设备可以防御本身及其保护的资源不受 DoS 和 DDoS 攻击。以下部分介绍可用的各种防御选项：

防火墙 DoS 攻击

如果发现存在 NetScreen 防火墙，则攻击者可能会发起针对防火墙的拒绝服务 (DoS) 攻击，而不是攻击防火墙后面的网络。对防火墙的成功 DoS 攻击等价于对所保护网络的成功 DoS 攻击，因为该攻击阻止合法信息流通过防火墙的尝试。本部分介绍攻击者可能用来填满 NetScreen 设备的会话表以实现 DoS 攻击的两种方法 : 会话表泛滥和 SYN-ACK-ACK 代理泛滥。

会话表泛滥

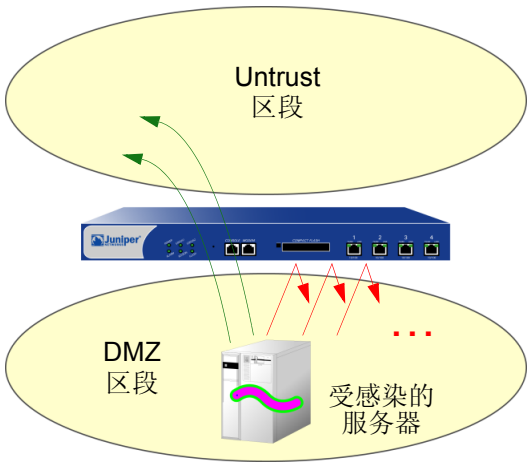
成功的 DoS 攻击会用巨大的假信息流阻塞耗尽受害者的资源，使其无法处理合法的连接请求。 DoS 攻击可以采用多种形式 — SYN 泛滥、 SYN-ACK-ACK 泛滥、 UDP 泛滥、 ICMP 泛滥，等等 — 但它们都会寻求相同的目标 : 填满受害者的会话表。当会话表填满时，该主机不能创建任何新会话，并开始拒绝新连接请求。下列 SCREEN 选项可帮助减轻这类攻击 :

- 基于源和目标的会话限制
- 主动调整会话时间

基于源和目标的会话限制

除了限制来自相同源 IP 地址的并发会话数目之外，也可以限制对相同目标 IP 地址的并发会话数目。设置基于源的会话限制的一个优点是该操作可以阻止像 Nimda 病毒 (实际上既是病毒又是蠕虫) 这样的攻击，该类病毒会感染服务器，然后开始从服务器生成大量的信息流量。由于所有由病毒生成的流量都始发自相同的 IP 地址，因此，基于源的会话限制可以保证 NetScreen 防火墙能抑制这类巨量的信息流。

基于源的会话限制：
Nimda 病毒 / 蠕虫信息流封锁

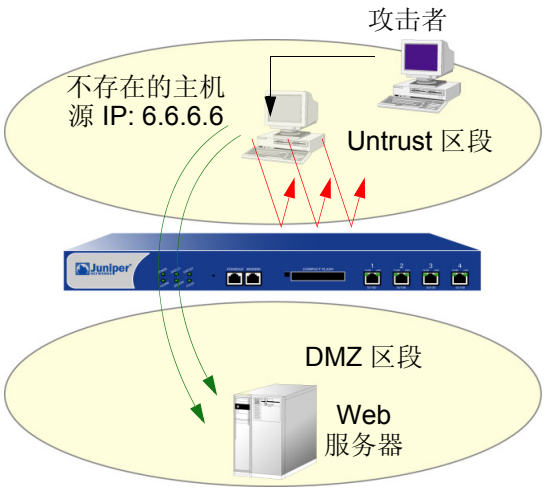


Web 服务器被感染了 Nimda 病毒 / 蠕虫混合体，导致该服务器生成巨大的信息流量。

在来自受感染服务器的并发会话数目达到最大限值后， NetScreen 设备开始封锁来自该服务器的所有其它连接尝试。

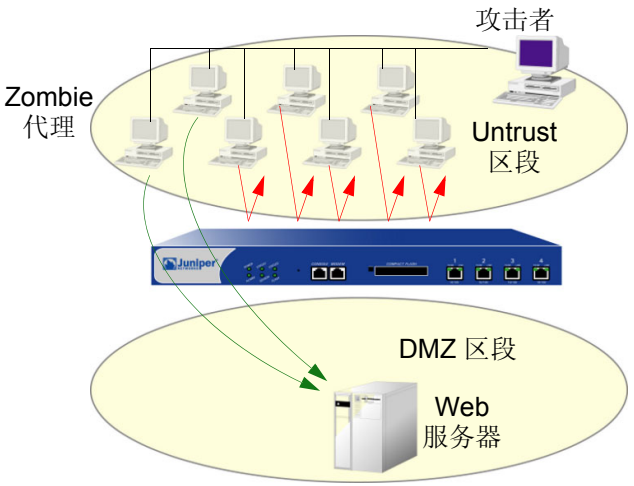
基于源的会话限制的另一个优点是能减轻填满 NetScreen 会话表的企图 — 如果所有连接尝试都始发自相同的源 IP 地址。但是，狡猾的攻击者会发起分布式的拒绝服务 (DDoS) 攻击。在 DDoS 攻击中，恶意信息流可来自上百个称为“zombie 代理”的主机，它们都处在攻击者的秘密控制下。除了 SYN、 UDP 和 ICMP 泛滥检测以及防护 SCREEN 选项外，设置基于目标的会话限制可以确保 NetScreen 设备只允许可接受数目的并发连接请求到达任一个主机 — 无论来源是什么。

基于源的会话限制：
拒绝服务攻击



当来自 6.6.6.6 的并发会话数超过最大限值时，NetScreen 设备开始封锁来自该 IP 地址的所有其它连接尝试。

基于目标的会话限制：
分布式拒绝服务攻击



当与 Web 服务器的并发会话数超过最大限值时，NetScreen 设备开始封锁到该 IP 地址的所有其它连接尝试。

为了确定构成可接受的连接请求数目的因素，需要经过一段时间的观察和分析，建立典型信息流量的基准。您也需要考虑填满所用的特定 NetScreen 平台的会话表所需的最大并发会话数。要查看会话表所支持的最大并发会话数，请使用 CLI 命令 **get session**，然后查找输出信息的第一行，其中列出了当前 (已分配的) 会话数、最大会话数以及失败的会话分配数：

```
alloc 420/max 128000, alloc failed 0
```

基于源和基于目标的最大会话数的缺省限值都是 128 个并发会话，您可能需要调整该值，以适应网络环境和平台的需要。

范例：基于源的会话限制

在本例中，将限制 DMZ 区段和 Trust 区段中的任一个服务器所能发起的会话数目。由于 DMZ 区段仅包含 Web 服务器，其中任一个服务器都不会发起信息流，因此，可将基于源的会话限值设置为可能的最低值：1 个会话。另一方面， Trust 区段包含个人计算机、服务器、打印机，等等，其中很多主机都会发出信息流。对于 Trust 区段，将源会话数最大限值设置为 80 个并发会话。

WebUI

Screening > Screen (Zone: DMZ): 输入以下内容，然后单击 **OK**:

Source IP Based Session Limit: (选择)
Threshold: 1 Sessions

Screening > Screen (Zone: Trust): 输入以下内容，然后单击 **OK**:

Source IP Based Session Limit: (选择)
Threshold: 80 Sessions

CLI

```
set zone dmz screen limit-session source-ip-based 1
set zone dmz screen limit-session source-ip-based
set zone trust screen limit-session source-ip-based 80
set zone trust screen limit-session source-ip-based
save
```

范例：基于目标的会话限制

在本例中，将限制发向地址为 1.2.2.5 的 Web 服务器的信息流量。该服务器位于 DMZ 区段中。在观察从 Untrust 区段发往该服务器的信息流量达一个月之后，您已确定服务器接收到的平均并发会话数是 2000。根据这个信息，您决定将新会话限值设置为 4000 个并发会话。尽管您的观察说明信息流峰值有时超过此限值，但您认为防火墙安全性相对于服务器的偶然不可访问性更为重要。

WebUI

Screening > Screen (Zone: Untrust): 输入以下内容，然后单击 **OK**:

Destination IP Based Session Limit: (选择)

Threshold: 4000 Sessions

CLI

```
set zone untrust screen limit-session destination-ip-based 4000
set zone untrust screen limit-session destination-ip-based
save
```

主动调整会话时间

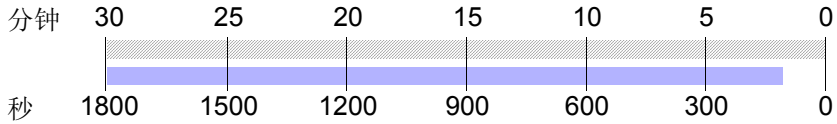
在缺省情况下，初始的三方握手 TCP 会话经过 20 秒钟便会超时 (即因无活动而终止)。在建立 TCP 会话后，超时值变为 30 分钟。 HTTP 和 UDP 会话的会话超时值分别是 5 分钟和 1 分钟。会话超时计数器在会话开始时开始计时，并在会话处于活动状态的情况下每 10 秒钟刷新一次。如果会话空闲时间超过 10 秒钟，则超时计数器的数字开始减小。

NetScreen 提供了一个机制，在会话表中的会话数超过指定的高位临界值时加速超时过程。当会话数下降到指定的低位临界值之下时，超时过程恢复正常。在这段时间内，当主动加速超时过程起作用时， NetScreen 设备将采用所指定的超时率，首先让最早的会话超时。这些超时效的会话被标记无效，并在下一次 “垃圾清扫” 时被删除，这种清扫操作每 2 秒执行一次。

主动加速超时选项将缺省的会话超时时间减去所输入的量值[1]。主动加速超时值可以介于 2 和 10 个单位之间，其中每个单位代表 10 秒 (也就是说，主动加速超时设置可以介于 20 和 100 秒之间)。缺省设置是 2 个单位 (20 秒)。例如，如果您将主动加速超时设置规定为 100 秒，则按照下列方式缩短 TCP 和 HTTP 会话超时时间 :

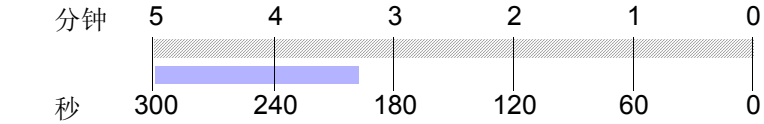
- TCP: 在主动调整时间过程生效的期间，会话超时值从 1800 秒 (30 分钟) 缩短到 1700 秒 (28 分 20 秒)。在此时段内， NetScreen 设备自动删除超时值超过 1700 秒的所有 TCP 会话，并会从首先删除最早的会话开始。

缺省 TCP 会话超时 : 30 分钟 (1800 秒)
主动加速超时 = 10 (从缺省值中减去 100 秒):
28 分 20 秒 (1700 秒)



- HTTP: 在主动调整时间过程生效的期间，会话超时值从 300 秒 (5 分钟) 缩短到 200 秒 (3 分 20 秒)。在此时段内， NetScreen 设备自动删除超时值超过 200 秒的所有 HTTP 会话，并会从首先删除最早的会话开始。

缺省 HTTP 会话超时 : 5 分钟 (300 秒)
主动加速超时 = 10 (从缺省值中减去 100 秒):
3 分 20 秒 (200 秒)

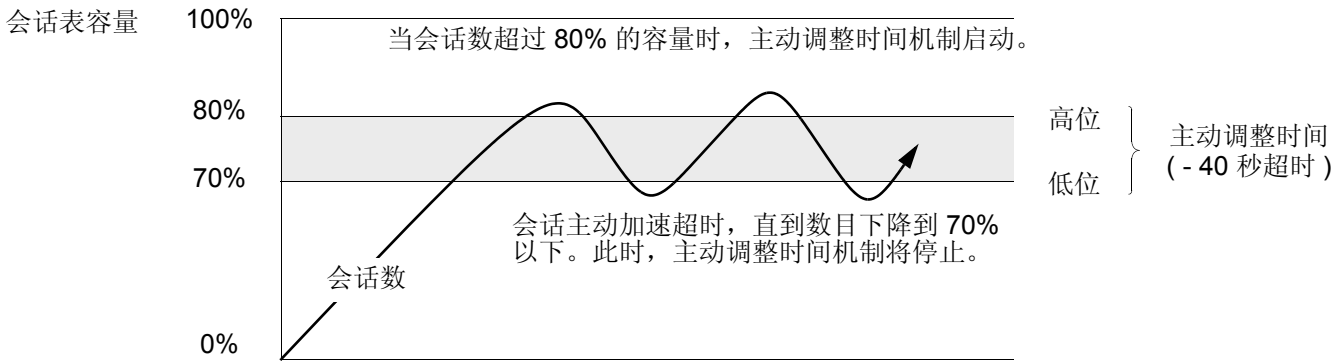


- UDP: 由于缺省的 UDP 会话超时值是 60 秒，规定 100 秒的提前超时设置会导致所有 UDP 会话超时并加上删除标记，以便在下一次垃圾清扫时删除。

1. 当您设置并启用了主动加速超时选项时，配置中显示的正常会话超时值保持不变 — TCP 会话是 1800 秒、HTTP 会话是 300 秒、UDP 会话是 60 秒。但是，当主动加速超时时段生效时，这些会话将提前超时 — 提前时间为您指定的提前超时值 — 而不是一直倒计时至零。

范例：主动加速超时会话

在本例中设置主动加速超时过程，使其在信息流超过 80% 的高位临界值时开始，在信息流降低到 70% 的低位临界值之下时停止。将主动加速超时间隔指定为 40 秒。当会话表充满 80% 以上的容量 (高位临界值) 时， NetScreen 设备将所有会话的超时时间减少 40 秒，并开始对最早的会话进行主动加速超时，直到会话表中的会话数目小于 70% 的容量 (低位临界值)。



WebUI

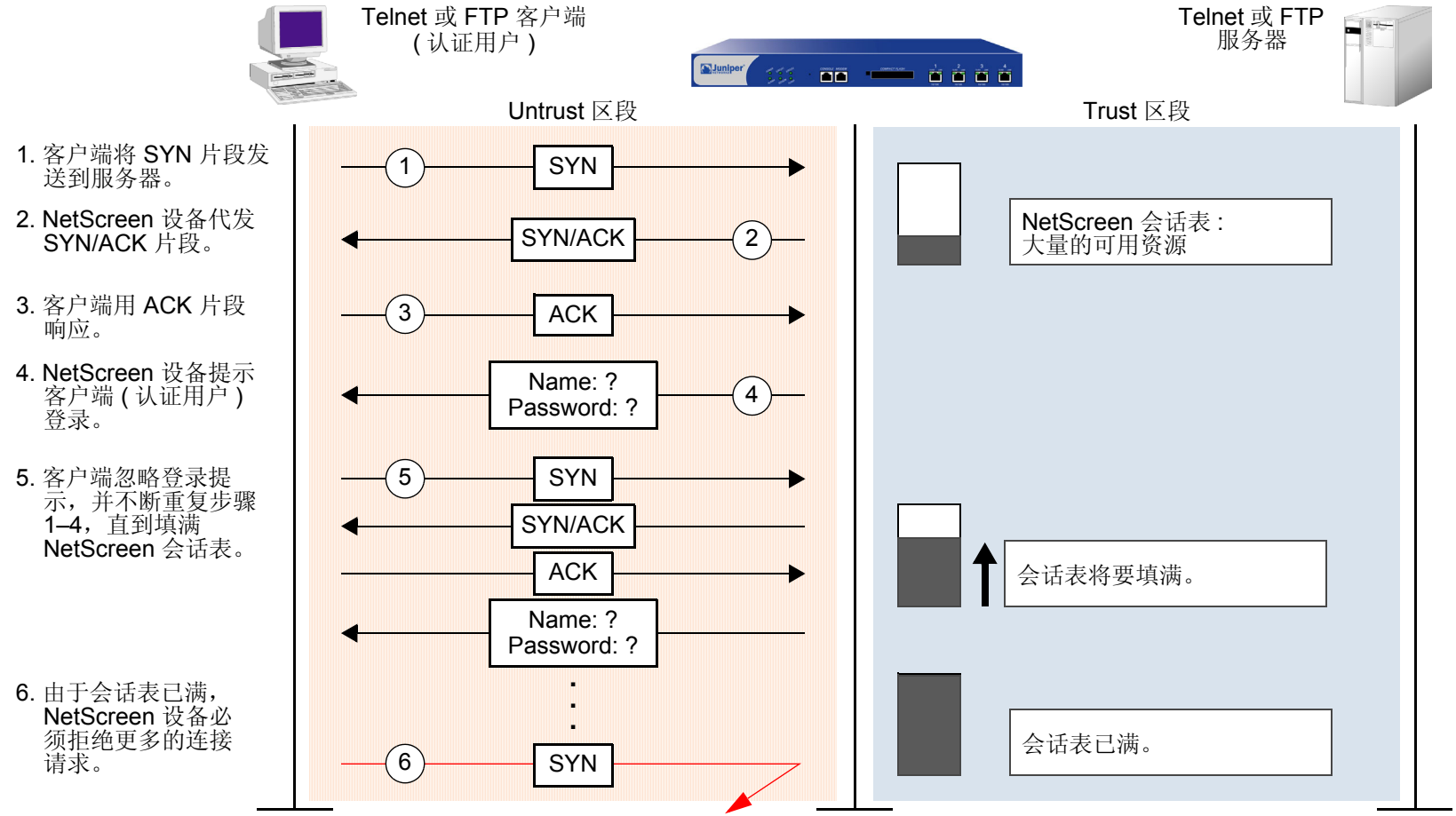
> ***注意：****必须使用 CLI 来配置主动加速超时设置。*

CLI

```
set flow aging low-watermark 70
set flow aging high-watermark 80
set flow aging early-ageout 4
save
```

SYN-ACK-ACK 代理泛滥

当认证用户发起 Telnet 或 FTP 连接时，该用户将 SYN 片段发送到 Telnet 或 FTP 服务器。 NetScreen 设备截取该 SYN 片段，在其会话表中创建一个条目，并代发一个 SYN-ACK 片段给该用户。然后该用户用 ACK 片段回复。至此就完成了初始三方握手。 NetScreen 设备然后向用户发出登录提示。如果怀有恶意的用户并未登录，而是继续发起 SYN-ACK-ACK 会话，则 NetScreen 会话表将被填满到设备开始拒绝合法连接请求的临界点。



为了阻挡这种攻击，可以启用 SYN-ACK-ACK 代理保护 SCREEN 选项。在来自相同 IP 地址的连接数目达到 SYN-ACK-ACK 代理临界值后， NetScreen 设备将拒绝来自该 IP 地址的更多其它连接请求。在缺省情况下，来自任何单个 IP 地址的连接数目临界值是 512。您可以更改此临界值 (改为 1 到 250,000 之间的任何整数)，以更好地适应网络环境的要求。

要启用对 SYN-ACK-ACK 代理泛滥的防御，请执行下列操作，其中指定的区段是攻击始发的位置 :

WebUI

Screening > Screen (Zone: 选择区段名称): 输入以下内容，然后单击 **Apply**:

SYN-ACK-ACK Proxy Protection: (选择)

Threshold: (输入触发 SYN-ACK-ACK 泛滥防护的值[2])

CLI

```
set zone zone screen syn-ack-ack-proxy threshold number
set zone zone screen syn-ack-ack-proxy
```

2. 该值的单位是每个源地址的连接数。缺省值是来自任何单个 IP 地址的 512 个连接。

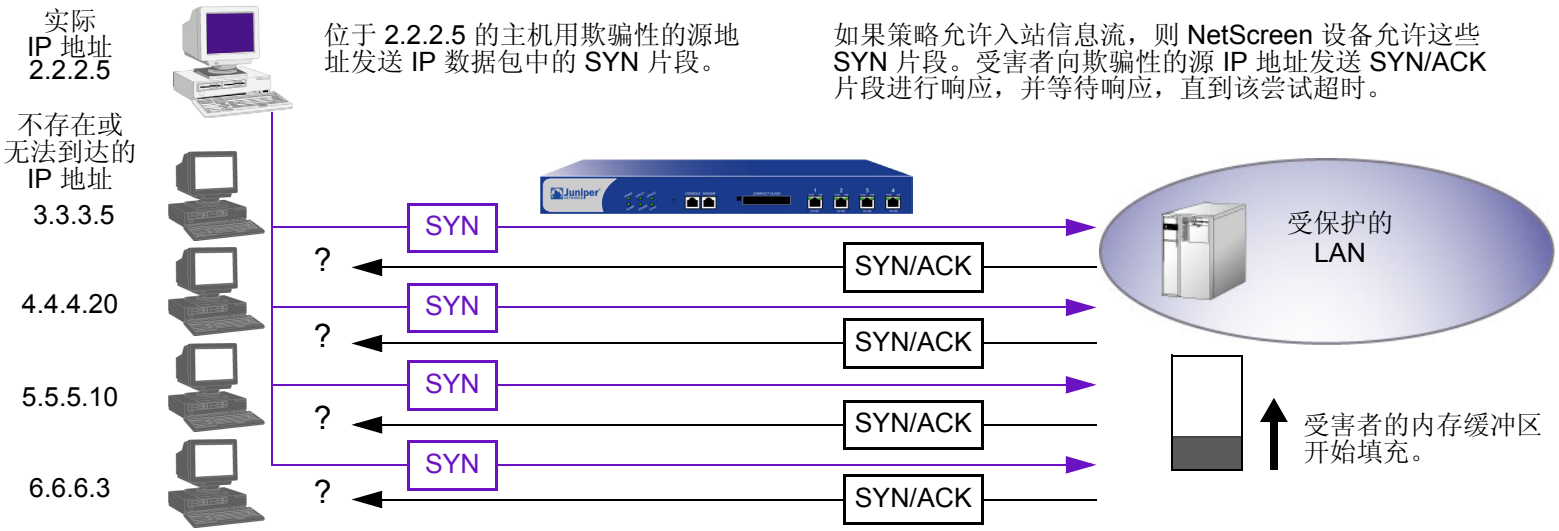
网络 DoS 攻击

针对网络资源的拒绝服务 (DoS) 攻击用压倒性数目的 SYN、 ICMP 或 UDP 数据包泛滥攻击目标，或者用压倒性数目的 SYN 碎片泛滥攻击目标。根据攻击者的意图以及前期情报收集工作的广度和成功，攻击者可能会选出特定的主机 (如路由器或服务器)，或可能会瞄准跨越目标网络的任意主机。这两个方案都有可能扰乱单一主机或整个网络的服务，具体取决于受害者对网络其余部分的影响程度。

SYN 泛滥

当主机中充满了会发出无法完成的连接请求的 SYN 片段，以至于主机无法再处理合法的连接请求时，就发生了 SYN 泛滥。

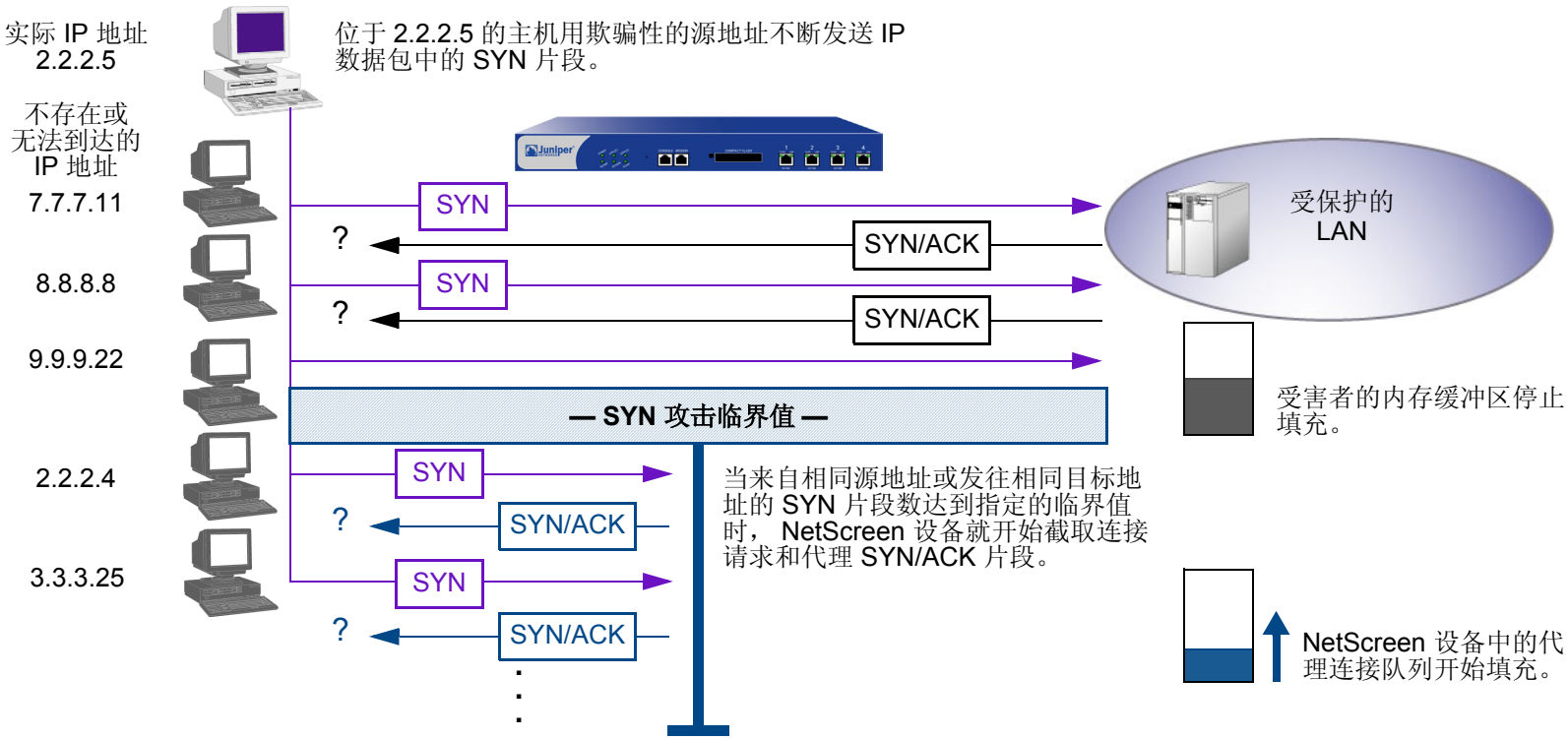
利用三次握手，两个主机之间建立 TCP 连接 : A 向 B 发送 SYN 片段； B 用 SYN/ACK 片段进行响应；然后 A 又用 ACK 片段进行响应。 SYN 泛滥攻击用含有伪造的 (“欺骗”) IP 源地址 (不存在或不可到达的地址) 的 SYN 片段塞满某一站点。 B 用 SYN/ACK 片段响应这些地址，然后等待响应的 ACK 片段。因为 SYN/ACK 片段被发送到不存在或不可到达的 IP 地址，所以它们不会得到响应并最终超时。



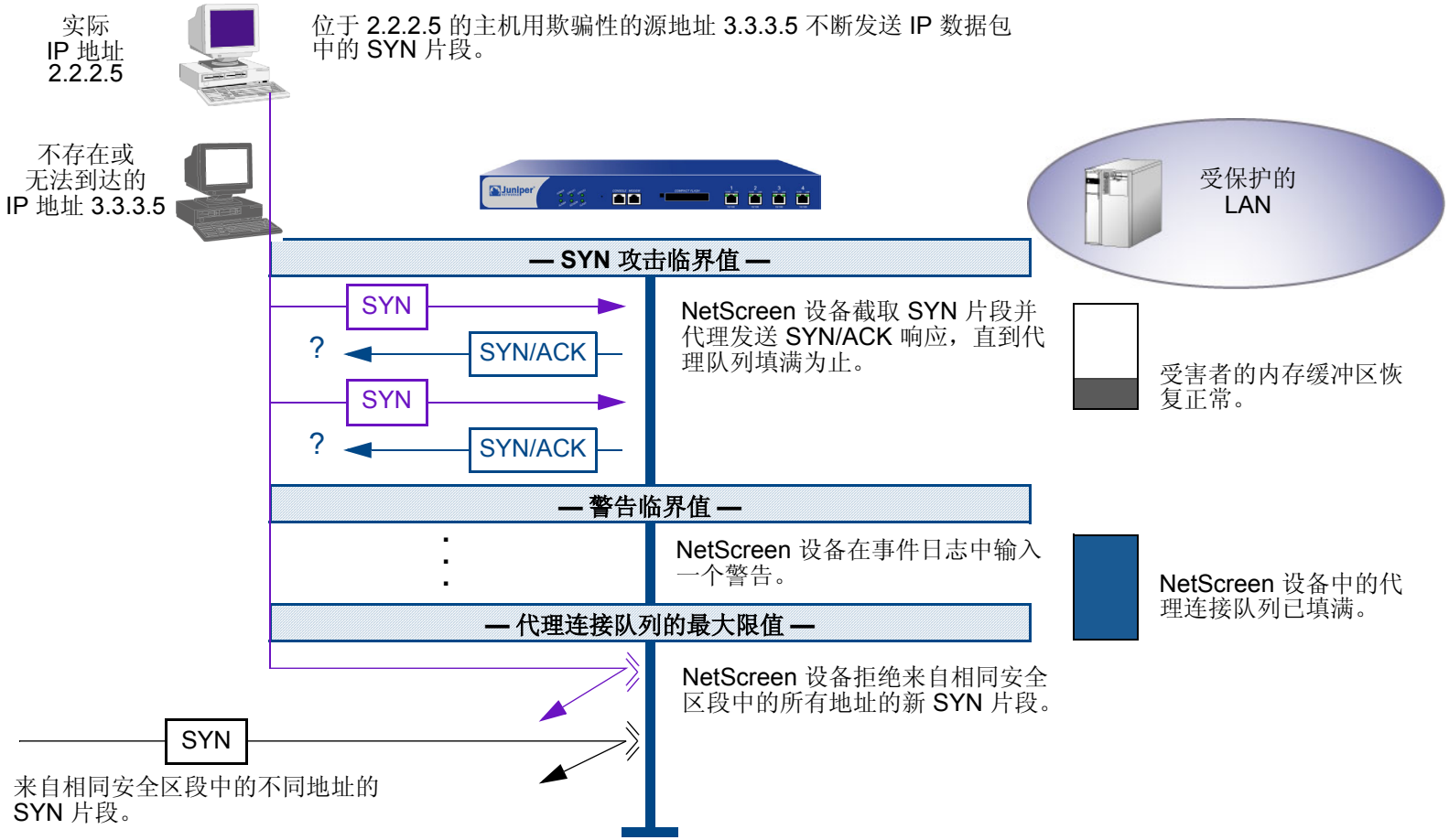
通过用无法完成的 TCP 连接泛滥攻击主机，攻击者最后填满受害者的内存缓冲区。当该缓冲区填满后，主机不能再处理新的 TCP 连接请求。这种泛滥甚至可能会破坏受害者的操作系统。总之，攻击使受害主机失去作用，无法进行正常的操作。

SYN 泛滥防护

NetScreen 设备可以对每秒钟允许通过防火墙的 SYN 片段数加以限制。您可以基于目标地址和端口、仅目标地址或仅源地址来设置攻击临界值。当每秒的 SYN 片段数超过这些临界值之一时， NetScreen 设备开始代理流入的 SYN 片段、用 SYN/ACK 片段回复、并将未完成的连接请求存储到连接队列中。未完成的连接请求将一直保留在队列中，直到连接完成或请求超时。在下面的示意图中，已超过了 SYN 攻击临界值， NetScreen 设备已经开始代理 SYN 片段。



在下一个示意图中，通过代理连接的队列已完全填满， NetScreen 设备正在拒绝新流入的 SYN 片段。此操作保护受保护网络中的主机，使其免遭不完整三方握手的轰击。



当代理队列下降到最大限值以下时， NetScreen 设备将重新开始接收新 SYN 数据包。

注意：*代理超过设定临界值的不完整 SYN 连接的过程只适用于现有策略允许的信息流。没有相关策略的信息流将被自动丢弃。*

要启用 SYN 泛滥防护 SCREEN 选项和定义其参数，请执行下列操作，其中指定的区段是泛滥攻击可能始发的区段：

WebUI

Screening > Screen (Zone: 选择区段名称): 输入以下内容，然后单击 **Apply**:

SYN Flood Protection: (选中以启用)

Threshold: (输入激活 SYN 代理机制所需的每秒 SYN 数据包数 — 即设置了 SYN 标志的 TCP 片段[3])

Alarm Threshold: (输入在事件日志中写入警告信息所需的代理 TCP 连接请求数)

Source Threshold: (输入每秒来自单个 IP 地址的 SYN 数据包数，该数目是 NetScreen 设备开始拒绝来自该来源的新连接请求所需的数目)

Destination Threshold: (输入每秒发向单个 IP 地址的 SYN 数据包数，该数目是 NetScreen 设备开始拒绝发向该目标的新连接请求所需的数目)

Timeout Value: (输入以秒为单位的时间长度，即 NetScreen 设备在代理连接队列中保留未完成的 TCP 连接尝试的时间)

Queue Size: (输入在 NetScreen 设备开始拒绝新的连接请求前，在代理连接队列中存放的代理 TCP 连接请求的数目)

3. 有关每个参数的详细信息，请参阅下列 CLI 部分中的说明。

CLI

启用 SYN 泛滥防护：

```
set zone zone screen syn-flood
```

您可以设置下列参数来代理未完成的 TCP 连接请求：

Attack Threshold: 激活 SYN 代理机制所需的每秒钟发向相同目标地址和端口号的 SYN 片段数 (即设置了 SYN 标志的 TCP 片段数)。虽然可以将该临界值设置为任意值，但您需要了解站点通常的流量模式，以便为其设置适当的临界值。例如，如果是一个通常每秒会收到 20,000 个 SYN 片段的电子商务站点，可将该临界值设为 30,000/ 秒。如果是一个通常每秒会收到 20 个 SYN 片段的小站点，则可将该临界值设为 40。

```
set zone zone screen syn-flood attack-threshold number
```

Alarm Threshold: 每秒钟代理的不完整 TCP 连接请求数，在达到该数目后 NetScreen 设备将在事件日志中加入一条警告。当每秒钟发向相同目标地址和端口号的不完整代理连接请求数超过为警告临界值设置的值时，就会触发警告。例如，如果 SYN 攻击临界值设为每秒 2000 个 SYN 片段且警告临界值为 1000，则每秒钟发往相同目标地址和端口号的 SYN 片段总数必须达到 3001 才会触发在日志中加入一个警告条目。更确切地来说：

1. 每秒钟内满足策略要求的前 2000 个 SYN 片段可通过防火墙。
2. 在同一秒内，防火墙代理随后的 1000 个 SYN 片段。
3. 第 1001 个代理连接请求 (即该秒内的第 3001 个连接请求) 会触发警报。

```
set zone zone screen syn-flood alarm-threshold number
```

对于超过警告临界值发向相同目标地址和端口号的每个 SYN 片段，攻击检测模块将产生一条消息。在该秒结束后，记录模块将所有类似的消息压缩到单个日志条目中，指出在超过警告临界值之后有多少 SYN 片段发向同一个目标地址和端口号。如果攻击持续超过一秒钟，则事件日志每秒写入一条警告条目，直到攻击停止。

Source Threshold: 此选项可用于指定在 NetScreen 设备开始丢弃来自该来源的连接请求之前，每秒从单个源 IP 地址接收的 SYN 片段数 (不管目标 IP 地址和端口号是什么)。

```
set zone zone screen syn-flood source-threshold number
```

按照源地址跟踪 SYN 泛滥时使用的检测参数，与按照目标地址和目标端口号跟踪 SYN 泛滥时使用的检测参数不相同。当设置 SYN 攻击临界值和源临界值时，也就让基本的 SYN 泛滥防护机制和基于源的 SYN 泛滥跟踪机制都生效。

Destination Threshold: 此选项用于指定在 NetScreen 设备丢弃到该目标的连接请求之前，每秒从单个目的 IP 地址接收的 SYN 片段数。如果受保护的主机运行多种服务，则可能要仅仅根据目标 IP 地址来设置临界限值 — 不管目标端口号是什么。

```
set zone zone screen syn-flood destination-threshold number
```

当设置 SYN 攻击临界值和目标临界值时，也就让基本的 SYN 泛滥防护机制和基于目标的 SYN 泛滥跟踪机制都生效。

按照目标地址跟踪 SYN 泛滥时使用的检测参数，与按照目标地址和目标端口号跟踪 SYN 泛滥时使用的检测参数不相同。请考虑下列案例，其中 NetScreen 设备使用了一些策略来允许向同一台服务器发送 FTP 请求 (端口 21) 和 HTTP 请求 (端口 80)。如果 SYN 泛滥攻击临界值是每秒 1000 个数据包 (pps)，且攻击者每秒发送 999 个 FTP 数据包和 999 个 HTTP 数据包，则任一组 (拥有相同目标地址和端口号的数据包定义为一组) 数据包都不会激活 SYN 代理机制。基本 SYN 泛滥攻击机制会跟踪目标地址和端口号，且每组数据包都未超过 1000 pps 的攻击临界值。但是，如果目标临界值是 1000 pps，则 NetScreen 设备将拥有相同目标地址和端口号的 FTP 和 HTTP 数据包看作是单个组的成员，并拒绝发往该目标的第 1001 个数据包 (FTP 或 HTTP)。

Timeout: 丢弃队列中完成一半的连接之前的最长时间。缺省值为 20 秒，您可以将该超时值设置为介于 0 到 50 秒之间的值。您可以试着缩短超时值，直到发现在正常的流量条件下开始有连接被丢弃。二十秒对于三方握手 ACK 响应而言，是一个十分保守的超时值。

```
set zone zone screen syn-flood timeout number
```

Queue size: NetScreen 设备开始拒绝新的连接请求前，代理连接队列中保留的代理连接请求的数量。队列长度值越大， NetScreen 设备就需要更长的时间来扫描该队列，以找到与代理连接请求匹配的有效 ACK 响应。这会略微减慢初始连接的建立；但是，由于开始数据传输的时间往往远远大于建立初始连接时较小的延迟时间，所以用户不会注意到有任何明显的不同。

```
set zone zone screen syn-flood queue-size number
```

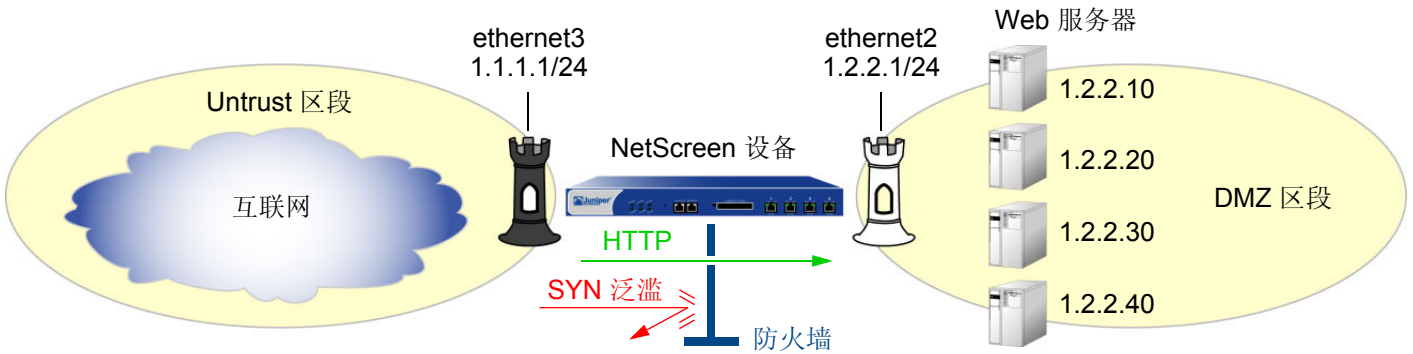
Drop Unknown MAC: 当 NetScreen 设备检测到 SYN 攻击时，它会代理所有的 TCP 连接请求。但是，如果目的 MAC 地址不在其 MAC 学习表中，则处于 “透明” 模式的 NetScreen 设备不能代理 TCP 连接请求。在缺省情况下，检测到 SYN 攻击且处于 “透明” 模式的 NetScreen 设备将允许含有未知 MAC 地址的 SYN 数据包通过。您可以使用此选项指示设备丢弃含有未知目的 MAC 地址的 SYN 数据包，而不是让其通过。

```
set zone zone screen syn-flood drop-unknown-mac
```

范例 : SYN 泛滥防护

在本例中，通过对 Untrust 区段启用 SYN 泛滥防护 SCREEN 选项，保护 DMZ 区段中的 Web 服务器免受始发自该 Untrust 区段中的 SYN 泛滥攻击。

注意 : *Juniper Networks 建议增强 SYN 泛滥防护，使得 NetScreen 设备对每个 Web 服务器都提供设备级的 SYN 泛滥防护。在本例中， Web 服务器正在运行 UNIX，同时还提供一些 SYN 泛滥防御功能，例如调整连接请求队列的长度以及更改未完成的连接请求的超时时间。*



为了为网络的 SYN 泛滥防护参数配置适当的值，首先必须建立典型信息流量的基准。您可以利用一周时间在 ethernet3 (此接口绑定到 Untrust 区段) 上运行一个嗅探器[4] — 以便为 DMZ 中的四个 Web 服务器监控每秒到达的新 TCP 连接请求数[5]。通过对一周监控累积的数据进行分析，产生下列统计信息 :

- 每台服务器的平均新连接请求数 : 250/ 秒
- 每台服务器的平均新连接请求峰值数 : 500/ 秒

4. 嗅探器是一个网络分析设备，它能捕获所连接的网段上的数据包。大多数嗅探器都允许定义过滤器，以便只采集感兴趣的信息流类型。稍后，可以查看和评估累积的信息。在本例中，希望嗅探器采集所有设置了 SYN 标志的 TCP 数据包，这些数据包到达 ethernet3，并发到 DMZ 中的四个 Web 服务器之一。

5. 您可能要继续定期运行嗅探器，以查看是否有基于本日时间、本周日期、本月时间或本年季节的信息流模式。例如，在圣诞节期间，信息流可能会显著地增加。显著的变化或许是对各种临界值进行调整的正当理由。

根据这些信息，为 Untrust 区段设置下列 SYN 泛滥防护参数：

参数	值	设置每个值的理由
Attack Threshold	每秒 625 个数据包 (pps)	此值比每台服务器每秒的平均新连接请求数峰值高 25%，这对于该网络环境来说是不寻常的。当四个 Web 服务器中任一个的每秒 SYN 数据包数超过此数目时，NetScreen 设备将开始代理到该服务器的新连接请求。(换言之，从一秒钟内发向相同目标地址和端口号的第 626 个 SYN 数据包起，NetScreen 设备将开始代理到该地址和端口号的连接请求。)
Alarm Threshold	250 pps	250 pps 是队列长度 (1000 个未完成的代理连接请求*) 的 1/4。当在一秒钟内代理 了 251 个新连接请求时， NetScreen 设备将在事件日志中写入一个警告条目。通过设置稍高于攻击临界值的警告临界值，可以避免为仅略超过攻击临界值的信息流峰值写入警告条目。
Source Threshold	25 pps	当设置了源临界值时，不管目标地址和端口号是什么， NetScreen 设备都将跟踪 SYN 数据包的源 IP 地址。(注意，这种基于源的跟踪已从基于目标地址和目标端口号的 SYN 数据包的跟踪中分离，后者构成了基本 SYN 泛滥防护机制。) 在一周的监控活动中，您观察到，在一秒钟时间间隔内，来自任一个来源的新连接请求数都不超过对所有服务器的新连接请求数的 1/25。因此，超过此临界值的连接请求是不寻常的，并为 NetScreen 设备执行其代理机制提供了足够的理由。(25 pps 是攻击临界值 625 pps 的 1/25。) 如果 NetScreen 设备发现有 25 个 SYN 数据包来自相同的源 IP 地址，它将从第 26 个数据包开始，拒绝来自该秒以及下一秒的更多 SYN 数据包。
Destination Threshold	0 pps	当设置了目标临界值时， NetScreen 设备仅执行对目标 IP 地址的跟踪，而不考虑目标端口号。由于四个 Web 服务器只接收 HTTP 信息流 (目标端口 80) — 没有流往其它目标端口号的信息流到达它们 — 因此，设置一个独立的目标临界值并不能提供附加的优势。

参数	值	设置每个值的理由
Timeout	20 秒	由于队列长度相对较短 (1000 个代理的连接请求)，因此，在此配置的队列中存放未完成的连接请求时， 20 秒的缺省值是一个合理的时间长度。
Queue Size	1000 个半完成的代理连接	1000 个半完成的代理连接是新连接请求数平均峰值 (500 pps) 的两倍。在丢弃新请求之前，NetScreen 最多每秒代理 1000 个请求。通过代理两倍于新连接请求数平均峰值的连接请求，可以提供保守的缓冲区让合法的连接请求通过。

* 半完成连接请求是未完成的三方握手。三方握手是 TCP 连接的初始阶段。它包括三个部分 : 一个设置了 SYN 标志的 TCP 片段、一个设置了 SYN 和 ACK 标志的响应、以及一个对设置了 ACK 标志的响应。有关完整说明，请参阅第 1 卷 “概述”中的 “词汇表”。

WebUI

1. 接口

Network > Interfaces > Edit (对于 ethernet2): 输入以下内容，然后单击 **OK**:

Zone Name: DMZ

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.2.2.1/24

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容，然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. 地址

Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

Address Name: ws1

IP Address/Domain Name:

IP/Netmask: (选择), 1.2.2.10/32

Zone: DMZ

Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

Address Name: ws2

IP Address/Domain Name:

IP/Netmask: (选择), 1.2.2.20/32

Zone: DMZ

Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

Address Name: ws3

IP Address/Domain Name:

IP/Netmask: (选择), 1.2.2.30/32

Zone: DMZ

Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

Address Name: ws4

IP Address/Domain Name:

IP/Netmask: (选择), 1.2.2.40/32

Zone: DMZ

Objects > Addresses > Groups > (对于 Zone: DMZ) New: 输入以下组名称，移动以下地址，然后单击 **OK**:

Group Name: web_servers

选择 **ws1**，并使用 **<<** 按钮将地址从 Available Members 栏移动到 Group Members 栏中。

选择 **ws2**，并使用 **<<** 按钮将地址从 Available Members 栏移动到 Group Members 栏中。

选择 **ws3**，并使用 **<<** 按钮将地址从 Available Members 栏移动到 Group Members 栏中。

选择 **ws4**，并使用 **<<** 按钮将地址从 Available Members 栏移动到 Group Members 栏中。

3. 策略

Policies > (From: Untrust, To: DMZ) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), web_servers

Service: HTTP

Action: Permit

4. SCREEN

Screening > Screen (Zone: Untrust): 输入以下内容，然后单击 **Apply**:

SYN Flood Protection: (选择)

Threshold: 625

Alarm Threshold: 250

Source Threshold: 25

Destination Threshold: 0

Timeout Value: 20[6]

Queue Size: 1000

6. 由于 20 秒是缺省设置，您不必设置 20 秒的超时时间，除非此前已将其设置为其它值。

CLI

1. 接口

```
set interface ethernet2 zone dmz
set interface ethernet2 ip 1.2.2.1/24

set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. 地址

```
set address dmz ws1 1.2.2.10/32
set address dmz ws2 1.2.2.20/32
set address dmz ws3 1.2.2.30/32
set address dmz ws4 1.2.2.40/32

set group address dmz web_servers add ws1
set group address dmz web_servers add ws2
set group address dmz web_servers add ws3
set group address dmz web_servers add ws4
```

3. 策略

```
set policy from untrust to dmz any web_servers HTTP permit
```

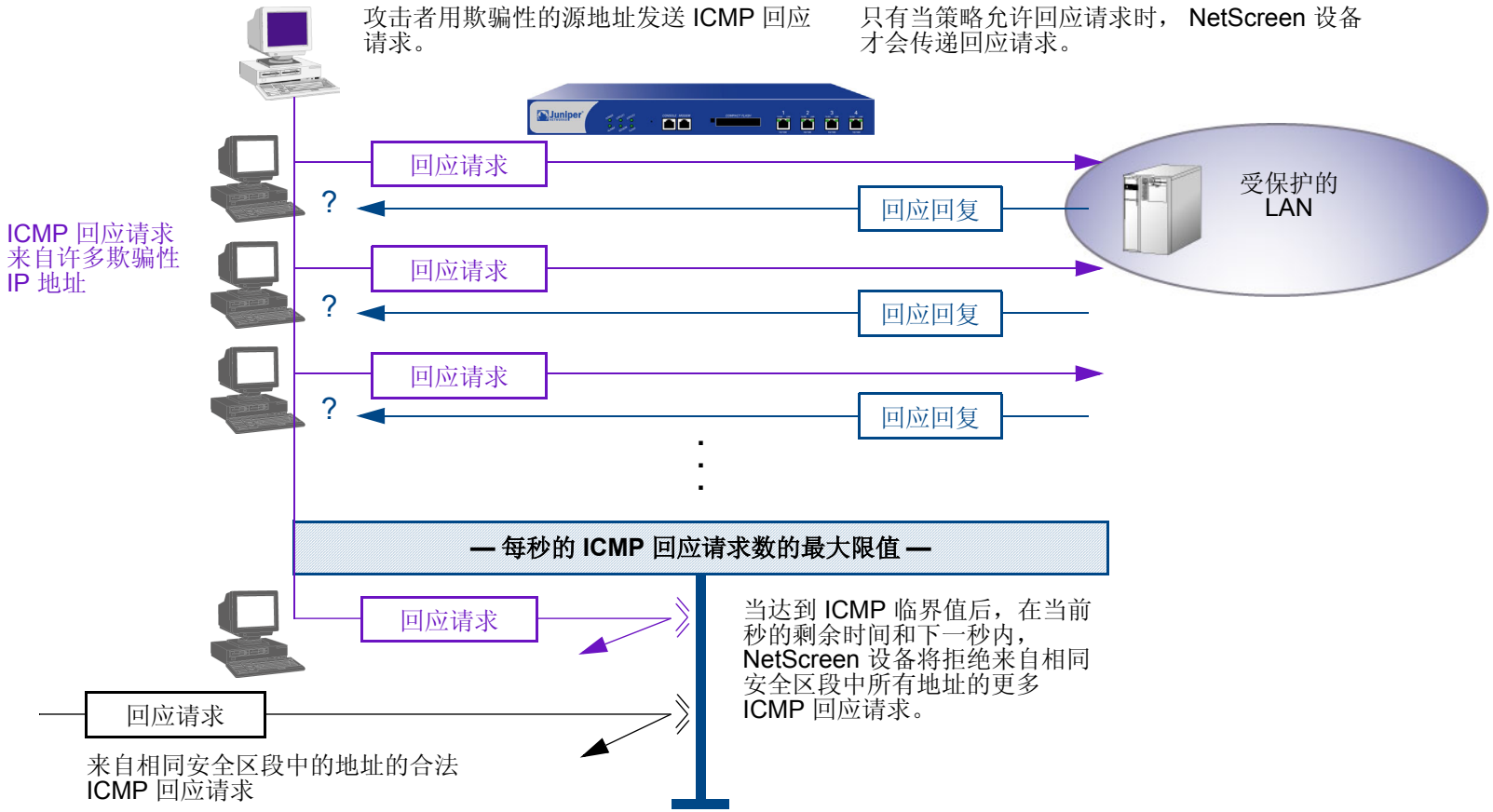
4. SCREEN

```
set zone untrust screen syn-flood attack-threshold 625
set zone untrust screen syn-flood alarm-threshold 250
set zone untrust screen syn-flood source-threshold 25
set zone untrust screen syn-flood timeout 20[7]
set zone untrust screen syn-flood queue-size 1000
set zone untrust screen syn-flood
save
```

7. 由于 20 秒是缺省设置，您不必设置 20 秒的超时时间，除非此前已将其设置为其它值。

ICMP 泛滥

当 ICMP 回应请求[8] 用很多请求使得受害者超负荷运行，以至于受害者耗尽所有资源来进行响应，直至再也无法处理有效的网络信息流时，通常就发生了 ICMP 泛滥。当启用了 ICMP 泛滥防护功能时，可以设置一个临界值，一旦超过此值就会调用 ICMP 泛滥攻击防护功能。(缺省的临界值为每秒 1000 个数据包。) 如果超过了该临界值，NetScreen 设备在该秒余下的时间和下一秒内会忽略其它的 ICMP 回应请求。



8. 注意 ICMP 泛滥可以包括任何类型的 ICMP 消息。因此， NetScreen 设备会监控所有 ICMP 消息类型，而不只是回应请求。

要启用 ICMP 泛滥防护，请执行下列操作之一，其中指定的区段是泛滥攻击可能始发的区段 :

WebUI

Screening > Screen (Zone: 选择区段名称): 输入以下内容，然后单击 **Apply**:

ICMP Flood Protection: (选择)

Threshold: (输入触发 ICMP 泛滥防护的值[9])

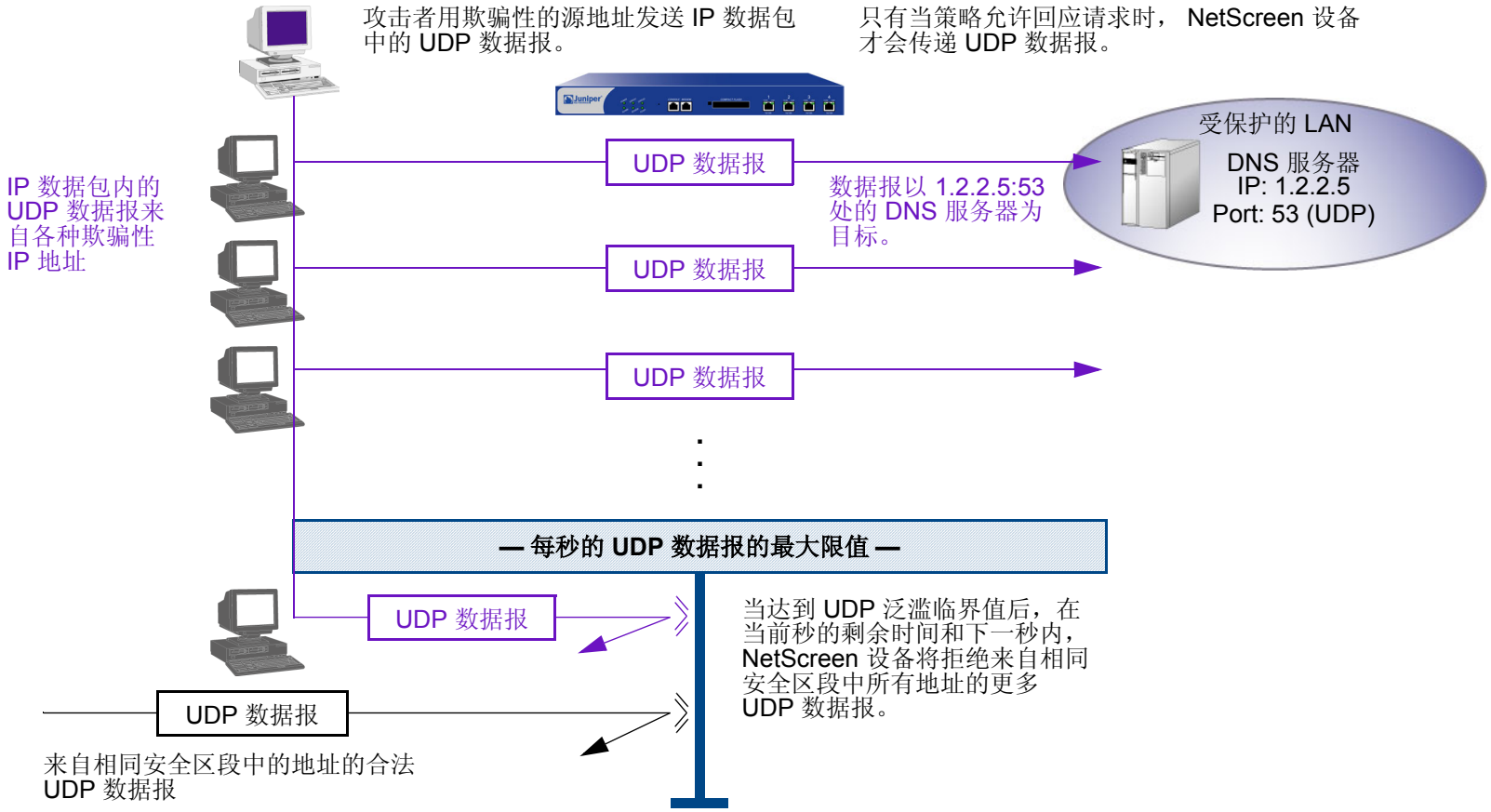
CLI

```
set zone zone screen icmp-flood threshold number
set zone zone screen icmp-flood
```

9. 该值的单位是每秒的 ICMP 数据包数。缺省值为每秒 1000 个数据包。

UDP 泛滥

与 ICMP 泛滥相似，当攻击者以减慢受害者的处理速度为目的而发送含有 UDP 数据报的 IP 数据包，以至于受害者再也无法处理有效的连接时，就发生了 UDP 泛滥。当启用了 UDP 泛滥防护功能时，可以设置一个临界值，一旦超过此临界值就会调用 UDP 泛滥攻击防护功能。(缺省的临界值为每秒 1000 个数据包。) 如果从一个或多个源向单个目标发送的 UDP 数据报数超过了此临界值，NetScreen 设备在该秒余下的时间和下一秒内会忽略其它发往该目标的 UDP 数据报。



要启用 UDP 泛滥防护，请执行下列操作之一，其中指定的区段是泛滥攻击可能始发的区段 :

WebUI

Screening > Screen (Zone: 选择区段名称): 输入以下内容，然后单击 **Apply**:

UDP Flood Protection: (选择)

Threshold: (输入触发 UDP 泛滥防护的值[10])

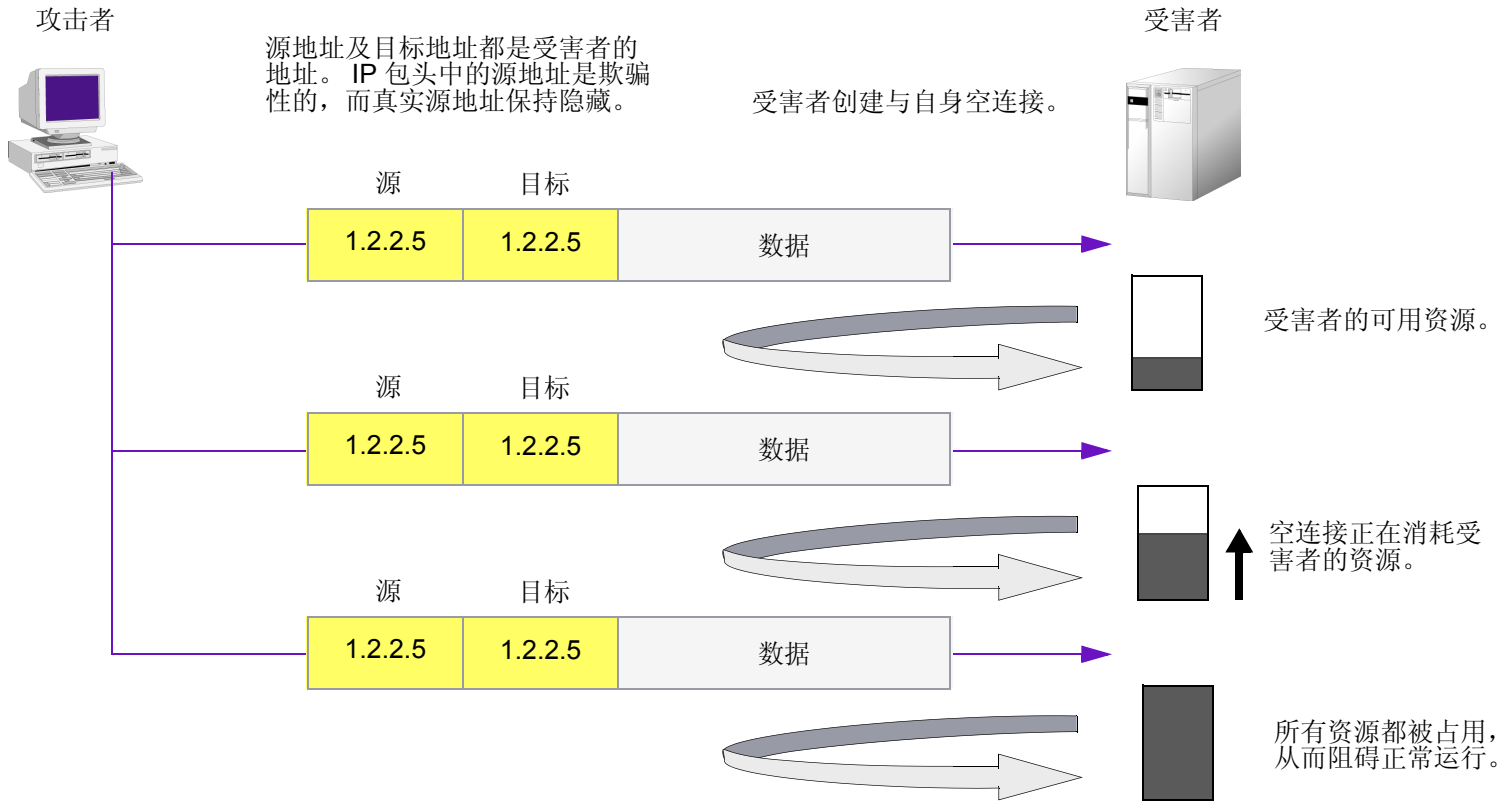
CLI

```
set zone zone screen udp-flood threshold number
set zone zone screen udp-flood
```

10. 该值的单位是每秒的 UDP 数据包数。缺省值为每秒 1000 个数据包。

Land 攻击

Land 攻击结合使用了 SYN 攻击和 IP 欺骗，当攻击者发送含有受害者 IP 地址的欺骗性 SYN 数据包，并将该地址作为目的和源 IP 地址时，就发生了 Land 攻击。接收系统通过向自己发送 SYN-ACK 数据包来进行响应，同时创建一个空的连接，该连接将会一直保持到达到空闲超时值为止。向系统堆积过多的这种空连接会耗尽系统资源，导致 DoS。



当启用 SCREEN 选项以封锁 Land 攻击时， NetScreen 设备将 SYN 泛滥防御和 IP 欺骗防护的元素有机结合在一起，以检测和封锁这种性质的攻击。

要启用对 Land 攻击的防护，请执行下列操作，其中指定的区段是攻击始发的位置 :

WebUI

Screening > Screen (Zone: 选择区段名称): 选择 **Land Attack Protection**，然后单击 **Apply**。

CLI

```
set zone zone screen land
```

与操作系统相关的 DoS 攻击

如果攻击者不仅识别出活动主机的 IP 地址和响应端口号，而且识别出其操作系统 (OS)，则攻击者可能会不借助于暴力攻击，而是发起会产生一两个数据包 “破坏” 的更高级的攻击。本部分介绍的攻击可以用最小的努力使系统瘫痪。如果 NetScreen 设备正在保护易受这些攻击的主机，您可以启用 NetScreen 设备来检测这些攻击，并且在其到达目标之前将其封锁。

Ping of Death

允许的最大 IP 数据包长度是 65,535 字节，其中包括长度通常为 20 字节的数据包包头[11]。 ICMP 回应请求是一个含长度为 8 字节长的伪包头的 IP 数据包[12]。因此，ICMP 回应请求的数据区的最大长度是 65,507 字节 (65,535 - 20 - 8 = 65,507)。

许多 ping 实现方案允许用户指定大于 65,507 字节的数据包大小。过大的 ICMP 数据包会引发一系列不利的系统反应，如拒绝服务 (DoS)、系统崩溃、死机以及重新启动。

当启用 Ping of Death SCREEN 选项时，即便是攻击者通过故意分段来隐藏总数据包大小，NetScreen 设备也将会检测并拒绝这些过大的且不规则的数据包大小。

***注意：**有关 Ping of Death 的信息，请访问 http://www.insecure.org/sploits/ping-o-death.html。*

此数据包的大小是 65,538 字节。它超过了 RFC 791, “Internet Protocol” 中规定的大小限值 (65,535 字节)。在传输该数据包时，它将被分解为很多碎片。重组过程可能导致接收系统崩溃。

11. 有关 IP 规范的信息，请参阅 RFC 791, “Internet Protocol”。
12. 有关 ICMP 规范的详细信息，请参阅 RFC 792, “Internet Control Message Protocol”。

要启用 Ping of Death 攻击的防护，请执行下列操作，其中指定的区段是攻击始发的位置 :

WebUI

Screening > Screen (Zone: 选择区段名称): 选择 **Ping of Death Attack Protection**，然后单击 **Apply**。

CLI

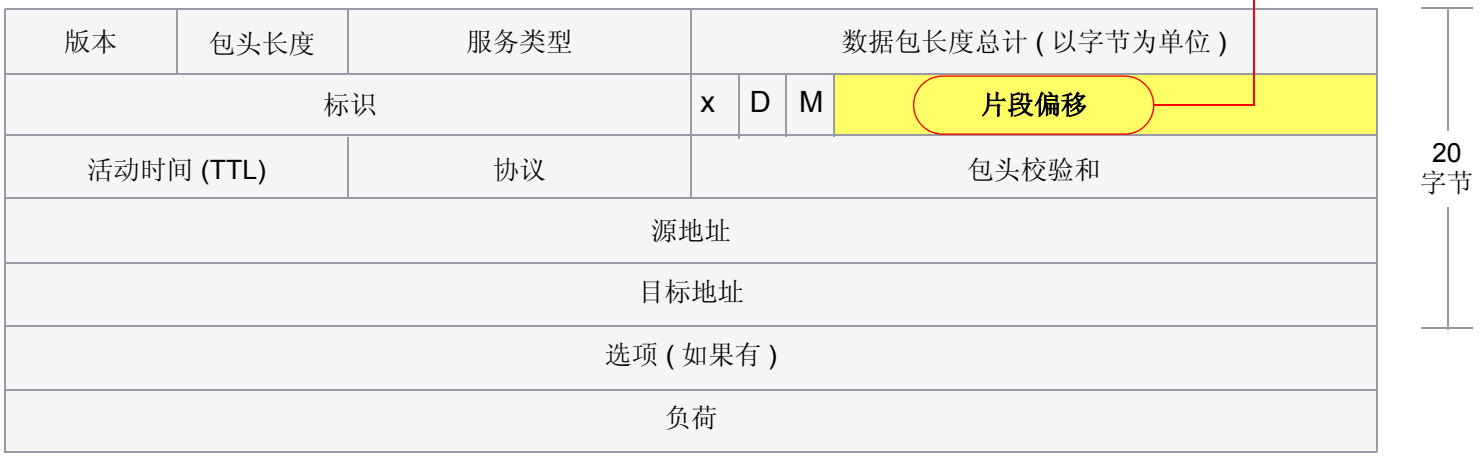
```
set zone zone screen ping-death
```

Teardrop 攻击

Teardrop 攻击利用了 IP 数据包碎片的重组。在 IP 包头中，有一个碎片偏移字段，它表示数据包碎片包含的数据相对于原始未分段数据包数据的开始位置 (或 “偏量”)。

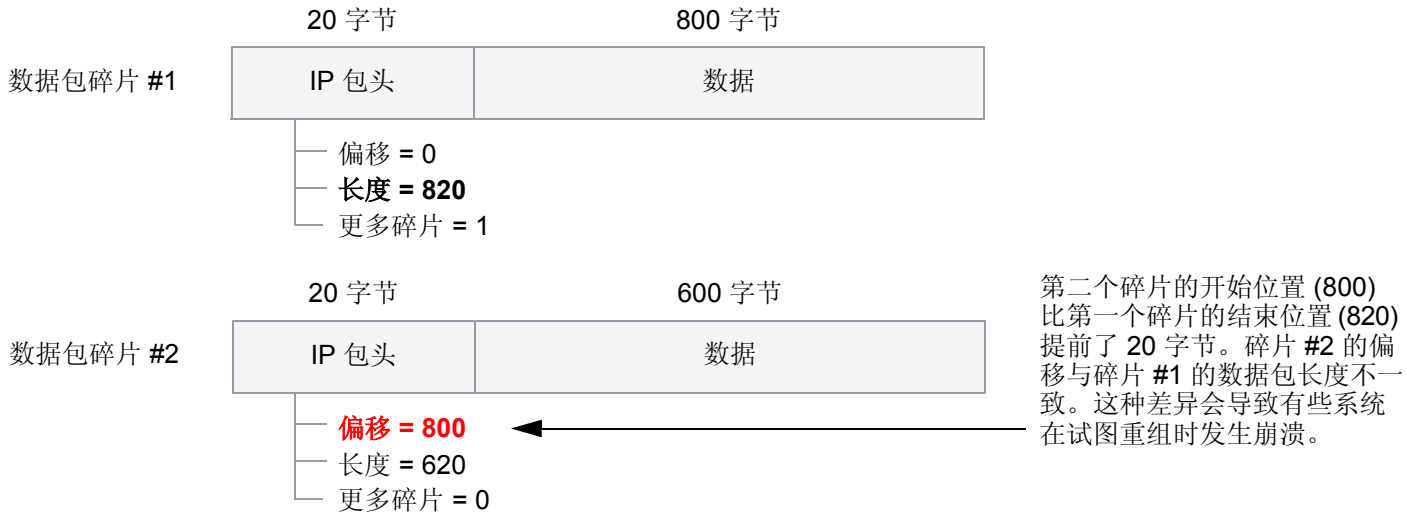
IP 包头

NetScreen 设备检查片段偏移字段中的差异。



当一个数据包碎片的偏移值与其大小之和小于下一数据包碎片的偏移值时，数据包发生重叠，并且服务器在尝试重新组合数据包时会引起系统崩溃，特别是如果服务器正在运行含有这种漏洞的旧版操作系统时更是如此。

碎片差异



在启用 Teardrop Attack SCREEN 选项后，只要 NetScreen 检测到数据包碎片中的这种差异，就会丢弃该碎片。要启用对 Teardrop 攻击的防护，请执行下列操作，其中指定的区段是攻击始发的位置：

WebUI

Screening > Screen (Zone: 选择区段名称): 选择 **Teardrop Attack Protection**，然后单击 **Apply**。

CLI

```
set zone zone screen tear-drop
```

WinNuke

WinNuke 是针对互联网上运行 Windows 的任何计算机的 DoS 攻击。攻击者将 TCP 片段 [通常发送给 NetBIOS 端口 139 并设置了紧急 (URG) 标志] 发送给具有已建连接的主机。这样就产生 NetBIOS 碎片重叠，从而导致运行 Windows 的机器崩溃。重新启动遭受攻击的机器后，会显示下列信息，指示已经发生了攻击：

> An exception OE has occurred at 0028:[address] in VxD MSTCP(01) + 000041AE. This was called from 0028:[address] in VxD NDIS(01) + 00008660. It may be possible to continue normally.
>
> Press any key to attempt to continue.
>
> Press CTRL+ALT+DEL to restart your computer. You will lose any unsaved information in all applications.
>
> Press any key to continue.

WinNuke 攻击指示器

如果启用了 WinNuke attack defense SCREEN 选项，则 NetScreen 设备会扫描所有流入的 Microsoft NetBIOS 会话服务 (端口 139) 数据包。如果观察到其中一个数据包中设置了 URG 标志，则 NetScreen 设备将取消设置该 URG 标志，清除 URG 指针，转发修改后的指针，然后在事件日志中写入一个条目，说明其已封锁了一个尝试的 WinNuke 攻击。

要启用对 WinNuke 攻击的防护，请执行下列操作，其中指定的区段是攻击始发的位置 :

WebUI

Screening > Screen (Zone: 选择区段名称): 选择 **WinNuke Attack Protection**，然后单击 **Apply**。

CLI

```
set zone zone screen winnuke
```

4

内容监控和过滤

Juniper Networks 通过 ScreenOS 功能以及将 ScreenOS 与 Websense、 SurfControl 和 Trend Micro 产品配合使用来提供对网络活动的广泛保护和控制。

Juniper Networks 在 ScreenOS 内部提供了一些内容监控和过滤功能，这些功能在 “malicious URL protection SCREEN” 选项中。而且，通过碎片重组功能， NetScreen 设备甚至可检测位于破碎的 TCP 片段和 IP 数据包碎片中的 URL。

对于防病毒 (AV) 保护来说，在有些 NetScreen 设备上，您可以选择获得高级许可密钥和防病毒订阅密钥，并使用内部防病毒扫描功能。对于 URL 过滤，可以对 NetScreen 设备进行配置，使其与一个内部 URL 过滤引擎或与一个或多个外部 URL 过滤服务器一起工作。

本章将介绍如何配置 NetScreen 设备，以执行片段和数据包重组，监控恶意 URL 的 HTTP 信息流，以及与其它设备通信来执行防病毒扫描和 URL 过滤。本章内容分为以下几个部分：

碎片重组

通常情况下，网络转发设备 (如 : 路由器或交换机) 不会重组其所收到的数据包碎片。当所有数据包碎片到达后，目标主机负责重新构建它们。由于转发设备是用于有效地传递信息流的，因此不必对数据包碎片进行排列、重组、然后重新分段以及转发，即使进行这样的处理，效率也不高。但是，将数据包碎片通过防火墙进行传送是不安全的。攻击者可能会故意打碎数据包，以隐藏防火墙将要对其进行检测和封锁的信息流串。

ScreenOS 允许为每个区段启用碎片重组。这样就允许 NetScreen 设备扩展其能力以检测和封锁恶意 URL 串，以及改进其能力以提供应用程序层网关 (ALG) 来检查数据包的数据部分。

恶意 URL 保护

除了本章后面所述的 URL 过滤功能 (请参阅第 121 页上的“重新定向 URL 过滤”) 之外，您还可以为每个区段最多定义 48 个恶意 URL 串模式，其中每个恶意 URL 串的长度可达 64 个字符，以便提供区段级别的恶意 URL 保护。在启用了恶意 URL 封锁功能后， NetScreen 设备将检查所有 HTTP 数据包的数据负荷。如果找到了一个 URL，并发现该 URL 串的开头部分 (其长度达到了指定的字符数目) 与所定义的模式相匹配，则 NetScreen 设备将封锁该数据包，不允许其通过防火墙。

狡猾的攻击者认识到， URL 串是已知的，并可能会被防御，因此他们会故意打碎 IP 数据包或 TCP 片段，从而使得在逐一检查数据包时无法识别该模式。例如，如果恶意 URL 串是 **120.3.4.5/level/50/exec**，则 IP 碎片可能会将该 URL 串分解为以下部分 :

- 第一个数据包 : **120.**
- 第二个数据包 : **3.4.5/level/50**
- 第三个数据包 : **/exec**

即便您已将 URL 串定义为长度为 20 个字符的 **120.3.4.5/level/50/exec**，各个 URL 串碎片也会通过 NetScreen 设备而不被检测出来。虽然第一个数据包中的字符串“120.”与所定义模式的第一部分相匹配，但其长度比所要求的 20 个匹配字符的长度要短。而第二和第三个数据包中的字符串与所定义模式的开头不匹配，因此这些数据包将顺利通过。

但是，如果将这些数据包进行重组，则碎片将组合，形成可识别字符串， NetScreen 设备可对该字符串进行封锁。利用碎片重组功能，NetScreen 设备可以将碎片缓存到队列中，将其重组为完整的数据包，然后检查该数据包中的恶意 URL。根据此重组过程和后续检查的结果， NetScreen 设备将执行下列步骤之一 :

- 如果发现了恶意 URL，则 NetScreen 设备将丢弃该数据包并在日志中输入事件。
- 如果 NetScreen 设备不能完成重组过程，则将强制时限超时，并丢弃碎片。
- 如果 NetScreen 设备确定该 URL 不是恶意的，但重组的数据包太大而无法转发，则 NetScreen 设备会将该数据包分成多个数据包后再进行转发。
- 如果确定该 URL 不是恶意的，而且不需要对其进行分解，则 NetScreen 设备将转发该数据包。

应用程序层网关

NetScreen 为很多协议提供了应用程序层网关 (ALG)，如 DNS、 FTP、 H.323 和 HTTP 协议。在这些协议中，碎片重组可以是实施包括 FTP 和 HTTP 服务的策略中的重要部分。 NetScreen 防火墙为 FTP-Get 和 FTP-Put 等协议筛选数据包的能力，要求其不仅检查数据包包头，而且检查负载中的数据。例如，可能有两个策略，其中的一个拒绝从 Untrust 区段到 DMZ 区段的 FTP-put，而另外一个允许从 Untrust 区段到 DMZ 区段的 FTP-get:

```
set policy from untrust to dmz any any ftp-put deny
set policy from untrust to dmz any any ftp-get permit
```

为了识别这两种类型的信息流， NetScreen 防火墙将检查负载。如果设备读取了 **RETR** *filename*，则 FTP 客户端已发送请求，以便从 FTP 服务器获取 (或 “检索”) 所指定的文件，且 NetScreen 设备允许该数据包通过。如果 NetScreen 设备找到 **STOR** *filename*，则客户端已发送请求，以便将所指定的文件放置 (或 “存储”) 到服务器上，且 NetScreen 设备封锁该数据包。

为了绕过这种防御，攻击者可能会故意将一个 FTP-put 数据包分解为两个数据包，在数据包各自的负载中包含下列文本 : 数据包 1: **ST** ； 数据包 2: **OR** *filename*。当分别检查每个数据包时， NetScreen 设备不会发现字符串 **STOR** *filename*，因此将允许这两个数据包通过。

但是，如果重组这些数据包，则碎片将组合，形成可识别字符串， NetScreen 设备会对其采取相应的措施。利用碎片重组功能， NetScreen 设备可以将碎片缓存到队列中，将其重组为完整的数据包，然后检查该数据包中的完整 FTP 请求。根据此重组过程和后续检查的结果， NetScreen 设备将执行下列步骤之一：

- 如果发现了 FTP-put 请求，则 NetScreen 设备将丢弃该数据包并在日志中输入事件。
- 如果 NetScreen 设备不能完成重组过程，则将强制时限超时，并丢弃碎片。
- 如果 NetScreen 设备发现了 FTP-get 请求，但重组的数据包太大而无法转发，则 NetScreen 设备会将该数据包分成多个数据包后再进行转发。
- 如果发现 FTP-get 请求，而且不需要将其分解，则 NetScreen 设备将转发该数据包。

范例：封锁数据包碎片中的恶意 URL

在本例中，将定义下列三个恶意 URL 字符串，并启用恶意 URL 封锁选项：

- 恶意 URL #1
  - ID: Perl
  - Pattern: scripts/perl.exe
  - Length: 14
- 恶意 URL #2
  - ID: CMF
  - Pattern: cgi-bin/phf
  - Length: 11
- 恶意 URL #3
  - ID: DLL
  - Pattern: 210.1.1.5/msadcs.dll
  - Length: 18

“length”的值表示 URL 中必须存在的模式中的字符数 — 从首个字符开始 (对于正向匹配而言)。注意，对于 #1 和 #3，不是每个字符都是必需的。

然后启用碎片重组，以便对到达 Untrust 区段接口的 HTTP 信息流碎片进行 URL 检测。

WebUI

Screening > Mal-URL (Zone: Untrust): 输入以下内容，然后单击 **OK**:

ID: perl

Pattern: /scripts/perl.exe

Length: 14

Screening > Mal-URL (Zone: Untrust): 输入以下内容，然后单击 **OK**:

ID: cmf

Pattern: cgi-bin/phf

Length: 11

Screening > Mal-URL (Zone: Untrust): 输入以下内容，然后单击 **OK**:

ID: dll

Pattern: 210.1.1.5/msadcs.dll

Length: 18

Network > Zones > Edit (对于 Untrust): 选中 **TCP/IP Reassembly for ALG** 复选框，然后单击 **OK**。

CLI

```
set zone untrust screen mal-url perl “scripts/perl.exe” 14
set zone untrust screen mal-url cmf “cgi-bin/phf” 11
set zone untrust screen mal-url dll “210.1.1.5/msadcs.dll” 18
set zone untrust reassembly-for-alg
save
```

防病毒扫描

病毒是一种可执行代码，可感染或附在其它可执行代码上，以便实现自我复制。有些病毒是恶意的，会删除文件或锁住系统。其它病毒仅仅在感染其它文件时出现问题，因为它们传播时会用大量的伪造数据来耗尽受感染主机或网络的资源。

选择 NetScreen 设备支持内部防病毒 (AV) 扫描引擎 (AV 扫描器)，扫描引擎可为特定应用层事务处理提供防病毒扫描[1]。可以对扫描器进行配置，使其可对使用以下协议的网络信息流进行检查 :

- 文件传输协议 (FTP)
- 超文本传输协议 (HTTP)
- 互联网邮件访问协议 (IMAP)
- 邮局协议，版本 3 (POP3)
- 简单邮件传输协议 (SMTP)

要应用防病毒保护，必须在安全策略中引用内部扫描器。当 NetScreen 设备接收到对其应用要求防病毒扫描的策略的信息流时，会将所接收到的内容引向其内部扫描器。在验证已收到 FTP、 HTTP、 IMAP、 POP3 或 SMTP 数据包的全部内容后，扫描器将检查数据中的病毒。扫描器通过参考病毒模式文件[2] 来识别病毒特征，从而完成病毒扫描。当扫描器检测到病毒后， NetScreen 设备将丢弃该内容，并发送消息给客户端，指出该内容已被感染。如果扫描器没有检测到病毒，则 NetScreen 设备会将该内容转发到其预期目的地。

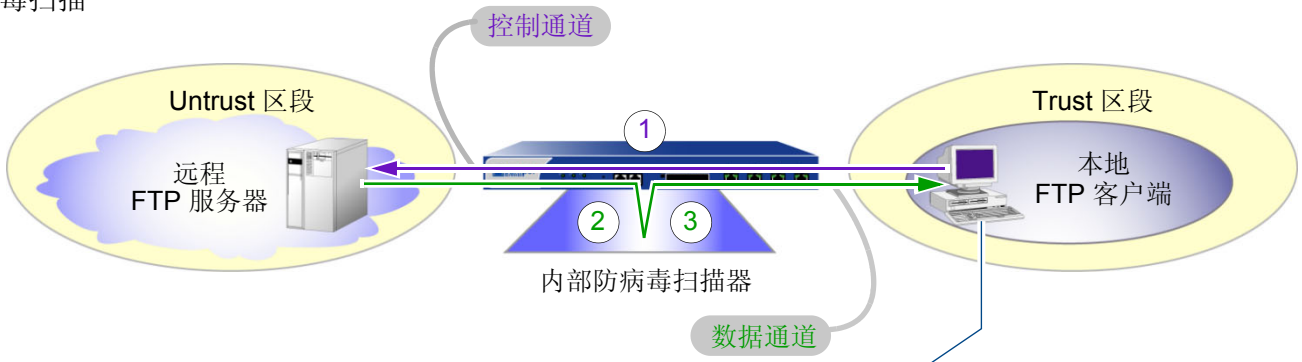
1. 尽管某些 NetScreen 设备在 CLI 和 WebUI 中显示有用于配置外部防病毒扫描的选项，但此版本的 ScreenOS 仅支持内部防病毒扫描。
2. 要查看有关将防病毒模式文件保存到 NetScreen 设备，之后再对其定期更新的信息，请参阅第 91 页上的 “更新防病毒模式文件”。

扫描 FTP 信息流

对于 FTP 信息流， NetScreen 设备监控控制通道，如果检测到用于传输数据的 FTP 命令之一 — RETR、 STOR、 STOU、APPE — 则设备将对通过数据通道发送的数据进行扫描。NetScreen 设备采取的后继动作如何取决于扫描结果以及您对失败模式行为所做的配置：

如果数据	并且 “失败模式”设置为	则 NetScreen 设备将
未被感染	丢弃或通过，	把数据通过数据通道传送到 FTP 客户端。
包含病毒	丢弃或通过，	丢弃来自数据通道的数据并通过控制通道向 FTP 客户端发送一条病毒通知消息。
超出了最大内容级别	丢弃，	丢弃来自数据通道的数据并通过控制通道向 FTP 客户端发送一条 “文件过大”消息。
超出了最大内容级别	通过，	把数据通过数据通道传送到 FTP 客户端。
无法成功扫描	丢弃，	丢弃来自数据通道的数据并通过控制通道向 FTP 客户端发送一条 “扫描错误”消息。
无法成功扫描	通过，	传送数据并通过控制通道向 FTP 客户端发送一条 “扫描错误”消息。

FTP 防病毒扫描



1. 本地 FTP 客户端打开通向 FTP 服务器的 FTP 控制通道并请求传输一些数据。
2. FTP 客户端和服务器就服务器发送被请求数据所通过的数据通道进行协商。NetScreen 设备截取数据并将其传送给其内部防病毒扫描引擎，由该引擎来扫描其中的病毒。
3. 完成扫描后， NetScreen 设备将执行以下两种操作中的其中一种：
   - 如果没有病毒，则将数据转发到客户端。
   - 如果有病毒，则丢弃数据，并通过控制通道向客户端发送一条消息，指出数据已被感染。

如果被扫描的数据超出了最大内容设置或者扫描不能成功完成，则 NetScreen 设备会根据失败模式的设置情况而执行其它相应的操作。有关详细信息，请参阅前表。

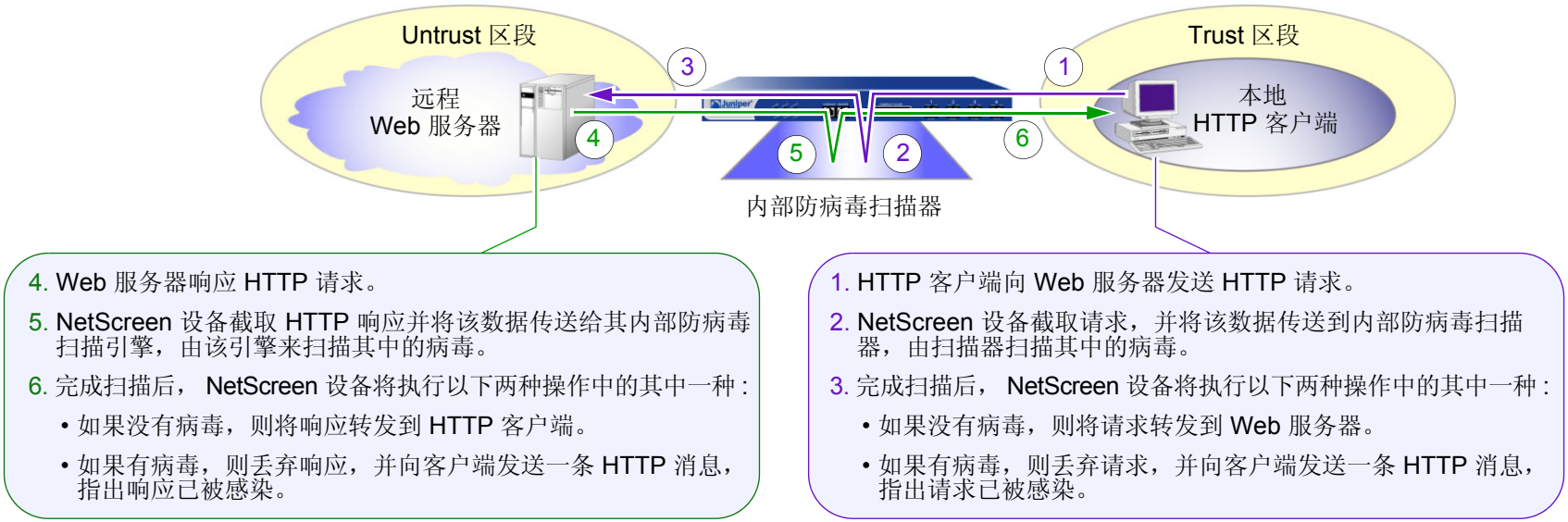
扫描 HTTP 信息流

对于 HTTP 信息流扫描， NetScreen 设备将扫描 HTTP 响应和 HTTP 请求 (get、 post 和 put 命令)。内部防病毒扫描器检查 HTTP 下载内容，也就是 Web 服务器针对来自客户端的 HTTP 请求所发出的响应中的 HTTP 数据。内部防病毒扫描器还将扫描上载内容，例如，当 HTTP 客户端完成 Web 服务器上的问卷调查时，或者当客户端在始发自 Web 服务器的电子邮件中编写消息时。

NetScreen 设备采取的后继动作如何取决于扫描结果以及您对失败模式行为所做的配置：

如果数据	并且 “失败模式”设置为	则 NetScreen 设备将
未被感染	丢弃或通过，	把数据传送到 HTTP 客户端。
包含病毒	丢弃或通过，	丢弃数据并向 HTTP 客户端发送一条病毒通知消息。
超出了最大内容级别	丢弃，	丢弃数据并向 HTTP 客户端发送一条 “文件过大”消息。
超出了最大内容级别	通过，	把数据传送到 HTTP 客户端。
无法成功扫描	丢弃，	丢弃数据并向 HTTP 客户端发送一条 “扫描错误”消息。
无法成功扫描	通过，	传送数据并向 HTTP 客户端发送一条 “扫描错误”消息。

HTTP 防病毒扫描



HTTP MIME 扩展

在缺省情况下， HTTP 扫描不扫描由以下任意多用途互联网邮件扩展 (MIME) 内容类型和子类型 (当跟在一个斜线后出现时) 组成的 HTTP 实体：

- application/x-director
- application/pdf
- image/
- video/
- audio/
- text/css
- text/html

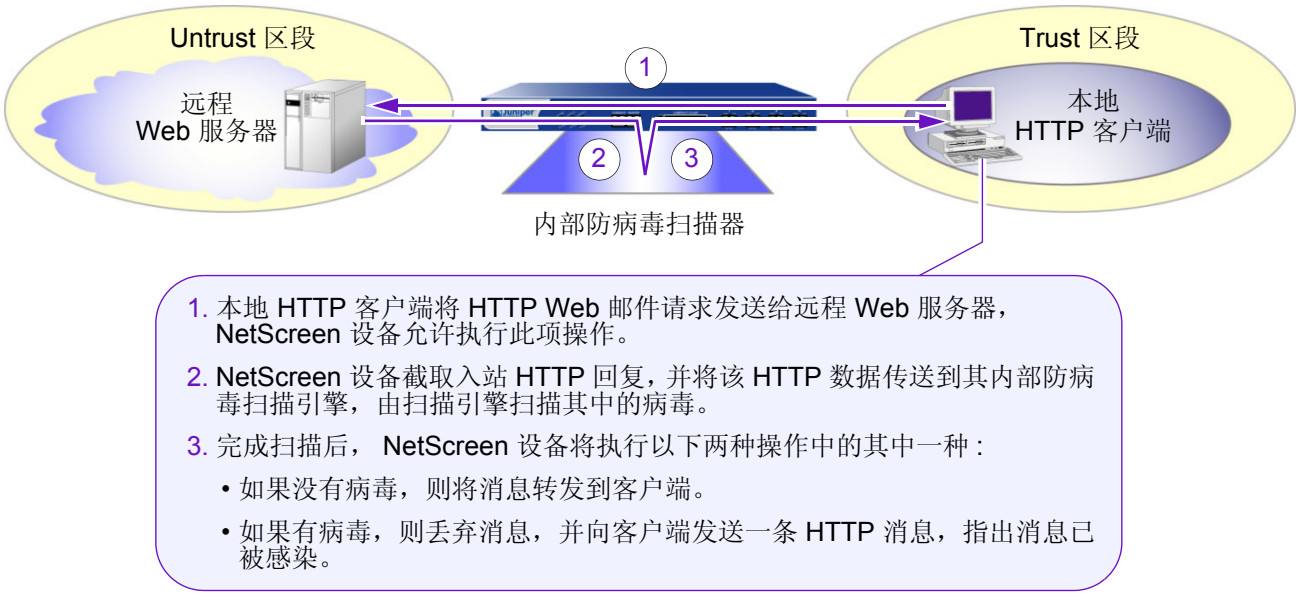
为了改善性能， NetScreen 设备不扫描上述 MIME 内容类型。由于大多数 HTTP 实体都由上述内容类型组成，因此 HTTP 扫描只适用于一小部分 HTTP 实体，例如病毒最有可能隐藏在其中的内容类型 /zip 和 application/exe。

要改变 HTTP 扫描行为，使得 NetScreen 设备不考虑 MIME 内容类型而扫描所有种类的 HTTP 信息流，请输入命令：**unset av http skipmime**。

HTTP Web 邮件

在扫描 HTTP Web 邮件信息流时， NetScreen 设备在将信息流转发到客户端之前，将 Web 服务器对发出 HTTP Web 邮件请求的客户端响应的回复重新定向到内部防病毒扫描器。

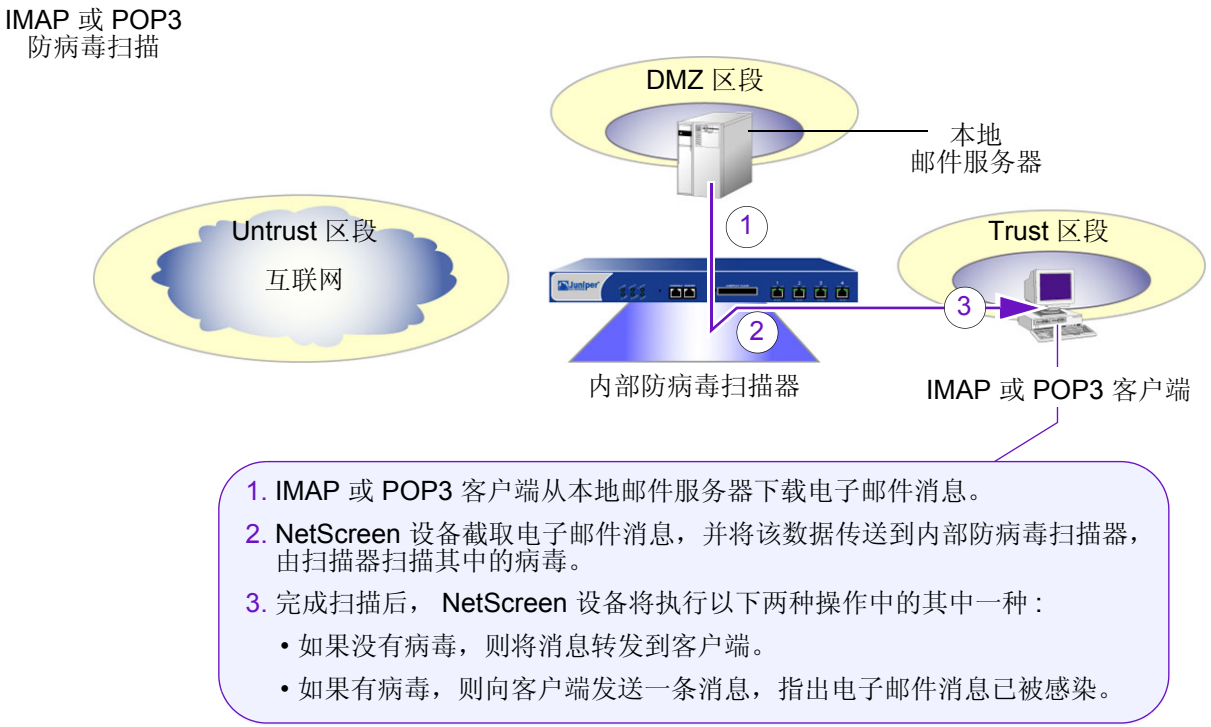
HTTP Web 邮件防病毒扫描



扫描 IMAP 和 POP3 信息流

在扫描 IMAP 和 POP3 信息流时， NetScreen 设备在将信息流发送到本地 IMAP 或 POP3 客户端之前，将信息流从本地邮件服务器重新定向到内部防病毒扫描器。NetScreen 设备采取的后继动作如何取决于扫描结果以及您对失败模式行为所做的配置：

如果消息	并且 “失败模式”设置为	则 NetScreen 设备将
未被感染	丢弃或通过，	传送消息到 IMAP 或 POP3 客户端。
包含病毒	丢弃或通过，	将内容类型更改为 “text/plain”，用以下通知替换消息正文，并将其发送到 IMAP 或 POP3 客户端： VIRUS WARNING. Contaminated File: *filename* Virus Name: *virus_name*
超出了最大内容级别 或 无法成功扫描	丢弃，	将内容类型更改为 “text/plain”，用以下通知替换消息正文，并将其发送到 IMAP 或 POP3 客户端： Content was not scanned for viruses because *reason_text_str* (code *number*), and it was dropped. *reason_text_str* 可能是以下某个字符串： the file was too large of an error or constraint the max. content size was exceeded the max. number of messages was exceeded
超出了最大内容级别 或 无法成功扫描	通过，	传送原始消息到 IMAP 或 POP3 客户端，将其原始主题行做如下修改： *original_subject_text_str* (No virus check because *reason_text_str*, code *number*)



如果被扫描的消息超出了最大内容设置或者扫描不能成功完成，则 NetScreen 设备会根据失败模式的设置情况而执行其它相应的操作。有关详细信息，请参阅前表。

扫描 SMTP 信息流

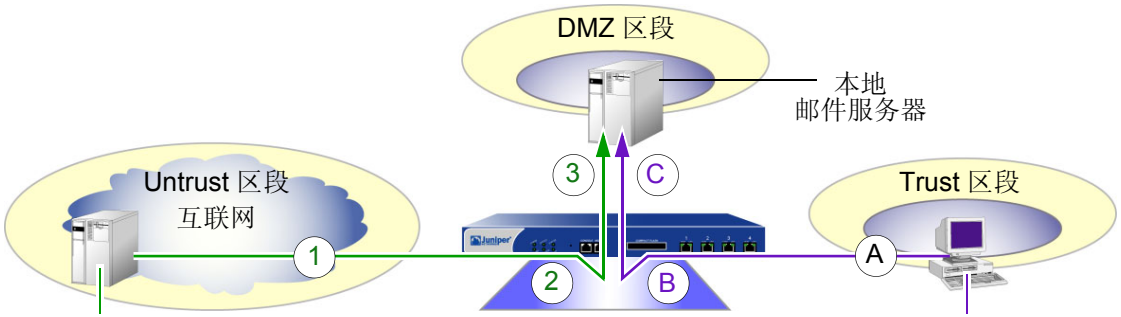
在扫描 SMTP 信息流时， NetScreen 设备在将信息流发送到本地邮件服务器之前，将信息流从本地 SMTP 客户端[3] 重新定向到内部防病毒扫描器。 NetScreen 设备采取的后继动作如何取决于扫描结果以及您对失败模式行为所做的配置：

如果消息	并且 “失败模式”设置为	则 NetScreen 设备将
未被感染	丢弃或通过，	传送消息给 SMTP 接收方。
包含病毒	丢弃或通过，	将内容类型更改为 “text/plain”，用以下通知替换消息正文，并将其发送到 SMTP 接收方： VIRUS WARNING. Contaminated File: *filename* Virus Name: *virus_name*
超出了最大内容级别 或 无法成功扫描	丢弃，	将内容类型更改为 “text/plain”，用以下通知替换消息正文，并将其发送到 SMTP 接收方： Content was not scanned for viruses because *reason_text_str* (code *number*), and it was dropped. *reason_text_str* 可能是以下某个字符串： the file was too large of an error or constraint the max. content size was exceeded the max. number of messages was exceeded

3. 由于 SMTP “客户端”指发送电子邮件的实体，因此，实际的 “客户端”可能是另外一个 SMTP 服务器。

如果消息	并且 “失败模式”设置为	则 NetScreen 设备将
超出了最大内容级别 或 无法成功扫描	通过，	传送原始消息到 SMTP 接收方，将其原始主题行做如下修改： *original_subject_text_str* (No virus check because *reason_text_str*, code *number*)

SMTP 防病毒扫描



1. 远程邮件服务器通过 SMTP 协议将电子邮件消息转发到本地邮件服务器。
2. NetScreen 设备截取电子邮件消息，并将该数据传送到内部防病毒扫描器，由扫描器扫描其中的病毒。
3. 完成扫描后，NetScreen 设备将执行以下两种操作中的其中一种:
   - 如果没有病毒，则将消息转发到本地服务器。
   - 如果有病毒，则向远程服务器发送一条消息，指出电子邮件消息已被感染。

A. SMTP 客户端将电子邮件消息发送给本地邮件服务器。

B. NetScreen 设备截取电子邮件消息，并将该数据传送到内部防病毒扫描器，由扫描器扫描其中的病毒。

C. 完成扫描后， NetScreen 设备将执行以下两种操作中的其中一种：
   - 如果没有病毒，则将消息转发到本地服务器。
   - 如果有病毒，则向客户端发送一条消息，指出电子邮件消息已被感染。

如果被扫描的消息超出了最大内容设置或者扫描不能成功完成，则 NetScreen 设备会根据失败模式的设置情况而执行其它相应的操作。有关详细信息，请参阅前表。

更新防病毒模式文件

在内部防病毒扫描时，要求将防病毒模式数据库加载到 NetScreen 设备上，并定期更新模式文件。为此，必须注册设备并购买对防病毒特征服务的预订。该预订允许您加载当前版本的数据库，并且在预订有效期内将数据库更新到可用的新版本。启动防病毒特征服务的过程不尽相同：

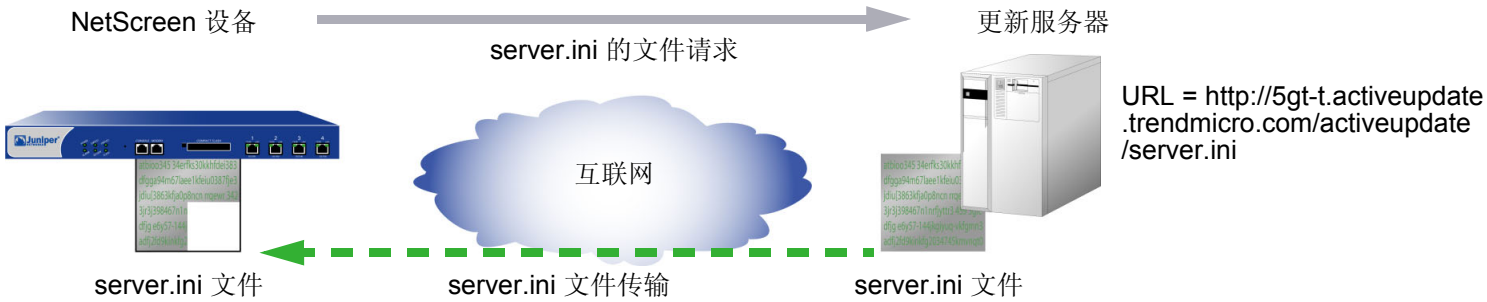
- 如果您购买了拥有防病毒功能的 NetScreen 设备，可以在初始购买后的短时间内加载防病毒模式文件。不过，只有注册该设备并购买对防病毒特征的预订，之后才能继续获取模式的升级版本。
- 如果您正在升级当前的 NetScreen 设备，使其使用内部防病毒扫描，则必须注册该设备并购买对防病毒特征的预订，之后才能开始加载防病毒模式文件。完成注册后，需要经过一段时间 (最长可达 4 个小时) 才可启动防病毒模式文件下载。

> ***注意：****有关防病毒特征服务的详细信息，请参阅第* ***2****-439 页上的“预定服务的注册与激活”。*

更新防病毒模式文件的过程如下：

1. 在 NetScreen 设备上指定更新服务器的 URL 地址，设备向更新服务器请求一个名为 *server.ini* 的服务器初始化文件。

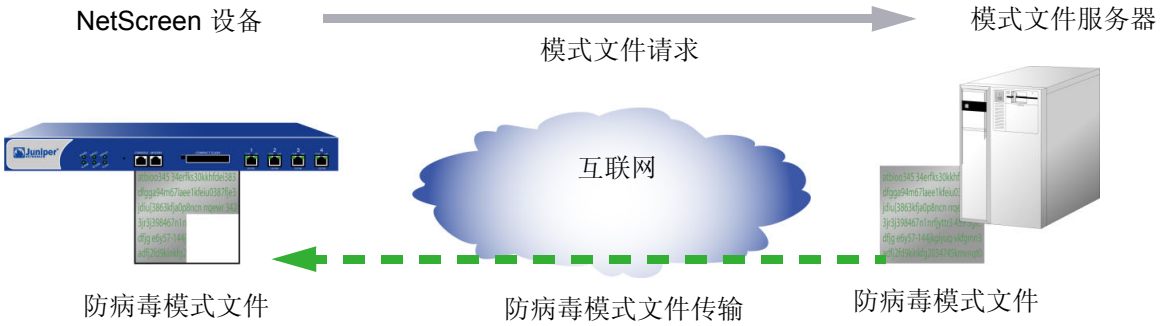
   例如：http://5gt-t.activeupdate.trendmicro.com/activeupdate/server.ini。



2. NetScreen 设备下载服务器初始化文件后，将检查 server.ini 文件是否有效。随后，NetScreen 设备对该文件进行分析以获取有关经过更新的模式文件的信息，包括模式文件的版本和大小以及模式文件服务器的位置。

   ***注意：**ScreenOS 含有用于对与模式文件服务器的通信进行认证的 CA 证书。*

3. 如果 NetScreen 设备上的模式文件已过期 (或者由于是第一次加载文件而不存在)，则 NetScreen 设备将从模式文件服务器自动检索更新的模式文件。



4. 下载模式文件后， NetScreen 设备将验证其防病毒模式更新服务预订是否仍然有效。如果预订有效，NetScreen 设备会将新模式文件保存到闪存和内存中，并将覆盖现有文件 (如果有的话)。如果预订已到期，则模式文件更新将失败，并会显示一条错误消息，指出防病毒预订已过期。

当新病毒传播时，将添加对模式文件的更新内容。可以对 NetScreen 设备进行配置，使其可定期自动更新模式文件，还可手动更新该文件。

***注意：**预订到期后，更新服务器将不再允许您更新防病毒模式文件。*

范例：自动更新

在本例中，将 NetScreen 设备配置为每 15 分钟自动更新一次模式文件。(缺省的防病毒模式更新时间间隔为 60 分钟。) 模式更新服务器所在的 URL 地址为 : http://5gt-t.activeupdate.trendmicro.com/activeupdate/server.ini

WebUI

Screening > Antivirus > Scan Manager: 输入以下内容，然后单击 **OK**:

Pattern Update Server:
http://5gt-t.activeupdate.trendmicro.com/activeupdate/server.ini

Auto Pattern Update: (选择), Interval: 15 minutes (10~10080)

CLI

```
set av scan-mgr pattern-update-url http://5gt-t.activeupdate.trendmicro.com/
    activeupdate/server.ini interval 15
save
```

范例：手动更新

在本例中，将手动更新模式文件。模式更新服务器所在的 URL 地址为：
http://5gt-t.activeupdate.trendmicro.com/activeupdate/server.ini

WebUI

Screening > Antivirus > Scan Manager: 输入以下内容，然后单击 **OK**:

Pattern Update Server:
http://5gt-t.activeupdate.trendmicro.com/activeupdate/server.ini

Update Now: (选择)

CLI

```
set av scan-mgr pattern-update-url
    http://5gt-t.activeupdate.trendmicro.com/activeupdate/server.ini
exec av scan-mgr pattern-update
```

应用防病毒扫描

要应用防病毒扫描到 FTP、 HTTP、 IMAP、 POP3 或 SMTP 信息流，必须在策略中引用防病毒扫描器 (“scan-mgr”)。

范例 : 内部防病毒扫描 (POP3)

在本例中，将在防火墙策略中引用内部防病毒扫描器，而该防火墙策略允许将来自 Trust 区段中的地址的 POP3 信息流发送到 DMZ 区段中的邮件服务器 (“mailsrv1”， 1.2.2.5)。所有区段都在 trust-vr 路由选择域中。

WebUI

1. 接口

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容，然后单击 **Apply**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

输入以下内容，然后单击 **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (对于 ethernet2): 输入以下内容，然后单击 **OK**:

Zone Name: DMZ

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.2.2.1/24

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容，然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. 地址

Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

Address Name: mailsrv1

IP Address/Domain Name:

IP/Netmask: (选择), 1.2.2.5/32

Zone: DMZ

3. POP3 防病毒扫描

Screening > Antivirus > Scan Manager: 输入以下内容，然后单击 **OK**:

Protocols to be scanned:

POP3: (选择)

4. 路由

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

5. 策略

Policies > (From: Trust, To: DMZ) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), mailsrv1

Service: POP3

Action: Permit

Antivirus Scanning: 选择 **scan-mgr**，并使用 **<<** 按钮将防病毒对象从 Available AV Object Names 栏移动到 Attached AV Object Names 栏。

CLI

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat

set interface ethernet2 zone dmz
set interface ethernet2 ip 1.2.2.1/24

set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. 地址

```
set address dmz mailsvr1 1.2.2.5/32
```

3. POP3 防病毒扫描

```
set av scan-mgr content pop3 timeout 20
```

4. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

5. 策略

```
set policy from trust to dmz any mailsvr1 pop3 permit av scan-mgr
save
```

防病毒扫描器设置

为了更好地满足网络环境的需要，可修改以下防病毒扫描器设置：

有选择性的内容扫描

在缺省情况下，防病毒扫描器检查 FTP、 HTTP (仅 Web 邮件)、 IMAP、 POP3 和 SMTP 信息流。

注意：*内部防病毒扫描器仅检查特定的 HTTP Web 邮件模式。 Yahoo!、 Hotmail 和 AOL 邮件服务的模式是预先定义的。*

可更改缺省行为，使得扫描器只检查特定类型的网络信息流。

还可更改每个协议的超时值。在缺省情况下，如果 NetScreen 设备未接收到完成扫描所需的所有数据，防病毒扫描操作将于 180 秒后超时。超时值的范围是 1 到 1800 秒。

```
set av scan-mgr content { ftp | http | imap | pop3 | smtp } timeout number
unset av scan-mgr content { ftp | http | imap | pop3 | smtp } timeout
```

上面的 **unset av** 命令将超时值还原为缺省值 (180 秒)。

范例：扫描所有信息流类型

在本例中，将配置防病毒扫描器检查 FTP、HTTP (仅 Web 邮件)、IMAP、POP3 和 SMTP 信息流。由于预计扫描器将处理大量信息流，因此还将把超时值从 180 秒 (缺省设置) 增加到 300 秒。

WebUI

Screening > Antivirus > Scan Manager: 输入以下内容，然后单击 **OK**:

Protocols to be scanned:

HTTP: (选择)

Webmail: (选择)

SMTP: (选择)

POP3: (选择)

FTP: (选择)

IMAP: (选择)

注意：*只能使用 CLI 来更改超时值。*

CLI

```
set av scan-mgr content http timeout 300
set av scan-mgr content smtp timeout 300
set av scan-mgr content pop3 timeout 300
set av scan-mgr content ftp timeout 300
set av scan-mgr content imap timeout 300
save
```

范例 : SMTP 和 HTTP 的防病毒扫描

在本例中，将对防病毒扫描器进行配置，使其检查所有 SMTP 和 HTTP 信息流。将两个协议的超时值均恢复为缺省值 : 180 秒。

WebUI

Screening > Antivirus > Scan Manager: 输入以下内容，然后单击 **OK**:

Protocols to be scanned:

HTTP: (选择)

ALL HTTP: (选择)

SMTP: (选择)

POP3: (清除)

FTP: (清除)

IMAP: (清除)

注意 : *只能使用 CLI 来更改超时值。*

CLI

```
set av scan-mgr content smtp timeout 180
set av scan-mgr content http timeout 180
unset av http webmail enable
unset av scan-mgr content pop3
unset av scan-mgr content ftp
unset av scan-mgr content imap
save
```

解压缩和最大信息量大小

接收到内容后，内部防病毒扫描器将解压缩所有压缩文件。在缺省情况下，扫描器最多可解开 2 层的压缩文件。例如，如果扫描器接收到一个带有附件的文件，并且该附件是嵌入另一个压缩文件内的压缩文件时，扫描器将对两个层进行解压缩以检测所有病毒。可对内部防病毒扫描器进行配置，使其最多可解压缩 4 个嵌入另一个文件内的压缩文件。

在任一特定时刻，防病毒扫描器最多可检查 16 条消息以及大小为 16 兆字节 (缺省值为 10 兆字节) 的 “解压缩” 文件内容。如果接收到的消息总数或内容大小同时超过其限定值，则在缺省情况下扫描器将传送内容而不对病毒进行检查。例如，扫描器可以同时接收并检查 4 条大小为 4 兆字节的消息。如果同时接收到 9 条大小为 2 兆字节的消息，扫描器将传送该内容而不对其进行扫描。可以更改此缺省行为，使得扫描器丢弃信息流，而不是对其进行传送。

范例 : 丢弃大文件

在本例中，将对防病毒扫描器进行配置，使其最多可解压缩 3 个嵌入另一个文件内的压缩文件。也可以这样配置扫描器，使得当同时接收到的消息总数超过 4 条或 “解压缩的” 内容总量超过 12 MB 时，扫描器就丢弃该内容。

WebUI

Screening > Antivirus > Scan Manager: 输入以下内容，然后单击 **OK**:

File decompression: 3 layers (1~4)

Drop: (选择) file if it exceeds 3000 KB (4000~16000)

Drop: (选择) file if the number of files exceeds 4 files (1~16)

CLI

```
set av scan-mgr decompress-layer 3
set av scan-mgr max-msgs 4
set av scan-mgr max-content-size 3000
set av scan-mgr max-content-size drop
save
```

防病毒资源分配

恶意用户可能会同时生成大量的信息流，试图消耗所有可用资源，从而降低了防病毒扫描器扫描其它信息流的能力。为了防止这类情况的发生，对于来自单个来源的信息流在任一时刻可消耗的防病毒资源，NetScreen 设备可以为其规定一个最大百分比。缺省的最大百分比是 70%。可以将此设置更改为介于 1% 和 100% 之间的任意值，其中 100% 表示对来自单个来源的信息流可消耗的 AV 资源不施加任何限制。

WebUI

> ***注意：****必须使用 CLI 来配置此选项。*

CLI

```
set av all resources number
unset av all resources
```

上面的 **unset av** 命令将每个来源的最大防病毒资源百分比恢复为缺省值 (70%)。

失败模式行为

失败模式是当 NetScreen 设备不能完成扫描操作 (允许未经检查的信息流或封锁它) 时所应用的行为。在缺省情况下，如果无法完成扫描， NetScreen 设备将封锁启用了防病毒检查的策略所允许的信息流。可以将该缺省行为由封锁改为允许。

WebUI

Screening > Antivirus > Global: 选中 **Fail Mode Traffic Permit** 以允许未经检查的信息流，或清除该选项的复选框以封锁未经检查的信息流，然后单击 **Apply**。

CLI

```
set av all fail-mode traffic permit
unset av all fail-mode traffic
```

上面的 **unset av** 命令将失败模式行为恢复为缺省值 (封锁未经检查的信息流)。

HTTP Keep-Alive

在缺省情况下，NetScreen 设备使用 HTTP “close” 连接选项来指示数据传输的结束。(必要时， NetScreen 设备会将连接标题字段中的标记从 “keep-alive” 更改为 “close”。) 这样，当完成其数据传输时， HTTP 服务器将发送一个 TCP FIN 来关闭 TCP 连接，从而表明数据发送结束。当接收到 TCP FIN 时， NetScreen 设备就拥有了来自服务器的所有 HTTP 数据，并可以指示防病毒扫描器开始扫描。

您可以更改 NetScreen 设备的缺省行为，以便使用 HTTP “keep-alive” 连接选项，该选项不发送 TCP FIN 来指示数据传输的终止。 HTTP 服务器必须用其它方式表明已发送了所有数据，例如，通过发送 HTTP 包头中的内容长度，或通过某些形式的编码。(服务器所使用的方法因服务器类型而异。) 此方法在执行防病毒检查时使 TCP 连接保持打开状态，从而减少了等待时间并提高了 CPU 性能。但是，该方法却不如 “close” 连接方法安全。如果您发现 HTTP 连接在防病毒扫描检查时超时，可以更改此行为。

WebUI

Screening > Antivirus > Global: 选中 **Keep Alive** 以使用 “keep-alive” 连接选项，或清除该选项的复选框以使用 “close” 连接选项，然后单击 **Apply**。

CLI

```
set av http keep-alive
unset av http keep-alive
```

HTTP Trickling

HTTP trickling 是指将指定数量的未扫描 HTTP 信息流转发到请求 HTTP 的客户端，以防止浏览器窗口在 VirusWall 检查下载的 HTTP 文件时发生超时。 (NetScreen 设备在传输整个扫描的文件之前将转发少量数据。) 在缺省情况下将禁用 HTTP trickling。要启用 HTTP trickling 并使用缺省的 HTTP trickling 参数，请执行下列任一操作 :

WebUI

Screening > Antivirus > Global: 选中 Trickling Default 复选框，然后单击 **Apply**。

CLI

```
set av http trickling default
```

使用缺省参数时，如果 HTTP 文件的大小达到或超过了 3MB，则 NetScreen 设备将采用 trickling。然后每发送 1MB 的扫描信息流，设备转发 500 字节的内容。

要更改 HTTP trickling 的参数，请执行以下任一操作：

WebUI

Screening > Antivirus > Global: 输入以下内容，然后单击 **Apply**:

Trickling:

Custom: (选择)

Minimum Length to Start Trickling: 输入 *number1*。

Trickle Size: 输入 *number2*。

Trickle for Every MB Sent for Scanning: 输入 *number3*。

CLI

```
set av http trickling number1 number3 number2
```

三个数值变量的具体含义如下：

- *number1:* 触发 trickling 的最小的 HTTP 文件大小 (单位为兆字节)
- *number2:* NetScreen 设备转发的未扫描信息流的大小 (单位为字节)
- *number3:* NetScreen 设备将 trickling 应用于其中的信息流块的大小 (单位为兆字节)

注意：*细流到客户端硬盘的数据显示为细小的、不可用的文件。由于使用 trickling 时将转发小量数据到客户端而不对数据进行扫描，因此在 NetScreen 设备细流到客户端的数据中可能含有病毒代码。 Juniper Networks 建议用户删除这些文件。*

您可以在 WebUI 中禁用 HTTP trickling (Screening > Antivirus: 单击 Trickling 部分的 **Disable**。) 或使用 CLI 命令 **set av http trickling 0 0 0** 禁用它。但是，如果正在下载的文件大于 8 兆字节，并且禁用了 HTTP trickling，则浏览器窗口将极有可能会超时。

URL 过滤

URL 过滤 (也称为 Web 过滤) 使您能管理互联网访问并阻止访问不合适的 Web 内容。 NetScreen 提供了两种 URL 过滤解决方案 :

- 集成 URL 过滤
- 重新定向 URL 过滤

使用集成 URL 过滤时，可以通过将 URL 过滤配置文件绑定到防火墙策略来允许或封锁对请求站点的访问。 URL 过滤配置文件指定了 URL 类别以及当 NetScreen 设备接收到访问每个类别中的 URL 的请求时所执行的动作 (允许或封锁)。 URL 类别是由 SurfControl 预先定义和维护的，或者是由用户定义的。有关配置集成 URL 过滤功能的信息，请参阅第 107 页上的 “集成 URL 过滤”。

使用重新定向 URL 过滤时， NetScreen 设备发送 TCP 连接中的第一个 HTTP 请求给 Websense 服务器或 SurfControl 服务器，从而使您能够根据其 URL、域名和 IP 地址来封锁或允许访问不同的站点。有关配置重新定向 URL 过滤功能的信息，请参阅第 121 页上的 “重新定向 URL 过滤”。

集成 URL 过滤

使用集成 URL 过滤时， NetScreen 设备将截取每个 HTTP 请求，然后通过以下方式来确定是允许还是封锁对请求站点的访问 : 对其 URL 进行分类，并将 URL 类别与 URL 过滤配置文件进行匹配。将 URL 过滤配置文件绑定到策略。URL 过滤配置文件按照每个类别定义当 NetScreen 设备接收到访问 URL 的请求时所执行的动作 (允许或封锁)。

URL 类别是按内容组织的 URL 列表。 NetScreen 设备使用 SurfControl 预定义的 URL 类别来确定某个 URL 的类别。SurfControl Content Portal Authority (CPA) 服务器负责维护包含各种类型 Web 内容 (被分成大约 40 个类别) 的最大数据库。有关预定义 URL 类别的列表以及每个类别中 URL 的描述，请参阅位于 www.surfcontrol.com 处的 SurfControl 网站。除了可以使用 SurfControl 预定义的 URL 类别外，还可对 URL 进行分组并创建特定于您的需要的类别。有关创建用户定义的类别的信息，请参阅第 110 页上的 “URL 类别”。

当 Trust 区段中的主机试图与 Untrust 区段中的服务器建立 HTTP 连接时，事件的基本顺序如下。

1. NetScreen 设备检查可应用到信息流的防火墙策略。
   - 如果没有信息流的防火墙策略， NetScreen 设备将丢弃信息流。
   - 如果有防火墙策略并且该策略启用了 URL 过滤， NetScreen 设备将截取所有 HTTP 请求。
2. NetScreen 设备检查是否有绑定到防火墙策略的用户定义的配置文件。如果没有， NetScreen 设备将使用缺省配置文件 **ns-profile**。
3. NetScreen 设备检查请求的 URL 的类别是否已经存入了高速缓存。如果该 URL 的类别没有存入高速缓存，NetScreen 设备会将该 URL 发送到 SurfControl CPA 服务器进行分类，然后再将结果存入高速缓存。
4. 一旦 NetScreen 设备确定了该 URL 的类别，它将检查该 URL 的类别是否位于绑定到防火墙策略的 URL 过滤配置文件中。
   - 如果该类别位于配置文件中，则设备将按照配置文件中所定义的内容来封锁或允许对该 URL 的访问。
   - 如果该类别不在配置文件中，则设备将执行所配置的缺省动作。

要配置 NetScreen 设备进行 URL 过滤，必须执行下列任务：

1. 设置域名 (DNS) 服务器。
2. 在 NetScreen 设备上启用集成 URL 过滤。
3. 定义类别。 (可选)
4. 定义配置文件。 (可选)
5. 在防火墙策略中启用 URL 过滤，还可将 URL 过滤配置文件应用到防火墙策略。

以下各节将就每个任务分别进行阐述。

域名服务器 (DNS)

NetScreen 设备集成了 DNS 支持，允许您使用域名和 IP 地址对位置进行标识。必须至少配置一个 DNS 服务器，以便 NetScreen 设备可将 CPA 服务器名称解析为一个地址。有关 DNS 的信息，请参阅第 **2**-359 页上的 “域名系统支持”。

URL 过滤环境

可以使用 WebUI 或 CLI 命令在 NetScreen 设备上启用集成 URL 过滤。如果使用 CLI，必须首先输入 URL 过滤环境，之后再输入特定于集成 URL 过滤的命令。输入以下命令：

```
set url protocol sc-cpa
```

在输入前一命令后，提示符将发生改变。

```
ns(url:sc-cpa)->
```

这种改变表明您已输入了 URL 过滤环境，可以配置集成 URL 过滤参数。

范例：启用 URL 过滤

在本例中，将在 NetScreen 设备上启用集成 URL 过滤。

WebUI

Screening > URL Filtering > Protocol Selection: 选择 **Integrated (SurfControl)**，然后单击 **Apply**。然后选择 **Enable URL Filtering via CPA Server**，并再次单击 **Apply**。

CLI

```
ns-> set url protocol sc-cpa
ns(url:sc-cpa)-> set enable
ns(url:sc-cpa)-> exit
ns-> save
```

URL 类别

类别是按内容分组的 URL 列表。有两种类型的类别 : 预定义的和用户定义的。 SurfControl 维护着约 40 个预定义的类别。有关预定义 URL 类别的列表以及每个类别中 URL 的描述，请参阅位于 www.surfcontrol.com 处的 SurfControl 网站。要查看 SurfControl 预定义的 URL 类别的列表，请执行以下命令 :

WebUI

Screening > URL Filtering > Profile > Predefine Category

CLI

```
ns-> set url protocol sc-cpa
ns(url:sc-cpa)-> get category pre
```

所显示的类别列表与下表类似 :

```
Type           code     Category name
-----------------------------------------
  PreDefine       90     Adult/Sexually Explicit
  PreDefine       76     Advertisements
  PreDefine       50     Arts & Entertainment
  PreDefine     3001     Chat
  PreDefine       75     Computing & Internet
  PreDefine       91     Criminal Skills
      .
      .
      .
```

预定义的类别列表中显示有类别及其 SurfControl 内部代码。尽管无法在类别中列出 URL，不过可以通过使用 SurfControl 网站 www.surfcontrol.com 上的 “Test A Site” 功能来确定某个网站的类别。

除了可以使用 SurfControl 预定义的 URL 类别外，还可对 URL 进行分组并创建特定于您所需要的类别。每个类别中最多可包含 20 个 URL。创建类别时，可以添加站点的 URL 或 IP 地址。当向用户定义的类别中添加 URL 时，NetScreen 设备将执行 “域名服务器” (DNS) 查找，将主机名解析为 IP 地址并将此信息存入高速缓存。当用户通过键入站点的 IP 地址来尝试访问某个站点时，NetScreen 设备将检查存入高速缓存的 IP 地址列表并尝试对主机名进行解析。

由于许多站点具有动态 IP 地址，因此它们的 IP 地址不断地变化。当试图访问某个站点时，用户可键入 NetScreen 设备上的存入高速缓存的列表中所没有的 IP 地址。因此，如果您知道要添加到类别中的站点的 IP 地址，请同时输入站点的 URL 和 IP 地址。

注意，如果某个 URL 同时存在于用户定义的类别和预定义的类别中，NetScreen 设备将把该 URL 与用户定义的类别相匹配。

范例 : URL 类别

在本例中，将创建一个名为 Competitors 的类别并添加 URL: www.games1.com 和 www.games2.com。

WebUI

Screening > URL Filtering > Profile > Custom List > New: 输入以下内容，然后单击 **Apply**:

Category Name: Competitors

URL: www.games1.com

输入以下内容，然后单击 **OK**:

URL: www.games2.com

CLI

```
ns-> set url protocol sc-cpa
ns(url:sc-cpa)-> set category competitors url www.games1.com
ns(url:sc-cpa)-> set category competitors url www.games2.com
ns(url:sc-cpa)-> exit
ns-> save
```

URL 过滤配置文件

URL 过滤配置文件由一组 URL 类别及其相应的动作组成：

- Permit – NetScreen 设备允许访问站点。
- Block – NetScreen 设备不允许访问站点。当 NetScreen 设备封锁对某个站点的访问时，会出现一条指出该 URL 的类别的消息。
- Black List – NetScreen 设备总是封锁对黑名单中的站点的访问。可以为黑名单创建一个用户定义的类别，也可使用预定义的类别。
- White List – NetScreen 设备总是允许对白名单中的站点的访问。可以为白名单创建一个用户定义的类别，也可使用预定义的类别。

NetScreen 提供了一个名为 **ns-profile** 的缺省配置文件。该文件中列有 SurfControl 预定义的 URL 类别及其相应动作。不能对该缺省配置文件进行编辑，或者添加黑名单或白名单。要查看 NetScreen 预定义的配置文件，请执行以下命令：

WebUI

Screening > URL Filtering > Profile > Predefined Profile

CLI

```
ns(url:sc-cpa)-> get profile ns-profile
```

NetScreen 设备将显示预定义的配置文件，如下所示：

```
  url filtering profile name: ns-profile
  black-list category: none
  white-list category: none
  Category                              Action
-----------------------------------------------
  Adult/Sexually Explicit               block
  Advertisements                        block
  Arts & Entertainment                  permit
  Chat                                  permit
  Computing & Internet                  permit
     .
     .
     .
  Violence                              block
  Weapons                               block
  Web-based Email                       permit
  other                                 permit
```

如果 HTTP 请求中的 URL 不在缺省配置文件中所列出的任何类别中，那么 NetScreen 设备的缺省动作是允许访问该站点。

通过复制 ns-profile 并编辑该新配置文件，可以创建一个类似于 ns-profile 的配置文件。请在 WebUI 中执行以下步骤来复制 ns-profile。

WebUI

Screening > URL Filtering > Profile > Custom Profile: ns-profile: 选择 **Clone**。

注意：*必须使用 WebUI 来复制预定义的配置文件 ns-profile。*

还可创建您自己的 URL 过滤配置文件。当创建 URL 过滤配置文件时，您可以：

- 添加用户定义的和 SurfControl 预定义的 URL 类别。
- 为黑名单和 / 或白名单指定一个类别。
- 更改缺省动作。

范例：URL 过滤配置文件

在本例中，将创建一个缺省动作为 “permit” 的名为 **my-profile** 的定制配置文件。然后，取出在前例 (Competitors) 中创建的类别，并将其添加到动作为 “block” 的 my-profile 中。注意，当使用 CLI 配置缺省动作时，将为 “Other” 类别指定动作。

WebUI

Screening > URL Filtering > Profile > Custom Profile > New: 输入以下内容，然后单击 **Apply**:

Profile Name: my-profile

Default Action: Permit

选择以下内容，然后单击 **OK**:

Subscribers Identified by:

Category Name: Competitors (选择)

Action: Block (选择)

Configure: Add (选择)

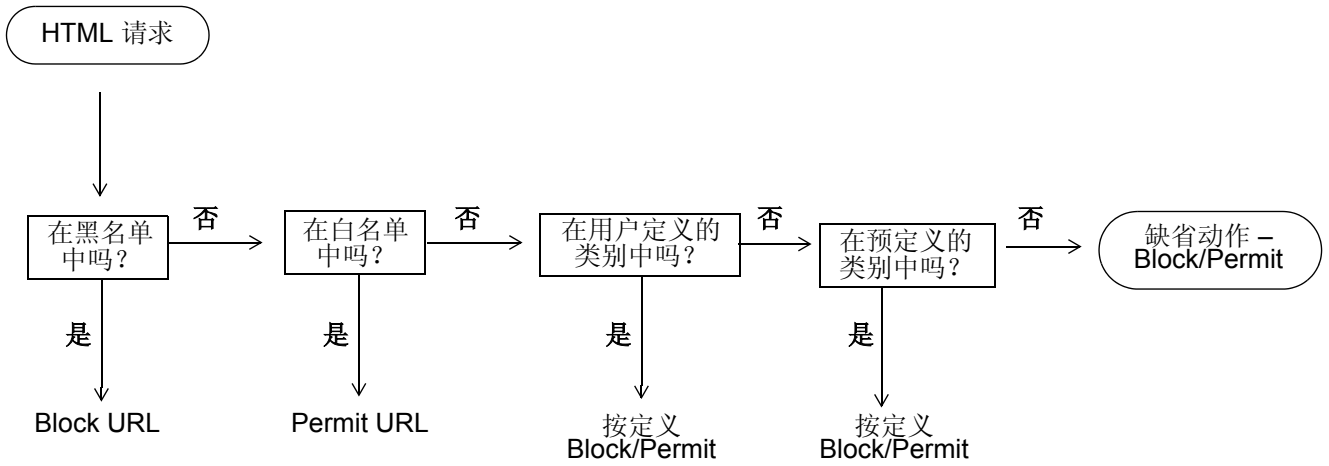
CLI

```
ns-> set url protocol sc-cpa
ns(url:sc-cpa)-> set profile my-profile other permit
ns(url:sc-cpa)-> set profile my-profile competitors block
ns(url:sc-cpa)-> exit
ns-> save
```

URL 配置文件和策略

防火墙策略可允许或拒绝两点间指定类型的单向信息流。 (有关防火墙策略的信息，请参阅第 **2** -293 页上的 “策略”。) 可以在策略中同时启用防病毒 (AV) 扫描和集成 URL 过滤。 (有关防病毒扫描的信息，请参阅第 81 页上的 “防病毒扫描”。)

当在策略中启用了集成 URL 过滤后， NetScreen 设备将截取所有 HTTP 请求。如果存在绑定到该策略的 URL 过滤配置文件， NetScreen 设备将按以下顺序将内向 HTTP 请求中的 URL 与配置文件中的类别相匹配 : 黑名单、白名单、用户定义的类别以及 SurfControl 预定义的 URL 类别。如果 NetScreen 设备找不到请求的 URL 的类别，那么将会根据所配置的缺省动作来封锁或允许对该 URL 的访问。



如果允许 URL 并且启用和配置了防病毒扫描，则 NetScreen 设备将对事务的内容执行防病毒扫描。如果封锁 URL，则 NetScreen 设备将关闭 TCP 连接，发送一条消息给用户，并不检查以进行防病毒扫描。

范例：集成 URL 过滤

在本例中，将在 NetScreen 设备上启用集成 URL 过滤并封锁对 competitors 的站点的访问。将进行如下配置：

1. 创建一个名为 Competitors 的类别。
2. 将以下 URL 添加到该类别中：www.comp1.com 和 www.comp2.com。
3. 创建一个名为 my-profile 的配置文件。
4. 将 Competitors 类别添加到 my-profile 中。
5. 将 my-profile 应用到防火墙策略。

WebUI

1. URL 过滤

Screening > URL Filtering > Protocol Selection: 选择 **Integrated (SurfControl)**，然后单击 **Apply**。然后选择 **Enable URL Filtering via CPA Server**，并再次单击 **Apply**。

2. URL 类别

Screening > URL Filtering > Profile > Custom List > New: 输入以下内容，然后单击 **Apply**:

Category Name: Competitors

URL: www.comp1.com

输入以下内容，然后单击 **OK**:

URL: www.comp2.com

3. URL 过滤配置文件

Screening > URL Filtering > Profile > Custom Profile > New: 输入以下内容，然后单击 **Apply**:

Profile Name: my-profile

Default Action: Permit

在 **Subscribers Identified by** 部分做如下选择，然后单击 **OK**:

Category Name: Competitors (选择)

Action: Block (选择)

Configure: Add (选择)

4. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: HTTP

URL Filtering: (选择), my-profile

Action: Permit

CLI

1. URL 过滤

```
ns-> set url protocol sc-cpa
ns(url:sc-cpa)-> set enable
```

2. URL 类别

```
ns(url:sc-cpa)-> set category competitors url www.comp.com
ns(url:sc-cpa)-> set category competitors url www.comp.com
```

3. URL 过滤配置文件

```
ns(url:sc-cpa)-> set profile my-profile other permit
ns(url:sc-cpa)-> set profile my-profile competitors block
ns(url:sc-cpa)-> exit
```

4. 防火墙策略

```
ns-> set policy id 23 from trust to untrust any any http permit url-filter
ns-> set policy id 23
ns(policy:23)-> set url protocol sc-cpa profile my-profile
ns(policy:23)-> exit
ns-> save
```

SurfControl 服务器

SurfControl 有三个服务器位置，每个都服务于某一特定的地理区域 : 美洲、亚太地区以及欧洲 / 中东 / 非洲。缺省主服务器是美洲服务器，而缺省备份服务器是亚太地区服务器。可以更改主服务器，而 NetScreen 设备将根据主服务器自动选择备份服务器。 (亚太地区服务器是美洲服务器的备份服务器，而美洲服务器也是其它两台服务器的备份服务器。)

SurfControl CPA 服务器定期更新其类别列表。由于更新列表时 CPA 服务器不通知其客户端，因此， NetScreen 设备必须定期轮询 CPA 服务器。在缺省情况下， NetScreen 设备每两周查询一次 CPA 服务器，以进行类别更新。可以更改此缺省设置以适合您的网络环境。也可以通过输入 URL 过滤环境并执行 **exec url cate-list-update** 命令来手动更新类别列表。

URL 过滤高速缓存

在缺省情况下，NetScreen 设备将 URL 的类别存入高速缓存。这就减少了每次设备接收先前请求的 URL 的新请求时访问 SurfControl CPA 服务器的开销。可以根据网络环境的性能和内存要求来配置高速缓存的大小以及将 URL 存入高速缓存所需的时间。缺省的高速缓存大小与平台无关，缺省超时为 24 小时。

范例：高速缓存参数

在本例中，将把高速缓存大小改为 400 千字节，并把超时改为 18 小时。

WebUI

Screening > URL Filtering > Protocol Selection > SC-CPA: 输入以下内容，然后单击 **Apply**:

Enable Cache: (选择)

Cache Size: 400 (K)

Cache Timeout: 18 (Hours)

CLI

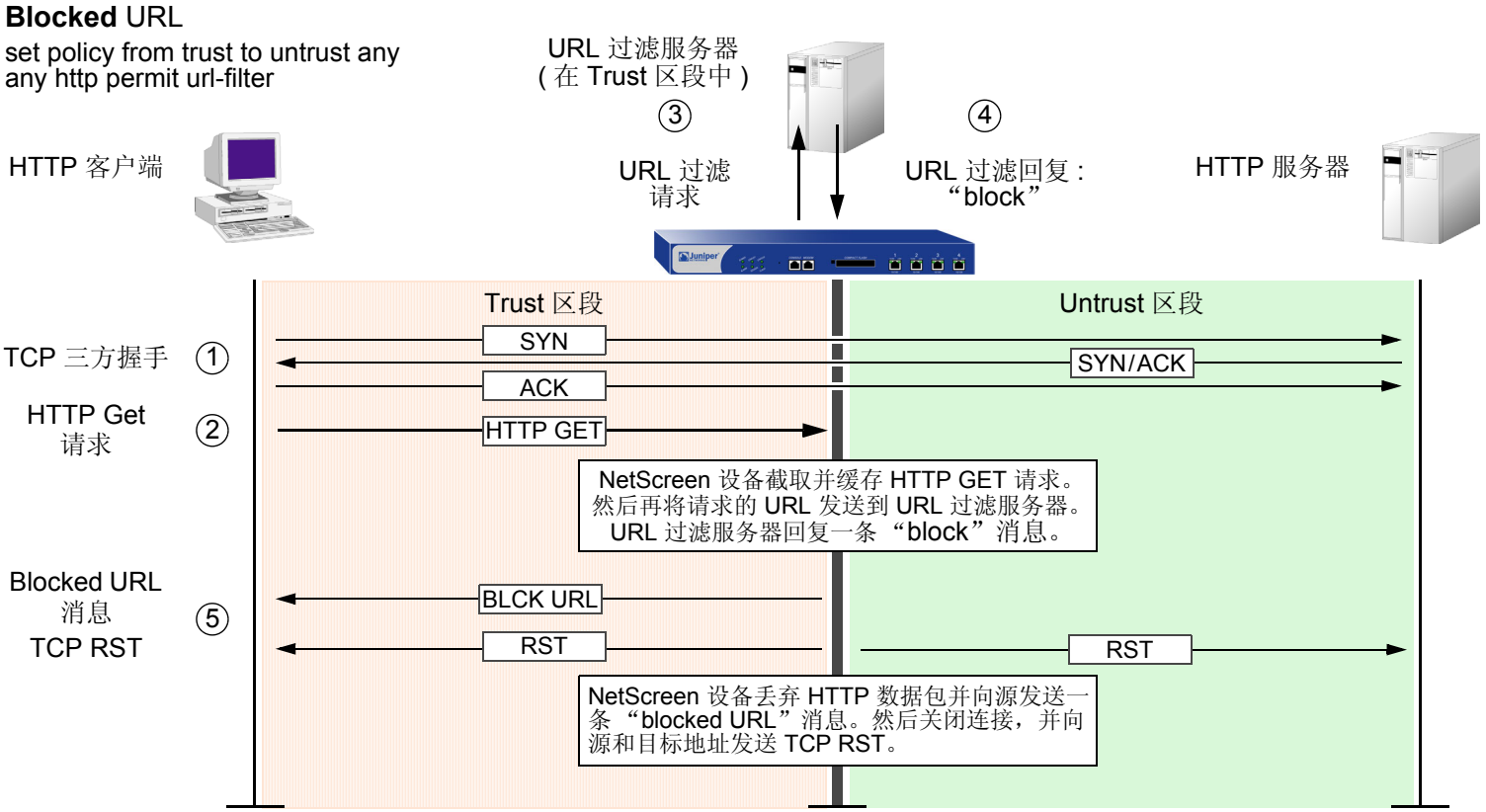
```
ns-> set url protocol sc-cpa
ns(url:sc-cpa)-> set cache size 400
ns(url:sc-cpa)-> set cache timeout 18
ns(url:sc-cpa)-> exit
ns-> save
```

重新定向 URL 过滤

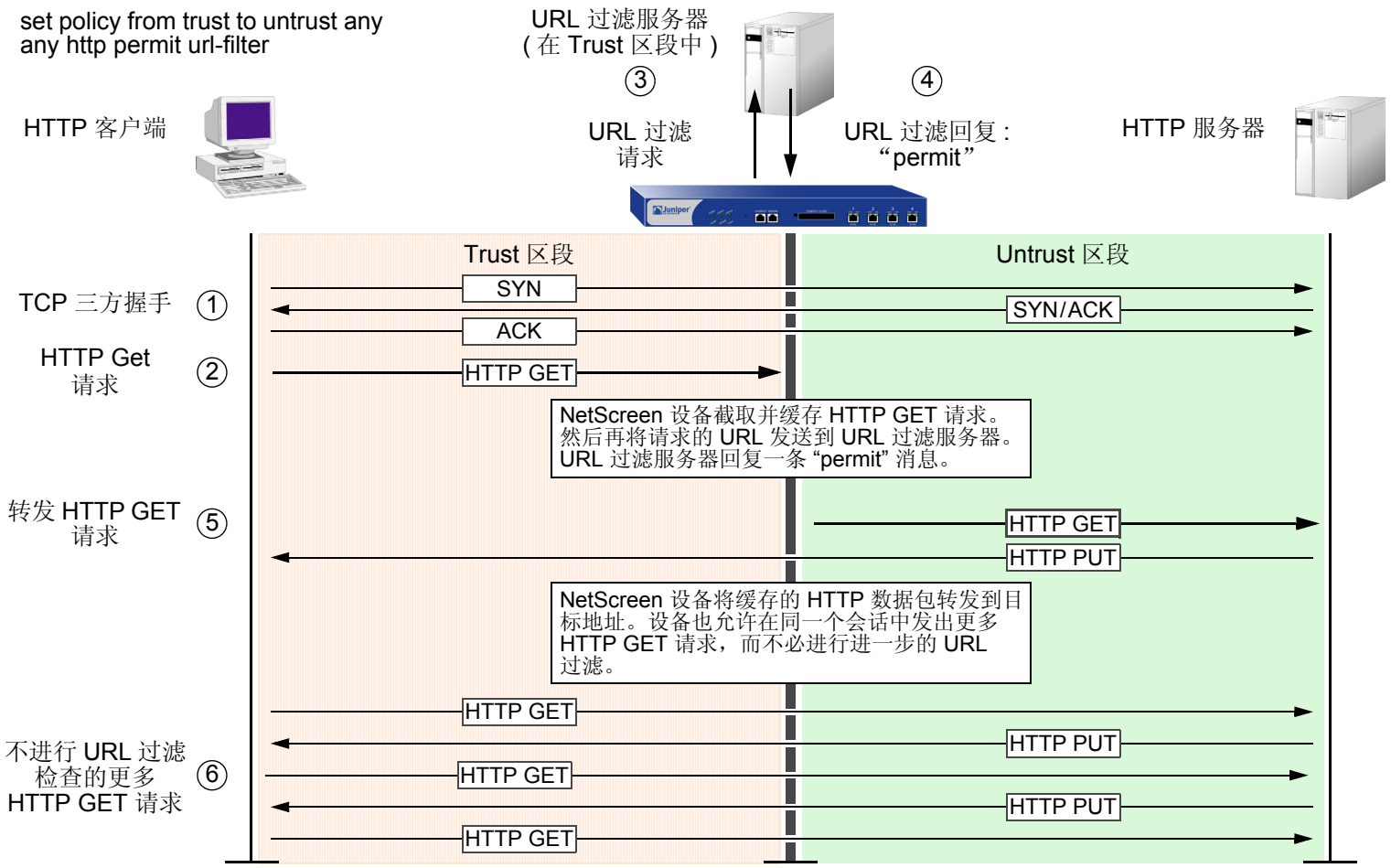
NetScreen 利用 Websense Enterprise Engine 或 SurfControl Web Filter 支持重新定向 URL 过滤，使您可以根据站点的 URL、域名和 IP 地址来封锁或允许对这些站点的访问。 NetScreen 设备可以直接链接到 Websense 或 SurfControl URL 过滤服务器。

***注意：**有关 Websense 的其它信息，请访问 www.websense.com。有关 SurfControl 的其它信息，请访问 www.surfcontrol.com。*

当 Trust 区段中的主机试图与 Untrust 区段中的服务器建立 HTTP 连接时，下图说明了事件的基本顺序。不过，URL 过滤确定所请求的 URL 是被禁止的。



如果 URL 过滤服务器允许访问该 URL，则 HTTP 连接尝试过程中的事件序列如下：



具有虚拟系统的 NetScreen 设备最多可支持八个不同的 URL 过滤服务器 – 保留一个服务器供根系统使用，根系统可与任意数量的虚拟系统共享该服务器；其余七个 URL 过滤服务器供虚拟系统专用。根级 admin 可以在根级和虚拟系统 (vsys) 级配置 URL 过滤模块。 vsys 级 admin 可以为其本身的 vsys 配置 URL 模块 (如果该 vsys 拥有其专用的 URL 过滤服务器)。如果 vsys 级 admin 使用根级 URL 过滤服务器设置，则该 admin 可以看到 (但不能修改) 根级 URL 过滤设置。

为了配置 NetScreen 设备进行重新定向 URL 过滤，必须执行下列任务 :

1. 建立与 URL 过滤服务器 (最多为 8 个) 的通信。
2. 定义一些系统级行为参数。一组参数可应用到根系统以及与根系统共享 URL 过滤配置的任何 vsys。其它各组参数可应用到已定义了专用 URL 过滤服务器的虚拟系统。
3. 在根级和 vsys 级激活 URL 过滤。
4. 在各个策略中启用 URL 过滤。

下面将对这些任务进行详细介绍。

1. 设备到设备的通信

可以配置 NetScreen 设备与 Websense 服务器或 SurfControl 服务器进行通信。必须首先选择要与 NetScreen 设备相连的服务器。选择下列之一 :

- Websense 服务器。
- 使用“SurfControl 内容过滤协议”(SCFP) 的 SurfControl 服务器。若需要此项功能，请选择此服务器。
- 使用 Content Portal Authority (CPA) 协议的 SurfControl 服务器。若要使用集成 URL 过滤解决方案，请使用该服务器。 (有关集成 URL 过滤的信息，请参阅第 107 页上的 “集成 URL 过滤”。)

可以使用以下 CLI 命令来选择服务器类型 :

```
set url protocol type { websense | scfp |sc-cpa }
```

在 WebUI 中，选择 Screening > URL Filtering > Protocol 页面中的协议。

然后定义 URL 过滤服务器的设置以及应用 URL 过滤时希望 NetScreen 设备采取的行为参数。如果在根系统中配置这些设置，它们也可应用到与根系统共享 URL 过滤配置的任何虚拟系统。对于拥有其本身专用的 URL 过滤服务器的 vsys，根 admin 或 vsys admin 必须单独为该 vsys 配置设置。

必须在系统级为设备到设备的通信定义的 URL 过滤设置如下：

- **Server Name:** 运行 Websense 或 SurfControl 服务器的计算机的 IP 地址或完全合格的域名 (FQDN)。
- **Server Port:** 如果更改了服务器上的缺省端口，则必须同时更改 NetScreen 设备上的该缺省端口。(Websense 的缺省端口是 15868，而 SurfControl 的缺省端口是 62252。) 有关详细信息，请参阅 Websense 或 SurfControl 文档。
- **Source Interface:** NetScreen 设备发起 URL 过滤请求到 URL 过滤服务器的源。
- **Communication Timeout:** NetScreen 设备等待 URL 过滤服务器响应的时间间隔 (以秒为单位)。如果服务器在该时间间隔内没有响应，NetScreen 设备将封锁或允许该请求，具体执行哪种操作将因您之前所做的选择而定。对于该时间间隔，可以输入一个介于 10 和 240 之间的数字。

可以使用以下 CLI 命令来配置这些设置：

```
set url server { ip_addr | dom_name } port_num timout_num
```

在 WebUI 中，在 Screening > URL Filtering > Protocol > Websense 页面或 Screening > URL Filtering > Protocol > SurfControl 页面下的相应字段中输入这些设置。

2. 系统级行为参数

接下来将定义应用 URL 过滤时希望系统 (根或 vsys) 采用的行为参数。行为选项如下 :

- **If connectivity to the server is lost:** 如果 NetScreen 设备与 URL 过滤服务器之间的连接丢失，您可以指定 **Block (封锁)** 或 **Permit (允许)** 所有 HTTP 请求。
- **Blocked URL Message Type:** 当 Websense 或 SurfControl 封锁某站点时，用户所接收到的消息源。如果选择 **NetPartners Websense/SurfControl**， NetScreen 设备将转发 Websense 或 SurfControl 服务器的 “block” 响应中接收到的消息。如果选择 **NetScreen**， NetScreen 设备将会发送此前在 NetScreen Blocked URL Message 字段内输入的消息。

  注意 : *如果选择* ***NetScreen****， Websense 提供的一些功能将被禁止，如重定向功能。*

- **NetScreen Blocked URL Message:** 这是封锁某站点后 NetScreen 设备返回给用户的消息。您可以使用从 Websense 或 SurfControl 服务器发来的消息，也可以创建一条要从 NetScreen 设备发送的消息 (最多可为 500 个字符)。

可以使用以下 CLI 命令来配置这些设置 :

```
set url fail-mode { block | permit }
set url type { netScreen | server }
set url message string
```

在 WebUI 中，在 Screening > URL Filtering > Protocol > Websense 页面或 Screening > URL Filtering > Protocol > SurfControl 页面下的相应字段中输入这些设置。

3. 系统级激活

完成配置后，必须在系统级启用 URL 过滤。对于具有多个虚拟系统的 NetScreen 设备而言，必须为要在其中应用 URL 过滤的每个系统启用 URL 过滤。例如，如果希望根系统和某个 vsys 应用 URL 过滤，则必须在根系统和该 vsys 中启用 URL 过滤。

可以使用以下 CLI 命令在系统级激活或禁用 URL 过滤 :

```
set url config { disable | enable }
```

在 WebUI 中，在 Screening > URL Filtering > Protocol > Websense 页面或 Screening > URL Filtering > Protocol > SurfControl 页面下选中或清除 **Enable URL Filtering** 复选框。

当在系统级启用 URL 过滤时，NetScreen 设备会通过将 HTTP 请求重新定向到 Websense 或 SurfControl 服务器来检查要求 URL 过滤的策略 (该系统中定义的) 所要应用到的所有 HTTP 信息流。如果在系统级禁用 URL 过滤，则 NetScreen 设备将忽略策略中的 URL 过滤组件，并将这些策略视为简单的 “允许” 策略。

4. 策略级应用

最后，将配置 NetScreen 设备，使其为每个策略连接 URL 过滤服务器。

可以使用以下 CLI 命令在策略中启用 URL 过滤 :

```
set policy from zone to zone src_addr dst_addr service permit url-filter
```

在 WebUI 中，在策略配置页面下，为要应用 URL 过滤的策略选中 **URL Filter** 复选框。

注意 : *NetScreen 设备可报告 Websense 或 SurfControl 服务器的状态。要更新状态报告，在 WebUI 的 Screening > URL Filtering > Protocol > Websense 页面或 Screening > URL Filtering > Protocol > SurfControl 页面下单击 Server Status 图标。*

范例：URL 过滤配置

在本例中，将配置 NetScreen 设备，使其与 IP 地址为 10.1.2.5、端口号为 62252 (缺省值) 的 SurfControl 服务器协同工作。 URL 过滤服务器位于 Trust 区段中。您要对从 Trust 区段中的主机发往 Untrust 区段中的主机的所有出站 HTTP 信息流执行 URL 过滤。如果 NetScreen 设备失去与 URL 过滤服务器的连接，则您希望 NetScreen 设备允许出站 HTTP 信息流。当 HTTP 客户端请求访问被禁止的 URL 时，您希望 NetScreen 设备发送下列消息：“We’re sorry, but the requested URL is prohibited. If this prohibition appears to be in error, contact ntwksec@mycompany.com.”

Untrust 区段的接口是 ethernet3，其 IP 地址为 1.1.1.1/24。Trust 区段的接口是 ethernet1，其 IP 地址为 10.1.1.1/24。两个区段都位于 trust-vr 路由选择域中。由于该 URL 过滤服务器不在其中任何一个 NetScreen 设备接口的直接子网中，因此将添加一个通过 ethernet1 和 IP 地址为 10.1.1.250 的内部路由器到达该 URL 过滤服务器的路由。

WebUI

1. 接口

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容，然后单击 **Apply**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

输入以下内容，然后单击 **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容，然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. URL 过滤服务器

Screening > URL Filtering > Protocol: 选择 **Redirect (SurfControl)**，然后单击 **Apply**。然后输入以下内容，并再次单击 **Apply**:

Enable URL Filtering: (选择)

Server Name: 10.1.2.5

Server Port: 15868

Communication Timeout: 10 (seconds)

If connectivity to the server is lost … all HTTP requests: Permit

Blocked URL Message Type: NetScreen

NetScreen Blocked URL Message: We’re sorry, but the requested URL is prohibited. Contact ntwksec@mycompany.com.

3. 路由

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 10.1.2.0/24

Gateway: (选择)

Interface: ethernet1

Gateway IP Address: 10.1.1.250

4. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: HTTP

Action: Permit

URL Filtering: (选择)

CLI

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. URL 过滤服务器

```
set url protocol type scfp
set url server 10.1.2.5 15868 10
set url fail-mode permit
set url type NetScreen
set url message "We're sorry, but the requested URL is prohibited. Contact
    ntwksec@mycompany.com."
set url config enable
```

3. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set vrouter trust-vr route 10.1.2.0/24 interface ethernet1 gateway 10.1.1.250
```

4. 策略

```
set policy from trust to untrust any any http permit url-filter
save
```

5

深入检查

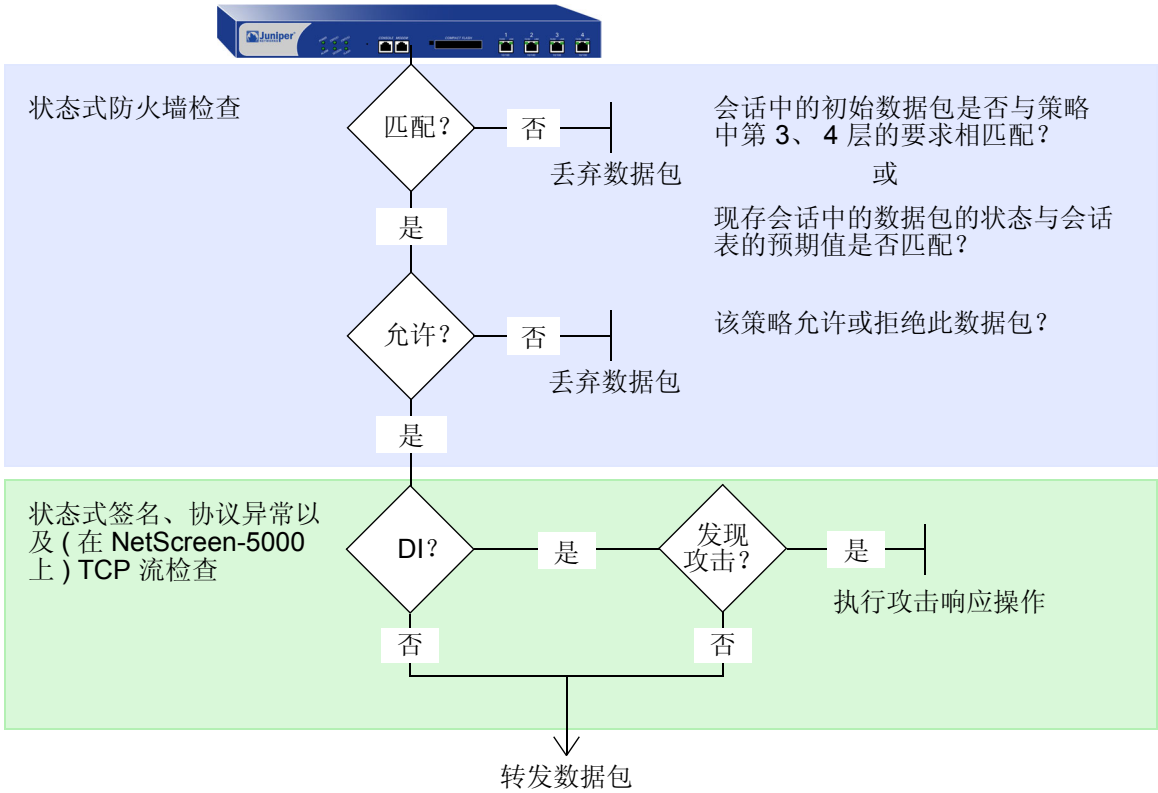
您可以在策略中启用 “深入检查” (DI)，以检查允许的信息流，并且在 ScreenOS 中的 DI 模块发现攻击签名或协议异常时采取措施。本章的以下部分介绍策略中的 “深入检查” 元素，并说明如何配置它们：

也可以在安全区段级为 HTTP 组件启用 “深入检查”。本章最后一节介绍 SCREEN 选项。

- 第 201 页上的 “精确封锁 HTTP 组件”
  - 第 201 页上的 “ActiveX 控件”
  - 第 202 页上的 “Java Applet”
  - 第 202 页上的 “EXE 文件”
  - 第 202 页上的 “ZIP 文件”

深入检查概述

“深入检查” (DI) 是过滤 NetScreen 防火墙允许的信息流的机制。“深入检查”检查第 3、 4 层数据包包头和第 7 层应用内容和协议特征，以便检测和防止可能出现的任何攻击或异常行为[1]。



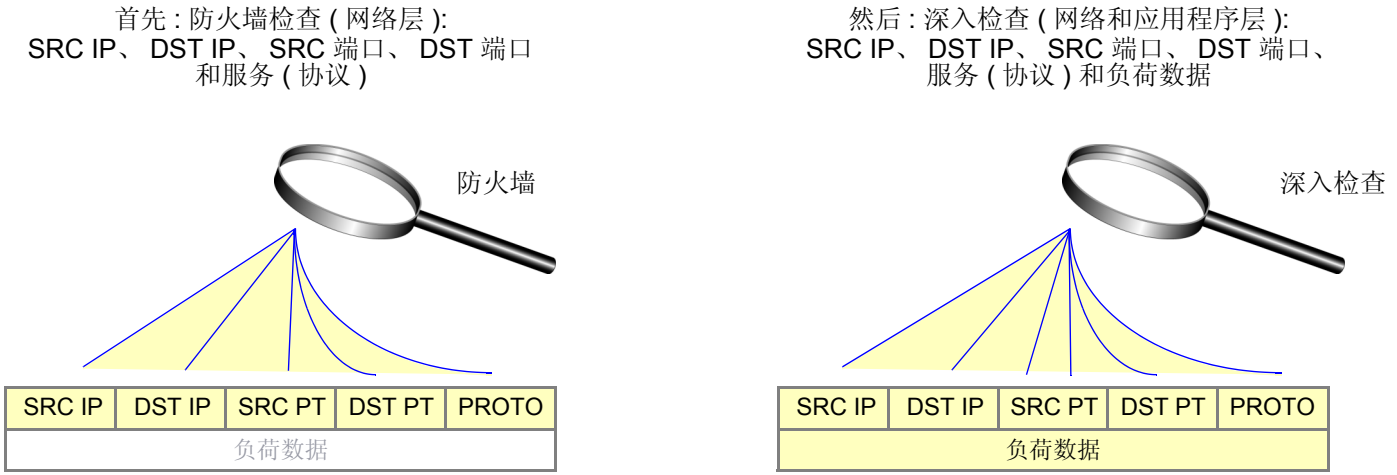
当 NetScreen 设备接收到会话的第一个数据包时，将检查 IP 数据包包头中的源和目标 IP 地址 (第 3 层检查)，并检查 TCP 片段或 UDP 数据报报头中的源和目标端口号与协议 (第 4 层检查)。如果第 3 层和第 4 层组件与策略中指定

1. NetScreen 设备通过在区段级 (而非策略级) 设置的 SCREEN 选项，来检测第 3 层和第 4 层 (IP 和 TCP) 的异常信息流模式。第 8 页上的 “IP 地址扫描”、第 10 页上的 “端口扫描”和第 49 页上的 “网络 DoS 攻击”中介绍的各种泛滥攻击都是 IP 和 TCP 信息流异常检测的范例。

的标准相匹配，则 NetScreen 设备将对该数据包执行指定的动作 — permit、 deny 或 tunnel[2]。当接收到已建立的会话的数据包时， NetScreen 设备会将该数据包与会话表中维护的状态信息进行比较，以确定其是否确实属于该会话。

如果您在应用到此数据包上的策略中启用了 “深入检查”，并且策略动作是 “permit”或 “tunnel”，则 NetScreen 设备将进一步检查该数据包及其关联的数据流中的攻击。设备将扫描数据包以检查与一个或多个攻击对象组中定义的模式相匹配的模式。攻击对象可以是攻击签名或协议异常，您可以自行定义它们，也可将它们从攻击对象数据库服务器下载到 NetScreen 设备中[3]。(有关详细信息，请参阅第 145 页上的 “攻击对象和组”和第 181 页上的 “定制攻击对象和组”。) 根据策略中指定的攻击对象， NetScreen 设备可能会执行下列检查 :

- 检查包头值和负载数据中的状态式攻击签名
- 将所传送协议的格式与该协议的 RFC 和 RFC 扩展中指定的标准相比较，以确定是否可能有人出于恶意而将其改变



2. 如果指定的动作是 tunnel，则暗指允许概念。注意，如果您在动作为 tunnel 的策略中启用 “深入检查” (DI)，则 NetScreen 设备将在加密出站数据包之前和解密入站数据包之后执行指定的 DI 操作。
3. 您需要先预订服务，之后才能从攻击对象数据库服务器下载攻击对象。有关详细信息，请参阅第 **2**-439 页上的 “预定服务的注册与激活”。

如果 NetScreen 设备检测到攻击，将执行为匹配的攻击对象所属的攻击对象组指定的动作 : close、 close-client、close-server、drop、drop-packet、ignore 或 none。如果未发现攻击，将转发数据包。(有关攻击操作的详细信息，请参阅第 158 页上的 “攻击操作”。)

从概念上讲，可以将 **set policy** 命令分为两部分 — 核心部分和 DI 组件 :

- 核心部分包含源和目标区段、源和目标地址、一个或多个服务以及动作[4]。
- DI 组件指示 NetScreen 设备 : 检查策略的核心部分所允许的信息流，以查找与一个或多个攻击对象组中的攻击对象相匹配的模式。如果 NetScreen 设备检测到攻击对象，将执行为相应组所定义的动作。

以下的 **set policy** 命令包含一个 DI 组件 :

以上命令指示 NetScreen 设备 : 允许从 Untrust 区段中的任何地址发送到 DMZ 区段中的目标地址 “websrv1” 的 HTTP 信息流。同时指示 NetScreen 设备检查该策略允许的所有 HTTP 信息流。如果信息流中的任一模式与攻击对象组 “HIGH:HTTP:ANOM” 中定义的某一攻击对象匹配，则 NetScreen 设备将丢弃数据包并发送 TCP RST 通知给源和目标地址处的主机，从而关闭连接。

4. 也可以向 **set policy** 命令的核心组件添加其它扩展信息 : VPN 和 L2TP 通道引用、时间表引用、地址转换规范、用户认证规范、防病毒检查、日志记录、计数、信息流管理设置，等等。尽管这些扩展信息是可选的，但策略的核心组成元素 — 源与目标区段、源与目标地址、服务和动作 — 是必需的。(全局策略是一个例外，这种策略中不指定源和目标区段 : **set policy global *src_addr dst_addr service action***。有关全局策略的详细信息，请参阅第 **2** -297 页上的 “全局策略”。)

可以通过使用 ID 号来输入现有策略的环境。例如：

```
ns-> set policy id 1
ns(policy:1)->
```

注意：命令提示符发生了变化，表明后续命令将位于特定策略环境内。

如果要输入与单个策略相关的几个命令，则输入策略环境将会很方便。例如，下面的一组命令将创建一个策略，允许从 Untrust 区段中的任何地址发出的 HTTP 和 HTTPS 信息流发送到 DMZ 区段中的 websrv1 和 websrv2，并查找高级和关键的 HTTP 状态式签名和协议异常攻击：

```
ns-> set policy id 1 from untrust to dmz any websrv1 http permit attack
    CRITICAL:HTTP:ANOM action close
ns-> set policy id 1
ns(policy:1)-> set dst-address websrv2
ns(policy:1)-> set service https
ns(policy:1)-> set attack CRITICAL:HTTP:SIGS action close-server
ns(policy:1)-> set attack HIGH:HTTP:ANOM action drop
ns(policy:1)-> set attack HIGH:HTTP:SIGS action close-server
ns(policy:1)-> exit
ns-> save
```

以上配置同时允许 HTTP 和 HTTPS 信息流，但只查找 HTTP 信息流中的攻击。为了能够向策略环境中添加攻击对象组，必须首先在顶级命令中指定 DI 攻击和动作。在上例中，可以添加 CRITICAL:HTTP:SIGS、HIGH:HTTP:ANOM 和 HIGH:HTTP:SIGS 攻击对象组，因为您首先配置了对 CRITICAL:HTTP:ANOM 组进行 “深入检查” 的策略。

注意：可以对策略中的每个攻击对象组指定不同的攻击操作。如果 NetScreen 设备同时检测到了多个攻击，将应用最严重的动作，即上例中的 “关闭”。有关七个攻击动作的信息 (包括它们的严重性级别)，请参阅第 158 页上的 “攻击操作”。

攻击对象数据库服务器

攻击对象数据库包含所有预定义的攻击对象，按照协议和严重性级别编组为攻击对象组。 Juniper Networks 在位于 https://services.netscreen.com/restricted/sigupdates 的服务器上存储攻击对象数据库。为了使用预定义的攻击对象，必须从该服务器下载数据库，将其加载到 NetScreen 设备中，然后在策略中引用特定的攻击对象组[5]。如要获得对攻击对象数据库服务器的访问权限，首先必须为 NetScreen 设备预订 DI 签名服务。 (有关如何执行此项操作的信息，请参阅第 **2** -439 页上的 “预定服务的注册与激活”。)

***注意：** 下载攻击对象数据库时可以加载认证证书 (imagekey.cer) 以验证攻击对象数据库的完整性。请参阅第 **2** -425 页上的 “认证固件和 DI 文件”。*

可通过四种方式来更新数据库 :

- **Immediate Update:** 对于此选项，将用攻击对象数据库服务器上存储的数据库立即更新 NetScreen 设备上的攻击对象数据库。为了执行此操作，必须首先配置攻击对象数据库服务器设置。 (有关具体范例，请参阅第 138 页上的 “范例 : 立即更新”。)

  ***注意：** 在执行数据库立即更新之前，可以使用 **exec attack-db check** 命令来检查服务器上的攻击对象数据库是否比 NetScreen 设备上的攻击对象数据库更新一些。*

- **Automatic Update:** 对于此选项，如果服务器上的数据库版本比先前在 NetScreen 设备上加载的数据库版本更新，则 NetScreen 设备将在用户预定的时间下载攻击对象数据库。 Juniper Networks 定期用新发现的攻击模式更新数据库。鉴于数据库不断地发生变化，因此也要求您定期更新 NetScreen 设备上的数据库。为了执行此操作，必须首先配置攻击对象数据库服务器设置。(有关具体范例，请参阅第 140 页上的 “范例 : 自动更新”。)
- **Automatic Notification and Immediate Update:** 对于此选项， NetScreen 设备在用户预定的时间检查攻击对象数据库服务器上的数据是否比 NetScreen 设备上的数据更新。如果服务器上的数据更新一些，则在您登录到 NetScreen 设备后，会在 WebUI 和 CLI 的主页上出现一个通知。然后可输入 **exec attack-db update** 命令，或在 WebUI 的 Configuration > Update > Attack Signature 页面中单击 **Update Now** 按钮，以将服务器上的数据库保存到 NetScreen 设备中。为使检查服务器的半自动操作过程起作用，首先必须配置攻击对象数据库服务器设置。 (有关具体范例，请参阅第 141 页上的 “范例 : 自动通知和立即更新”。)

5. 也可以使用 NetScreen-Security Manager 下载攻击对象数据库。有关该操作的信息，请参阅 *NetScreen-Security Manager Administration Guide*。

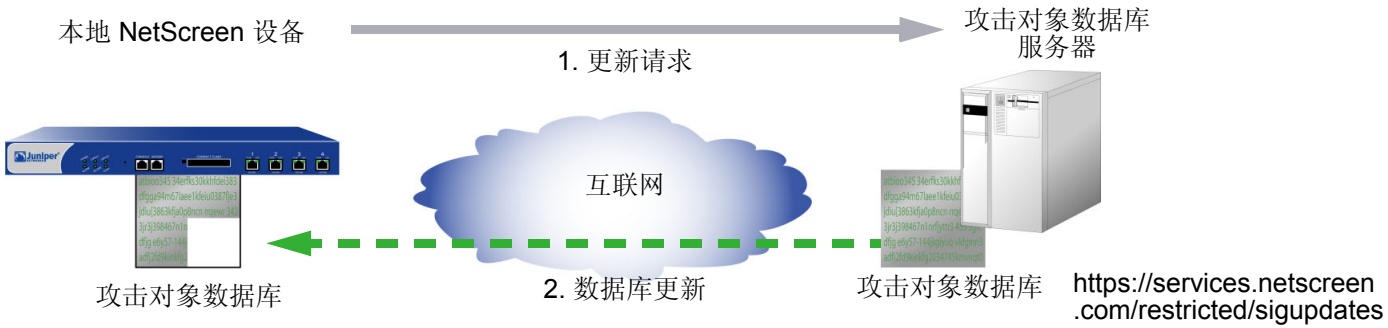
- **Manual Update:** 对于此选项，首先使用 Web 浏览器将攻击对象数据库下载到本地目录或 TFTP 服务器目录中。然后可使用 WebUI (从本地目录) 或 CLI (从 TFTP 服务器目录) 在 NetScreen 设备上加载数据库。(有关具体范例，请参阅第 143 页上的 “范例 : 手动更新”。)

范例 : 立即更新

在本例中，将攻击对象数据库服务器中的攻击对象数据库 (attacks.bin 文件) 立即保存到 NetScreen 设备中。将使用缺省的 URL: https://services.netscreen.com/restricted/sigupdates。不必为数据库服务器设置此 URL。在缺省情况下， NetScreen 设备使用此 URL。

将不设置时间表来更新 NetScreen 设备上的数据库。而是将服务器上的数据库直接保存到 NetScreen 设备中。

注意 : *此范例假定您已经为 NetScreen 设备获得并激活了对 DI 签名服务的预订。(有关预订的信息，请参阅第 **2**-439 页上的 “预定服务的注册与激活”。)*



WebUI

Configuration > Update > Attack Signature: 单击 **Update Now** 按钮。

CLI

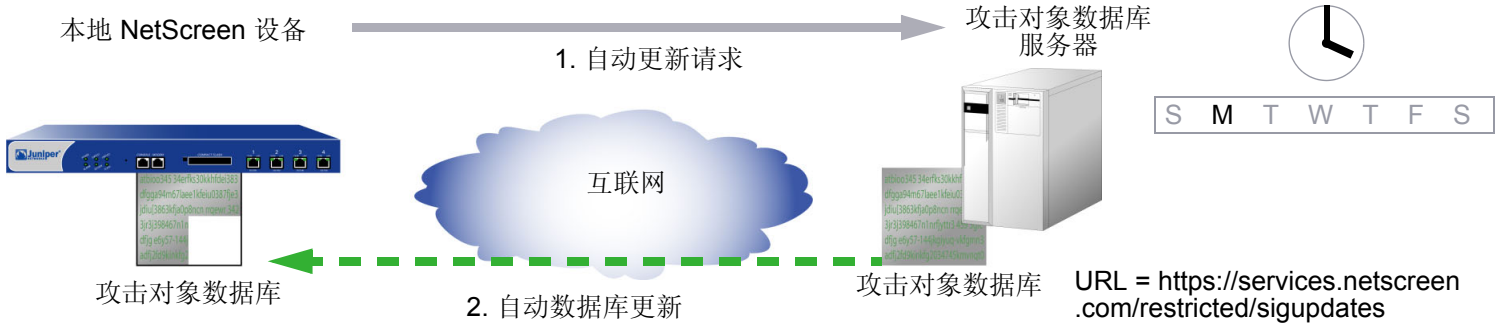
```
ns-> exec attack-db update
Loading attack database.............
Done.
Done.
Switching attack database...Done
Saving attack database to flash...Done.
ns->
```

范例：自动更新

在本例中，将设置一个时间表，使得每星期一 04:00 更新 NetScreen 设备上的数据库。在到达该预定时间时，NetScreen 设备将服务器上的数据库版本与 NetScreen 设备上的数据库版本进行比较。如果服务器上的版本比 NetScreen 设备上的版本更新，则 NetScreen 设备自动用较新版本替代其数据库。

> ***注意：****此范例假定您已经为 NetScreen 设备获得并激活了对 DI 签名服务的预订。（有关预订的信息，请参阅第* ***2****-439 页上的“预定服务的注册与激活”。）*

将使用缺省的 URL: https://services.netscreen.com/restricted/sigupdates。不必为数据库服务器设置此 URL。在缺省情况下， NetScreen 设备使用此 URL。



WebUI

Configuration > Update > Attack Signature: 输入以下内容，然后单击 **OK**:

Database Server: (保留空白)
Update Mode: Automatic Update
Schedule:
Weekly on: Monday[6]
Time (hh:mm): 04:00

6. 如果您计划每月更新一次，而在某个月份中并没有您所要选择的日期 (例如，某些月份中没有 31 号)，则 NetScreen 设备将在该月使用可能的最后日期。

CLI

```
set attack db mode update
set attack db schedule weekly monday 04:00
save
```

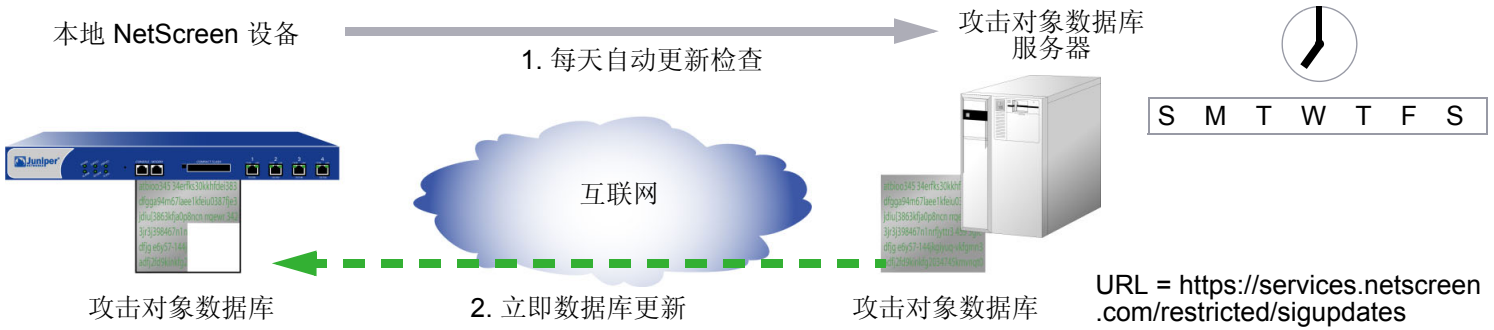
范例：自动通知和立即更新

在本例中，将设置时间表，使得每天 07:00 检查 NetScreen 设备上的数据库。

当您接收到服务器上的数据库已更新的通知时，单击 WebUI 的 Configuration > Update > Attack Signature 页面上的 **Update Now** 按钮，或输入 **exec attack-db update** 命令，以将服务器上的数据库保存到 NetScreen 设备中。

***注意：**此范例假定您已经为 NetScreen 设备获得并激活了对 DI 签名服务的预订。（有关预订的信息，请参阅第 **2**-439 页上的“预定服务的注册与激活”。）*

将使用缺省的 URL: https://services.netscreen.com/restricted/sigupdates。不必为数据库服务器设置此 URL。在缺省情况下， NetScreen 设备使用此 URL。



WebUI

1. 预定的数据库检查

   Configuration > Update > Attack Signature: 输入以下内容，然后单击 **OK**:

   Database Server: (保留空白)
   Update Mode: Automatic Notification
   Schedule:
   Daily
   Time (hh:mm): 07:00

2. 立即数据库更新

   当您接收到一个通知，指出服务器上的攻击数据库比 NetScreen 设备上的数据库更新时，请执行下列操作：

   Configuration > Update > Attack Signature: 单击 **Update Now** 按钮。

CLI

1. 预定的数据库检查

```
set attack db mode notification
set attack db schedule daily 07:00
```

2. 立即数据库更新

   当您接收到一个通知，指出服务器上的攻击数据库比 NetScreen 设备上的数据库更新时，请执行下列操作：

```
exec attack-db update
```

范例：手动更新

在本例中，将手动把最新的攻击对象数据库保存到本地目录“C:\netscreen\attacks-db”（如果要使用 WebUI 加载数据库）或“C:\Program Files\TFTP Server”（如果要使用 CLI 加载数据库）。然后从本地目录加载数据库到 NetScreen 设备上[7]。

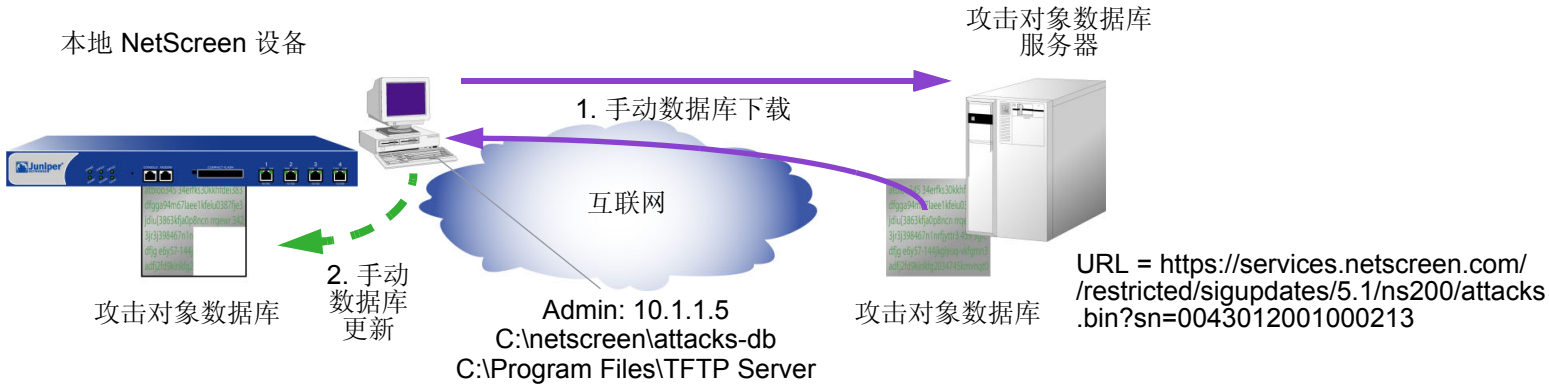
对于自动更新， NetScreen 设备将自动向 URL 添加下列元素：

- NetScreen 设备的序列号
- 设备上运行的 ScreenOS 的主版本号
- 平台类型

当您手动更新数据库时，必须自行添加这些元素。在本例中，序列号是 0043012001000213， ScreenOS 版本是 5.1，平台是 NetScreen-208 (ns200)。因此，产生的 URL 是：

https://services.netscreen.com//restricted/sigupdates/5.1/ns200/attacks.bin?sn=0043012001000213

***注意：**此范例假定您已经为 NetScreen 设备获得并激活了对 DI 签名服务的预订。（有关预订的信息，请参阅第 **2**-439 页上的“预定服务的注册与激活”。）*



7. 在下载攻击对象数据库后，也可以将其发送到本地服务器上并进行设置，以便其它 NetScreen 设备进行访问。然后其它设备的 admin 必须将数据库服务器 URL 更改为此新位置的 URL。他们可以在 Configuration > Update > Attack Signature 页面上的 Database Server 字段中输入新 URL，也可使用以下 CLI 命令：**set attack db server** *url_string*。

1. 数据库下载

在 Web 浏览器的地址字段中输入下列 URL:

https://services.netscreen.com//restricted/sigupdates/5.1/ns200/attacks.bin?sn=0043012001000213

将 *attacks.bin* 保存到本地目录 “C:\netscreen\attacks-db” (如果要通过 WebUI 加载)，或者保存到 TFTP 服务器目录 “C:\Program Files\TFTP Server” (如果要使用 CLI 加载)。

WebUI

2. 数据库更新

Configuration > Update > Attack Signature: 输入以下内容，然后单击 **OK**:

Deep Inspection Signature Update:

Load File: 输入 **C:\netscreen\attacks-db\attacks.bin**，或单击 **Browse** 以找到该目录，选择 **attacks.bin**，然后单击 **Open**。

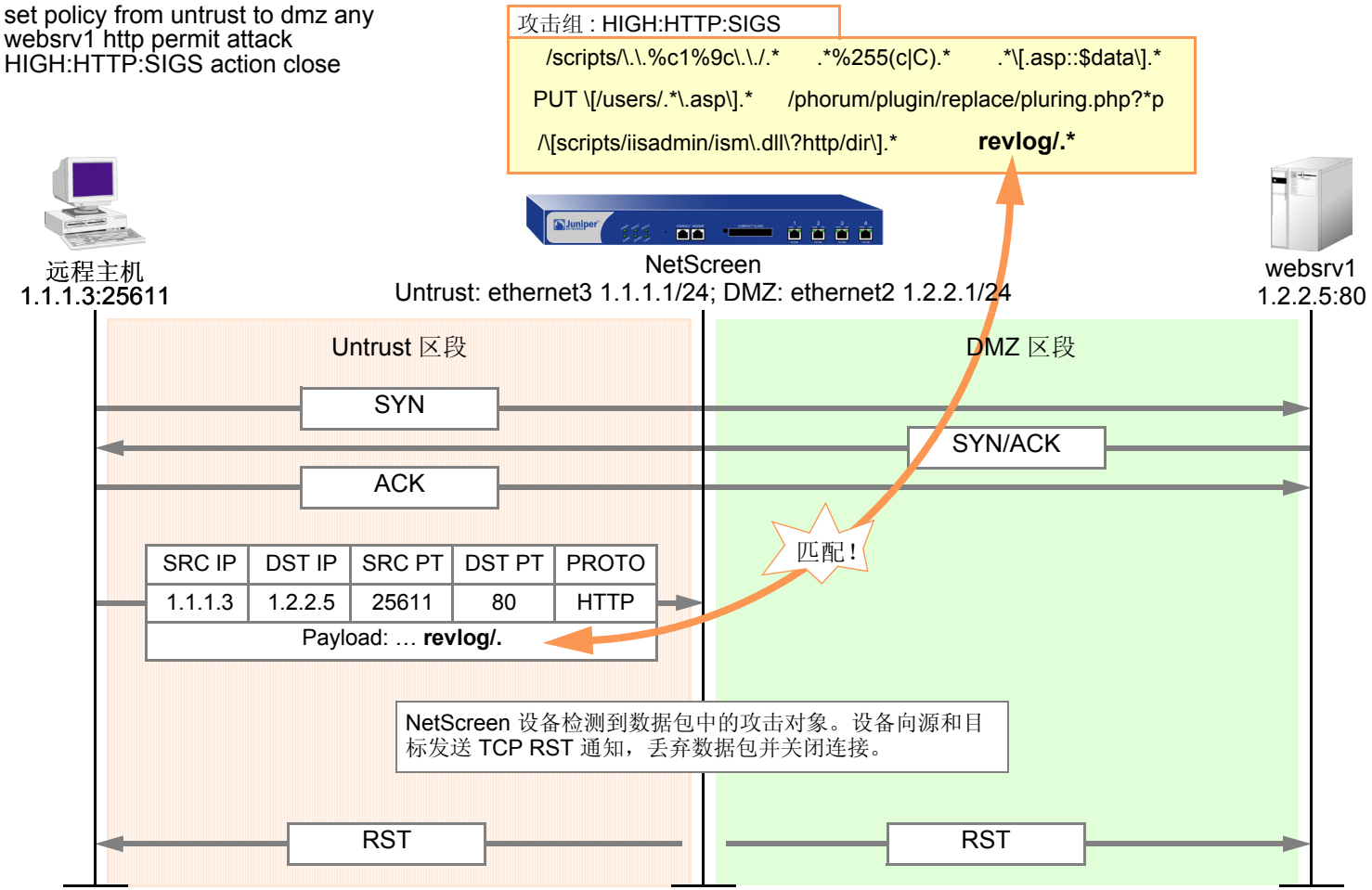
CLI

2. 数据库更新

```
save attack-db from tftp 10.1.1.5 attacks.bin to flash
```

攻击对象和组

攻击对象是一些状态式签名、流式签名 (在 NetScreen-5000 系列上) 和协议异常， NetScreen 设备使用它们来检测旨在破坏网络上的一个或多个主机的攻击。攻击对象先按照协议类型再按照严重性编排成组。当您将 “深入检查” (DI) 添加到策略时，对于与所引用的攻击对象组中的模式相匹配的任何模式， NetScreen 设备将检查该策略允许的信息流。



策略的 DI 组件中所引用的攻击对象组必须以策略允许的同一服务类型作为目标。例如，如果策略允许 SMTP 信息流，则攻击对象组必须以针对 SMTP 信息流的攻击为目标。以下策略举例说明有效的配置：

```
set policy id 2 from trust to untrust any any smtp permit attack CRIT:SMTP:SIGS
    action close
```

下一个策略是错误的，因为该策略允许 SMTP 信息流，但攻击对象组却用于 POP3 信息流：

```
set policy id 2 from trust to untrust any any smtp permit attack CRIT:POP3:SIGS
    action close
```

第二个策略的配置是错误的，如果执行该策略，将使 NetScreen 设备消耗不必要的资源，来检查 SMTP 信息流中永远也不可能找到的 POP3 攻击对象。如果策略 2 同时允许 SMTP 和 POP3 信息流，则可以配置 DI 组件来检查 SMTP 攻击对象和 / 或 POP3 攻击对象。

```
set group service grp1
set group service grp1 add smtp
set group service grp1 add pop3
set policy id 2 from trust to untrust any any grp1 permit attack
    CRIT:SMTP:SIGS action close
set policy id 2 attack CRIT:POP3:SIGS action close
```

支持的协议

对于以下协议和应用程序，“深入检查”模块支持状态式签名攻击对象和协议异常攻击对象：

基本网络协议

协议	状态式签名	协议异常	定义
DNS	是	是	域名系统 (DNS) 是用于将域名转换为 IP 地址的数据库系统，例如 www.juniper.net = 207.17.137.68。
FTP	是	是	“文件传输协议” (FTP) 是用于在网络上的计算机间交换文件的协议。
HTTP	是	是	“超文本传输协议”(HTTP) 是主要用于从 Web 服务器向 Web 客户端传输信息的协议。
IMAP	是	是	“互联网邮件访问协议” (IMAP) 是可提供内向电子邮件存储和检索服务的协议，用户可使用其所带的选项下载他们的电子邮件或者将电子邮件留在 IMAP 服务器上。
NetBIOS	是	是	NetBIOS (网络基本输入输出系统) 是一个应用程序接口，它允许用户工作站上的应用程序访问网络传输 (例如 NetBEUI、SPX/IPX 和 TCP/IP) 所提供的网络服务。
POP3	是	是	“邮局协议版本 3” (POP3) 是可提供内向电子邮件存储和检索服务的协议。
SMTP	是	是	“简单邮件传输协议” (SMTP) 是用于在邮件服务器之间传输电子邮件的协议。

即时消息应用程序

协议	状态式签名	协议异常	定义
AIM	是	是	America Online Instant Messaging (AIM) 是 “美国在线” 的即时消息应用程序。
MSN Messenger	是	是	Microsoft Network Messenger (MSN Messenger) 是微软提供的即时消息服务。
Yahoo! Messenger	是	是	Yahoo! Messenger 是 Yahoo! 提供的即时消息服务。

对等连接 (P2P) 网络应用程序[8]

协议	状态式签名	协议异常	定义
BitTorrent	是	否	BitTorrent 是一个 P2P 文件发布工具，可使下载文件的每个人将文件上传给其他人，从而提供了一种将同一文件发布给一个大型群组的有效方式。
DC (Direct Connect)	是	否	DC (Direct Connect) 是一个 P2P 文件共享应用程序。 DC 网络使用集线器来连接用户组，经常要求它们共享一定数量的字节或文件。通过为所连接的用户创建小型公共组，许多集线器可以对所需的特定区域起作用。
eDonkey	是	否	eDonkey 是使用 “多源文件传输协议” (MFTP) 的分散式 P2P 文件共享应用程序。eDonkey 网络支持两种应用程序 : 客户端和服务器。客户端连接到网络并共享文件。服务器对客户端起会聚集线器的作用。
Gnutella	是	是	Gnutella 是没有任何集中服务器的 P2P 文件共享协议和应用程序。有一些使用 Gnutella 协议的其它应用程序，例如 BearShare、 Limewire、 Morpheus 和 ToadNode。

协议	状态式签名	协议异常	定义
KaZaa	是	否	KaZaa 是使用 FastTrack 协议的分散式 P2P 文件共享应用程序。 KaZaa 主要用于共享 MP3 文件。
MLdonkey	是	否	MLdonkey 是一个 P2P 客户端应用程序，它可以运行在多个平台上，并可访问多个 P2P 网络，例如 BitTorrent、 DC、eDonkey、 FastTrack (KaZaa 及其它) 以及 Gnutella 和 Gnutella2。
Skype	是	否	Skype 是一个免费 P2P 互联网电话服务，它允许用户通过 TCP/IP 网络 (例如互联网) 互相交谈。
SMB	是	是	SMB (服务器消息块) 是用于在计算机间共享诸如文件和打印机等资源的协议。 SMB 运行在 NetBIOS 协议的顶层。
WinMX	是	否	WinMX 是一个 P2P 文件共享应用程序，它允许客户端同时与多个服务器相连。

应用程序层网关 (ALG)

协议	状态式签名	协议异常	定义
MSRPC	是	是	MSRPC (Microsoft 远程过程调用) 是一种用于在远程计算机上运行进程的机制。

8. 许多列出的 P2P 应用程序使用它们自己的专有协议。

如果 NetScreen 设备拥有对 http://help.juniper.net/sigupdates/english 的访问权限，则可以看到所有预定义攻击对象组的内容和预定义攻击对象的说明。打开 Web 浏览器，并在 “地址”栏中输入下列 URL 之一：

http://help.juniper.net/sigupdates/english/AIM.html

http://help.juniper.net/sigupdates/english/DNS.html

http://help.juniper.net/sigupdates/english/FTP.html

http://help.juniper.net/sigupdates/english/GNUTELLA.html

http://help.juniper.net/sigupdates/english/HTTP.html

http://help.juniper.net/sigupdates/english/IMAP.html

http://help.juniper.net/sigupdates/english/MSN.html

http://help.juniper.net/sigupdates/english/NBDS.html

http://help.juniper.net/sigupdates/english/NBNAME.html

http://help.juniper.net/sigupdates/english/POP3.html

http://help.juniper.net/sigupdates/english/SMTP.html

http://help.juniper.net/sigupdates/english/MSRPC.html

http://help.juniper.net/sigupdates/english/SMB.html

http://help.juniper.net/sigupdates/english/YMSG.html

以上每个 URL 都可链接到 HTML 页面，该页面中包含适用于特定协议的预定义攻击对象的列表 — 按照严重性编成组。要查看某个攻击对象的说明，请单击其名称。

状态式签名

攻击签名是当特定攻击正在进行时的模式[9]。该签名可以是第 3 层或第 4 层信息流模式，例如当某个地址发送很多数据包到位于另一个地址处的不同端口号时 (请参阅第 10 页上的 “端口扫描”)；也可以是文本模式，例如当恶意 URL 字符串出现在单个 HTTP 或 FTP 数据包的数据负荷中时。该字符串也可以是特殊的代码段或数据包包头中的特定值。但是，在搜索文本模式时， NetScreen 设备中的 “深入检查” (DI) 模块不仅查找数据包中的签名，也在数据包的特定部分中查找该签名 (即便是数据包碎片或片段)，在会话生存期内的特定时间发送的数据包内查找签名，以及在由连接发起方或响应方发送的数据包内查找签名。

当检查文本模式时，DI 模块会将参与者的角色视为客户端或服务器，并监控会话的状态，从而缩小搜索范围，只搜索与攻击者使用模式的攻击相关的那些元素。通过使用上下文信息来改进数据包检查可以大大减少错误的警报 (或 “主动错误信息”)，并避免不必要的处理。术语 “状态式签名” 是指在参与者的角色和会话状态的环境内查找签名。

欲了解考虑出现签名的环境的优点，在启用 NetScreen DI 模块以检测 EXPN Root 攻击时，请注意该模块检查数据包的方式。攻击者使用 EXPN Root 攻击来扩展和暴露邮件服务器上的邮寄列表。为了检测 EXPN Root 攻击，NetScreen 设备在 “简单邮件传输协议” (SMTP) 会话的控制部分中搜索签名 “expn root”。NetScreen 设备只检查控制部分，因为这是唯一可能会发生攻击的部分。如果 “expn root” 出现在会话的任何其它部分，则不是一个攻击。

通过使用简单的文本数据包签名检测技术，即使签名 “expn root” 出现在 SMTP 连接的数据部分 (即电子邮件消息的正文中)，该签名也可以触发警报。例如，如果您正在给同事写关于 EXPN Root 攻击的邮件，则单个数据包签名检测器会将此邮件视为攻击。通过使用状态式签名， NetScreen DI 模块可以区分预示攻击的文本字符串和无害的字符串。

***注意：** 对于拥有预定义状态式签名攻击对象的协议列表，请参阅第 147 页上的 “支持的协议”。*

9. 由于 NetScreen DI 模块支持规则表达式，因此可在搜索模式时使用通配符。这样，单个攻击签名定义可以适用于多种攻击模式的变体。有关规则表达式的信息，请参阅第 182 页上的 “规则表达式”。

TCP 流式签名

和状态式签名一样， TCP 流式签名是当攻击正在进行时存在的模式。但是，当检查信息流中的状态式签名时， DI 模块只在特定上下文内搜索。当 DI 模块检查信息流中的 TCP 流式签名时，不考虑上下文。两种类型签名的另一个区别是：尽管状态式签名既可以是预定义的也可以是用户定义的，而 TCP 流式签名必须是用户定义的。当您将流式签名攻击对象添加到攻击对象组后，即可在应用 “深入检查” 的策略中引用该组。 (有关 TCP 流式签名的更多信息，请参阅第 189 页上的 “TCP 流式签名攻击对象”。)

***注意：** 只能在 NetScreen-5000 系列系统上定义 TCP 流式签名。*

协议异常

搜索协议异常的攻击对象检测与 RFC 和通用 RFC 扩展中定义的标准有偏差的信息流。对于签名攻击对象，必须使用预定义的模式或创建新模式；因此，它们只能检测已知的攻击。当捕捉新攻击或不能用文本模式定义的攻击时，协议异常检测特别有用。

***注意：** 有关具有预定义协议异常攻击对象的协议列表，请参阅第 147 页上的 “支持的协议”。*

攻击对象组

预定义的攻击对象组包含用于特定协议的攻击对象。对于每个协议，这些组均被分成协议异常和状态式签名，然后粗略地按照严重性加以分组。三个攻击对象组严重性级别分别为关键、高级和中级：

Critical (关键): 包含与试图躲避检测、导致网络设备崩溃或获得系统级访问权限的攻击相匹配的攻击对象。

High (高级): 包含与下述攻击相匹配的攻击对象：试图破坏服务、获得对网络设备的用户级访问权限或者激活之前在设备上加载的特洛伊木马程序。

Medium (中级): 包含与下述攻击相匹配的攻击对象：检测试图通过目录浏览或信息漏洞来访问关键信息的侦查尝试。

Low (低级): 包括与试图获取非关键信息或用扫描工具扫描网络的攻击相匹配的攻击对象。

Info (信息): 包括与正常的无害信息流相匹配的攻击对象，该信息流包括 URL、 DNS 查找失败、 SNMP 公共组字符串和对等连接 (P2P) 参数。可以使用信息攻击对象来获取有关您的网络的信息。

更改严重性级别

尽管攻击对象组是按照协议和严重性级别 (critical、 high、 medium) 进行分类的，但每个攻击对象都有其自身特定的严重性级别：critical、 high、 medium、 low、 info。这些攻击对象严重性级别可映射到事件日志条目严重性级别，如下所示：

攻击对象 严重性级别	– 映射到 –	事件日志条目 严重性级别
Critical (关键)		Critical
High (高级)		Error
Medium (中级)		Warning
Low (低级)		Notification
Info (信息)		Information

例如，如果 NetScreen 设备检测到某个攻击的严重性级别为 “Medium”，则事件日志中的相应条目的严重性级别将为 “Warning”。

可以覆盖策略中引用的一个或多个攻击对象组中的所有攻击对象的缺省严重性级别。可通过以下方式在策略级别执行此项操作：首先输入现有策略的环境，然后再为该策略所引用的所有攻击对象组分配新的严重性级别。

下面介绍如何通过 WebUI 和 CLI 更改策略中所引用的攻击对象组的严重性级别：

WebUI

Policies > Edit (对于现有的策略): 执行以下操作，然后单击 **OK**:

> Deep Inspection: 在 Severity 下拉列表中选择一个严重性选项，然后单击 **OK**。

CLI

```
ns-> set policy id number
ns(policy:number)-> set di-severity { info | low | medium | high | critical }
```

如要将每个攻击对象的严重性级别恢复为其原始设置，可再次输入策略环境，并执行以下任一操作：

WebUI

Policies > Edit (对于现有的策略): 执行以下操作，然后单击 **OK**:

> Deep Inspection: 在 Severity 下拉列表中选择 **Default**，然后单击 **OK**。

CLI

```
ns-> set policy id number
ns(policy:number)-> unset di-severity
```

范例：针对 P2P 的深入检查

在本例中，允许 Trust 区段中的任何主机使用 HTTP、DNS 和 Gnutella 服务发起与 Untrust 区段中的任何主机之间的对等连接 (P2P) 会话[10]。然后将“深入检查”(DI) 应用到所允许的信息流，检查以下攻击对象组中定义的状态式签名和协议异常：

- INFO:DNS:SIGS
- INFO:GNUTELLA:ANOM
- INFO:HTTP:SIGS

如果 NetScreen 设备检测到签名或异常行为，将中断连接并向客户端发送 TCP RST 以关闭会话。在缺省情况下，还将启用记录任何被发现的攻击。

注意：*有关 NetScreen 设备可以执行的各种攻击动作的信息，请参阅第 158 页上的“攻击操作”。有关记录检测到的攻击的信息，请参阅第 170 页上的“攻击记录”。*

WebUI

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: DNS

> 单击 **Multiple**，选择 **GNUTELLA** 和 **HTTP**，然后单击 **OK** 返回基本策略配置页。

Action: Permit

10. 出于安全方面的考虑，不定义这样一个策略：允许 Untrust 区段中的任何主机发起与 Trust 区段中的主机之间的 P2P 会话。

> 单击 **Deep Inspection**，输入以下内容，单击 **Add** 以输入每个攻击对象组，然后单击 **OK** 返回基本策略配置页：

Severity: Default
Group: INFO:DNS:SIGS
Action: Close Client
Log: (选择)
Severity: Default
Group: INFO:GNUTELLA:ANOM
Action: Close Client
Log: (选择)
Severity: Default
Group: INFO:HTTP:SIGS
Action: Close Client
Log: (选择)

CLI

```
set policy id 1 from trust to untrust any any dns permit attack
INFO:DNS:SIGS action close-client[11]
set policy id 1
ns(policy:1)-> set service gnutella
ns(policy:1)-> set service http
ns(policy:1)-> set attack INFO:GNUTELLA:ANOM action close-client
ns(policy:1)-> set attack INFO:HTTP:SIGS action close-client
ns(policy:1)-> exit
save
```

11. 由于在缺省情况下将启用记录检测到的攻击，所以不必通过 CLI 命令对记录进行指定。

禁用攻击对象

当在策略中引用了一个攻击对象组时，NetScreen 设备将检查策略应用到的信息流，查找与该组中的任何攻击对象相匹配的模式。某些时候，如果某个特定攻击对象反复产生主动错误信息 (即错误地将合法信息流解释为攻击)，您可能不想使用该攻击对象。如果问题是由于定制的攻击对象所导致的，则只需从其定制的攻击对象组中删除该攻击对象即可。不过，您无法删除预定义攻击对象组中的预定义攻击对象。在该情况下，最好的方法就是禁用该对象。

注意 : 预定义攻击对象仅在禁用它的根系统或虚拟系统 (vsys) 中被禁用。例如，在根系统中禁用预定义攻击对象并不会自动在任何虚拟系统中禁用它。同样，在一个 vsys 中禁用某个攻击对象也不会影响任何其它 vsys 中的该对象。

注意 : *禁用攻击对象不会改善吞吐量性能。*

要禁用某个攻击对象，请执行下列操作之一 :

WebUI

Objects > Attacks > Predefined: 在要禁用的攻击对象的 Configure 栏中，清除复选框。

CLI

```
set attack disable attack_object_name
```

要重新启用先前禁用的攻击对象，请执行以下任一操作 :

WebUI

Objects > Attacks > Predefined: 在要启用的攻击对象的 Configure 栏中，选中复选框。

CLI

```
unset attack disable attack_object_name
```

攻击操作

当 NetScreen 设备检测到攻击时，将执行您为攻击组所指定的操作，该攻击组包含与该攻击相匹配的对象。七个操作按严重性程度由高到低列出如下：

- **Close (关闭)** (中断连接，并将 RST 发送给客户端和服务器[12])

  对 TCP 连接使用此选项。 NetScreen 设备丢弃连接，并将 TCP RST 发送给客户端 (源) 和服务器 (目标)。由于传送 RST 通知是不可靠的，因此，通过同时向客户端和服务器发送 RST，使得至少一方获得该 RST 并关闭会话的机会大大增加。

- **Close Server (关闭服务器)** (中断连接，并将 RST 发送给服务器)

  对于从不可信的客户端到受保护服务器的入站 TCP 连接，请使用此选项。例如，如果客户端企图发起攻击，则 NetScreen 设备将丢弃连接，并仅给服务器发送 TCP RST，使其在客户端还未完成时清除资源。

- **Close Client (关闭客户端)** (中断连接，并将 RST 发送给客户端)

  对于从受保护的客户端到不可信服务器的出站 TCP 连接，请使用此选项。例如，如果服务器发送恶意 URL 字符串，则 NetScreen 设备将丢弃连接，并仅给客户端发送 RST，使其在服务器还未完成时清除资源。

- **Drop (丢弃)** (中断连接，但不向任何一方发送 RST)

  对于 UDP 或其它非 TCP 连接 (如 DNS)，请使用此选项。 NetScreen 设备丢弃会话中的所有数据包，但不发送 TCP RST。

- **Drop Packet (丢弃数据包)** (丢弃特定的数据包，但不中断连接)

  此选项丢弃出现攻击签名或协议异常的数据包，但不终止会话本身。使用此选项可丢弃残缺的数据包而不中断整个会话。例如，如果 NetScreen 设备检测到来自某个 AOL 代理的攻击签名或协议异常，则丢弃一切信息将会中断所有 AOL 服务。反之，仅丢弃数据包将停止有问题的数据包，而不会停止所有其它数据包的流动。

12. 客户端总是会话的发起方，也就是策略中的源地址。服务器总是响应方或目标地址。

- **Ignore (忽略)** (在检测到攻击签名或异常后， NetScreen 设备将生成一个日志条目，并停止检查或忽略连接的其余部分)

  如果检测到攻击签名或协议异常，则 NetScreen 设备将生成一个事件日志条目，但不中断会话本身。在实现“深入检查” (DI) 的初始设置阶段，使用此选项来揪出主动错误信息。此外，当服务将标准端口号用于非标准协议活动时，请使用此选项；例如， Yahoo Messenger 将端口 25 (SMTP 端口) 用于传输非 SMTP 信息流。 NetScreen 设备对每个会话记录一次事件 (使其不会用主动错误信息填写日志)，但不采取任何措施。

- **None (无)** (无操作)

  在实现 “深入检查” (DI) 的初始设置阶段，当首次识别攻击类型时很有用。当检测到攻击签名或协议异常时， NetScreen 设备将在事件日志中生成一个条目，但不对信息流本身采取任何措施。 NetScreen 设备继续检查该会话中的后续信息流，如果检测到其它攻击签名和异常，将生成相应的日志条目。

可以创建一个引用多个攻击对象组的策略，每个组各有一个不同的操作。如果 NetScreen 设备同时检测到了属于不同的攻击对象组的多个攻击，则将应用其中一个攻击对象组所指定的最严重的操作。

范例 : 攻击操作 – Close Server、 Close、 Close Client

在本例中有三个区段 : Trust、 Untrust 和 DMZ。通过对攻击的分析，您断定将需要下列三个策略 :

- **策略 ID 1:** 允许从 Untrust 区段中的任何地址发往 DMZ 区段中的 Web 服务器 (websrv1 和 websrv2) 的 HTTP、 HTTPS、 PING 和 FTP-GET 信息流

  策略 ID 1 的攻击设置 :

  - CRITICAL:HTTP:ANOM, CRITICAL:HTTP:SIGS
  - HIGH:HTTP:ANOM, HIGH:HTTP:SIGS
  - MEDIUM:HTTP:ANOM, MEDIUM:HTTP:SIGS
  - CRITICAL:FTP:SIGS
  - 对所有攻击对象组的操作 : Close Server
  - Logging: Enabled (缺省设置)

  选择丢弃连接，并仅向受保护的 Web 服务器发送 TCP RST 通知，使其能终止会话和清除资源。您预料攻击来自 Untrust 区段。

- **策略 ID 2:** 允许从 Trust 区段中的任何地址发往 DMZ 区段中的 Web 服务器 (websrv1 和 websrv2) 的 HTTP、HTTPS、 PING 和 FTP 信息流

  策略 ID 2 的攻击设置 :

  - CRITICAL:HTTP:ANOM, CRITICAL:HTTP:SIGS
  - HIGH:HTTP:ANOM, HIGH:HTTP:SIGS
  - MEDIUM:HTTP:ANOM, MEDIUM:HTTP:SIGS
  - CRITICAL:FTP:SIGS
  - 对所有攻击对象组的操作 : Close
  - Logging: Enabled (缺省设置)

  选择丢弃连接，并向受保护的客户端和服务器发送 TCP RST 通知，使得不管攻击的严重性级别如何，它们都能终止会话和清除资源。

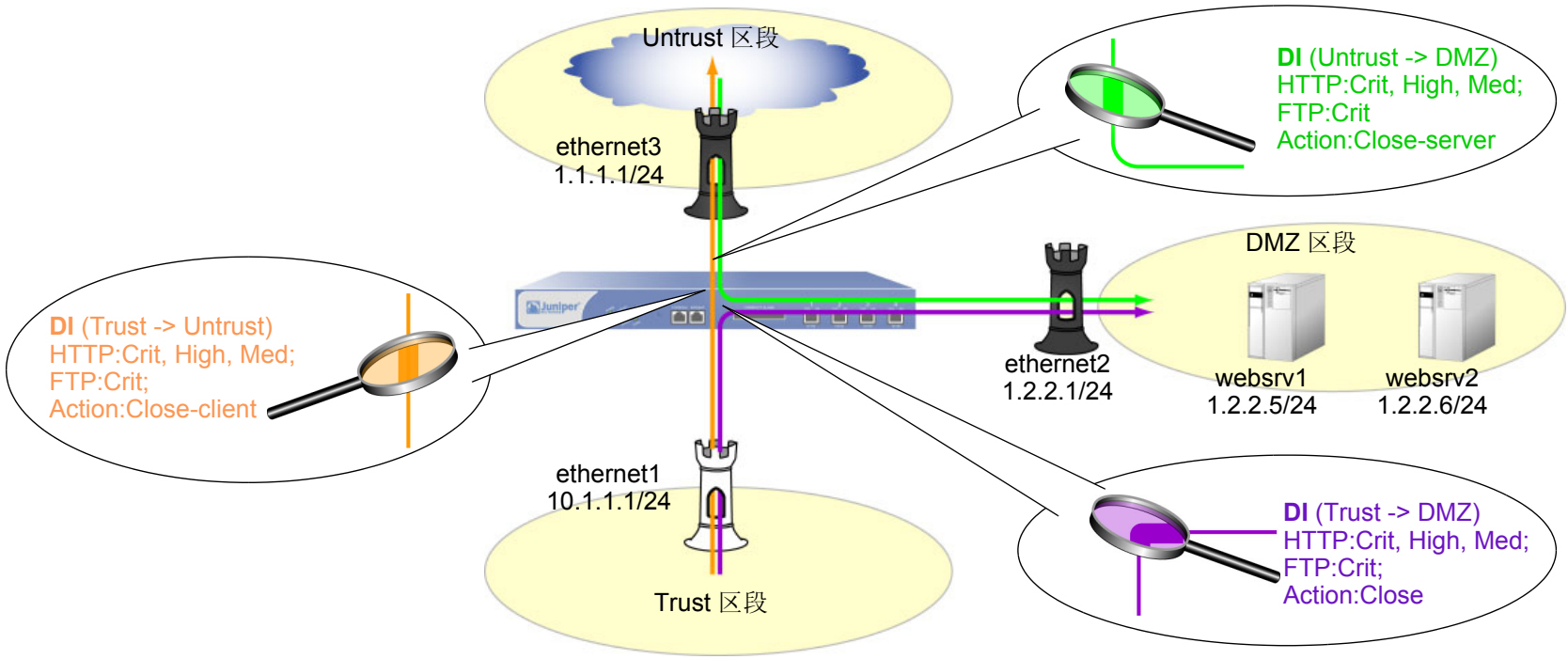
- **策略 ID 3:** 允许从 Trust 区段中的任何地址发往 Untrust 区段中的任何地址的 FTP-GET、 HTTP、 HTTPS、 PING 信息流

  策略 ID 3 的攻击设置 :

  - CRITICAL:HTTP:ANOM, CRITICAL:HTTP:SIGS
  - HIGH:HTTP:ANOM, HIGH:HTTP:SIGS
  - MEDIUM:HTTP:ANOM, MEDIUM:HTTP:SIGS
  - CRITICAL:FTP:SIGS
  - 对所有攻击对象组的操作 : Close Client
  - Logging: Enabled (缺省设置)

  选择丢弃连接，并仅向受保护的客户端发送 TCP RST 通知，使其能终止其会话和清除资源。在这种情况下，您预料攻击来自不可信的 HTTP 或 FTP 服务器。

尽管这些策略允许 HTTP、 HTTPS、 Ping 和 FTP-Get 或 FTP，但 NetScreen 设备仅对 HTTP 和 FTP 信息流激活“深入检查”。所有区段都在 trust-vr 路由选择域中。



WebUI

1. 接口

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容，然后单击 **Apply**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

输入以下内容，然后单击 **OK**:

Interface Mode: NAT

Service Options:

Management Services: (全选)

Other services: Ping

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容，然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > Edit (对于 ethernet2): 输入以下内容，然后单击 **OK**:

Zone Name: DMZ

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.2.2.1/24

2. 地址

Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

Address Name: websrv1

IP Address/Domain Name:

IP/Netmask: (选择), 1.2.2.5/32

Zone: DMZ

Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

Address Name: websrv2

IP Address/Domain Name:

IP/Netmask: (选择), 1.2.2.6/32

Zone: DMZ

3. 路由

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

4. 策略 ID 1

Policies > (From: Untrust, To: DMZ) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), websrv1

> 单击 **Multiple**，选择 **websrv2**，然后单击 **OK** 以返回基本策略配置页。

Service: HTTP

> 单击 **Multiple**，选择 **FTP-GET**、 **HTTPS**、 **PING**，然后单击 **OK** 以返回基本策略配置页。

Action: Permit

> 单击 **Deep Inspection**，输入以下内容，单击 **Add** 以输入每个攻击对象组，然后单击 **OK** 返回基本策略配置页 :

Group: CRITICAL:HTTP:ANOM

Action: Close Server

Log: (选择)

Group: CRITICAL:HTTP:SIGS

Action: Close Server

Log: (选择)

Group: HIGH:HTTP:ANOM

Action: Close Server

Log: (选择)

Group: HIGH:HTTP:SIGS
Action: Close Server
Log: (选择)
Group: MEDIUM:HTTP:ANOM
Action: Close Server
Log: (选择)
Group: MEDIUM:HTTP:SIGS
Action: Close Server
Log: (选择)
Group: CRITICAL:FTP:SIGS
Action: Close Server
Log: (选择)

5. 策略 ID 2

Policies > (From: Trust, To: DMZ) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), websrv1

> 单击 **Multiple**，选择 **websrv2**，然后单击 **OK** 以返回基本策略配置页。

Service: HTTP

> 单击 **Multiple**，选择 **FTP-GET**、 **HTTPS**、 **PING**，然后单击 **OK** 以返回基本策略配置页。

Action: Permit

> 单击 **Deep Inspection**，输入以下内容，单击 **Add** 以输入每个攻击对象组，然后单击 **OK** 返回基本策略配置页：

Group: CRITICAL:HTTP:ANOM
Action: Close
Log: (选择)
Group: CRITICAL:HTTP:SIGS
Action: Close
Log: (选择)
Group: HIGH:HTTP:ANOM
Action: Close
Log: (选择)
Group: HIGH:HTTP:SIGS
Action: Close
Log: (选择)
Group: MEDIUM:HTTP:ANOM
Action: Close
Log: (选择)
Group: MEDIUM:HTTP:SIGS
Action: Close
Log: (选择)
Group: CRITICAL:FTP:SIGS
Action: Close
Log: (选择)

6. 策略 ID 3

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: HTTP

> 单击 **Multiple**，选择 **FTP-GET**、 **HTTPS**、 **PING**，然后单击 **OK** 以返回基本策略配置页。

Action: Permit

> 单击 **Deep Inspection**，输入以下内容，单击 **Add** 以输入每个攻击对象组，然后单击 **OK** 返回基本策略配置页：

Group: CRITICAL:HTTP:ANOM

Action: Close Client

Log: (选择)

Group: CRITICAL:HTTP:SIGS

Action: Close Client

Log: (选择)

Group: HIGH:HTTP:ANOM

Action: Close Client

Log: (选择)

Group: HIGH:HTTP:SIGS

Action: Close Client

Log: (选择)

Group: MEDIUM:HTTP:ANOM

Action: Close Client

Log: (选择)

Group: MEDIUM:HTTP:SIGS

Action: Close Client

Log: (选择)

Group: CRITICAL:FTP:SIGS

Action: Close Client

Log: (选择)

CLI

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 manage
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet2 zone dmz
set interface ethernet2 ip 2.1.1.1/24
```

2. 地址

```
set address dmz websrv1 1.2.2.5/32
set address dmz websrv2 1.2.2.6/32
```

3. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

4. 策略 ID 1

```
set policy id 1 from untrust to dmz any websrv1 http permit attack
    CRITICAL:HTTP:ANOM action close-server
set policy id 1
ns(policy:1)-> set dst-address websrv2
ns(policy:1)-> set service ftp-get
ns(policy:1)-> set service https
ns(policy:1)-> set service ping
ns(policy:1)-> set attack CRITICAL:HTTP:SIGS action close-server
ns(policy:1)-> set attack HIGH:HTTP:ANOM action close-server
ns(policy:1)-> set attack HIGH:HTTP:SIGS action close-server
ns(policy:1)-> set attack MEDIUM:HTTP:ANOM action close-server
ns(policy:1)-> set attack MEDIUM:HTTP:SIGS action close-server
ns(policy:1)-> set attack CRITICAL:FTP:SIGS action close-server
ns(policy:1)-> exit
```

5. 策略 ID 2

```
set policy id 2 from trust to dmz any websrv1 http permit attack
    CRITICAL:HTTP:ANOM action close
set policy id 2
ns(policy:2)-> set dst-address websrv2
ns(policy:2)-> set service ftp
ns(policy:2)-> set service https
ns(policy:2)-> set service ping
ns(policy:2)-> set attack CRITICAL:HTTP:SIGS action close
ns(policy:2)-> set attack HIGH:HTTP:ANOM action close
ns(policy:2)-> set attack HIGH:HTTP:SIGS action close
ns(policy:2)-> set attack MEDIUM:HTTP:ANOM action close
ns(policy:2)-> set attack MEDIUM:HTTP:SIGS action close
ns(policy:2)-> set attack CRITICAL:FTP:SIGS action close
ns(policy:2)-> exit
```

6. 策略 ID 3

```
set policy id 3 from trust to untrust any any http permit attack
    CRITICAL:HTTP:ANOM action close-client
set policy id 3
ns(policy:3)-> set service ftp-get
ns(policy:3)-> set service https
ns(policy:3)-> set service ping
ns(policy:3)-> set attack CRITICAL:HTTP:SIGS action close-client
ns(policy:3)-> set attack HIGH:HTTP:ANOM action close-client
ns(policy:3)-> set attack HIGH:HTTP:SIGS action close-client
ns(policy:3)-> set attack MEDIUM:HTTP:ANOM action close-client
ns(policy:3)-> set attack MEDIUM:HTTP:SIGS action close-client
ns(policy:3)-> set attack CRITICAL:FTP:SIGS action close-client
ns(policy:3)-> exit
save
```

攻击记录

可以对每个策略的每个攻击组启用记录检测到的攻击。换句话说，在同一策略内，可以应用多个攻击组并只对其中的某些攻击组有选择性地启用记录检测到的攻击。

在缺省情况下，启用记录。您可能想禁用记录这样的攻击：对您而言，其优先级较低，且您未对其给予过多的关注。禁用记录这类攻击有助于防止事件日志变得混乱（由于存在从不打算对其进行查看的条目）。

范例：按攻击组禁用记录

在本例中，将在策略中引用以下五个攻击组，并只对前两个攻击组启用记录：

- HIGH:IMAP:ANOM
- HIGH:IMAP:SIGS
- MEDIUM:IMAP:ANOM
- LOW:IMAP:ANOM
- INFO:IMAP:ANOM

该策略将应用到从 Trust 区段中的所有主机发往 DMZ 区段中的一个名为 “mail1” 的邮件服务器的 IMAP 信息流。只要上述五个攻击组中的任何预定义 IMAP 攻击对象与某个攻击相匹配，NetScreen 设备即会关闭连接。不过，它仅针对与前两组中的攻击对象相匹配的检测到的攻击创建日志条目。

WebUI

1. 地址

   Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

   Address Name: mail1

   IP Address/Domain Name:

   IP/Netmask: (选择), 1.2.2.10/32

   Zone: DMZ

2. 策略

Policies > (From: Trust, To: DMZ) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), mail1

Service: IMAP

Action: Permit

> 单击 **Deep Inspection**，输入以下内容，单击 **Add** 以输入每个攻击对象组，然后单击 **OK** 返回基本策略配置页：

Group: HIGH:IMAP:ANOM

Action: Close

Log: (选择)

Group: HIGH:IMAP:SIGS

Action: Close

Log: (选择)

Group: MEDIUM:IMAP:ANOM

Action: Close

Log: (清除)

Group: LOW:IMAP:ANOM

Action: Close

Log: (清除)

Group: INFO:IMAP:ANOM

Action: Close

Log: (清除)

CLI

1. 地址

```
set address dmz mail1 1.2.2.10/32
```

2. 策略

```
ns-> set policy id 1 from trust to dmz any mail1 imap permit attack
    HIGH:IMAP:ANOM action close
ns-> set policy id 1
ns(policy:1)-> set attack HIGH:IMAP:SIGS action close
ns(policy:1)-> set attack MEDIUM:IMAP:ANOM action close
ns(policy:1)-> unset attack MEDIUM:IMAP:ANOM logging
ns(policy:1)-> set attack LOW:IMAP:ANOM action close
ns(policy:1)-> unset attack LOW:IMAP:ANOM logging
ns(policy:1)-> set attack INFO:IMAP:ANOM action close
ns(policy:1)-> unset attack INFO:IMAP:ANOM logging
ns(policy:1)-> exit
ns-> save
```

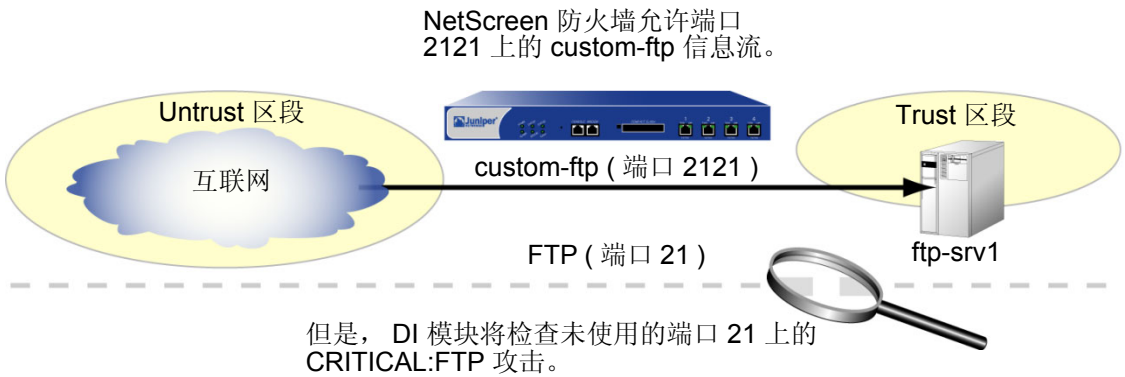
将定制服务映射到应用程序

当在含 “深入检查” (DI) 组件的策略中使用定制服务时，必须明确指定在该服务上运行的应用程序，以使 DI 模块能够正确工作。例如，如果您为 FTP 创建了一个运行在非标准端口号 2121 上的定制服务，则可以在策略中按照如下方式引用该定制服务：

```
set service ftp-custom protocol tcp src-port 0-65535 dst-port 2121-2121
set policy id 1 from untrust to trust any ftp-srv1 custom-ftp permit
```

但是，如果您将 DI 组件添加到了引用定制服务的策略中，则该 DI 组件将无法识别应用程序，因为该定制服务正在使用非标准端口号。

```
set policy id 1 from untrust to trust any ftp-srv1 custom-ftp permit attack
    CRITICAL:FTP:SIGS action close-server
```



为了避免出现此问题，您必须通知 DI 模块该 FTP 应用程序正运行在端口 2121 上。实际上，您必须将 “应用程序层” 中的协议映射到 “传输层” 中的特定端口号。可以在策略级完成这种绑定：

```
set policy id 1 application ftp
```

当您将 FTP 应用程序映射到定制服务 “custom-ftp” 并配置 DI，使其针对引用 custom-ftp 的策略中的 CRITICAL:FTP:SIGS 攻击对象组中定义的攻击检查 FTP 信息流时， DI 模块将在端口 2121 上执行该检查。

```
set policy id 1 from untrust to trust any ftp-srv1 custom-ftp permit attack
    CRITICAL:FTP:SIGS action close-server
set policy id 1 application ftp
```

范例：将应用程序映射到定制服务上

在本例中，将定义名为 “HTTP1” 的使用目标端口 8080 的定制服务。对于允许从 Untrust 区段中的任何地址发往 DMZ 区段中名为 “server1” 的 Web 服务器的 HTTP1 信息流的策略，将 HTTP 应用程序映射到该定制服务上。然后将 “深入检查” 应用到在端口 8080 上运行的允许 HTTP 信息流。该策略的 “深入检查” 设置如下：

- 攻击对象组：
  - CRITICAL:HTTP:ANOM, CRITICAL:HTTP:SIGS
  - HIGH:HTTP:ANOM, HIGH:HTTP:SIGS
  - MEDIUM:HTTP:ANOM, MEDIUM:HTTP:SIGS
- 对所有攻击对象组的操作：Close Server
- Logging: Enabled (缺省设置)

WebUI

1. 定制服务

   Objects > Services > Custom > New: 输入以下内容，然后单击 **OK**:

   Service Name: HTTP1

   Transport Protocol: TCP (选择)

   Source Port Low: 0

   Source Port High: 65535

   Destination Port Low: 8080

   Destination Port High: 8080

2. 地址

   Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

   Address Name: server1

   IP Address/Domain Name:

   IP/Netmask: 1.2.2.5/32

   Zone: DMZ

3. 策略

   Policies > (From: Untrust, To: DMZ) New: 输入以下内容，然后单击 **OK**:

   Source Address:

   Address Book Entry: (选择), Any

   Destination Address:

   Address Book Entry: (选择), server1

   Service: HTTP1

   Application: HTTP

   Action: Permit

> 单击 **Deep Inspection**，输入以下内容，单击 **Add** 以输入每个攻击对象组，然后单击 **OK** 返回基本策略配置页：

Group: CRITICAL:HTTP:ANOM
Action: Close Server
Log: (选择)
Group: CRITICAL:HTTP:SIGS
Action: Close Client
Log: (选择)
Group: HIGH:HTTP:ANOM
Action: Close Client
Log: (选择)
Group: HIGH:HTTP:SIGS
Action: Close Client
Log: (选择)
Group: MEDIUM:HTTP:ANOM
Action: Close Client
Log: (选择)
Group: MEDIUM:HTTP:SIGS
Action: Close Client
Log: (选择)

CLI

1. 定制服务

```
set service HTTP1 protocol tcp src-port 0-65535 dst-port 8080-8080
```

2. 地址

```
set address dmz server1 1.2.2.5/32
```

3. 策略

```
ns-> set policy id 1 from untrust to dmz any server1 HTTP1 permit attack
    CRITICAL:HTTP:ANOM action close-server
ns-> set policy id 1
ns(policy:1)-> set attack CRITICAL:HTTP:SIGS action close-server
ns(policy:1)-> set attack HIGH:HTTP:ANOM action close-server
ns(policy:1)-> set attack HIGH:HTTP:SIGS action close-server
ns(policy:1)-> set attack MEDIUM:HTTP:ANOM action close-server
ns(policy:1)-> set attack MEDIUM:HTTP:SIGS action close-server
ns(policy:1)-> exit
ns-> set policy id 1 application http
save
```

范例 : HTTP 攻击的应用程序至服务映射

一些已知的 HTTP 攻击使用 TCP 端口 8000。发布本指南时，当前在 “深入检查” (DI) 攻击对象数据库中存在两种这样的攻击 :

- 3656, App: HP Web JetAdmin Framework Infoleak

  DOS:NETDEV:WEBJET-FW-INFOLEAK (位于攻击对象组 MEDIUM:HTTP:SIGS 中)
- 3638, App: HP Web JetAdmin WriteToFile Vulnerability,

  DOS:NETDEV:WEBJET-WRITETOFILE (位于攻击对象组 CRITICAL:HTTP:SIGS 中)

但是，在缺省情况下， ScreenOS 仅将端口 80 上的 TCP 信息流当作 HTTP。因此，如果 NetScreen 设备接收到使用端口 8000 的 TCP 信息流，将不会把它视为 HTTP。因此， DI 引擎不扫描这样的 HTTP 信息流以查找攻击，即使发生了攻击也检测不到它们 — 除非您将 HTTP 作为应用程序映射到某个使用端口 8000 的定制服务上。

在本例中，您将使用非标准端口 8000 的信息流与 HTTP 相关联以检测上述攻击。

注意 : *一般来说，如果您正在网络中运行使用非标准端口号的某些服务，且您想让 DI 引擎扫描该信息流，您必须将非标准端口号与服务相关联。*

WebUI

1. 定制服务

Objects > Services > Custom > New: 输入以下内容，然后单击 **OK**:

Service Name: HTTP2

Transport Protocol: TCP (选择)

Source Port Low: 0

Source Port High: 65535

Destination Port Low: 8000

Destination Port High: 8000

2. 策略

Policies > (From: Untrust, To: DMZ) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: HTTP2

Application: HTTP

Action: Permit

> 单击 **Deep Inspection**，输入以下内容，单击 **Add** 以输入每个攻击对象组，然后单击 **OK** 返回基本策略配置页：

Group: CRITICAL:HTTP:SIGS

Action: Close

Log: (选择)

Group: MEDIUM:HTTP:SIGS

Action: Close

Log: (选择)

CLI

1. 定制服务

```
set service HTTP2 protocol tcp src-port 0-65535 dst-port 8000-8000
```

2. 策略

```
ns-> set policy id 1 from untrust to dmz any any HTTP2 permit attack
    CRITICAL:HTTP:SIGS action close
ns-> set policy id 1
ns(policy:1)-> set attack MEDIUM:HTTP:SIGS action close
ns(policy:1)-> exit
ns-> set policy id 1 application http
save
```

定制攻击对象和组

您可以定义新的攻击对象和对象组，以定制 “深入检查” (DI) 应用程序来最好地满足自己的需要。用户定义的攻击对象可以是状态式签名，在 NetScreen-5000 上，也可以是 TCP 流式签名。也可以调整各种参数来修改预定义协议异常攻击对象。

用户定义的状态式签名攻击对象

可以为 FTP、 HTTP 和 SMTP 创建状态式签名攻击对象。创建攻击对象时，将执行下列步骤 :

- 命名攻击对象。 (所有用户定义的攻击对象名称必须以 “CS:” 作为开头。)
- 设置 “深入检查” 搜索的环境。 (对于创建攻击对象时可以使用的所有环境的完整列表，请参阅附录 A，“用户定义签名的环境”。)
- 定义签名。 (下节第 182 页上的 “规则表达式”将对定义签名时可以使用的规则表达式进行介绍。)
- 为攻击对象分配严重性级别。 (有关严重性级别的信息，请参阅第 153 页上的 “更改严重性级别”。)

然后必须将用户定义的攻击对象放在用户定义的攻击对象组中供策略使用。

注意 : *用户定义的攻击对象组只能包含用户定义的攻击对象。同一攻击对象组中不能同时包含预定义的攻击对象和用户定义的攻击对象。*

规则表达式

在为签名输入文本字符串时，可以输入由普通字符组成的字母数字字符串，以便搜索字符精确匹配项，还可通过规则表达式来扩大搜索以查找字符集的可能匹配项。 ScreenOS 支持以下规则表达式：

作用	元字符	范例	含义
直接二进制匹配 (八进制)*	\O*octal_number*	\0162 匹配值： 162	精确匹配八进制数 “162”。
直接二进制匹配 (十六进制)†	\X*hexadecimal_number*\X	\X01 A5 00 00\X 匹配值： 01 A5 00 00	精确匹配五个十六进制数：“01 A5 00 00”。
不区分大小写的匹配	\[*characters*\]	\[cat\] 匹配值： Cat, cAt, caT CAt, CaT, CAT cat, cAt	匹配 “cat” 中的字符而不区分每个字符的大小写。
匹配任何字符	.	c . t 匹配值： cat, cbt, cct, … czt cAt, cBt, cCt, … cZt c1t, c2t, c3t, … c9t	匹配 “c- 任何字符 -t”。

作用	元字符	范例	含义
0 次或多次匹配前一个字符，而不是仅一次	*	a*b+c 匹配值： bc bbc abc aaabbbbc	匹配值为：0 个、1 个或多个“a”，之后为 1 个或多个“b”，最后为 1 个“c”。
1 次或多次匹配前一个字符	+	a+b+c 匹配值： abc aabc aaabbbbc	匹配值为：1 个或多个“a”，之后为 1 个或多个“b”，最后为 1 个“c”。
0 次或 1 次匹配前一个字符	?	drop-?packet 匹配值： drop-packet droppacket	匹配值为“drop-packet”或“droppacket”。
组表达式	( )		
前一个或后一个字符 – 通常与 ( ) 配合使用	|	(drop | packet) 匹配值： drop packet	匹配值为“drop”或“packet”。

作用	元字符	范例	含义
字符范围	[*start-end*]	[c-f]a(d | t) 匹配值 : cad, cat dad, dat ead, eat fad, fat	匹配值为所有以 “c”、“d”、“e” 或 “f” 开头、以字母 “d” 或 “t” 结尾且中间字母为 “a” 的所有字符串。
后面字符的相反值	[^*character*]	[^0-9A-Z] 匹配值 : a, b, c, d, e, … z	匹配值为小写字母。

* 八进制是以 8 为基数的记数法，只使用数字 0–7。

† 十六进制是以 16 为基数的记数法，通常使用数字 0–9，并使用字母 A–F 来表示其十进制值为 10–15 的十六进制数字。

范例：用户定义的状态式签名攻击对象

在本例中， DMZ 区段中具有一个 FTP 服务器、一个 Web 服务器以及一个邮件服务器。为以下用途定义下列攻击对象：

攻击对象名称	可用于
cs:ftp-stor	禁止某人将文件放到 FTP 服务器上。
cs:ftp-user-dm	拒绝登录名为 “dmartin” 的用户的 FTP 访问。
cs:url-index	封锁含有任何 HTTP 请求中已定义的 URL 的 HTTP 数据包。
cs:spammer	封锁从 “spam.com” 处的电子邮件地址发出的电子邮件。

然后将它们编组为名为 “DMZ DI” 的用户定义的攻击对象组，并在策略中引用它，该策略允许从 Untrust 区段发往 DMZ 区段中的服务器的信息流。

WebUI

1. 攻击对象 1: ftp-stor

   Objects > Attacks > Custom > New: 输入以下内容，然后单击 **OK**:

   Attack Name: cs:ftp-stor

   Attack Context: FTP Command

   Attack Severity: Medium

   Attack Pattern: STOR

2. 攻击对象 2: ftp-user-dm

   Objects > Attacks > Custom > New: 输入以下内容，然后单击 **OK**:

   Attack Name: cs:ftp-user-dm

   Attack Context: FTP User Name

   Attack Severity: Low

   Attack Pattern: dmartin

3. 攻击对象 3: url-index

Objects > Attacks > Custom > New: 输入以下内容，然后单击 **OK**:

Attack Name: cs:url-index

Attack Context: HTTP URL Parsed

Attack Severity: High

Attack Pattern: .*index.html.*

4. 攻击对象 4: spammer

Objects > Attacks > Custom > New: 输入以下内容，然后单击 **OK**:

Attack Name: cs:spammer

Attack Context: SMTP From

Attack Severity: Info

Attack Pattern: .*@spam.com

5. 攻击对象组

Objects > Attacks > Custom Groups > New: 输入以下组名称，移动下列定制攻击对象，然后单击 **OK**:

Group Name: CS:DMZ DI

选择 **cs:ftp-stor**，并使用 **<<** 按钮将地址从 Available Members 栏移动到 Selected Members 栏中。

选择 **cs:ftp-user-dm**，并使用 **<<** 按钮将地址从 Available Members 栏移动到 Selected Members 栏中。

选择 **cs:url-index**，并使用 **<<** 按钮将地址从 Available Members 栏移动到 Selected Members 栏中。

选择 **cs:spammer**，并使用 **<<** 按钮将地址从 Available Members 栏移动到 Selected Members 栏中。

6. 策略

Policies > (From: Untrust, To: DMZ) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: HTTP

> 单击 **Multiple**，选择 **FTP**，然后单击 **OK** 以返回基本策略配置页。

Action: Permit

> 单击 **Deep Inspection**，输入以下内容，单击 **Add** 以输入每个攻击对象组，然后单击 **OK** 返回基本策略配置页：

Group: CS:DMZ DI

Action: Close Server

Log: (选择)

CLI

1. 攻击对象 1: ftp-stor

```
set attack cs:ftp-stor ftp-command STOR severity medium
```

2. 攻击对象 2: ftp-user-dm

```
set attack cs:ftp-user-dm ftp-username dmartin severity low
```

3. 攻击对象 3: url-index

```
set attack cs:url-index http-url-parsed index.html severity high
```

4. 攻击对象 4: spammer

```
set attack cs:spammer smtp-from .*@spam.com severity info
```

5. 攻击对象组

```
set attack group "CS:DMZ DI"
set attack group "CS:DMZ DI" add cs:ftp-stor
set attack group "CS:DMZ DI" add cs:ftp-user-dm
set attack group "CS:DMZ DI" add cs:url-index
set attack group "CS:DMZ DI" add cs:spammer
```

6. 策略

```
set policy id 1 from untrust to dmz any any http permit attack "CS:DMZ DI"
    action close-server
set policy id 1
ns(policy:1)-> set service ftp
ns(policy:1)-> exit
save
```

TCP 流式签名攻击对象

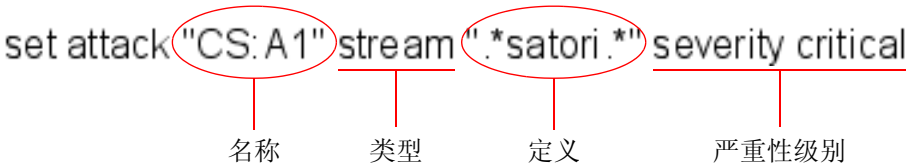
状态式签名在特定应用程序中是基于环境的，如 FTP 用户名或 SMTP 包头字段。 TCP 流式签名查找任何种类的 TCP 信息流中所有位置的模式，而不管所使用的应用协议是什么。

***注意：**只能在 NetScreen-5000 系列系统上定义 TCP 流式签名。*

由于没有预定义的 TCP 流式签名攻击对象，因此必须对其进行定义。在创建签名攻击对象时，将定义下列组件：

- 攻击对象名称 (所有用户定义的攻击对象名称必须以 “CS:” 作为开头。)
- 对象类型 (“流式”)
- 模式定义
- 严重性级别

TCP 流式签名攻击对象的范例



范例 : 用户定义的流式签名攻击对象

在本例中，将定义一个流式签名对象 “.*satori.*”。将其命名为 “CS:A1”，并将其严重性级别定义为 “关键”。由于策略只能引用攻击对象组，因此，将首先创建一个名为 “CS:Gr1” 的攻击对象组，然后再将该对象添加到该攻击对象组中。最后，将定义一个引用 CS:Gr1 的策略，该策略指示 NetScreen 设备 : 如果该模式出现在此策略所应用的任何信息流中，将中断连接并将 TCP RST 发送给客户端。

WebUI

1. 流式签名攻击对象

   Objects > Attacks > Custom > New: 输入以下内容，然后单击 **OK**:

   Attack Name: CS:A1

   Attack Context: Stream

   Attack Severity: Critical

   Attack Pattern: .*satori.*

2. 流式签名攻击对象组

   Objects > Attacks > Custom Groups > New: 输入以下内容，然后单击 **OK**:

   Group Name: CS:Gr1

   选择 Available Members 栏中的 **CS:A1**，然后单击 **<<** 将其移动到 Selected Members 栏中。

3. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Permit

> 单击 **Deep Inspection**，输入以下内容，单击 **Add** 以输入每个攻击对象组，然后单击 **OK** 返回基本策略配置页 :

Group: CS:Gr1

Action: Close Client

Log: (选择)

CLI

1. 流式签名攻击对象

```
set attack "CS:A1" stream ".*satori.*" severity critical
```

2. 流式签名攻击对象组

```
set attack group "CS:Gr1"
set attack group "CS:Gr1" add "CS:A1"
```

3. 策略

```
set policy from trust to untrust any any any permit attack CS:Gr1 action
    close-client
save
```

可配置的协议异常参数

可以修改协议异常攻击对象的某些参数。尽管 Juniper 定义协议异常攻击对象来查找偏离在 RFC 和通用 RFC 扩展中所定义的协议标准的情况，但并非所有的执行过程都遵守这些标准。如果您发现某个协议异常攻击对象的应用程序正在产生大量的主动错误信息，您可以修改其参数以更好地匹配网络中该协议的认同用法。

注意：*有关所有可配置参数的完整列表，请参阅* NetScreen CLI Reference Guide *中的* ***di*** *命令。*

范例：修改参数

在本例中，将为以下参数设置较大的值以减少使用缺省设置时所产生的主动错误信息的数量：

协议参数	缺省值	新值
SMB – 每分钟登录失败的最大次数	失败 4 次	失败 8 次
Gnutella – 最大活动时间 (TTL) 跳跃数	8 个跳跃	10 个跳跃

对于以下参数，将为其设置较小的值以检测 NetScreen 设备使用缺省设置时检测不到的异常行为：

协议参数	缺省值	新值
AOL Instant Messenger (AIM) – OSCAR 文件传输 (OFT) 文件名最大长度 OSCAR = 用于实时通信的开放式系统， AIM 客户端使用的协议。	10,000 字节	5,000 字节
AOL Instant Messenger – FLAP 帧 (由总长度为 6 字节的 FLAP 包头外加数据组成) 的最大长度 OSCAR 使用 FLAP 协议创建连接并打开 AIM 客户端之间的通道。	10,000 字节	5,000 字节

WebUI

***注意：**必须使用 CLI 来修改协议异常参数。*

CLI

```
set di service smb failed_logins 8
set di service gnutella max_ttl_hops 10
set di service aim max_flap_length 5000
set di service aim max_oft_frame 5000
save
```

排除

通常使用攻击对象来匹配表示恶意或异常活动的模式。不过，也可以使用它们来匹配表示善意或合法活动的模式。使用这种方法时，只有当某种类型的信息流与某一特定模式*不*相匹配时才会发生错误。要以这种方式来使用攻击对象，应使用排除的概念。

攻击对象排除的一个很有用应用就是封锁除使用正确用户名和密码进行登录之外的所有其它登录尝试。虽然定义所有无效用户名和密码相当困难，但定义正确的用户名和密码，之后再应用排除以逆转 NetScreen 设备将其视为攻击的对象 (即除了指定攻击对象之外的所有事情) 却是一件很容易的事情。

范例：攻击对象排除

在本例中，将定义两个攻击对象：其中一个指定了登录到 FTP 服务器所需的正确用户名，而另一个则指定了正确的密码。然后对这两个攻击对象应用排除，使得 NetScreen 设备封锁所有使用除攻击对象中所定义的用户名或密码之外的任何其它用户名或密码登录该服务器的尝试。

本例使用以下设置：

- 正确的用户名和密码是 *admin1* 和 *pass1*。
- FTP 服务器位于 DMZ 区段中的 1.2.2.5 处。其地址名是 *ftp1*。
- 对从 Untrust 和 Trust 区段中的所有主机发往该服务器的 FTP 信息流应用 “深入检查”。
- 所有安全区段都在 trust-vr 路由选择域中。

将创建以下两个攻击对象：

攻击对象 #1:

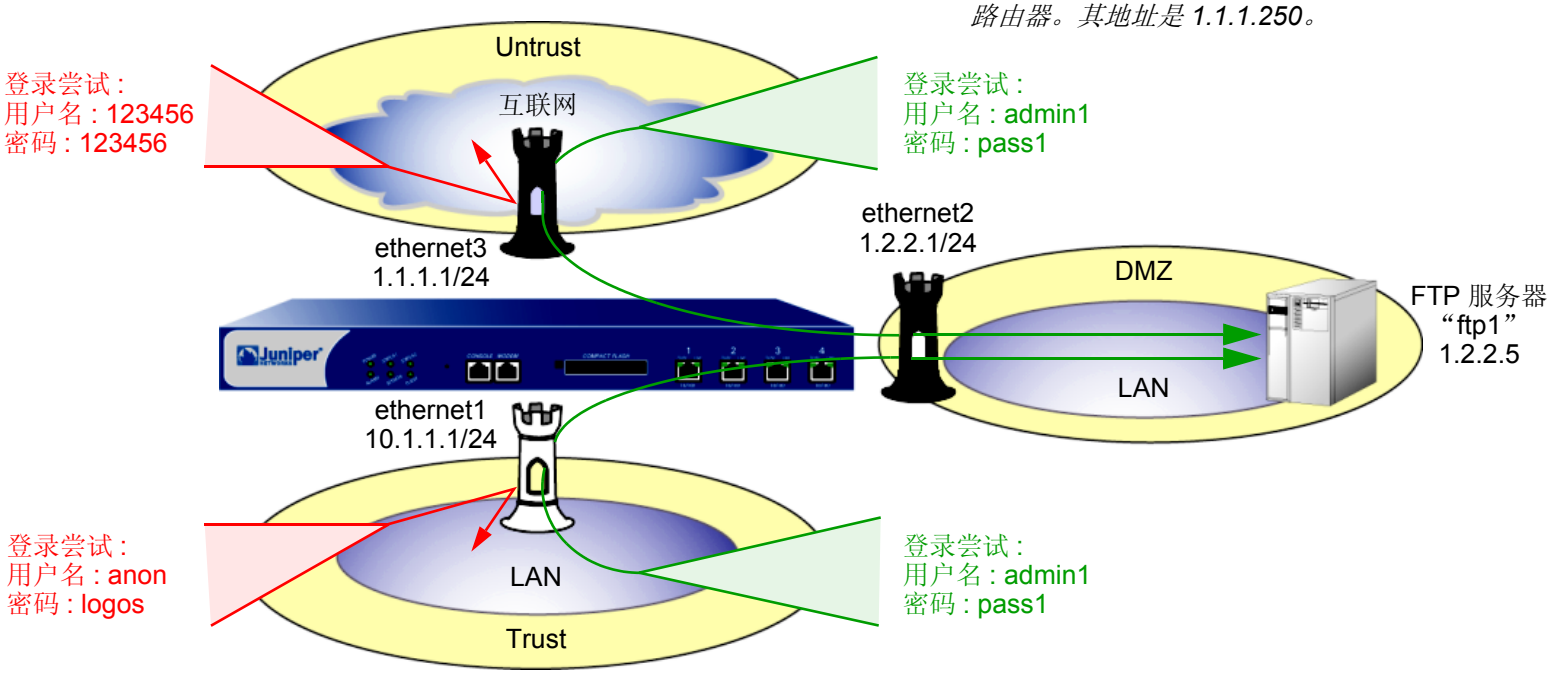
- Name: CS:FTP1_USR_OK
- Negation: enabled
- Context: ftp-username
- Pattern: admin1
- Severity: high

攻击对象 #2:

- Name: CS:FTP1_PASS_OK
- Negation: enabled
- Context: ftp-password
- Pattern: pass1
- Severity: high

然后将这两个对象都放到名为 *CS:FTP1_LOGIN* 的攻击对象组中，并在两个策略中引用该攻击对象组，这两个策略允许 FTP 信息流从 Trust 和 Untrust 区段流向 DMZ 区段中的 ftp1。

***注意：**为清晰起见，未显示 Untrust 区段中的外部路由器。其地址是 1.1.1.250。*



WebUI

1. 接口

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容，然后单击 **Apply**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT (选择)[13]

Network > Interfaces > Edit (对于 ethernet2): 输入以下内容，然后单击 **OK**:

Zone Name: DMZ

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.2.2.1/24

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容，然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

13. 在缺省情况下，绑定到 Trust 区段的所有接口都处于 NAT 模式。因此，对于绑定到 Trust 区段的接口，此选项已经启用。

2. 地址

Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

Address Name: ftp1

IP Address/Domain Name:

IP/Netmask: (选择), 1.2.2.5/32

Zone: DMZ

3. 攻击对象 1: CS:FTP1_USR_OK

Objects > Attacks > Custom > New: 输入以下内容，然后单击 **OK**:

Attack Name: CS:FTP1_USR_OK

Attack Context: ftp-username

Attack Severity: High

Attack Pattern: admin1

Pattern Negation: (选择)

4. 攻击对象 2: CS:FTP1_PASS_OK

Objects > Attacks > Custom > New: 输入以下内容，然后单击 **OK**:

Attack Name: CS:FTP1_PASS_OK

Attack Context: ftp-password

Attack Severity: High

Attack Pattern: pass1

Pattern Negation: (选择)

5. 攻击对象组

Objects > Attacks > Custom Groups > New: 输入以下组名称，移动下列定制攻击对象，然后单击 **OK**:

Group Name: CS:FTP1_LOGIN

选择 **CS:FTP1_USR_OK**，并使用 **<<** 按钮将地址从 Available Members 栏移动到 Selected Members 栏中。

选择 **CS:FTP1_PASS_OK**，并使用 **<<** 按钮将地址从 Available Members 栏移动到 Selected Members 栏中。

6. 路由

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: (选择) 1.1.1.250

7. 策略

Policies > (From: Untrust, To: DMZ) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), ftp1

Service: FTP

Action: Permit

> 单击 **Deep Inspection**，输入以下内容，单击 **Add** 以输入每个攻击对象组，然后单击 **OK** 返回基本策略配置页：

Group: CS:FTP1_LOGIN

Action: Drop

Log: (选择)

Policies > (From: Trust, To: DMZ) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), ftp1

Service: FTP

Action: Permit

> 单击 **Deep Inspection**，输入以下内容，单击 **Add** 以输入每个攻击对象组，然后单击 **OK** 返回基本策略配置页：

Group: CS:FTP1_LOGIN

Action: Drop

Log: (选择)

CLI

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat

set interface ethernet2 zone dmz
set interface ethernet2 ip 1.2.2.1/24

set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. 地址

```
set address dmz ftp1 1.2.2.5/32
```

3. 攻击对象

```
set attack CS:FTP1_USR_OK ftp-username not admin1 severity high
set attack CS:FTP1_PASS_OK ftp-password not pass1 severity high
set attack group CS:FTP1_LOGIN
set attack group CS:FTP1_LOGIN add CS:FTP1_USR_OK
set attack group CS:FTP1_LOGIN add CS:FTP1_PASS_OK
```

4. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

5. 策略

```
set policy from untrust to dmz any ftp1 ftp permit attack CS:FTP1_LOGIN action
    drop
set policy from trust to dmz any ftp1 ftp permit attack CS:FTP1_LOGIN action
    drop
save
```

精确封锁 HTTP 组件

NetScreen 设备可以有选择性地封锁通过 HTTP 发送的 ActiveX 控件、Java applet、.zip 文件以及 .exe 文件。这些组件对网络安全造成的危险是：它们为不可信方提供了一种先加载而后再控制受保护网络中的主机上的应用程序的方法。

当在安全区段中启用对一个或多个这些组件的封锁时，NetScreen 设备将检查每个到达绑定到该区段的接口的 HTTP 包头。设备检查包头中列出的内容类型是否指示数据包负荷中有任何目标组件。如果内容类型是 Java、 .exe 或 .zip，并且已配置 NetScreen 设备使其封锁这些 HTTP 组件类型，则 NetScreen 设备将封锁数据包。如果内容类型仅列出 “octet stream”，而未列出特定的组件类型，则 NetScreen 设备将检查负荷中的文件类型。如果文件类型是 Java、 .exe 或 .zip，并且已配置 NetScreen 设备使其封锁这些组件类型，则 NetScreen 设备将封锁数据包。

当启用封锁 ActiveX 控件时， NetScreen 设备将封锁其负荷中包含任何类型 HTTP 组件 (ActiveX 控件、 Java applet、 .exe 文件或 .zip 文件) 的所有 HTTP 数据包。

注意：*当启用了 ActiveX 封锁后， NetScreen 设备将封锁 Java applet、 .exe 文件和 .zip 文件 — 无论它们是否包含在 ActiveX 控件内。*

ActiveX 控件

Microsoft ActiveX 技术为 Web 设计者提供了创建动态和交互式网页的工具。 ActiveX 控件是允许不同的程序彼此相互作用的组件。例如， ActiveX 允许 Web 浏览器打开电子表格或显示来自后端数据库的个人帐户。 ActiveX 组件也可以包含其它组件 (如 Java applet) 或文件 (如 .exe 文件和 .zip 文件)。

当您访问启用了 ActiveX 的网站时，该站点会提示您将 ActiveX 控件下载到您的计算机上。 Microsoft 提供了一条弹出式消息，显示对供下载的 ActiveX 代码进行认证的公司或编程者的名称。如果您信任该代码的来源，则可以继续下载这些控件。如果您不信任该来源，则可以拒绝它们。

如果您将 ActiveX 控件下载到了您的计算机中，则该控件即可实现其创建者设计的任何功能。如果其为恶意代码，则该控件可能会立即重新格式化您的硬盘、删除所有文件、将您的个人电子邮件发送给您的老板，等等。

Java Applet

与 ActiveX 的用途类似，Java applet 也通过允许与其它程序交互来增强网页的功能。您将 Java applet 下载到计算机上的 Java Virtual Machine (VM)。在最初的 Java 版本中，VM 不允许 applet 与计算机上的其它资源交互。从 Java 1.1 开始，已放宽了一些限制来提供更强的功能。因此，现在 Java applet 可以访问 VM 外部的本地资源。由于攻击者可以编制可在 VM 外部运行的 Java applet，因此它们会像 ActiveX 控件那样造成同样的安全威胁。

EXE 文件

如果您下载并运行从 Web 上获得的可执行文件 (即扩展名为 .exe 的文件)，您将无法确保该文件未被感染。即使您信任下载该可执行文件的网站，但从该网站嗅探下载请求的人可能已截取了您的请求，并用经过修改的包含恶意代码的 .exe 文件做出响应。

ZIP 文件

zip 文件 (即扩展名为 .zip 的文件) 是包含一个或多个压缩文件的一类文件。上一节介绍的有关下载 .exe 文件的危险也适用于 .zip 文件，因为 .zip 文件中可能包含一个或多个 .exe 文件。

范例：封锁 Java Applet 和 .exe 文件

在本例中，将封锁到达 Untrust 区段接口的数据包中包含 Java applet 和 .exe 文件的所有 HTTP 信息流。

WebUI

Screening > Screen (Zone: Untrust): 选择 **Block Java Component** 和 **Block EXE Component**，然后单击 **Apply**。

CLI

```
set zone untrust screen java
set zone untrust screen exe
save
```

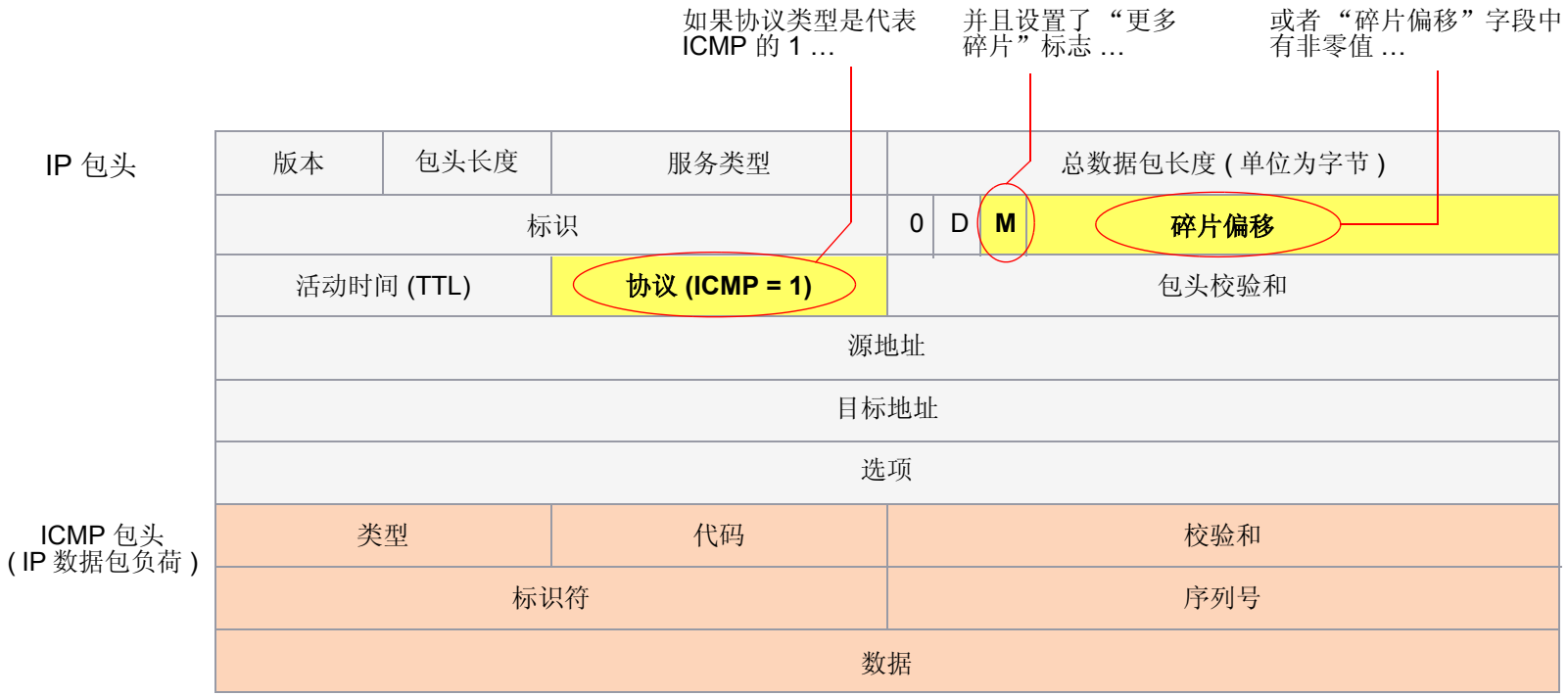
6

可疑数据包属性

如本卷其它章所述，攻击者可以通过精心设计数据包来执行侦查或发起拒绝服务 (DoS) 攻击。有时候，我们不太清楚精心设计的数据包的意图，但由于是精心设计的，这就暗示它会被用于某种阴险用途。本章中介绍的所有 SCREEN 选项都能封锁可能包含隐藏威胁的数据包：

ICMP 碎片

“互联网控制信息协议” (ICMP) 提供了错误报告和网络侦查功能。由于 ICMP 数据包只包含很短的信息，因此没有合法理由将 ICMP 数据包分为碎片。如果 ICMP 数据包太大，必须分为碎片，则可能会产生一些问题。当启用 ICMP Fragment Protection SCREEN 选项时， NetScreen 设备将封锁设置了 “更多碎片” 标志的任何 ICMP 数据包，或者含有偏移字段中指示的偏移值的任何 ICMP 数据包。



… NetScreen 设备封锁数据包。

要封锁 ICMP 数据包碎片，请执行以下任一操作，其中指定的安全区段是数据包碎片始发的区段：

WebUI

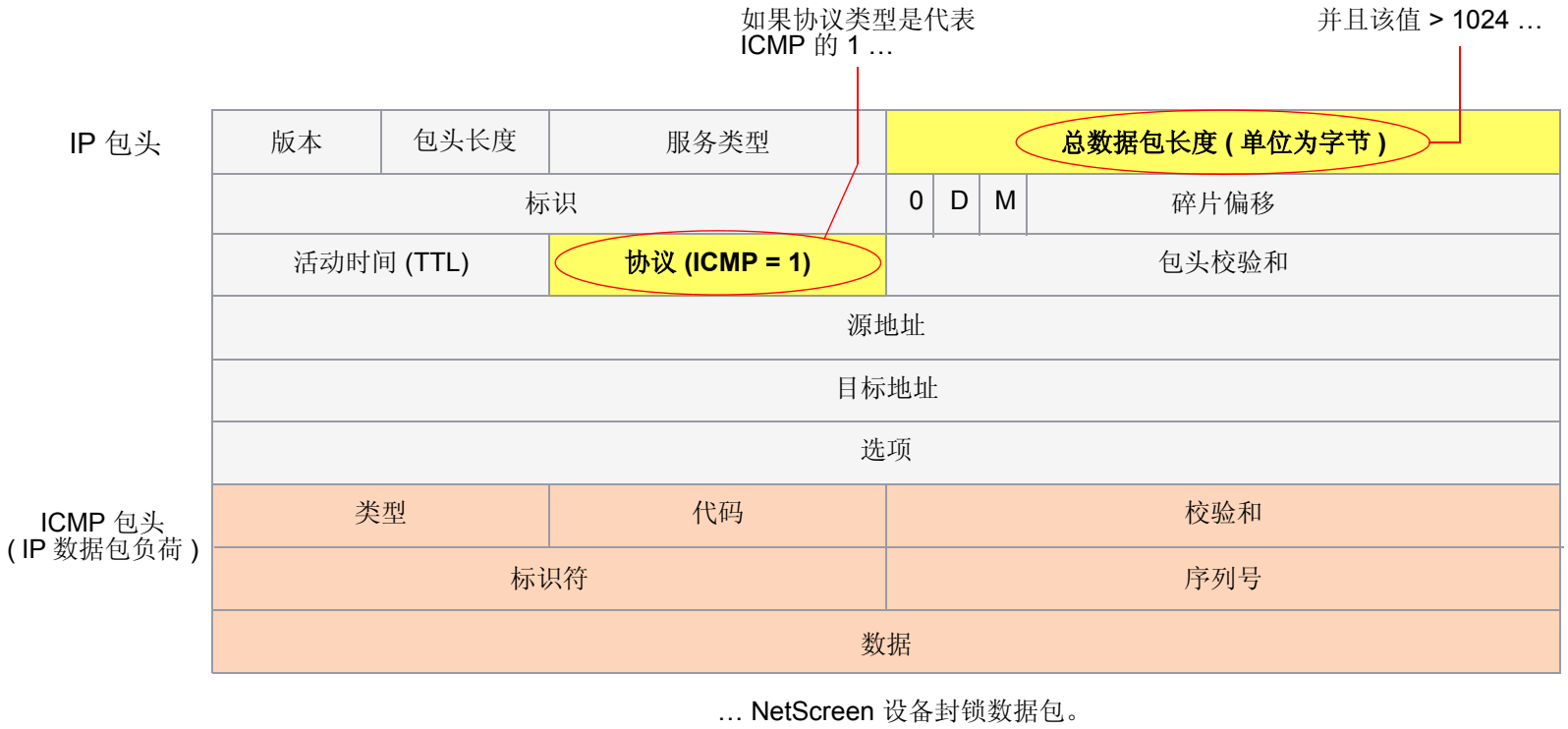
Screening > Screen (Zone: 选择区段名称): 选择 **ICMP Fragment Protection**，然后单击 **Apply**。

CLI

```
set zone zone screen icmp-fragment
```

大型 ICMP 数据包

如上节第 206 页上的 “ICMP 碎片”所述，“互联网控制信息协议” (ICMP) 提供了错误报告和网络侦查功能。由于 ICMP 数据包只包含很短的信息，因此没有合法理由适用于大型 ICMP 数据包。如果 ICMP 数据包异常地大，则可能有错误。例如， Loki 程序使用 ICMP 作为传送隐秘消息的通道。大型 ICMP 数据包的出现可能会使作为 Loki 代理的受损机器暴露。也可能预示某种欺骗活动。



当启用 Large Size ICMP Packet Protection SCREEN 选项时， NetScreen 设备检查并丢弃长度大于 1024 字节的 ICMP 数据包。

要封锁大型 ICMP 数据包，请执行以下任一操作，其中指定的安全区段是 ICMP 数据包始发的区段 :

WebUI

Screening > Screen (Zone: 选择区段名称): 选择 **Large Size ICMP Packet (Size > 1024) Protection**，然后单击 **Apply**。

CLI

```
set zone zone screen icmp-large
```

有害 IP 选项

互联网协议标准 “RFC 791, Internet Protocol” 指定了提供特殊路由选择控制、诊断工具和安全性的一组选项，共八个。尽管这些选项最初预定的用途发挥了作用，但某些人已想出了曲解这些选项的方法，以达到不可恭维的目的。(有关攻击者可利用 IP 选项施加的攻击的概要，请参阅第 12 页上的 “使用 IP 选项的网络侦查”。)

攻击者有时会故意或偶然地错误配置 IP 选项，产生不完整或残缺的字段。不管精心设计该数据包的人的目的如何，错误设置格式都是反常的，并且对目标接收者有着潜在的危害。

IP 包头

如果启用了 Bad IP Option Protection SCREEN 选项，当 IP 数据包包头中的任何 IP 选项的格式被错误设置时，NetScreen 设备将封锁这些数据包。 NetScreen 设备会在事件日志中记录该事件。

要检测和封锁含有错误格式 IP 选项的 IP 数据包，请执行以下任一操作，其中指定的安全区段是数据包始发的区段：

WebUI

Screening > Screen (Zone: 选择区段名称): 选择 **Bad IP Option Protection**，然后单击 **Apply**。

CLI

```
set zone zone screen ip-bad-option
```

未知协议

目前，这些 ID 号 为 137 或更大的协议类型被保留，尚未定义。恰恰因为这些协议未定义，从而无法事先得知某一特定的未知协议是善意的还是恶意的。除非您的网络使用 ID 号 为 137 或更大的非标准协议，否则谨慎的做法是封锁这类未知的元素进入受保护网络。

如果启用了 Unknown Protocol Protection SCREEN 选项，当协议字段包含 ID 号 为 137 或更大数的协议时，NetScreen 设备将丢弃这些数据包。

要丢弃采用未知协议的数据包，请执行以下任一操作，其中指定的安全区段是数据包始发的区段：

WebUI

Screening > Screen (Zone: 选择区段名称): 选择 **Unknown Protocol Protection**，然后单击 **Apply**。

CLI

```
set zone zone screen unknown-protocol
```

IP 数据包碎片

数据包通过不同的网络时，有时必须根据每个网络的最大传输单位 (MTU)，将数据包分成更小的部分 (碎片)。攻击者可能会利用 IP 栈实现方案的数据包重组代码中的漏洞，通过 IP 碎片进行攻击。当受害系统收到这些数据包时，造成的结果小到无法正确处理数据包，大到使整个系统崩溃。

如果允许 NetScreen 设备拒绝安全区段上的 IP 碎片，设备将封锁在绑定到该区段的接口处接收到的所有 IP 数据包碎片。

要丢弃 IP 数据包碎片，请执行以下任一操作，其中指定的安全区段是数据包碎片始发的区段：

WebUI

Screening > Screen (Zone: 选择区段名称): 选择 **Block Fragment Traffic**，然后单击 **Apply**。

CLI

```
set zone zone screen block-frag
```

SYN 碎片

互联网协议 (IP) 在发起 TCP 连接的 IP 数据包中，封装了 “传输控制协议” (TCP) SYN 片段。由于这种数据包的用途是发起连接并在响应时调用 SYN/ACK 片段，因此 SYN 片段通常不包含任何数据。因为 IP 数据包很小，没有必要将其分为片段。分为片段的 SYN 数据包是不正常的，要引起怀疑。为安全起见，请封锁这类未知的元素进入受保护的网络。

如果启用了 SYN Fragment Detection SCREEN 选项，那么，当 IP 包头表明数据包已分为碎片，并且在 TCP 包头中设置了 SYN 标志时， NetScreen 设备将会检测到这些数据包。 NetScreen 设备将在进入接口的 SCREEN 计数器列表中记录该事件。

要丢弃包含 SYN 碎片的 IP 数据包，请执行以下任一操作，其中指定的安全区段是数据包始发的区段 :

WebUI

Screening > Screen (Zone: 选择区段名称): 选择 **SYN Fragment Protection**，然后单击 **Apply**。

CLI

```
set zone zone screen syn-frag
```


如果设置了 “更多碎片” 标志 …
或者在 “碎片偏移” 字段中有非零值 …
IP 包头
版本
包头长度
服务类型
总数据包长度 (单位为字节)
标识
0
D
M
碎片偏移
活动时间 (TTL)
协议
包头校验和
源地址
目标地址
选项 (如果有)
TCP 包头
16 位源端口号
16 位目标端口号
32 位序列号
32 位确认编号
4 位包头长度
保留 (6 位)
URG
ACK
PSH
RST
SYN
FIN
16 位窗口大小
16 位 TCP 校验和
16 位紧急指针
选项 (如果有)
数据 (如果有)
… 并且设置了 SYN 标志 …
… 则 NetScreen 设备丢弃数据包。

7

GPRS 超额计费攻击防护

可以配置 NetScreen 设备以防止 GPRS (通用分组无线业务) 超额计费攻击。只有 NetScreen-500 和 NetScreen-5000 系列设备支持此功能。

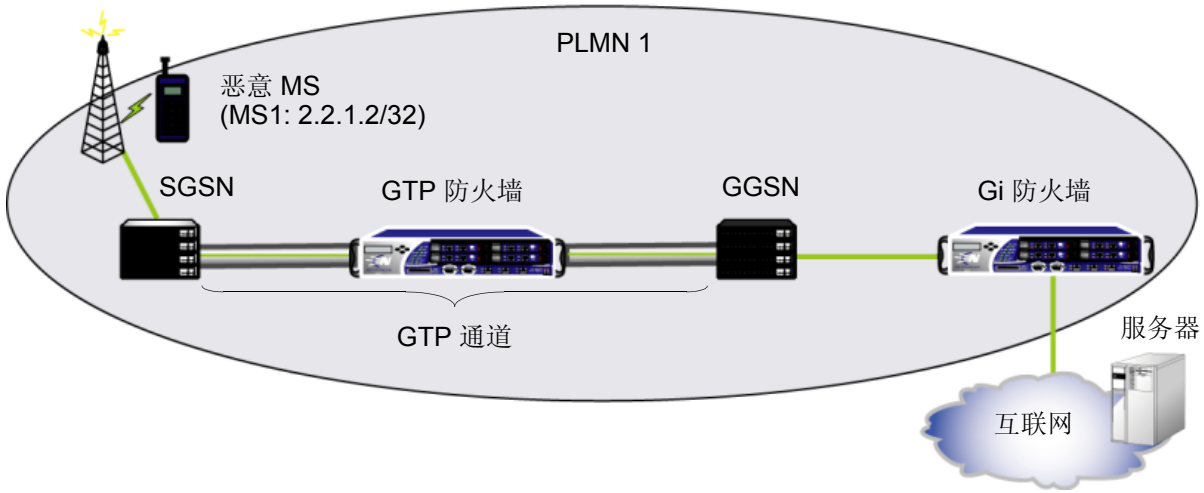
本章包括以下部分 :

超额计费攻击说明

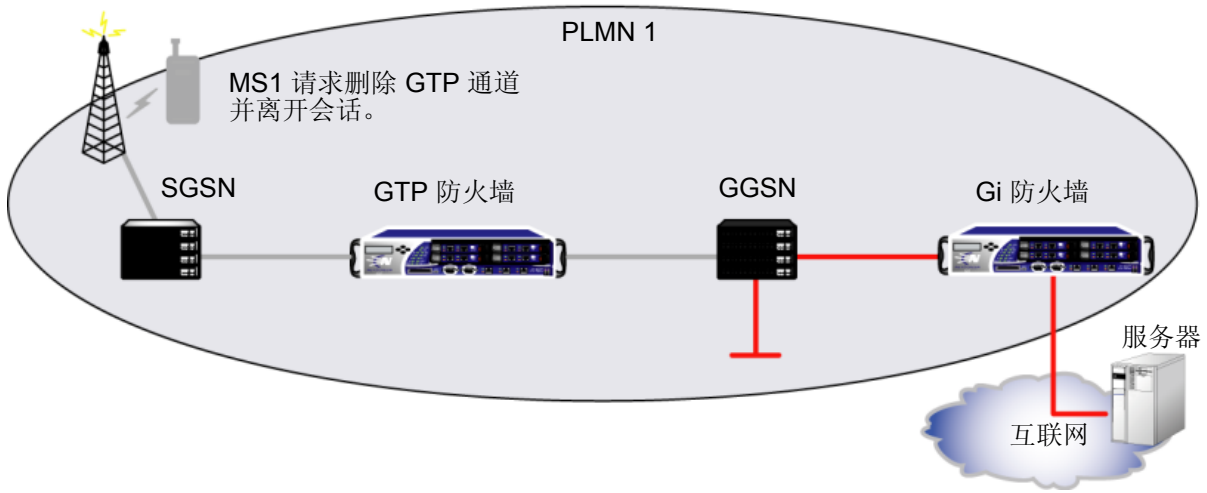
在解释什么是超额计费攻击之前，首先要了解移动站 (MS) 是从 IP 池取得 IP 地址的，这一点十分重要。这就是说，超额计费攻击可以多种方式发生。换言之，超额计费攻击可以在合法用户将其 IP 地址返回 IP 池时发生，此时攻击者可以劫持该 IP 地址，由于会话是打开的，IP 地址易受攻击。攻击者控制了 IP 地址后，即可免费下载数据 (更准确地说，是由合法用户付费)，或者发送数据给其他用户，而不会被检测到和报告。

IP 地址变为可用并被重新指定给另一个 MS 时也可能发生超额计费攻击。由前一个 MS 发起的信息流可能被转发到新的 MS，从而引起新 MS 因未经请求的信息流被计费。下图详细说明了这种情况。

MS1 取得 IP 地址并请求到 GGSN 的 GTP 通道。 SGSN 根据 MS1 的请求建立一个 GTP 通道。 MS1 发起一个与服务器的会话。



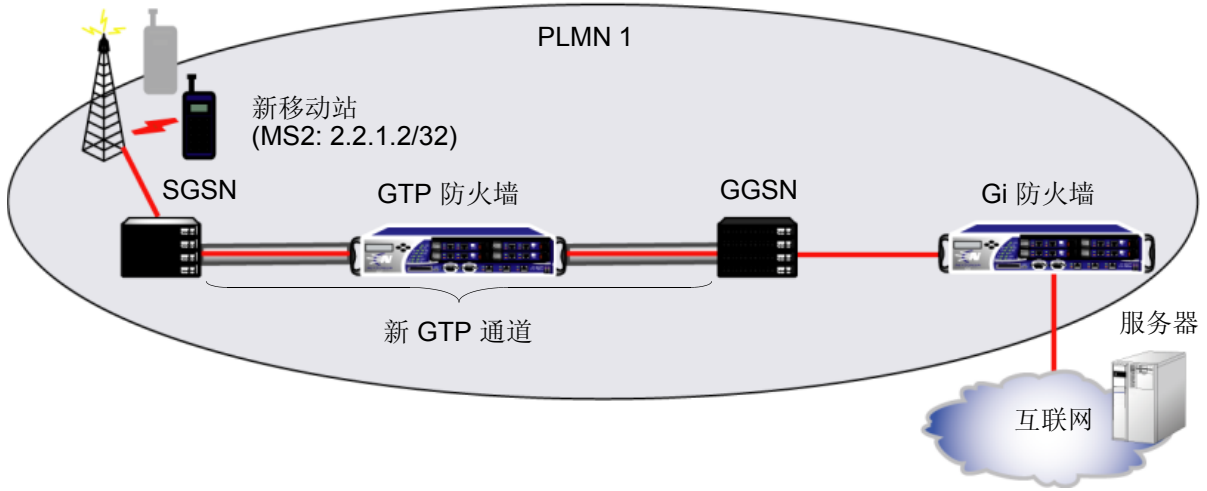
当服务器开始向 MS1 发送数据包时， MS1 同时向 SGSN 发送请求删除 GTP 通道，但在 Gi 防火墙上将与服务器的会话保留为打开状态。服务器继续向 GGSN 发送数据包。 Gi 防火墙不知道 GTP 通道已被删除，将数据包转发给 GGSN。由于 GTP 通道不再存在， GGSN 会丢弃数据包。



一个新移动站 MS2 (受害者) 向 SGSN 发送请求，要求获得到 GGSN 的 GTP 通道并接收到 IP 地址 2.2.1.2/32 (MS1 使用的同一 IP 地址)。SGSN 创建一个到 GGSN 的新 GTP 通道。

检测到目标 IP 地址 2.2.1.2 的新 GTP 通道后，一直在为具有同一目标 IP 地址但不同 MS (MS1) 的旧会话接收数据包的 GGSN 即把这些数据包转发给 MS2。

尽管 MS2 没有请求应发给 MS1 的信息流， MS2 因此而被计费。



超额计费攻击解决方案

要保护 PLMN (公共陆地移动网络) 的用户免受超额计费攻击，需要两个 NetScreen 设备并需要 NSGP (NetScreen 网守协议) 和 NSGP 模块。

NSGP 模块

NSGP 模块包括两个组件 : 客户端和服务器。此版本的 ScreenOS 支持 NSGP 的服务器组件，这意味着可以将 NetScreen 设备配置为服务器，又称为 Gi 防火墙。客户端设备 [又称为 GTP (GPRS 通道协议) 防火墙] 必须运行 ScreenOS 5.0.0 GPRS 固件 (有关详细信息，请参考 *ScreenOS 5.0.0 GPRS Reference Guide*)。

在 GPRS 网络中，NetScreen 设备部署在 Gi 接口时，称为 Gi 防火墙。Gi 接口是 GGSN (网关 GPRS 支持节点) 和互联网或连接到 PLMN 的目标网络之间的连接。

NetScreen 设备部署在同一 PLMN 内的 GGSN 和 SGSN (服务 GPRS 支持节点) 之间时，称为 GTP 防火墙。

NetScreen 网守协议

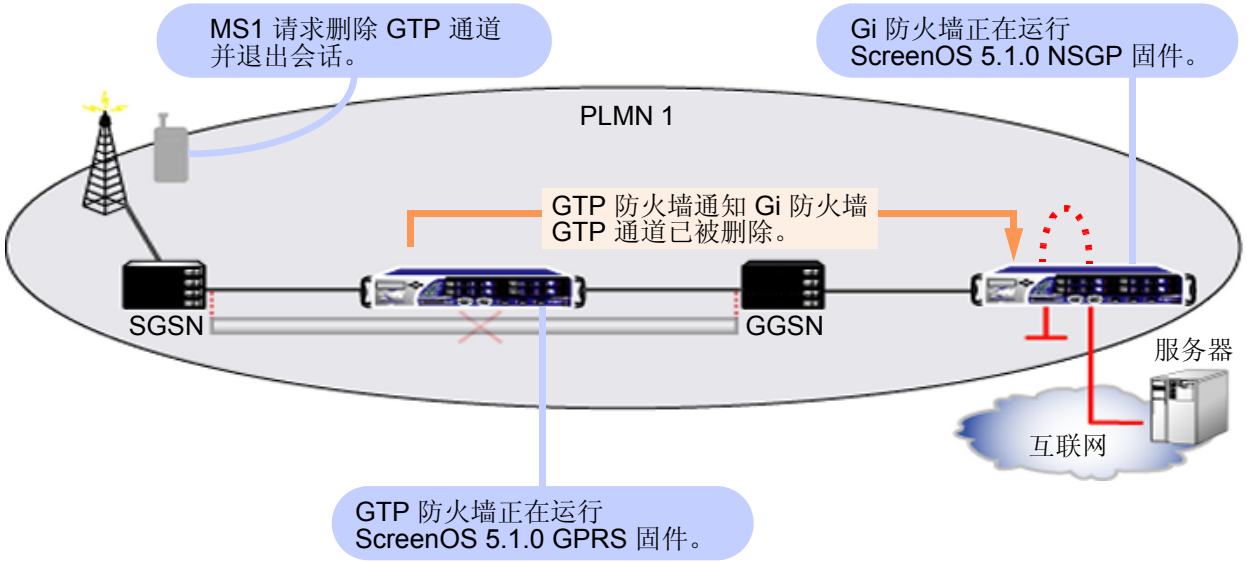
NSGP 使用 “传输控制协议” (TCP) 并通过以设定的时间间隔发送 Hello 消息监控客户端和服务器之间的连通性。NSGP 当前只支持 “session” 类型的环境，该环境是保留用户会话信息的空间，它被绑定到一个安全区段并由一个唯一数字 (环境 ID) 标识。

在客户端和服务器设备上配置 NSGP 时，必须在每个设备上使用相同的环境 ID。当客户端向服务器发送 “清除会话” 请求时，该请求必须包括服务器的环境 ID 和 IP 地址。接收到 “清除会话” 消息后，服务器即匹配环境 ID，然后从其表中清除会话。

将 GTP 防火墙上的 NSGP 配置为删除 GTP 通道时向 Gi 防火墙发出通知，将 Gi 防火墙上的 NSGP 配置为当 Gi 防火墙从 GTP 防火墙得到 GTP 通道被删除的通知时能够自动清除会话。通过清除会话， Gi 防火墙可以停止未经请求的信息流。

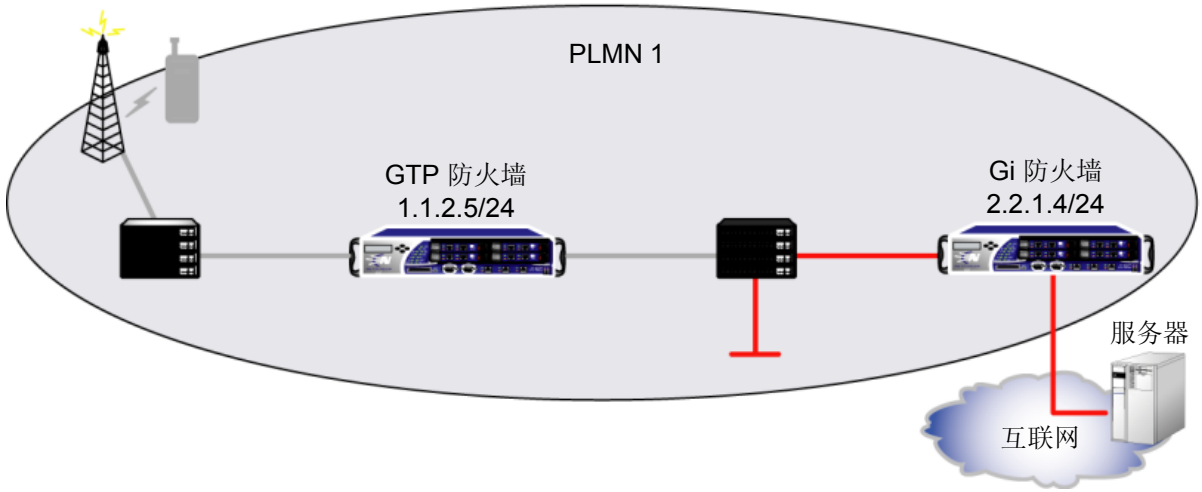
下图说明了 NetScreen 设备如何阻止超额计费攻击。

发起与服务器的会话之后，在服务器开始向 MS1 发送数据包时， MS1 即向 SGSN 发送请求，要求删除 GTP 通道并退出会话。删除通道后， GTP 防火墙立即通知 Gi 防火墙 GTP 通道已被删除。 Gi 防火墙从其表中移除会话。
此后，当服务器试图向 GGSN 发送数据包时， Gi 防火墙会拦截并丢弃数据包。
因此，新 MS 即使使用与以前的 MS 相同的 IP 地址，也不会接收到不是它自己发起的信息流并因此被计费。



范例：配置超额计费攻击防护功能

在本例中，您要设置 NetScreen 设备接口[1] 上的 Overbilling 选项以允许 “超额计费攻击”信息交换并要配置 NSGP。



WebUI

Network > Interface > Edit (ethernet1/2): 输入以下内容，然后单击 **Apply**:

Zone Name: Untrust (选择)

IP Address/Netmask: 2.2.1.4/24

Management Services: Telnet (选择)

Other Services: Overbilling (选择)

1. 必须在每个 NetScreen 设备，即 GTP 防火墙 (客户端) 和 Gi 防火墙 (服务器) 的接口上启用，此功能才能生效。客户端的接口和服务器必须具有不同的 IP 地址。另外，只能在物理以太网接口上启用 NSGP。

Configuration > Advanced > NSGP (Overbilling): 输入以下内容，单击 **Add**，然后单击 **OK**:

Context ID: 2

Zone: Untrust

CLI

```
ns500-> set interface ethernet1/2 zone Untrust
ns500-> set interface ethernet1/2 ip 2.2.1.4/24
ns500-> set interface ethernet1/2 manage telnet
ns500-> set interface ethernet1/2 nsgp
ns500-> set nsgp context 2 type session zone untrust
save
```

A

用户定义签名的环境

环境定义数据包中的位置，从中 NetScreen 深入检查 (DI) 模块搜索与攻击对象模式相匹配的签名。定义状态式签名攻击对象时，可以指定以下列表中的任何环境。定义攻击对象后，必须把它放到用户定义的攻击对象组中以在策略中使用。

注意：*用户定义的攻击对象组只能包含用户定义的攻击对象。不能在同一个攻击对象组中混用预定义的和用户定义的攻击对象。*

协议	环境	说明 (将环境设置为 …)
AIM	aim-chat-room-desc	对 America Online Instant Messenger (AIM) 或 ICQ (网络寻呼机) 会话中的聊天室的描述。
	aim-chat-room-name	AIM 或 ICQ 会话中的聊天室名称。
	aim-get-file	用户当前从对等方传输的文件的名称。
	aim-nick-name	AIM 或 ICQ 用户的昵称。
	aim-put-file	用户当前向对等方传输的文件的名称。
	aim-screen-name	AIM 或 ICQ 用户的登录名。
DNS	dns-cname	域名系统 (DNS) 请求或响应中的 CNAME (规范名称)，该规范名称在 RFC 1035, “Domain Names – Implementation and Specification” 中定义。

协议	环境	说明 (将环境设置为 …)
FTP	ftp-command	RFC 959, “File Transfer Protocol (FTP)” 中指定的 FTP 命令之一。
	ftp-password	FTP 登录密码。
	ftp-pathname	任何 FTP 命令中的目录或文件名。
	ftp-username	用户登录 FTP 服务器时输入的名称。
Gnutella	gnutella-http-get-filename	Gnutella 客户端试图检索的文件名。
HTTP	http-authorization	从授权解码的用户名和密码 : 在 RFC 1945, “Hypertext Transfer Protocol – HTTP/1.0” 中说明的超文本传输协议 (HTTP) 请求的基本报头。
	http-header-user-agent	HTTP 请求报头中的用户代理字段。 (当用户访问 Web 站点时，他们在此字段提供有关其浏览器的信息。)
	http-request	HTTP 请求行。
	http-status	HTTP 回复中的状态行。 (状态行是 Web 服务器发送给客户端传达连接状态的三位代码。例如， 401 表示 “未经授权”， 404 表示 “未找到”。)
	http-text-html	HTTP 事务中的文本，或者说是超文本标记语言 (HTML) 数据。
	http-url	HTTP 请求中的统一资源定位器 (URL)，与其在数据流中的显示一致。
	http-url-parsed	从包含 HTTP 中使用的 URL 的 unicode 字符串解码的 “规格化” 文本字符串。
	http-url-variable-parsed	HTTP-GET 请求的 URL 中一个解码的通用网关接口 (CGI) 变量。

协议	环境	说明 (将环境设置为 …)
IMAP	imap-authenticate	互联网邮件访问协议 (IMAP) AUTHENTICATE 命令的一个参数。该参数表明 IMAP 客户端向服务器建议的认证机制的类型。例如， KERBEROS_V4、GSSAPI (请参阅 RFC 1508, “Generic Security Service Application Program Interface”) 和 SKEY。 有关 IMAP 的信息，请参阅 RFC 1730, “Internet Message Access Protocol – Version 4” 和 RFC 1731, “IMAP4 Authentication Mechanisms”。
	imap-login	IMAP LOGIN 命令中的用户名或明文密码。
	imap-mailbox	IMAP SELECT 命令中的邮箱文本字符串。
	imap-user	IMAP LOGIN 命令中的用户名。
MSN Messenger	msn-display-name	Microsoft Network (MSN) Instant Messaging 会话中用户的显示名称。
	msn-get-file	客户端要从对等方下载的文件的名称。
	msn-put-file	客户端要向对等方发送的文件的名称。
	msn-sign-in-name	MSN Instant Messaging 用户的屏幕名 (登录名)。
POP3	pop3-auth	邮局协议版本 3 (POP3) 会话中的 AUTH 命令。有关 POP3 的信息，请参阅 RFC 1939, “Post Office Protocol – Version 3”。
	pop3-header-from	在 “发件人 :” 中的文本字符串 POP3 事务中的电子邮件的报头。
	pop3-header-line	POP3 事务中电子邮件的任何报头行中的文本字符串。
	pop3-header-subject	在 “主题 :” 中的文本字符串 POP3 事务中的电子邮件的报头。
	pop3-header-to	在 “收件人 :” 中的文本字符串 POP3 事务中的电子邮件的报头。
	pop3-mime-content-filename	POP3 会话中多用途互联网邮件扩展 (MIME) 附件的内容文件名。

协议	环境	说明 (将环境设置为 …)
POP3 (续)	pop3-user	POP3 会话中的用户名。
SMB	smb-account-name	SMB 会话中 SESSION_SETUP_ANDX 请求的服务器消息块 (SMB) 的帐户名。
	smb-connect-path	SMB 会话中 TREE_CONNECT_ANDX 请求的连接路径。
	smb-connect-service	SMB 会话中 TREE_CONNECT_ANDX 请求的连接服务的名称。
	smb-copy-filename	SMB 会话中 COPY 请求的文件名。
	smb-delete-filename	SMB 会话中 DELETE 请求的文件名。
	smb-open-filename	SMB 会话中 NT_CREATE_ANDX 和 OPEN_ANDX 请求的文件名。
SMTP	smtp-from	简单邮件传输协议 (SMTP) 会话中 “MAIL FROM” 命令行中的文本字符串，相关信息在 RFC 2821, “Simple Mail Transfer Protocol” 进行了说明。
	smtp-header-from	在 “发件人 :” 中的文本字符串 SMTP 会话中的报头。
	smtp-header-line	SMTP 会话中任何报头行中的文本字符串。
	smtp-header-subject	在 “主题 :” 中的文本字符串 SMTP 会话中的报头。
	smtp-header-to	在 “收件人 :” 中的文本字符串 SMTP 会话中的报头。
	smtp-mime-content-filename	SMTP 会话中多用途互联网邮件扩展 (MIME) 附件的内容文件名。
	smtp-rcpt	SMTP 会话中 “RCPT TO” 命令行的文本字符串。

协议	环境	说明 (将环境设置为 …)
–	stream256	重新组合的规格化 TCP 数据流的头 256 个字节。
Yahoo! Messenger	ymsg-alias	与 Yahoo! Instant Messaging 用户的主用户名关联的备用识别名。
	ymsg-chatroom-message	Yahoo! Instant Messaging 聊天室中交换的消息文本。
	ymsg-chatroom-name	Yahoo! Instant Messaging 聊天室的名称。
	ymsg-nickname	Yahoo! Instant Messaging 用户的昵称。
	ymsg-p2p-get-filename-url	Yahoo! Instant Messaging 对等方机器上的文件位置，以便能够从该位置下载相应的文件。
	ymsg-p2p-put-filename-url	Yahoo! Instant Messaging 对等方机器上的文件位置，以便能够将文件下载到该位置。

索引

T

U

W

X

Y

Z