NetScreen 概念与范例

ScreenOS 参考指南

第 4 卷：攻击检测和防御机制

ScreenOS 5.0.0

编号 093-0927-000-SC

修订本 E

Copyright Notice

NetScreen, NetScreen Technologies, GigaScreen, NetScreen-Global PRO, ScreenOS and the NetScreen logo are registered trademarks of NetScreen Technologies, Inc. in the United States and certain other countries. NetScreen-5GT, NetScreen-5GT Extended, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-500 GPRS, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, NetScreen-IDP 1000, NetScreen-SA 1000, NetScreen-SA 3000, NetScreen-SA 5000, NetScreen-SA Central Manager, NetScreen-SM 3000, NetScreen-Security Manager, NetScreen-Security Manager 2004, NetScreen-Hardware Security Client, NetScreen ScreenOS, NetScreen Secure Access Series, NetScreen Secure Access Series FIPS, NetScreen-IDP Manager, GigaScreen ASIC, GigaScreen-II ASIC, Neoteris, Neoteris Secure Access Series, Neoteris Secure Meeting Series, Instant Virtual Extranet, and Deep Inspection are trademarks of NetScreen Technologies, Inc. All other trademarks and registered trademarks are the property of their respective companies.

Information in this document is subject to change without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without receiving written permission from:

NetScreen Technologies, Inc.
Building #3
805 11th Avenue
Sunnyvale, CA 94089
www.netscreen.com

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 卷的 “攻击检测和防御机制” 介绍 ScreenOS 中可用的网络安全选项。这些选项很多都是可在安全区级启用的 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) 上的任一接口而到达 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应用到可在策略级启用的网络安全选项时，才会粗略地介绍该主题。有关策略的完整解释，请参阅第* ***2****-213 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 “内容监视和过滤” 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 “可疑封包属性” 介绍保护网络资源的几个 SCREEN 选项，防止网络资源受到由不寻常 IP 和 ICMP 封包属性所指示的潜在攻击。

约定

本文档包含几种类型的约定，以下部分将加以介绍：

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：

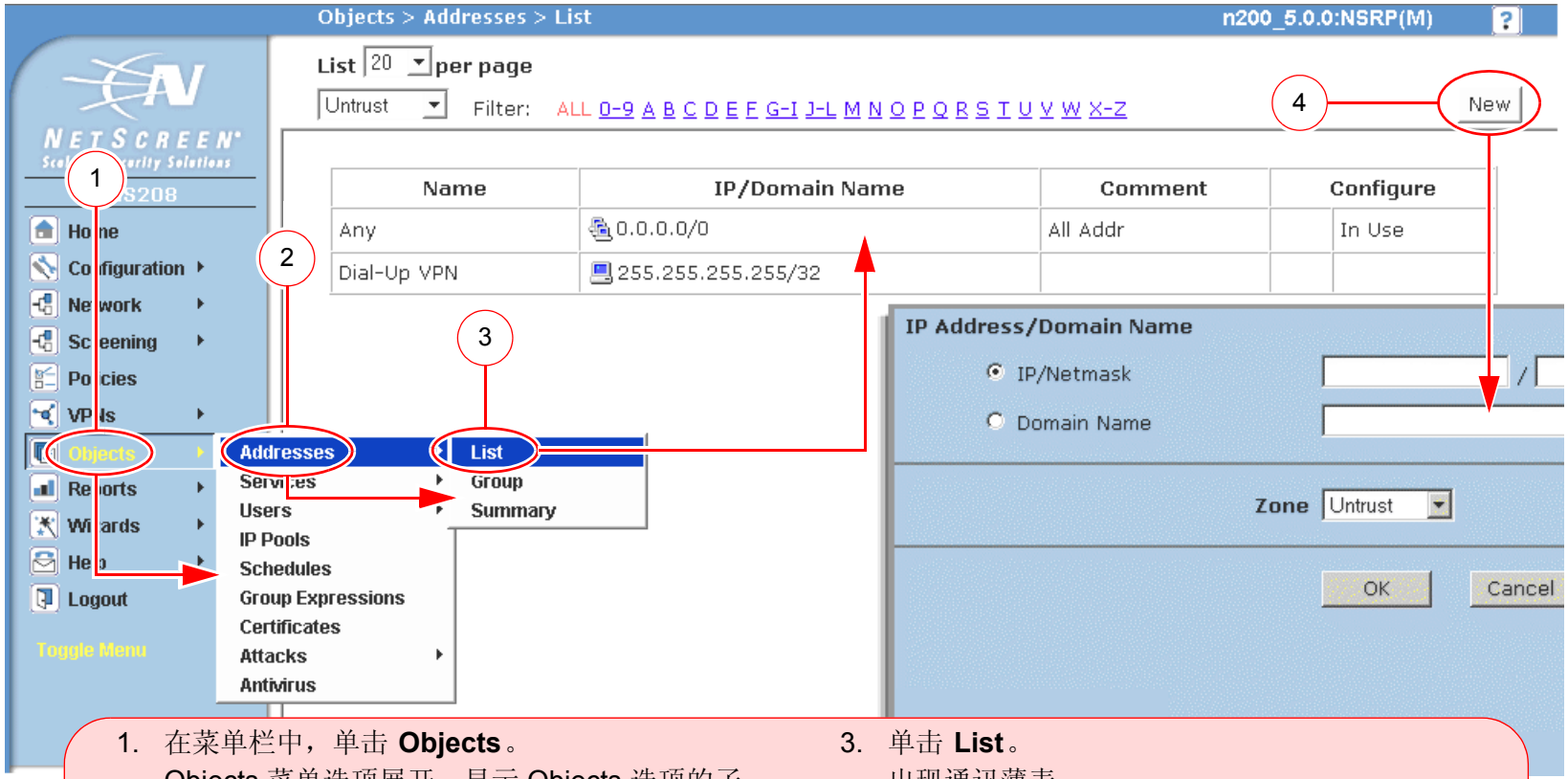
  ```
  set admin user name password
  ```

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，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：

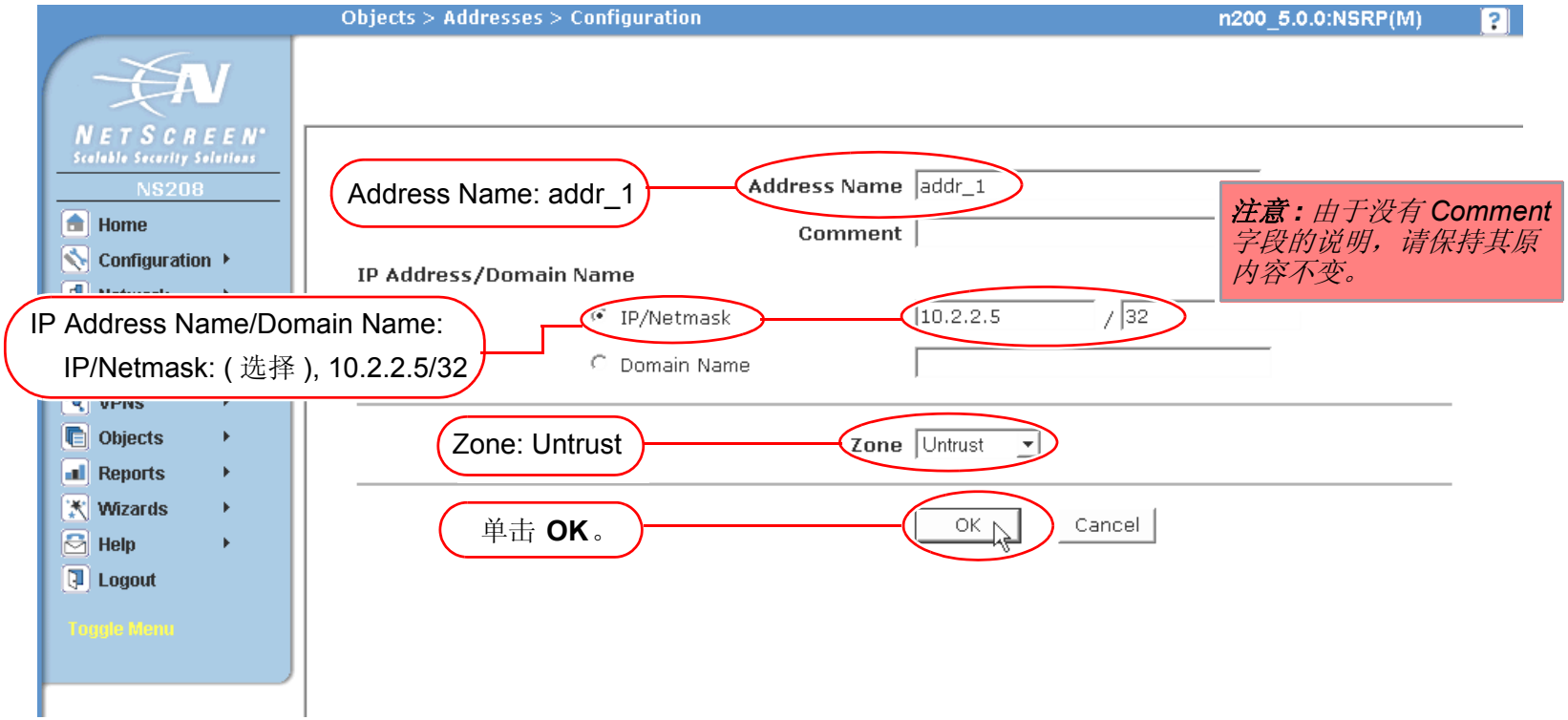
Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

Address Name: addr_1

IP Address/Domain Name:

IP/Netmask: (选择), 10.2.2.5/32

Zone: Untrust

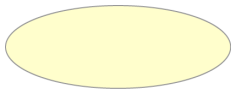


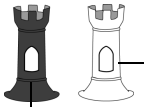
插图约定

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

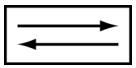

安全区段


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，则整个名称字符串的两边必须用双引号 (“) ；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 将多个连续的空格处理为单个空格。
- 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。*

- ASCII 字符从 32 (十六进制 0x20) 到 255 (0xff)，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。

NETSCREEN 文档

要获取任何 NetScreen 产品的技术文档，请访问 www.netscreen.com/resources/manuals/。

要获取 NetScreen 软件的最新版本，请访问 www.netscreen.com。您必须先注册成为经过授权的用户，然后才能执行此类下载。

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@netscreen.com

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，并因此诱发对其后面的网络的 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数据
- 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

每个攻击通常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，或者建议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。

NetScreen 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。

- 在安全区 (Zone) 上设置的 Screen 选项[1]
- 基于安全区之间、安全区内和超安全区策略的防火墙策略。 (“超区段” 表示全局策略，不涉及任何安全区)

为保护所有连接尝试的安全， NetScreen 设备使用了一种动态封包过滤方法，即通常所说的状态式检查。使用此方法， NetScreen 设备在 IP 封包和 TCP 片段包头中记入各种不同的信息单元 — 源和目的 IP 地址、源和目的端口号，以及封包序列号 — 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 封包到达时， 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，允许响应封包通过防火墙。如果不相符，则丢弃该封包。

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域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，但仍可为这些区段设置 SCREEN 选项。 VLAN 区段支持与第 3 层安全区相同的一组 SCREEN 选项。 (第 2 层安全区支持第 3 层安全区不支持的一个附加 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 网络保护设置工作在两个级别 : 安全区域和策略。 NetScreen 设备在安全区域级执行侦查威慑和 DoS 攻击防御。在内容监视和过滤区域中， NetScreen 设备在区域级应用碎片重组，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，这些活动在区域级发生。区域级防火墙设置是 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一个特定的攻击 — 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。增加了对网络的威胁的了解之后，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，通常是在晚上 9:00 点与 12:00 之间。当含有欺骗性源 IP 地址的封包到来时，您希望 NetScreen 设备发出通知，但不将其丢弃，而是让其通过，或许是将其引导到您在 DMZ 接口连接上连接的 “蜜罐” (honeypot)[2] 中。晚上 8:55 时，您将更改防火墙的行为，从通知并拒绝属于已检测到的攻击的封包，变为通知并接受。当该攻击发生时，即可使用该 “蜜罐” 监视攻击者越过防火墙后的活动。也可以与上游 ISP (互联网服务提供商) 合作，开始跟踪封包来源以找出其来源。

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。

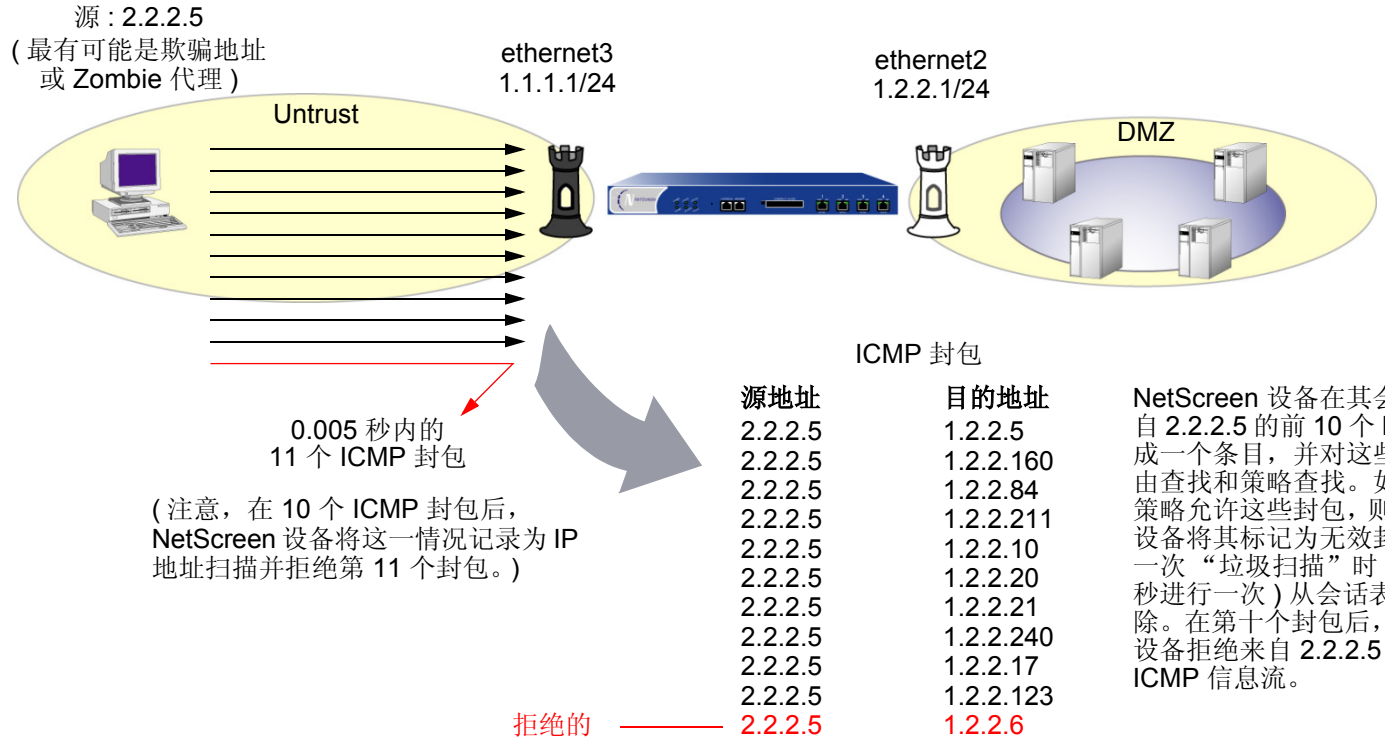
2

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。 NetScreen 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 封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 封包 (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 封包数目。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 封包。



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 地址扫描保护的值[1])

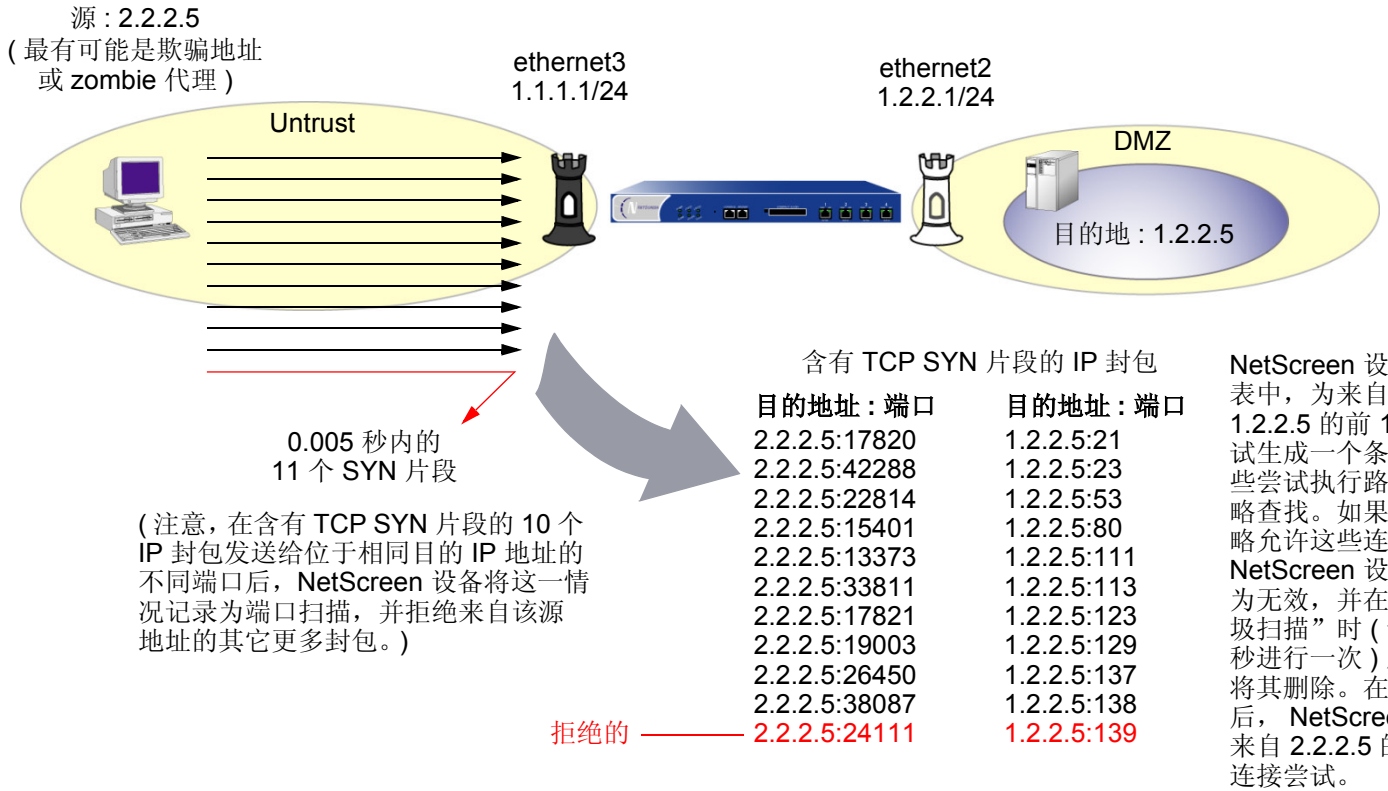
CLI

```
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 5,000 微秒) 将含有 TCP SYN 片段的 IP 封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 (5,000 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封包 (不论目标 IP 地址为何)。



要封锁在特定的安全区内始发的端口扫描，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: (输入触发端口扫描保护的值[2])

CLI

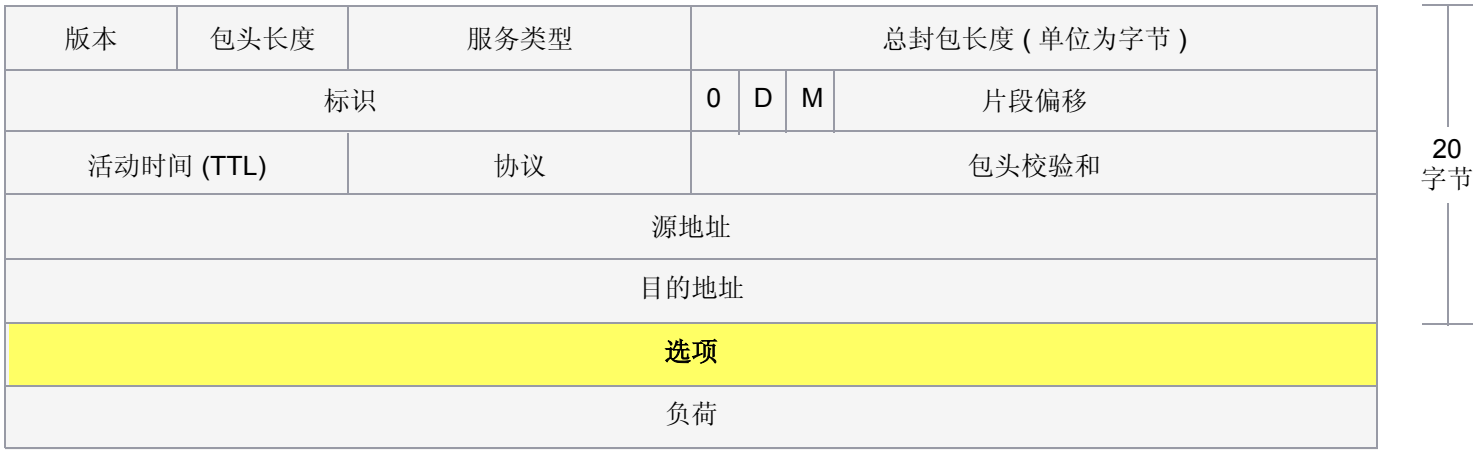
```
set zone zone screen port-scan threshold number
set zone zone screen port-scan
```

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 封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 封包包头中。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 选项及其伴随的属性的列表 :

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，可发送符合“国防部” (DoD) 要求兼容的安全性、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 和 RFC 1038 中说明，目前已废弃。)	未知，但由于此选项已不用，当其在 IP 包头出现时则是可疑的。
松散源路由	0	3	变化	指定一个部分路由列表，供封包在从源到目标的行程中选择。封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封包的真实来源，或者获得对受保护网络的访问权限。 (请参阅第 34 页上的 “IP 源路由选项”。)
记录路由	0	7	变化	记录沿 IP 封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的 40 字节大小限制，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封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，当其在 IP 包头出现时则是可疑的。

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，供封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封包的真实来源，或者获得对受保护网络的访问权限。 (请参阅第 34 页上的 “IP 源路由选项”。)
时戳	2†	4		在封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封包的时间 (采用世界时‡)。网络设备用 IP 编号加以标识。 此选项建立沿封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封包所通过的网络拓扑和寻址方案的信息。

* 标识为 “0” 的选项类的设计目的是提供额外的封包或网络控制。

† 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 (Record Route) 的封包，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 (Internet Timestamp) 的封包，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 (security) 的封包，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 (Stream ID) 的封包，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 选项的封包，请执行以下任一操作，其中指定的安全区是封包始发的区段 :

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)。有此信息，攻击者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 (依赖于操作系统)。

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。如果设备发现这样的包头，则会丢弃封包。

要封锁同时设置了 SYN 和 FIN 标志的封包，请执行以下任一操作，其中指定的安全区是封包始发的区段 :

WebUI

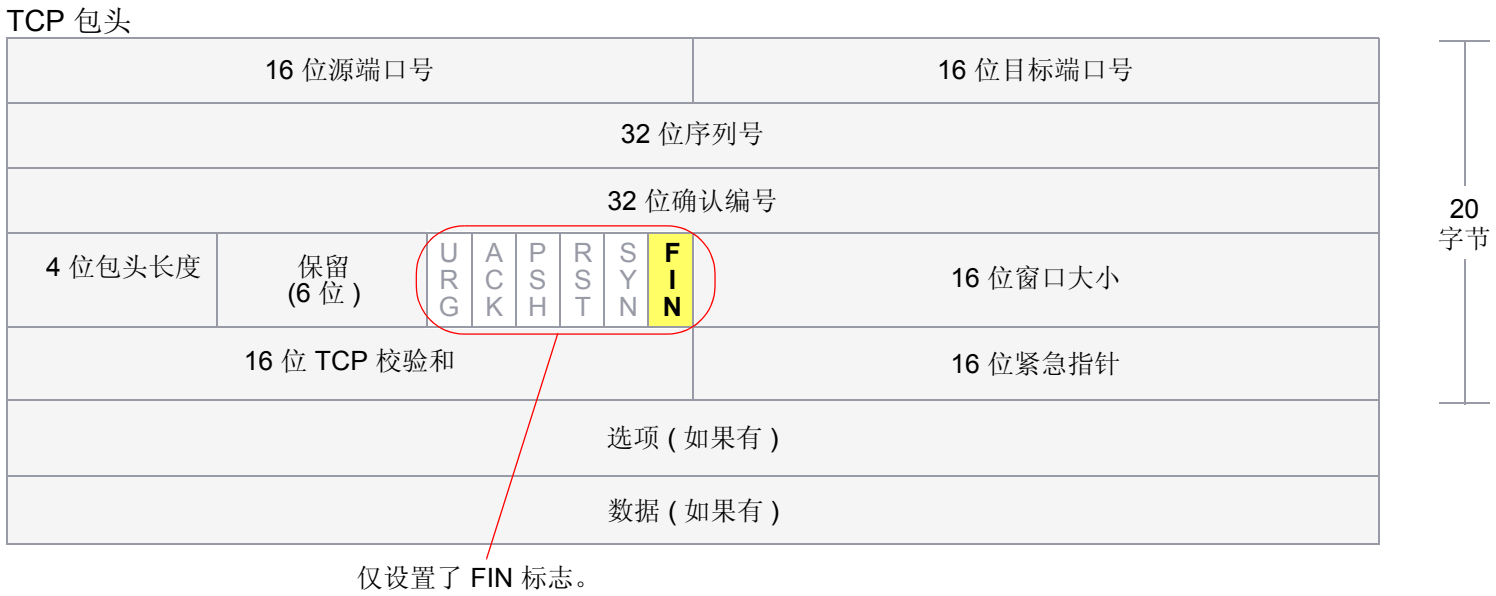
Screening > Screen (Zone: 选择区段名称): 选择 **SYN and FIN Bits Set Protection**，然后单击 **Apply**。

CLI

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

没有 ACK 标志的 FIN 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封包)。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]。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。其它方面可能会完全忽略它。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 片段的其它目的是 : 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。如果设备发现含这种包头的封包，则会丢弃该封包。

3. 在设计 TCP/IP 实现方案时，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。有些则丢弃封包而不发送 RST。

要封锁设置了 FIN 标志而未设置 ACK 标志的封包，请执行以下任一操作，其中指定的安全区是封包始发的区段 :

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 封包。

要封锁未设置标志的封包，请执行以下任一操作，其中指定的安全区是封包始发的区段 :

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

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）这类技巧表明侦查和攻击技术的发展，以躲避检测并成功完成其任务。

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，请执行以下一个或全部操作：

- 启用 SCREEN 选项，以便明确封锁设置了 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: 从区段下拉列表中选择要应用 SCREEN 选项的区段，然后选择 **FIN Bit With No ACK Bit in Flags Protection**。

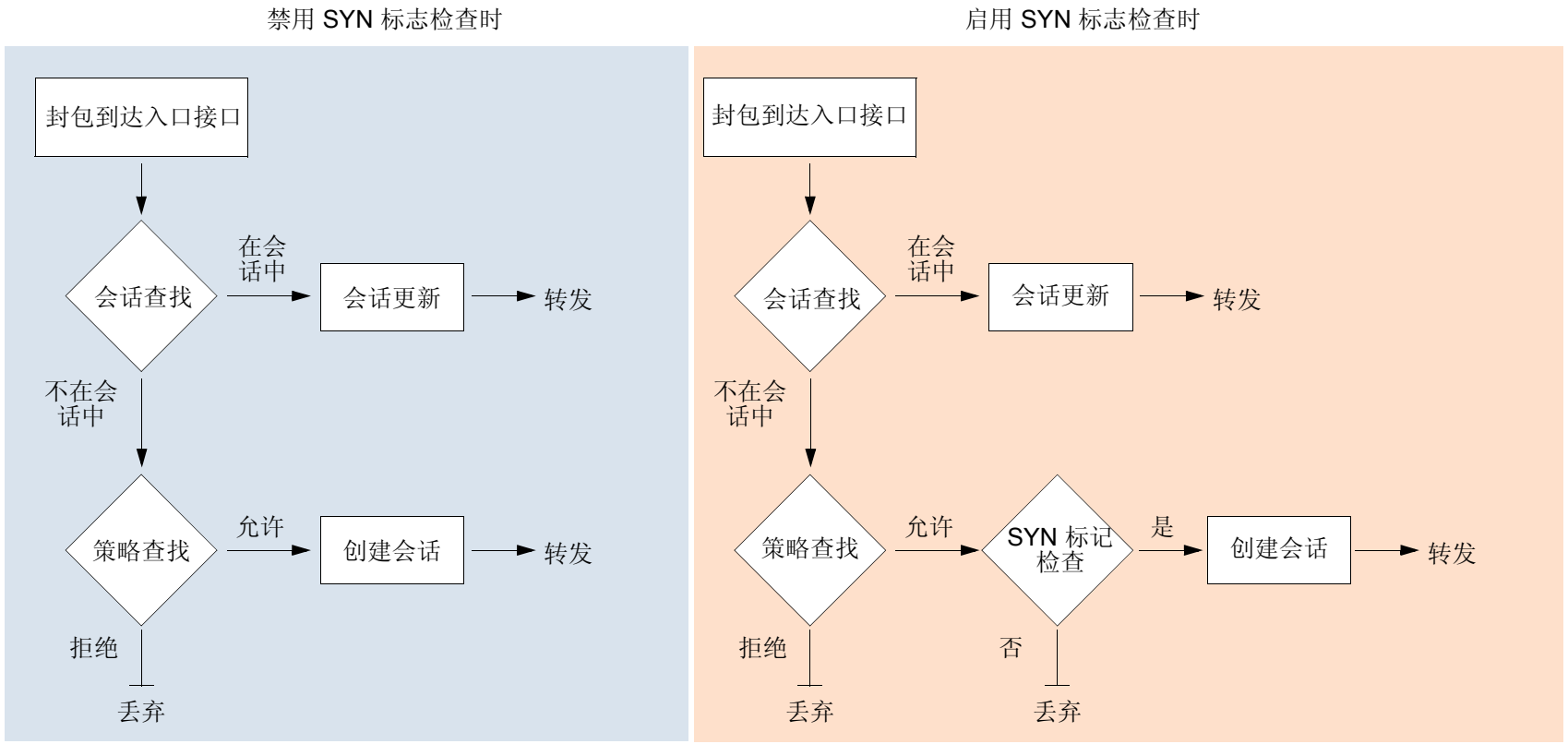
  CLI：输入 **set zone** *name* **screen fin-no-ack**，其中 *name* 是要应用 SCREEN 选项的区段的名称

- 通过输入 CLI 命令 **set flow tcp-syn-check**，更改封包的处理行为，以拒绝所有不属于现有会话的非 SYN 封包。（有关 SYN 标志检查的详细信息，请参阅下节，第 23 页上的 “非 SYN 标志”。）

注意： *更改封包流以检查不属于现有会话的封包是否设置了 SYN 标志，同时阻止其它类型的非 SYN 扫描，例如空扫描 （未设置 TCP 标志时）。*

非 SYN 标志

在缺省情况下， NetScreen 设备不检查会话第一个封包的 SYN 标志。只要策略允许信息流通过防火墙，设备就允许设置了非 SYN 标志的 TCP 片段发起会话。您可以保持此封包流不变，也可以更改此封包流以加强 SYN 标志检查，而后创建会话。禁用和启用 SYN 标志检查时的封包流顺序如下所示 :



可使用以下 CLI 命令来启用或禁用 SYN 检查 :

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

不检查第一封包的 SYN 标志有以下好处 :

- **具有不对称路由功能的 NSRP:** 在动态路由环境下的双活动 NSRP 配置中，主机可能向一个 NetScreen 设备 (NetScreen-A) 发送设置了 SYN 标志的初始 TCP 片段，但是 SYN/ACK 可能被路由到集群中的另一个 NetScreen 设备 (NetScreen-B)。如果此不对称路由发生在 NetScreen-A 让会话与 NetScreen-B 同步之后，则一切正常。另一方面，如果 SYN/ACK 的响应在 NetScreen-A 同步会话并启用 SYN 检查之前到达 NetScreen-B，则 NetScreen-B 拒绝 SYN/ACK，也不会建立会话。禁用 SYN 检查后， NetScreen-B 接受 SYN/ACK 的响应 （即使该响应所属会话不存在）并为该响应创建新的会话表条目。
- **不中断会话 :** 如果 SYN 检查已启用并在工作网络中添加在 “透明” 模式下运行的 NetScreen 设备，会中断所有现有会话，随后必须重新启动会话[4]。这种中断对于长会话 （例如，大的数据传输或数据库备份）是很不利的。同样地，如果重新设置 NetScreen 设备甚或更改策略核心部分的组件[5]，并启用 SYN 检查，则所有现有会话或策略变更所涉及的会话都会中断，必须重新启动。禁用 SYN 检查可以避免对网络信息流造成此类中断。

但是，请注意，以上好处会牺牲下列安全性 :

- **侦查漏洞 :** 当设置了非 SYN 标志的初始 TCP 片段 （如， ACK、 URG、 RST、 FIN）到达一个已关闭的端口，许多操作系统 （例如， Windows）都会用设置了 RST 标志的 TCP 片段响应。如果端口处于开启状态，则接受方不生成任何响应。

  通过对这些响应或不作响应的分析，情报收集者可对受保护的网络以及 NetScreen 策略组进行侦查。如果情报收集者发送设置了非 SYN 标志的 TCP 片段并且策略允许其通过，则接收此类片段的目的主机可能丢弃该片段并用设置了 RST 标志的 TCP 片段进行响应。此类响应通知情报收集者，位于特定地址的活动主机存在以及目标端口号已关闭。情报收集者还获悉防火墙策略允许访问主机上的端口号。

4. 处理这种情况的解决方案是在安装 NetScreen 设备之始禁用 SYN 检查。过几个小时以后 （当建立的会话正在通过 NetScreen 设备时) 再启用 SYN 检查。
5. 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、一个或多个服务、以及操作。

通过启用 SYN 标志检查， NetScreen 设备丢弃不属于现有会话的未设置 SYN 标志的 TCP 片段，也不返回 TCP RST 片段。因此，不论策略组如何或者目标主机上的端口是否打开，扫描器都收不到回复。

- **会话表泛滥：**如果禁用 SYN 检查，攻击者通过使用设置了非 SYN 标志的 TCP 片段的阻塞泛滥攻击受保护的网络，可绕过 NetScreen SYN 泛滥保护功能。尽管目标主机丢弃了封包（并可能用 TCP RST 片段回复），此类泛滥仍能填满 NetScreen 设备的会话表。当会话表被填满时， NetScreen 设备就无法处理合法信息流的新会话。

  通过启用 SYN 检查和 SYN 泛滥保护，可以阻挡此类攻击。检查会话的初始封包上是否设置了 SYN 标志，迫使所有会话都以设置了 SYN 标志的 TCP 片段开头。然后 SYN 泛滥保护限制每秒通过的 TCP SYN 片段的数量，这样会话表就不会被填满。

  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”**。*

如果不需要禁用 SYN 检查，NetScreen 强烈建议您用以下命令启用 SYN 检查：**set flow tcp-syn-check**。启用 SYN 检查后， NetScreen 设备拒绝设置了非 SYN 标志的 TCP 片段，除非片段属于已建立的会话。

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，在封包包头中插入虚假的源地址，以使该封包看似发自信任来源。这种技术称为 IP 欺骗。 NetScreen 具有两种 IP 欺骗检测方法，这两种方法能完成同样的任务：确定封包并非来自其包头所指示的位置。 NetScreen 设备使用的方法取决于 NetScreen 设备是工作于 OSI 模型的第 3 层还是第 2 层。

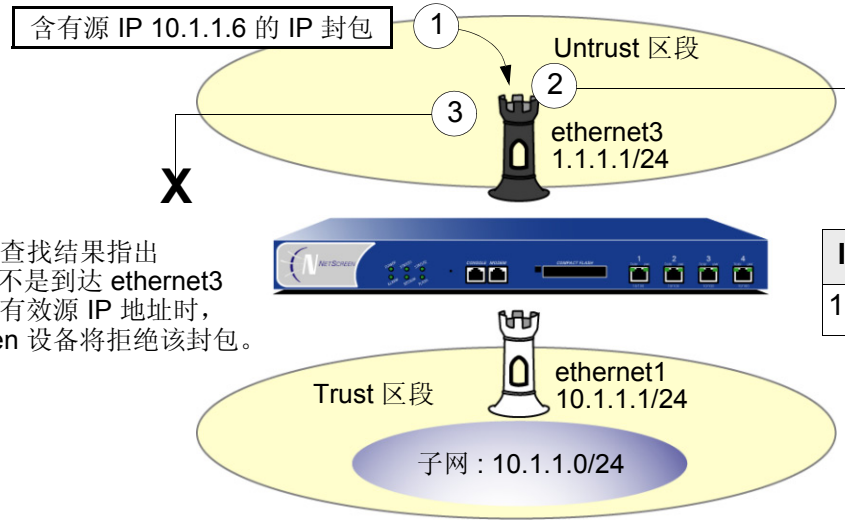
- **第 3 层 –** 当 NetScreen 设备上的接口在路由或 NAT 模式下工作时，检测 IP 欺骗的机制依赖于路由表条目。例如，如果含有源 IP 地址 10.1.1.6 的封包到达 ethernet3，但 NetScreen 设备拥有通过 ethernet1 到 10.1.1.0/24 的路由，那么 IP 欺骗检查会指出该地址到达无效的接口 – 根据路由表中的定义，来自 10.1.1.6 的有效封包只能通过 ethernet1 到达，而不能通过 ethernet3 到达。因此，设备断定该封包含有欺骗性源 IP 地址并将其丢弃。

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

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

1. IP 封包到达 ethernet3。
   其源 IP 地址是 10.1.1.6。

2. 由于在 Untrust 区段中启用了 IP 欺骗保护，因此 NetScreen 设备将检查 10.1.1.6 是否是到达 ethernet3 的封包的有效源 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

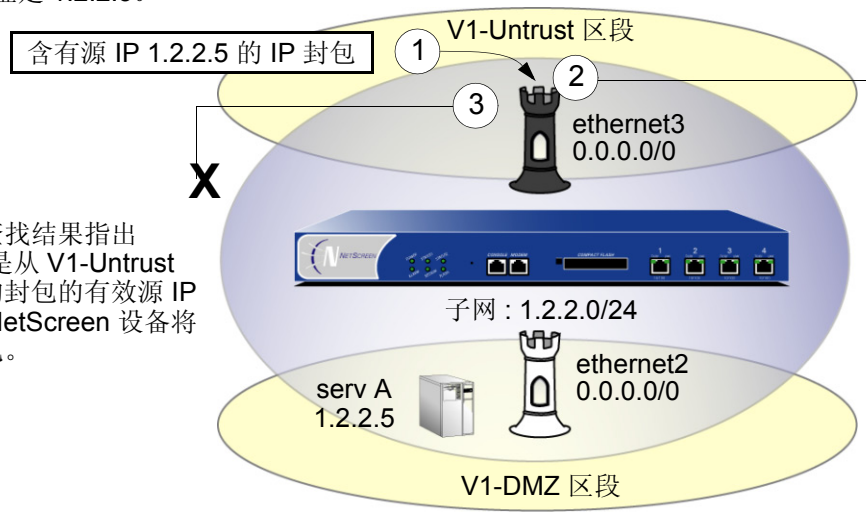
3. 当路由表查找结果指出 10.1.1.6 不是到达 ethernet3 的封包的有效源 IP 地址时，NetScreen 设备将拒绝该封包。

- **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通讯簿条目。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 的封包到达 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。设备断定该封包含有欺骗性源 IP 地址并将其丢弃。

1. IP 封包从 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 欺骗保护，因此 NetScreen 设备将检查 1.2.2.5 是否是从 V1-Untrust 来到此处的封包的有效源 IP 地址。

3. 当通讯簿查找结果指出 1.2.2.5 不是从 V1-Untrust 来到此处的封包的有效源 IP 地址时， NetScreen 设备将拒绝该封包。



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

为跨越多个安全区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 欺骗检查将参考通讯簿找出 V1-Untrust 区段中的 1.2.2.0/24。因此， NetScreen 设备封锁该信息流。

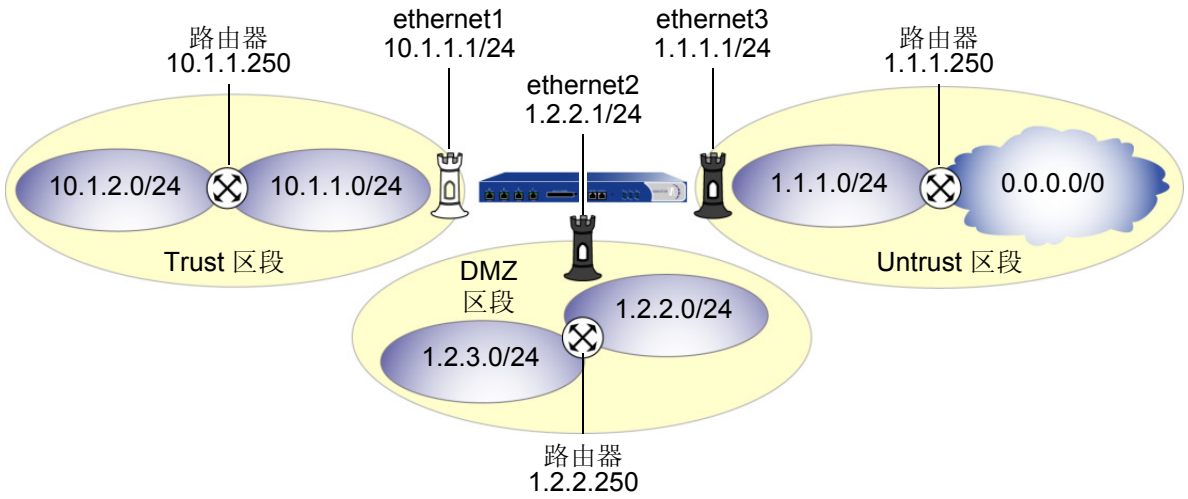
范例 : L3 IP 欺骗保护

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 欺骗保护。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 欺骗保护 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 的封包到达 ethernet1，并且没有通过 ethernet1 到 10.1.2.0/24 子网的路由，则 NetScreen 设备将确定该封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: (有此选项时将其选定)

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: (有此选项时将其选定)

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: (有此选项时将其选定)

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 欺骗保护

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 欺骗保护

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

范例 : L2 IP 欺骗保护

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。

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 设备会将该地址与通讯簿中的地址进行核对。当发现来自 V1-Untrust 区段的封包中的源 IP 地址属于 V1-DMZ 区段的地址时，NetScreen 设备将拒绝该封包。

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 欺骗保护

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

CLI

1. 地址

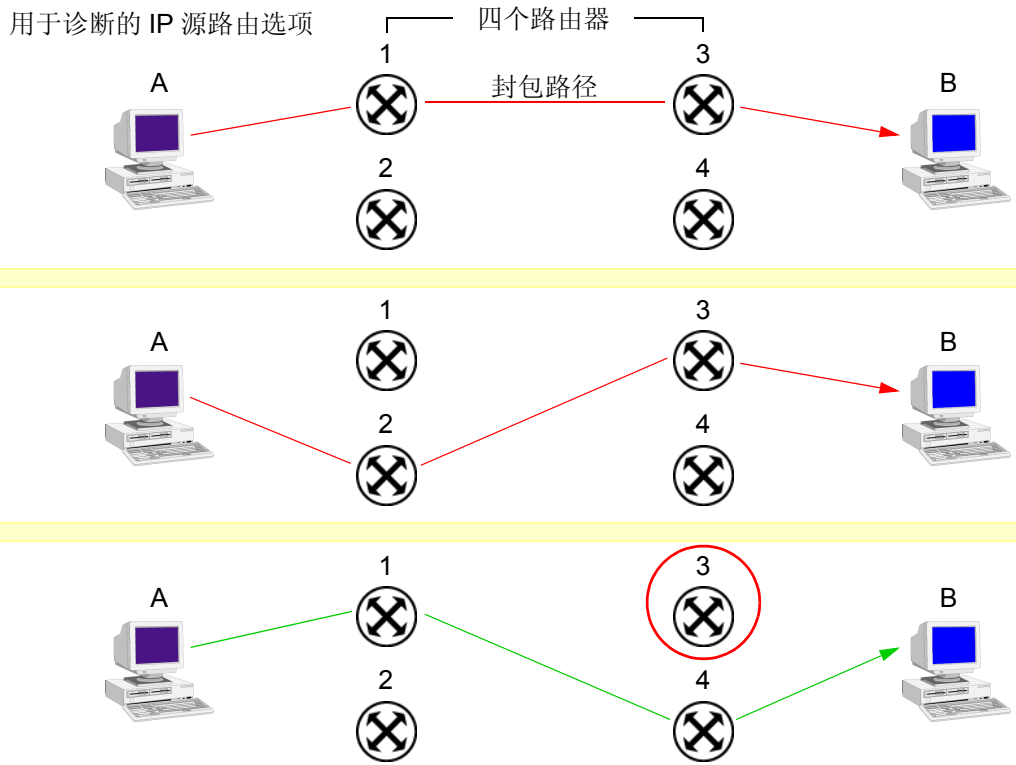
```
set address v1-dmz servA 1.2.2.10/32
set address v1-dmz servB 1.2.2.20/32
set address v1-dmz servC 1.2.2.30/32
```

2. IP 欺骗保护

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

IP 源路由选项

经过设计，源路由允许位于 IP 封包传输来源的用户，指定沿着某一路径的路由器的 IP 地址 (也称为 “hops”)，用户希望 IP 封包在通往目的地的行程中采用该路径。 IP 源路由选项的初始目的是提供路由控制工具，以协助进行诊断分析。例如，如果向特定目的地的封包传输获得不合常规的成功，您可以首先使用记录路由或时戳 IP 选项，来发现沿着该封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，按照从记录路由或时戳选项产生的结果中所了解的地址，沿特定的路径引导信息流。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封包，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。



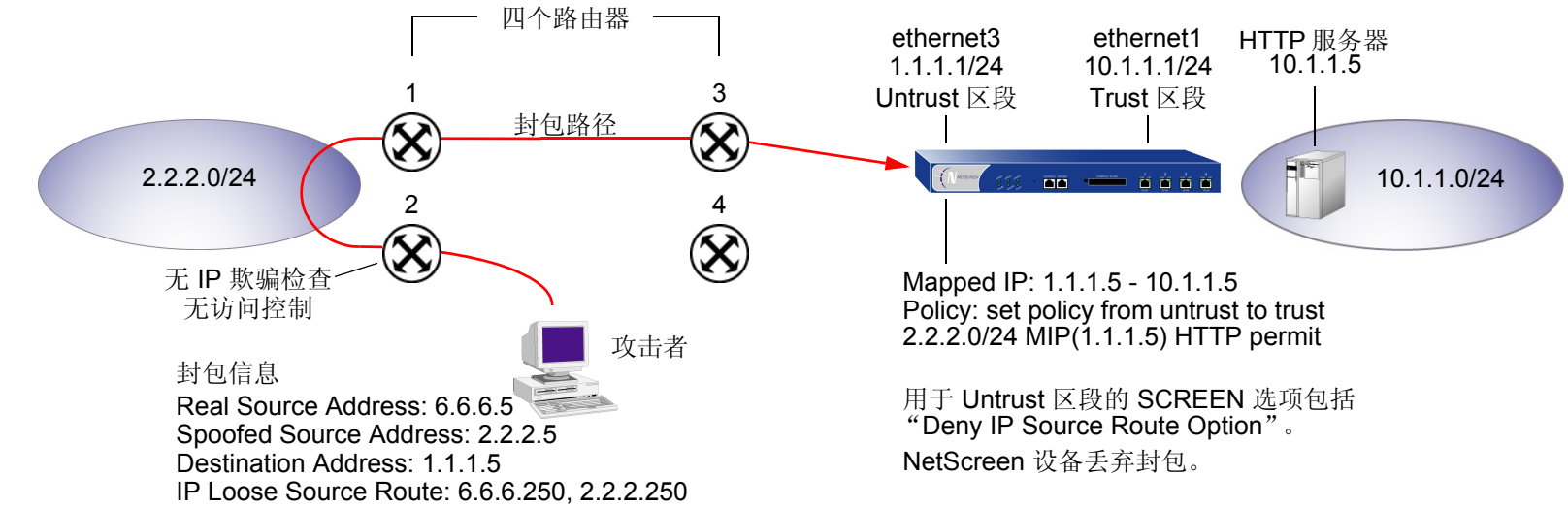
使用路由器 1 和 3 从 A 传输到 B 时，50% 的时间是成功的。

通过利用 IP 源路由， A 发送通过路由器 2 和 3 的信息流。从 A 传输到 B 时仅 50% 的时间保持成功。

通过利用 IP 源路由， A 发送通过路由器 1 和 4 的信息流。从 A 传输到 B 时 100% 的时间都成功。因此，可以断定问题出在路由器 3 中。

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。要了解说明攻击者如何能使用两种欺骗手段的范例，请考虑下面的情况。

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。攻击者欺骗源地址，并且通过使用松散源路由选项，将封包引导通过路由器 2 而到达 2.2.2.0/24 网络，并在此处从路由器 1 发出。路由器 1 将其发送到路由器 3，而后者将其发送到 NetScreen 设备。由于该封包来自 2.2.2.0/24 子网，并且含有来自该子网的源地址，因此该封包看似有效。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。当封包到达 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封包，或者检测这些封包，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) 的封包，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，供封包在从源到目标的行程中选择。封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) 的封包，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，供封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封包，请执行以下任一操作，其中指定的安全区是封包始发的区段：

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封包，请执行以下任一操作，其中指定的安全区是封包始发的区段 :

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拟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。本部分介绍两个方法，攻击者可能会用这些方法填满 NetScreen 设备的会话表，从而产生 DoS 攻击 : 第 40 页上的 “会话表泛滥”和第 47 页上的 “SYN-ACK-ACK 代理泛滥”

会话表泛滥

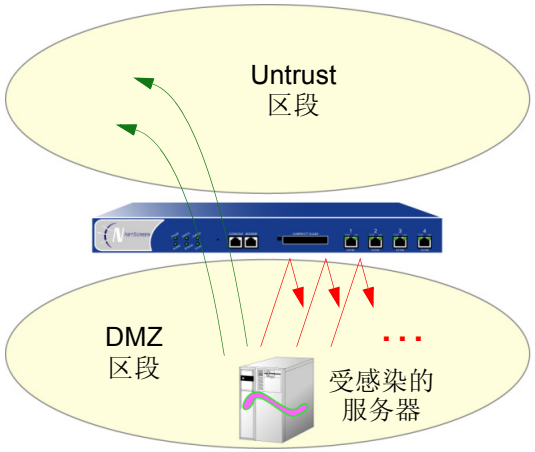
成功的 DoS 攻击会用巨大的假信息流阻塞耗尽受害者的资源，使其无法处理合法的连接请求。 DoS 攻击可以采用多种形式 — SYN 泛滥、SYN-ACK-ACK 泛滥、UDP 泛滥、ICMP 泛滥，等等 — 但它们都会寻求相同的目标 : 填满受害者的会话表。当会话表填满时，该主机不能创建任何新会话，并开始拒绝新连接请求。下列 SCREEN 选项可帮助减轻这类攻击 :

- “基于源和目标的会话限制”
- 第 44 页上的 “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。由于所有由病毒生成的信息流都始发自相同的 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

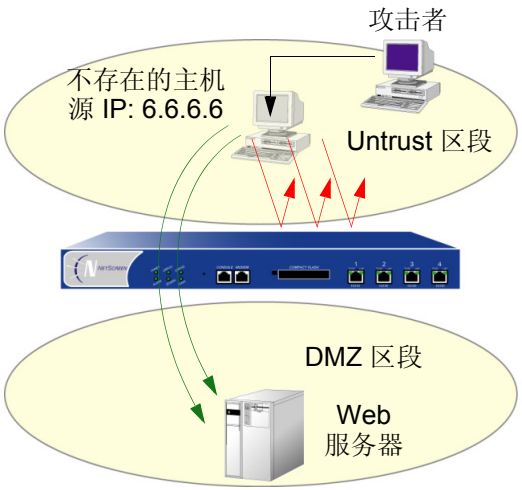


Web 服务器被感染了 Nimda 病毒 / 蠕虫混合体，导致该服务器生成巨大的信息流。

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。

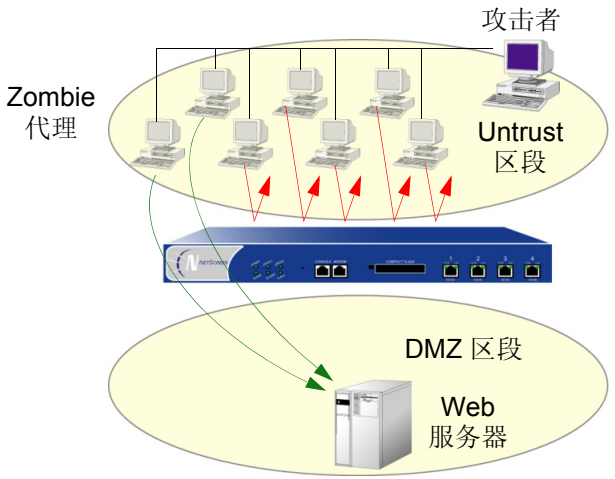
基于源的会话限制的另一个优点是能减轻填满 NetScreen 会话表的企图 — 如果所有连接尝试都始发自相同的源 IP 地址。但是，狡猾的攻击者会发起分布式的拒绝服务 (DDoS) 攻击。在 DDoS 攻击中，恶意信息流可来自上百个称为“zombie 代理”的主机，它们都处在攻击者的秘密控制下。除了 SYN、 UDP 和 ICMP 泛滥检测以及防护 SCREEN 选项外，设置基于目标的会话限制可以确保 NetScreen 设备只允许可接受数目的并发连接请求到达任一个主机 — 无论来源是什么。

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 区段仅保护 Web 服务器，其中任一个主机都不应发起信息流，因此，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。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，但您所选择的防火墙安全性高于偶然的服务器不可访问性。

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

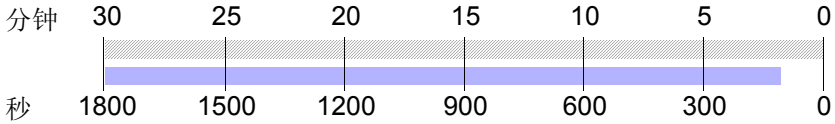
在缺省情况下，初始的三方握手 TCP 会话 20 秒钟超时 (即因无活动而终止)。在建立 TCP 会话后，超时值变为 30 分钟。 HTTP 和 UDP 会话的会话超时值分别是 5 分钟和 1 分钟。当会话开始时，会话超时计数器开始计时，并且当会话活动时每 10 秒钟刷新一次。如果会话空闲时间超过 10 秒钟，则超时计数器的数字开始减小。

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 :

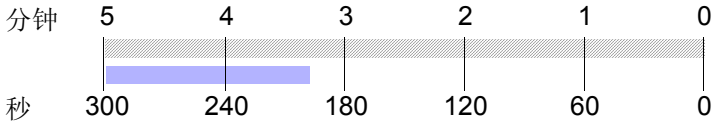
- TCP: 在主动调整时间过程生效的期间，会话超时值从 1800 秒 (30 分钟) 缩短到 1700 秒 (28 分 20 秒)。在此时段内， NetScreen 设备自动删除超时值超过 1700 秒的所有 TCP 会话，首先开始删除最早的会话。

缺省 TCP 会话超时 : 30 分钟 (1800 秒)
主动加速超时 = 10 (-100 秒，从缺省值中减去):
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，首先开始删除最早的会话。

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

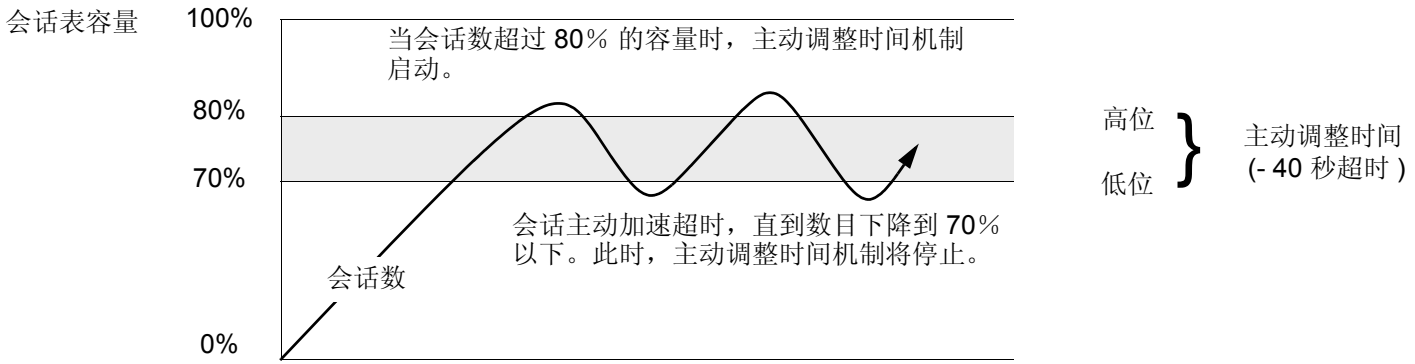


- UDP: 由于缺省的 UDP 会话超时值是 60 秒，规定 100 秒的提前超时设置会导致所有 UDP 会话超时并加上删除标记，在下一次垃圾清扫时被删除。

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

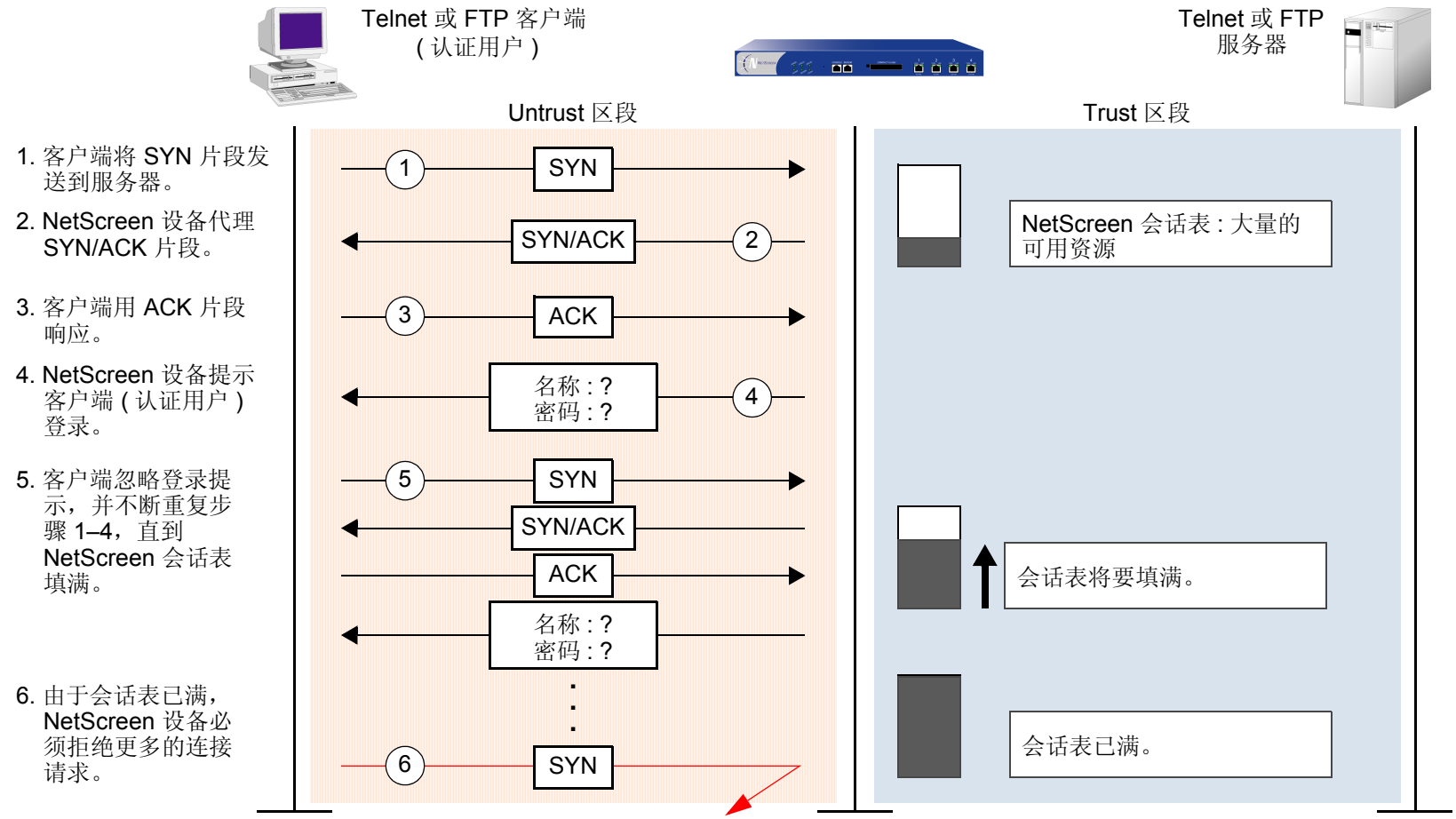
***注意：**必须使用 CLI 来配置主动加速超时设置。*

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 设备向用户发出登录提示。如果怀有恶意的用户没有登录，而是继续发起 SYN-ACK-ACK 会话，则 NetScreen 会话表将填满到设备开始拒绝合法连接请求的状态。



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都是 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 代理泛滥的保护，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): 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 泛滥保护的值[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。

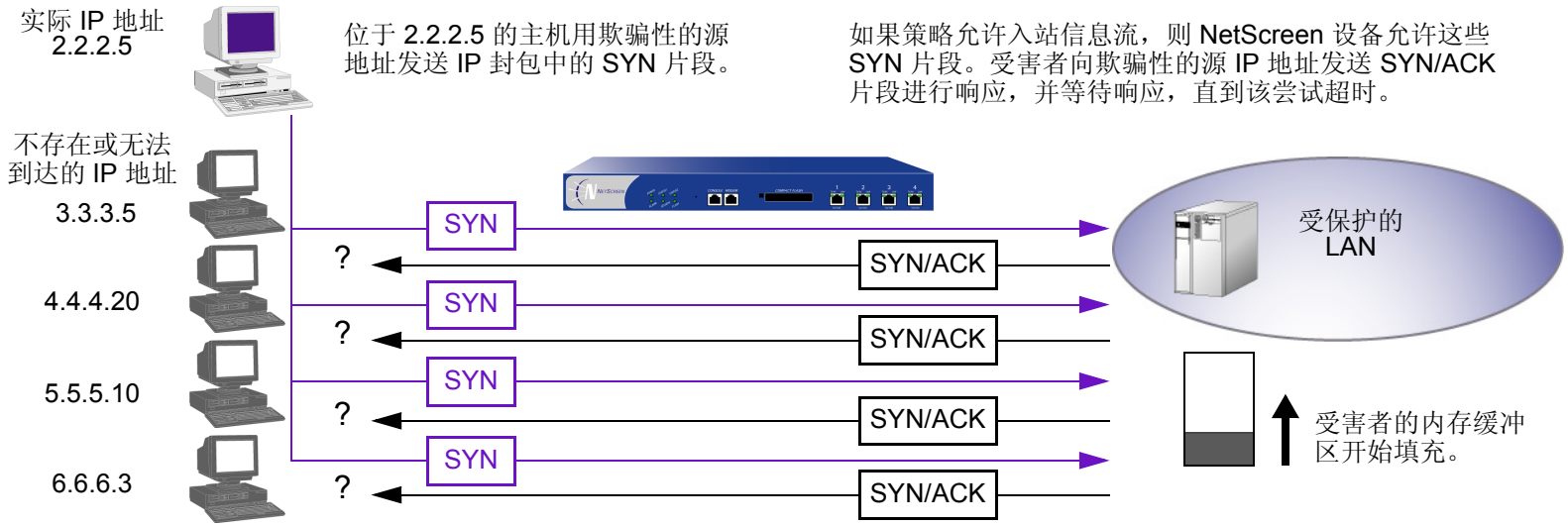
网络 DoS 攻击

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 封包泛滥攻击目标，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。

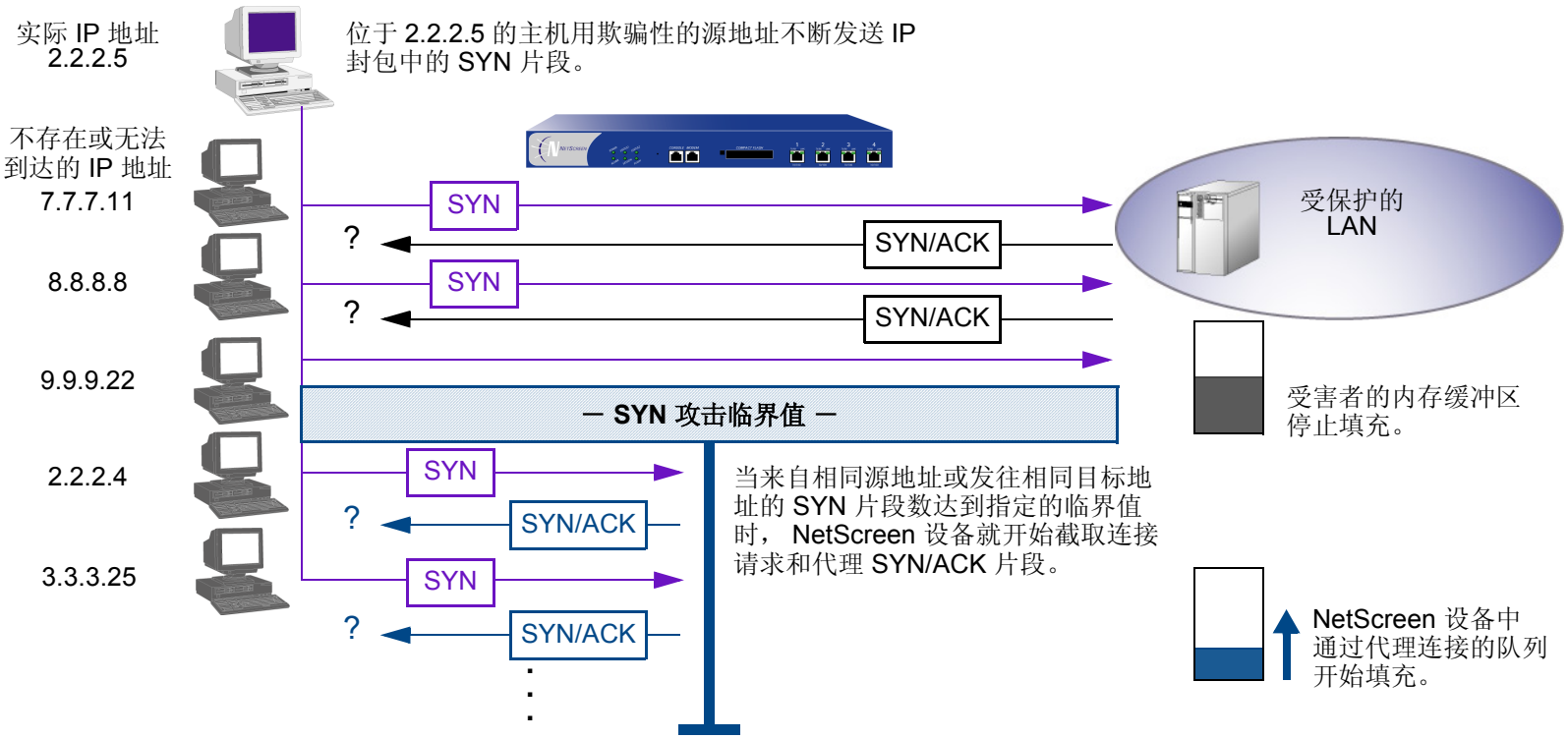
利用三方封包交换，即常说的三方握手，两个主机之间建立 TCP 连接 : A 向 B 发送 SYN 片段； B 用 SYN/ACK 片段进行响应；然后 A 又用 ACK 片段进行响应。 SYN 泛滥攻击用含有伪造的 (“欺骗”) IP 源地址 (不存在或不可到达的地址) 的 SYN 片段塞满某一站点。 B 用 SYN/ACK 片段响应这些地址，然后等待响应的 ACK 片段。因为 SYN/ACK 片段被发送到不存在或不可到达的 IP 地址，所以它们不会得到响应并最终超时。



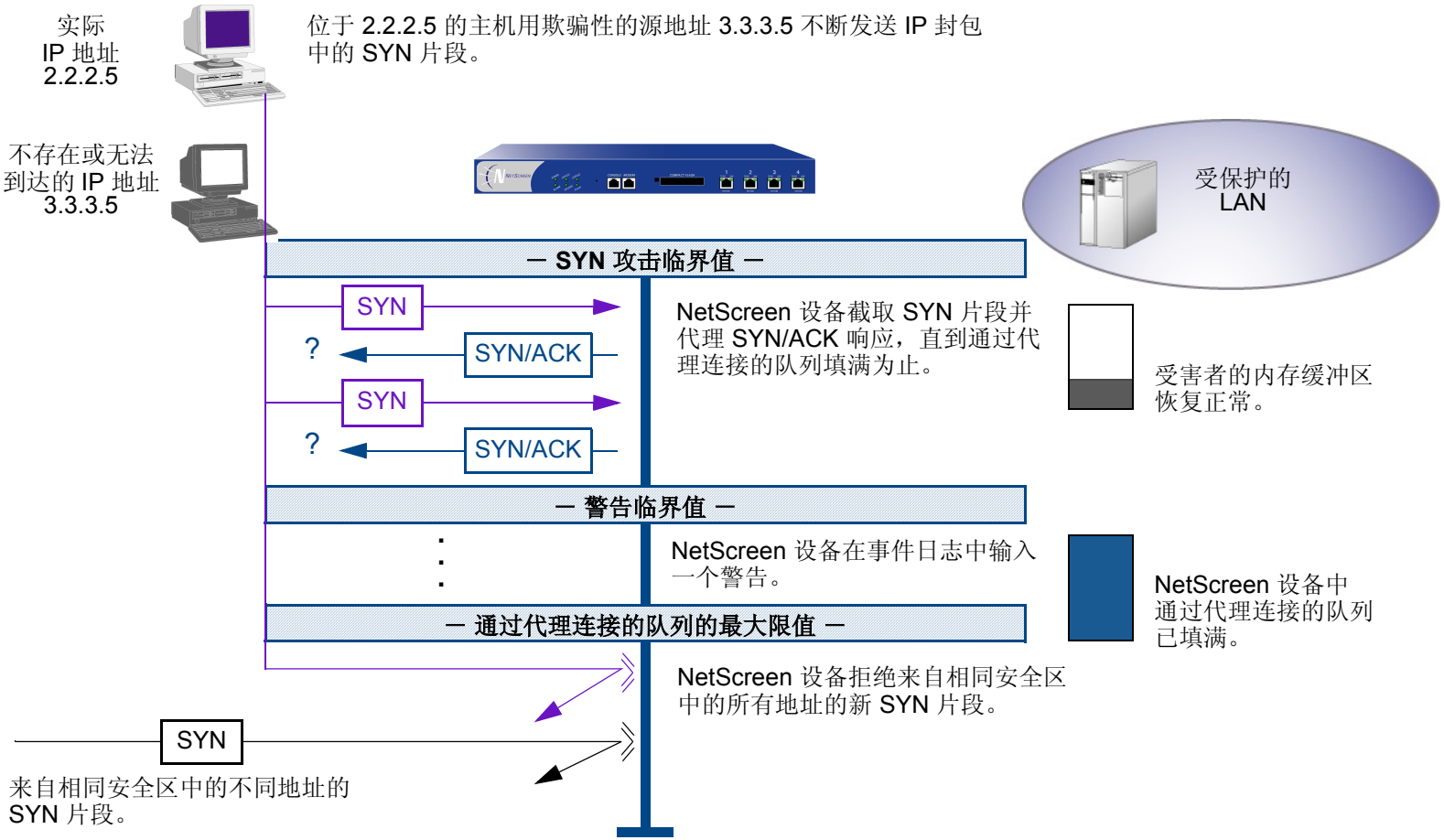
通过用无法完成的 TCP 连接泛滥攻击主机，攻击者最后填满受害者的内存缓冲区。当该缓冲区填满后，主机不能再处理新的 TCP 连接请求。泛滥甚至可能会破坏受害者的操作系统。无论用哪种方法，攻击已使受害主机失去作用，无法进行正常的操作。

SYN 泛滥保护

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。您可以将目标地址和端口、仅目标地址或仅源地址上的攻击临界值作为基础。当每秒的 SYN 片段数超过这些临界值之一时， NetScreen 设备开始代理发送流入的 SYN 片段、用 SYN/ACK 片段回复、并将不完全的连接请求存储到连接队列中。未完成的连接请求保留在队列中，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 设备开始接收新 SYN 封包。

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 泛滥保护 SCREEN 选项和定义其参数，请执行下列操作，其中指定的区段可能是泛滥攻击始发的区段：

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 封包数 — 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 封包数，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 封包数，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 设备在通过代理连接的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，通过代理连接的队列中存放的代理 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 泛滥保护。

```
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信息流模式，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: 每秒钟代理的半完成 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。为警告临界值设置的值，当每秒钟代理的发向相同目标地址和端口号的半完成连接请求数超过该值时，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 时，才会触发警告将其写入日志。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，防火墙代理后面的 1000 个 SYN 片段。
3. 第 1001 个代理连接请求 (或该秒内的第 3001 个连接请求) 会触发警报。

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

当发向相同目标地址和端口号的每个 SYN 片段超过警告临界值时，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，该条目指出在超过警告临界值后，有多少 SYN 片段到达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 泛滥保护机制和基于源的 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 泛滥保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 设备拥有一些策略，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 个封包 (pps)，且攻击者每秒发送 999 个 FTP 封包和 999 个 HTTP 封包，则任一组 (拥有相同目标地址和端口号的封包定义为一组) 封包都不会激活 SYN 代理机制。基本 SYN 泛滥攻击机制跟踪目标地址和端口号，且每组封包都未超过 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 封包看作是单个组的成员，并拒绝发往该目标的第 1001 个封包 (FTP 或 HTTP)。

Timeout: 半开连接从队列中被丢弃之前的最长等待时间。缺省值为 20 秒，您可以将该超时值设置为 0–50 秒。您可以试着缩短超时值，直到发现在正常的信息流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
```

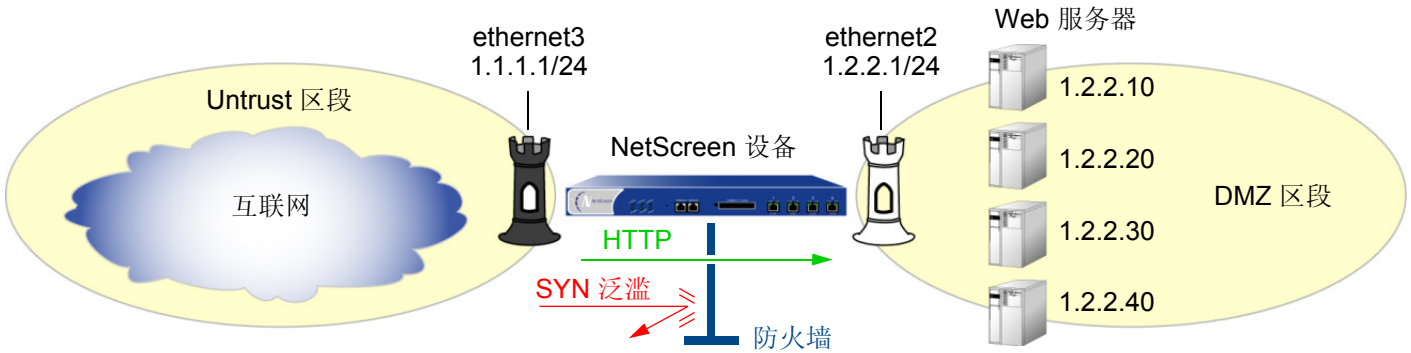
Drop Unknown MAC: 当 NetScreen 设备检测到 SYN 攻击时，它会代理所有的 TCP 连接请求。但是，如果目的 MAC 地址不在其 MAC 获知表中，则处于 “透明”模式的 NetScreen 设备不能代理 TCP 连接请求。缺省情况下，检测到 SYN 攻击且处于 “透明”模式的 NetScreen 设备将允许含有未知 MAC 地址的 SYN 封包通过。您可以使用此选项指示设备丢弃含有未知目的 MAC 地址的 SYN 封包，而不是让其通过。

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

范例 : SYN 泛滥保护

在本例中，通过为 Untrust 区段启用 SYN 泛滥保护 SCREEN 选项，保护 DMZ 区段中的 Web 服务器，使其免受始发自 Untrust 区段中的 SYN 泛滥攻击。

注意 : *NetScreen 建议增加 SYN 泛滥保护，使得 NetScreen 设备在每个 Web 服务器上都提供设备级的 SYN 泛滥保护。在本例中， Web 服务器正在运行 UNIX，该操作系统也提供一些 SYN 泛滥防御，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 泛滥保护参数配置适当的值，首先必须建立典型信息流的基准。在一周内，您可以在 ethernet3 (此接口绑定到 Untrust 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封包。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 封包，这些封包到达 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。显著的变化可能有理由对各种临界值进行调整。

根据这些信息，为 Untrust 区段设置下列 SYN 泛滥保护参数 :

参数	值	每个值的理由
Attack Threshold	每秒 625 个封包 (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 封包数超过此数目时，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 封包起，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 个代理的半完成的连接请求*) 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 封包的源 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 封包的跟踪中分离，后者构成了基本 SYN 泛滥保护机制。) 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来自所有服务器的总数的 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 设备从第 26 个封包开始，跟踪来自相同源 IP 地址的 25 个 SYN 封包，则对于该秒的剩余时间以及下一秒内，设备将拒绝从该来源发出的所有其它 SYN 封包。

参数	值	每个值的理由
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。
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 个代理的半完成的连接	1000 个代理的半完成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: (有此选项时将其选定)

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: (有此选项时将其选定)

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
```

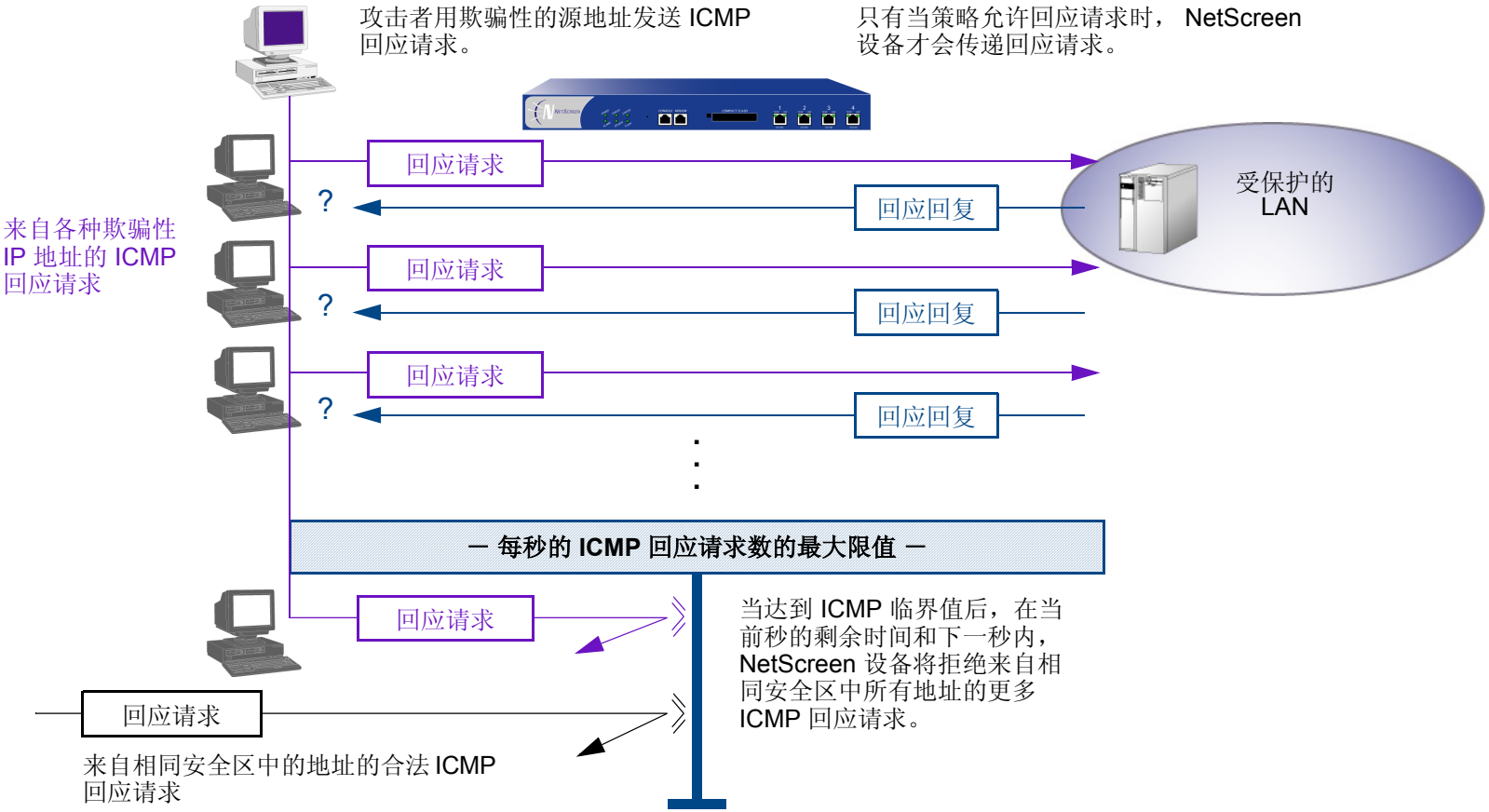
4. SCREEN

```
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 回应请求用很多请求超出了受害者的最大限度，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，就发生了 ICMP 泛滥。当启用了 ICMP 泛滥保护功能时，可以设置一个临界值，一旦超过此值就会调用 ICMP 泛滥攻击保护功能。(缺省的临界值为每秒 1000 个封包)。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 回应要求。



要启用 ICMP 泛滥保护，请执行下列操作之一，其中指定的区段可能是泛滥攻击始发的区段 :

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 泛滥保护的值[8])

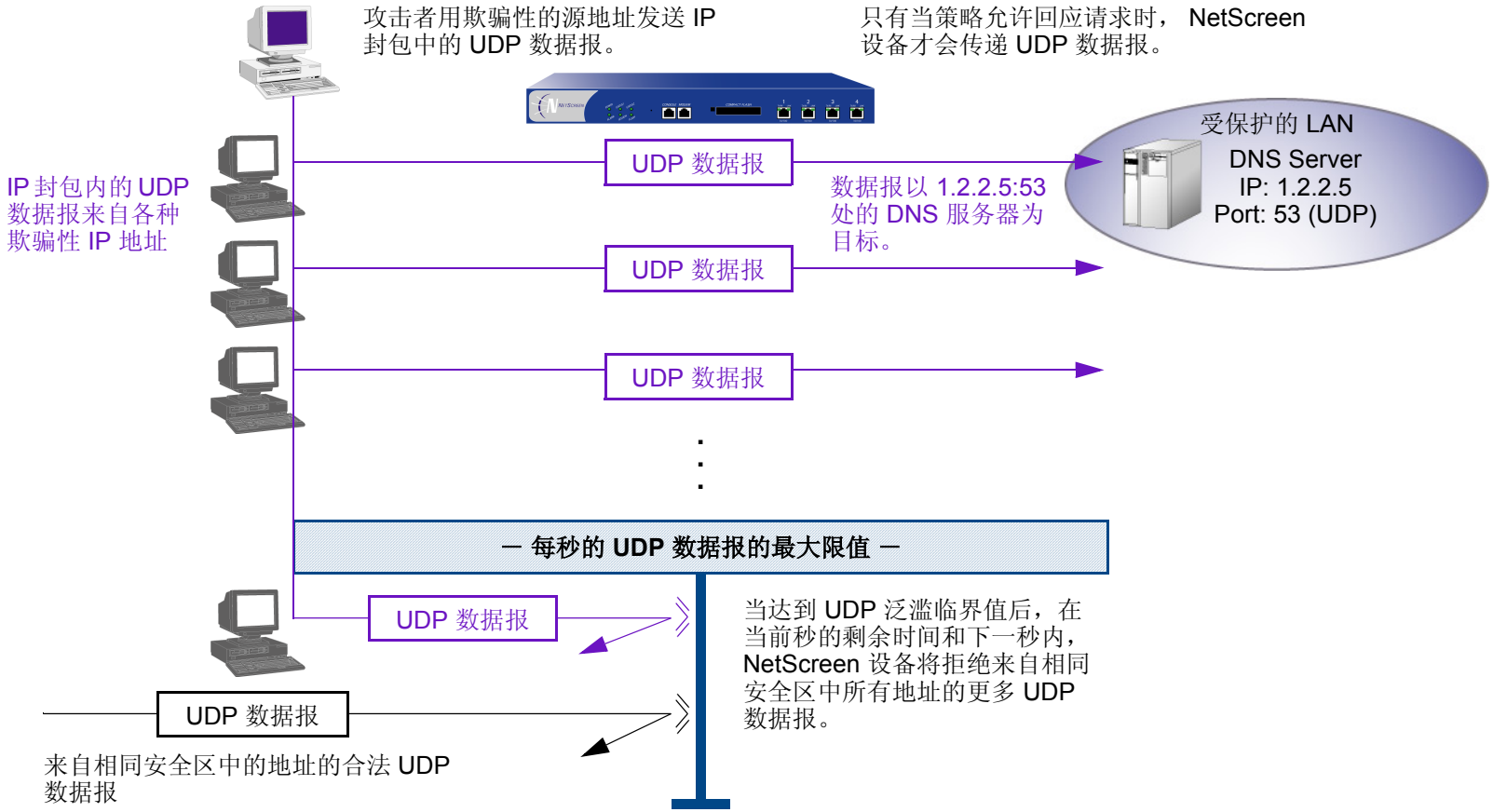
CLI

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

8. 该值的单位是每秒的 ICMP 封包数。 (缺省界值为每秒 1000 个封包)。

UDP 泛滥

与 ICMP 泛滥相似，当攻击者以减慢受害者速度为目的向该点发送含有 UDP 数据报的 IP 封包，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 泛滥保护功能时，可以设置一个临界值，一旦超过此临界值就会调用 UDP 泛滥攻击保护功能。(缺省的临界值为每秒 1000 个封包)。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到该目标的 UDP 数据报。



要启用 UDP 泛滥保护，请执行下列操作之一，其中指定的区段可能是泛滥攻击始发的区段 :

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 泛滥保护的值[9])

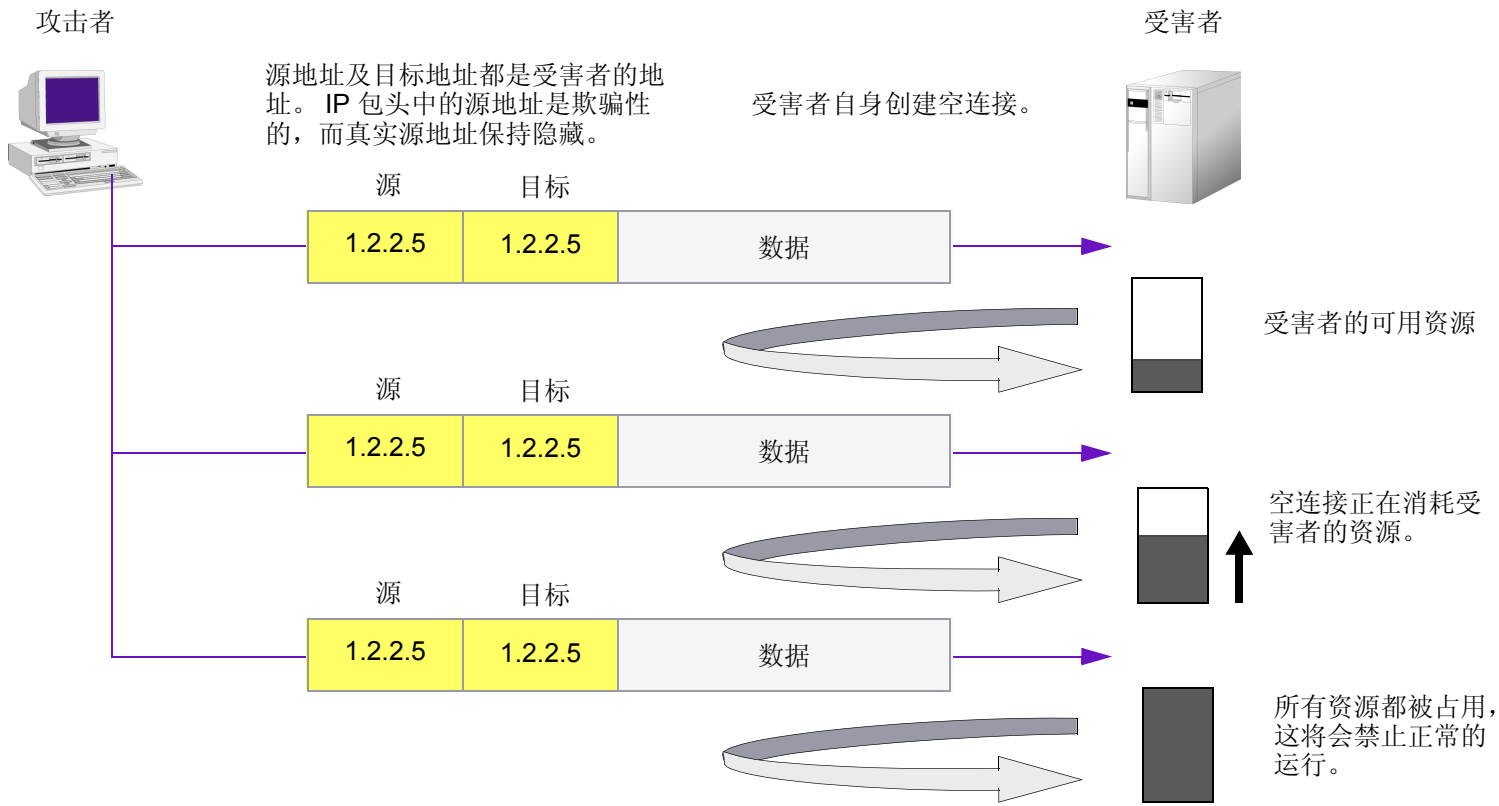
CLI

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

9. 该值的单位是每秒的 UDP 封包数。 (缺省界值为每秒 1000 个封包。)

陆地攻击

“陆地”攻击将 SYN 攻击和 IP 欺骗结合在了一起，当攻击者发送含有受害者 IP 地址的欺骗性 SYN 封包，将其作为目的和源 IP 地址时，就发生了陆地攻击。接收系统通过向自己发送 SYN-ACK 封包来进行响应，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 选项以封锁陆地攻击时， NetScreen 设备将 SYN 泛滥防御和 IP 欺骗保护的元素有机结合在一起，以检测和封锁这种性质的企图。

要启用对 “陆地”攻击的保护，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封包 “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 封包长度是 65,535 字节，其中包括长度通常为 20 字节的封包包头[10]。 ICMP 回应请求是一个含长度为 8 字节长的伪包头的 IP 封包[11]。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 字节的封包大小。过大的 ICMP 封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，NetScreen 设备检测并拒绝这些过大的且不规则的封包大小，即便是攻击者通过故意分段来隐藏总封包大小。

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

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

10. 有关 IP 规范的信息，请参阅 RFC 791 “Internet Protocol”。
11. 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 攻击的保护，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

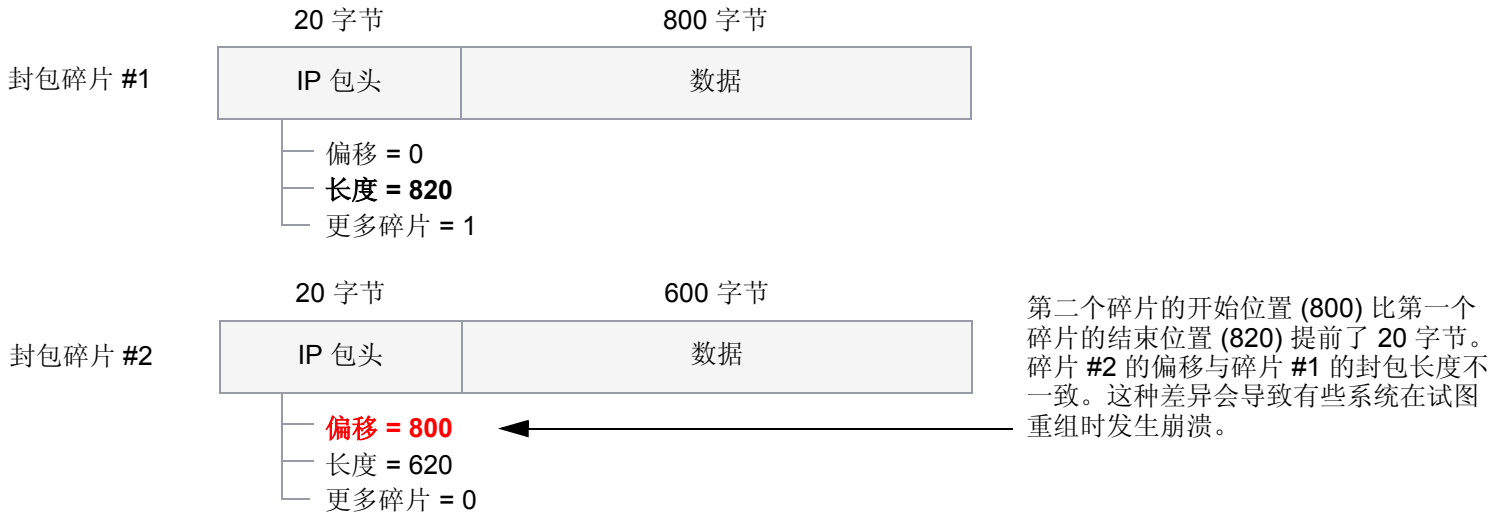
```
set zone zone screen ping-death
```

Teardrop 攻击

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

当一个封包碎片的偏移值与大小之和不同于下一封包碎片时，封包发生重叠，并且服务器尝试重新组合封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 检测到封包碎片中的这种差异，就会丢弃该碎片。要启用对 Teardrop 攻击的保护，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 (通常发送给设置了紧急 (URG) 标志的 NetBIOS 端口 139) 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) 封包。如果观察到其中一个封包中设置了 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 攻击的保护，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

内容监视和过滤

NetScreen 通过 ScreenOS 功能以及 NetScreen 与 Websense 和 Trend Micro 产品的配合，来提供广泛的网络活动保护和控制。

NetScreen 在 ScreenOS 内部提供了一些内容监视和过滤功能，这些功能在恶意 URL 保护 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 封包碎片中的 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许可密钥，并使用内部防病毒扫描功能。也可以配置 NetScreen 设备，使之与最多三个外部 Trend Micro 防病毒扫描器协同工作 (在先获得并加载两个许可密钥后)。对于 URL 过滤而言，可以配置 NetScreen 设备，使之与一个或多个 Websense 服务器协同工作。

本章研究如何配置 NetScreen 设备，以执行片段和封包重组，监视恶意 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) 并不重组其所收到的封包碎片。当所有封包碎片到达后，目标主机要负责重新构建它们。由于转发设备的目的是有效地传递信息流，因此对封包碎片的排列、重组、然后重新分段并转发，这些处理不是必要的，效率也不高。但是，将封包碎片传递通过防火墙是不安全的。攻击者可以故意打碎封包，以隐藏防火墙将有可能检测和封锁的信息流串。

ScreenOS 允许按照区段启用碎片重组。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层网关 (ALG) 来检查封包的数据部分。

恶意 URL 保护

除了本章后面说明的 URL 过滤功能外 (参阅第 117 页上的 “URL 过滤”)，在每个区段您最多可以定义 48 个恶意 URL 串模式，其中每一个都可以长达 64 个字符，以便提供区段级的恶意 URL 保护。在启用了恶意 URL 封锁功能后，NetScreen 设备将检查所有 HTTP 封包的数据负荷。如果找到 URL，并发现 URL 串的开头 (其取决于指定的字符数目) 与所定义的模式相匹配， NetScreen 设备将封锁该封包，阻止其通过防火墙。

机智的攻击者认识到， URL 串是已知的，并可能会被防御，因此他们会故意打碎 IP 封包或 TCP 片段，从而使得在逐一检查封包的过程中无法识别该模式。例如，如果恶意 URL 串是 **120.3.4.5/level/50/exec**，则 IP 碎片可能会将 URL 串分解为以下部分 :

- 第一个封包 : **120.**
- 第二个封包 : **3.4.5/level/50**
- 第三个封包 : **/exec**

当单独传输时，URL 串碎片会通过 NetScreen 设备而不被检测出来，即便是您将 URL 串定义为长度为 20 个字符的 **120.3.4.5/level/50/exec**。第一个封包中的字符串 “120.” 与所定义的模式的第一部分相匹配，但它比所要求的 20 个匹配字符长度要短。第二和第三个封包中的字符串与所定义的模式的开头不匹配，因此也将毫无阻碍地通过。

但是，如果重组这些封包，则碎片将组合形成可识别字符串， NetScreen 设备将会封锁它。利用碎片重组功能，NetScreen 设备可以将碎片缓存到队列中，将其重组为完整的封包，然后检查该封包中的恶意 URL。根据这个重组过程和后续检查的结果， NetScreen 设备执行下列步骤之一 :

- 如果发现了恶意 URL，则 NetScreen 设备将丢弃该封包并在日志中输入事件。
- 如果 NetScreen 设备不能完成重组过程，则对生存期施加时间限制，并丢弃碎片。
- 如果 NetScreen 设备确定该 URL 不是恶意的，但重组的封包太大而无法转发，则 NetScreen 设备会将该封包分成多个封包后转发。
- 如果确定该 URL 不是恶意的，而且不需要将其分解，则 NetScreen 设备随后转发该封包。

应用层网关

NetScreen 为很多协议提供了应用层网关 (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 等协议筛选封包的能力，要求其不仅检查封包包头，而且检查负载中的数据。例如，可能有两个策略，一个拒绝从 Untrust 到 DMZ 区段的 FTP-put，另一个允许从 Untrust 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
```

为了区分两种类型的信息流， NetScreen 防火墙将检查负载。如果设备读到 **RETR** *文件名*，则 FTP 客户端已发送请求，以从 FTP 服务器获得 (或 “检索”) 所指定的文件，且 NetScreen 设备允许该封包通过。如果 NetScreen 设备找到 **STOR** *文件名*，则客户端已发送请求，以将所指定的文件放置 (或“存储”) 到服务器上，且 NetScreen 设备封锁该封包。

为了绕过这种防御，攻击者可以故意将一个 FTP-put 封包分解为两个封包，在封包各自的负载中包含下列文本 : 封包 1: **ST**；封包 2: **OR** *文件名*。当单别检查每个封包时， NetScreen 设备不会发现 **STOR** *文件名*，因此将允许这两个封包通过。

但是，如果重组这些封包，则碎片将组合形成可识别字符串， NetScreen 设备将会对其采取措施。利用碎片重组功能， NetScreen 设备可以将碎片缓存到队列中，将其重组为完整的封包，然后检查该封包中的完整 FTP 请求。根据这个重组过程和后续检查的结果， NetScreen 设备执行下列步骤之一 :

- 如果发现了 FTP-put 请求，则 NetScreen 设备将丢弃该封包并在日志中输入事件。
- 如果 NetScreen 设备不能完成重组过程，则对生存期施加时间限制，并丢弃碎片。
- 如果 NetScreen 设备发现了 FTP-get 请求，但重组的封包太大而无法转发，则 NetScreen 设备会将该封包分成多个封包后转发。
- 如果发现 FTP-get 请求，而且不需要将其分解，则 NetScreen 设备随后转发该封包。

范例 : 封锁封包碎片中的恶意 URL

在本例中，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

“长度”的值表示必须在 URL 中出现的模式的字符数 — 从第一个字符开始 — 对于正确匹配而言。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

Screening > Mal-URL (Zone: Untrust): 选择 **IP/TCP 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 screen reassembly-for-alg
save
```

防病毒扫描

病毒是一种可执行代码，会感染或附在其它可执行代码上，以便能实现自我复制。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，因为他们传播时会用极多的伪造数据耗尽受感染主机或网络的资源。

结合 Trend Micro 防病毒 (AV) 技术， NetScreen 提供两个防病毒解决方案 :

- 内部防病毒扫描
- 外部防病毒扫描

对于内部防病毒扫描来说，防病毒扫描器在 NetScreen 设备内部，是 ScreenOS 的一部分。使用支持内部防病毒的 NetScreen 设备可简化部署和管理。对于远程站点、小型办公室、零售市场和远程工作人员来说，这是一个颇具成本效益的选择方案。有关配置内部防病毒扫描功能的信息，请参阅第 81 页上的 “内部防病毒扫描”。

对于外部防病毒扫描来说，防病毒扫描器是一个独立的设备， NetScreen 设备将需要扫描的信息流转发到该设备上。使用支持一个或多个外部防病毒扫描器的 NetScreen 设备可以提供灵活而可升级的方案。您开始时可以使用一个防病毒扫描器，但如果受保护的网络扩大了，就可以增加更多扫描器 (总计最多三个) 来处理不断增加的信息流负荷。有关配置外部防病毒扫描功能的信息，请参阅第 94 页上的 “外部防病毒扫描”。

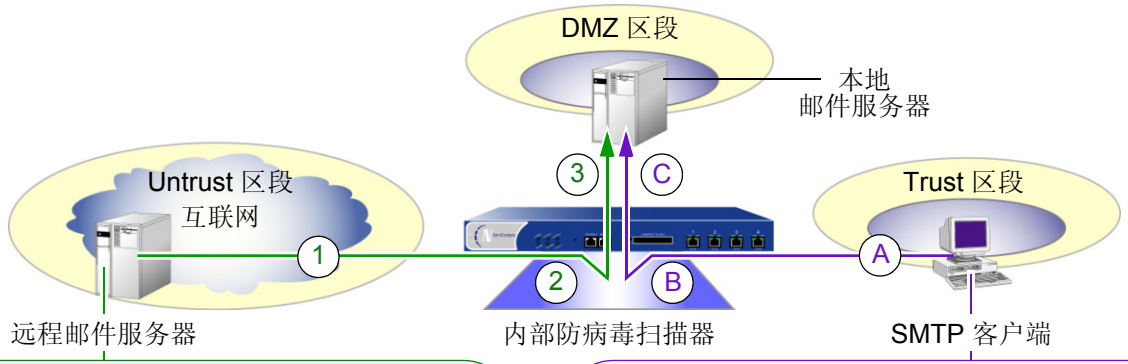
内部防病毒扫描

有些 NetScreen 设备使用 Trend Micro 开发的内部防病毒扫描器，为特殊的应用层事务处理提供防病毒 (AV) 扫描。为了使用内部防病毒扫描器扫描网络信息流中的病毒，您要在安全策略中引用内部防病毒扫描器。

可以配置内部防病毒扫描器来检查来自几个协议的网络信息流，包括 “简单邮件传输协议” (SMTP)、“超文本传输协议” (HTTP) 和 “邮局协议版本 3” (POP3)。在验证已收到 SMTP、HTTP 或 POP3 封包的全部内容后，内部防病毒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来识别病毒特征，从而完成病毒扫描。当内部防病毒扫描器检测到病毒时， 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 设备将该内容转发到其预期目的地。

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 客户端改发到内部防病毒扫描器。

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，并将数据传递到内部防病毒扫描器，由扫描器扫描其中的病毒。
3. 在完成扫描后， NetScreen 设备遵循下面两条路线之一：
   - 如果没有病毒，则将消息转发到本地服务器。
   - 如果有病毒，则发送一条消息给远程服务器，报告感染情况。

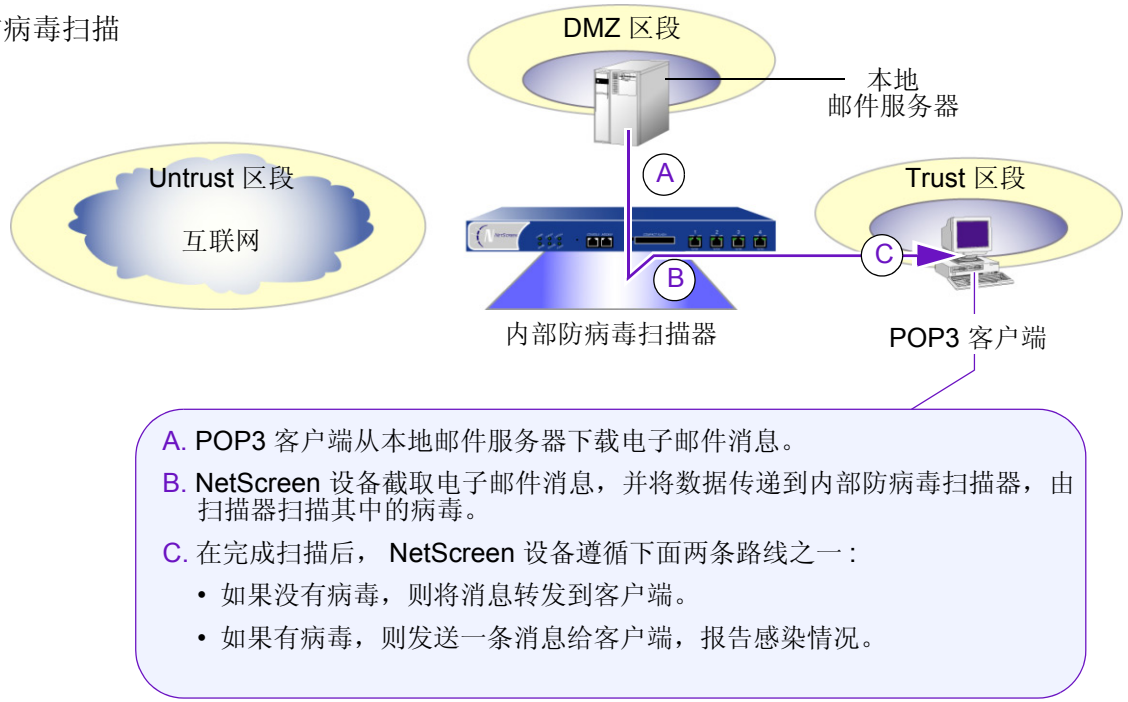
A. SMTP 客户端将电子邮件消息发送给本地邮件服务器。

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

C. 在完成扫描后， NetScreen 设备遵循下面两条路线之一：
   - 如果没有病毒，则将消息转发到本地服务器。
   - 如果有病毒，则发送一条消息给客户端，报告感染情况。

在扫描 POP3 信息流时， NetScreen 设备在将信息流发送到本地 POP3 客户端之前，将信息流从本地邮件服务器改发到内部防病毒扫描器。

POP3 防病毒扫描



A. POP3 客户端从本地邮件服务器下载电子邮件消息。

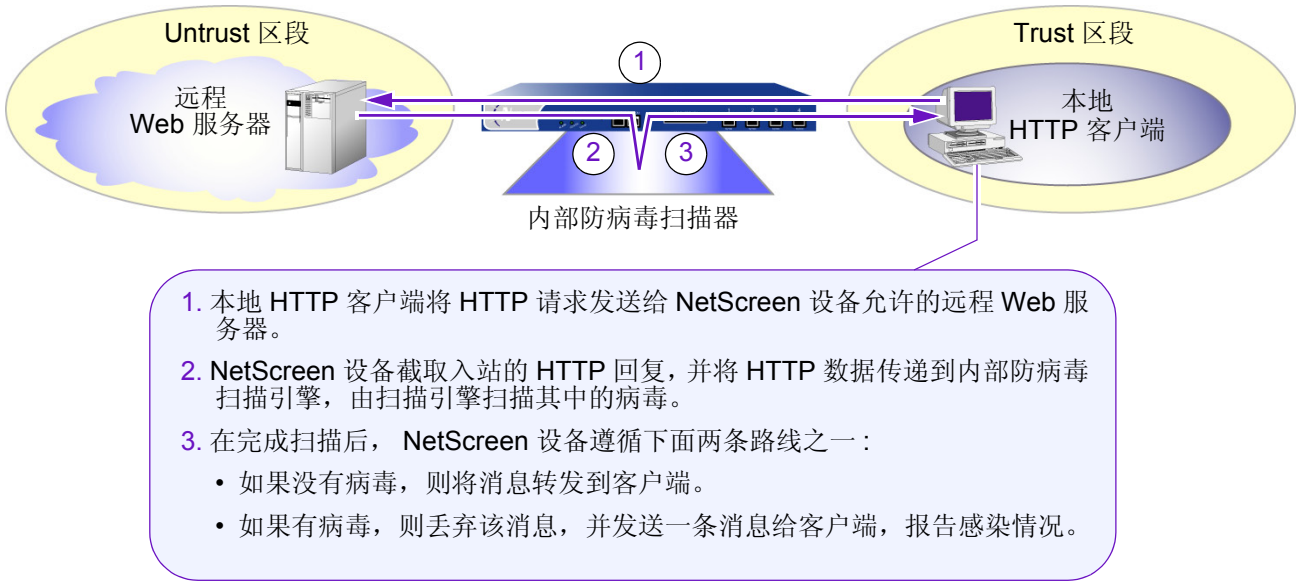
B. NetScreen 设备截取电子邮件消息，并将数据传递到内部防病毒扫描器，由扫描器扫描其中的病毒。

C. 在完成扫描后， NetScreen 设备遵循下面两条路线之一：

- 如果没有病毒，则将消息转发到客户端。
- 如果有病毒，则发送一条消息给客户端，报告感染情况。

在扫描 HTTP 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 请求的客户端响应的回复改发到内部防病毒扫描器。

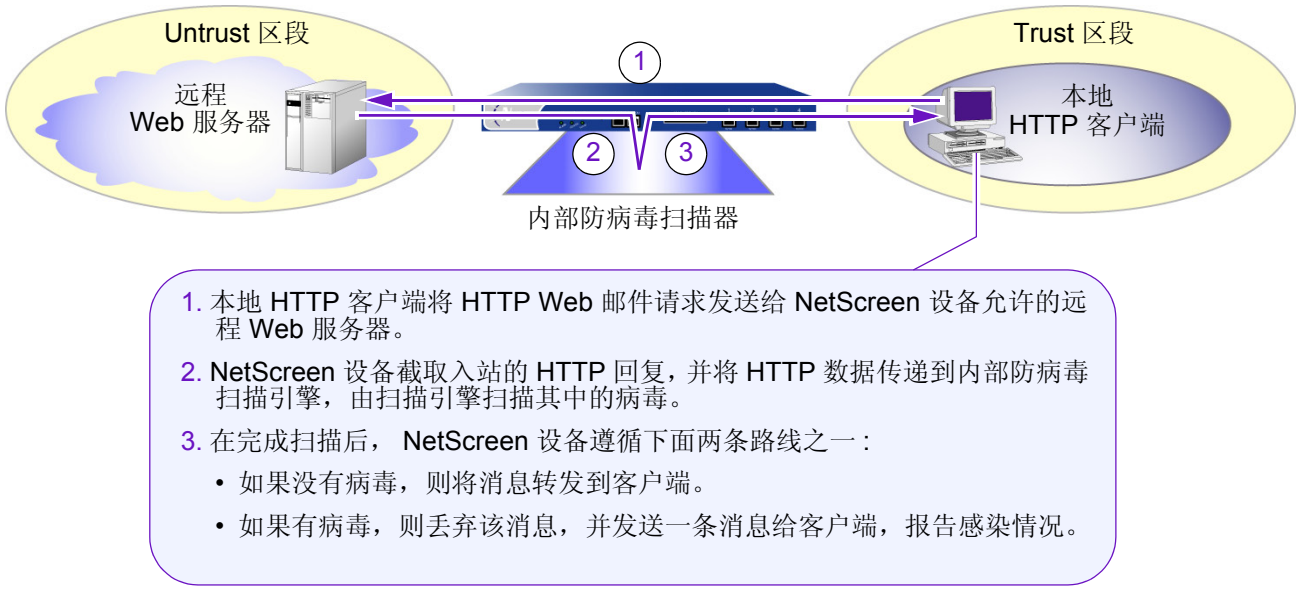
HTTP 防病毒扫描



***注意：**内部防病毒扫描器检查 HTTP 下载内容，也就是针对来自客户端的 HTTP 请求， Web 服务器所发送的回复中的 HTTP 数据。内部防病毒扫描器不扫描上载内容，例如，当 HTTP 客户端完成 Web 服务器上的调查问卷时，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。*

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改发到内部防病毒扫描器。

HTTP Web 邮件防病毒扫描



启用内部防病毒扫描

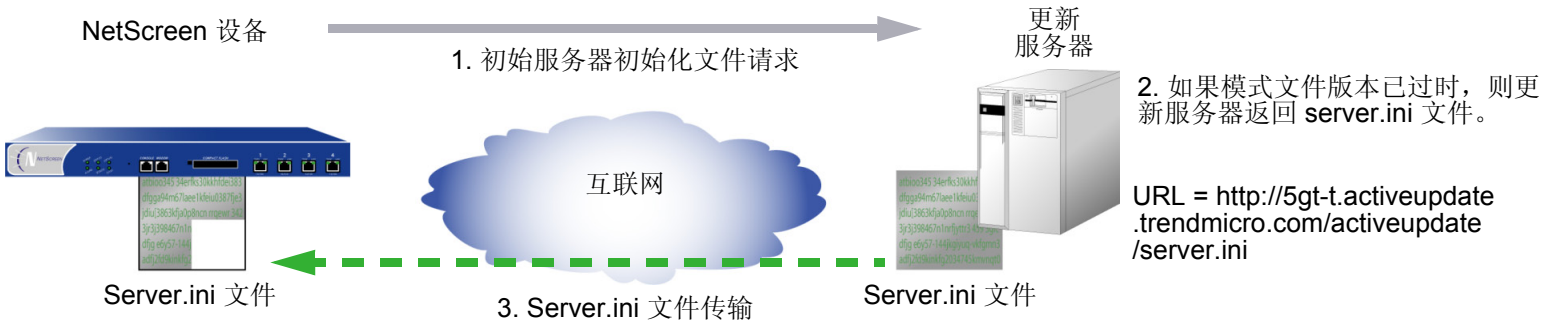
内部防病毒扫描时，要求将防病毒模式数据库加载到 NetScreen 设备上，并定期更新模式文件。为此，必须注册设备并购买对防病毒特征服务的预订。该预订允许您加载当前版本的数据库，并且在预订有效期内将数据库更新到可用的新版本。启动防病毒特征服务的过程有多种多样：

- 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。但是，您必须注册该设备并购买对防病毒特征服务的预订，才能继续获得模式的升级版本。
- 如果您正在升级目前的 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服务的预订，才能开始加载防病毒模式文件。在完成注册过程后，必须等待少于 4 个小时的一段时间，之后才能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**-554 页上的“签名服务的注册与激活”。*

更新防病毒模式文件的过程如下：

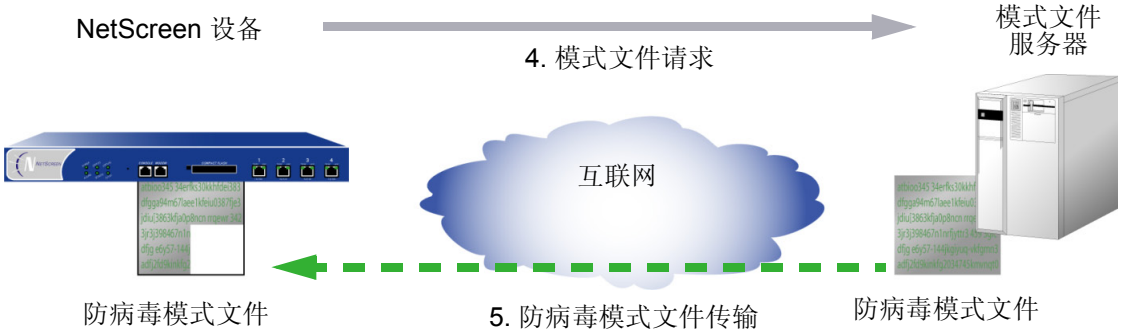
1. 从 NetScreen 设备中，指定外部模式文件服务器的 URL 地址，以检索名称为 server.ini 的服务器初始化文件。



2. 当 NetScreen 设备下载服务器初始化文件之后，便对其进行分析，以获得有关更新的模式文件的信息，包括模式文件的版本和大小以及外部模式文件服务器的位置。

> ***注意：**ScreenOS 含有用于认证与模式文件服务器通信的 CA 证书。*

3. 如果当前模式文件已过时，则 NetScreen 设备自动从外部模式文件服务器检索更新的模式文件。



4. 当下载模式文件后， NetScreen 设备验证防病毒预订是否仍然有效。如果防病毒特征服务预订是有效的，则更新模式文件。如果预订已到期，则模式文件更新失败，并显示一条错误信息，指出防病毒预订已过期。

注意： *完成模式更新的总时间估计大约是 3 分钟。此时间可能因模式文件大小和现有的网络信息流而异。在完成模式文件更新后， NetScreen 设备重新初始化内部防病毒扫描器，以便使用新的模式。*

自动或半自动地更新模式文件

当新病毒传播时，添加对模式文件的更新。可以将 NetScreen 设备配置为自动定期地或半自动地更新模式文件。

注意： *当预订到期后，更新服务器将不再允许您更新防病毒模式文件。*

范例：自动模式更新

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是 60 分钟)。模式更新服务器位于下列 URL 地址中：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：半自动模式更新

在本例中，将 NetScreen 设备配置为半自动地更新模式文件。模式更新服务器位于下列 URL 地址中：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
```

配置内容处理

在缺省情况下，内部防病毒扫描器将检查 SMTP、 HTTP (仅 Web 邮件) 和 POP3 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。*

您可以更改缺省行为，使得内部防病毒扫描器只检查特定的网络信息流。

范例 : 对 SMTP 信息流的内部防病毒扫描

在此例中，配置内部防病毒扫描器，使其仅检查 SMTP 信息流。

WebUI

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

Protocols to be scanned:

SMTP: (选择)

CLI

```
set av scan-mgr content smtp timeout 20
save
```

范例：对 SMTP 和 HTTP 信息流的内部防病毒扫描

在此例中，配置内部防病毒扫描器，使其检查所有 SMTP 和 HTTP 信息流。

WebUI

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

Protocols to be scanned:

SMTP: (选择)

HTTP: (选择); ALL HTTP: (选择)

CLI

```
set av scan-mgr content smtp timeout 20
set av scan-mgr content http timeout 20
unset av http webmail enable
save
```

配置解压缩和最大信息量大小

当接收到内容时，内部防病毒扫描器解压缩任何压缩的文件。在缺省情况下扫描器最多解开 2 层的压缩文件。例如，如果扫描器接收到带有附件的文件，并且该附件是嵌入另一个压缩文件内的压缩文件时，扫描器将会进行两层解压缩以检测所有病毒。您可以将内部防病毒扫描器配置为解压缩最多 20 个嵌入另一个文件内的压缩文件。

在任一时刻，内部防病毒扫描器最多检查 8 条消息和 16 MB 的 “解压缩” 文件内容。如果接收到的消息总数或总信息量同时超过这些限值，则在缺省情况下扫描器将传递该信息而不检查病毒。例如，扫描器可以同时接收和检查四个 4MB 的消息。如果同时接收到九个 2MB 的消息，扫描器将不加扫描地传递该内容。可以更改该缺省行为，使得内部防病毒扫描器丢弃信息流，而不是将其传递。

范例：丢弃大文件

在本例中，您将内部防病毒扫描器配置为解压缩最多 10 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 个或 “解压缩的”信息量超过 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: 10 layers (1~4)

Drop: (选择) file if it exceeds 3000 KB (4000~20000)

Drop: (选择) file if the number of files exceeds 4 files (1~8)

CLI

```
set av scan-mgr decompress-layer 10
set av scan-mgr max-msgs 4
set av scan-mgr max-content-size 3000
set av scan-mgr max-content-size drop
save
```

应用内部防病毒扫描

如要对 SMTP、 HTTP 获 POP3 网络信息流应用防病毒扫描，则必须在策略中引用预先定义的内部防病毒扫描器。

范例：内部防病毒扫描 (POP3)

在本例中，您引用防火墙策略中的内部防病毒扫描器，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: (有此选项时将其选定)

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: (有此选项时将其选定)

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: (有此选项时将其选定)

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 内部防病毒扫描

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

> Advanced: 移动下列防病毒对象，然后单击 **Return** 以设置高级选项并返回基本配置页：

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 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 内部防病毒扫描

```
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
```

外部防病毒扫描

大多数 NetScreen 设备可以与由 Trend Micro 研制的名称为 InterScan VirusWall Edition 3.6 的外部防病毒 (AV) 扫描器实现互操作。您可以配置 NetScreen 设备，使其将“简单邮件传输协议”(SMTP) 和“超文本传输协议”(HTTP) 信息流转发到 VirusWall 防病毒扫描器。用于 NetScreen 设备和 VirusWall 扫描器之间的通信协议称为“内容扫描协议” (CSP) 版本 1.5。

***注意：** NetScreen 不支持虚拟系统的防病毒。在同时支持虚拟系统和防病毒的系统上，只有在根一级才可使用防病毒。*

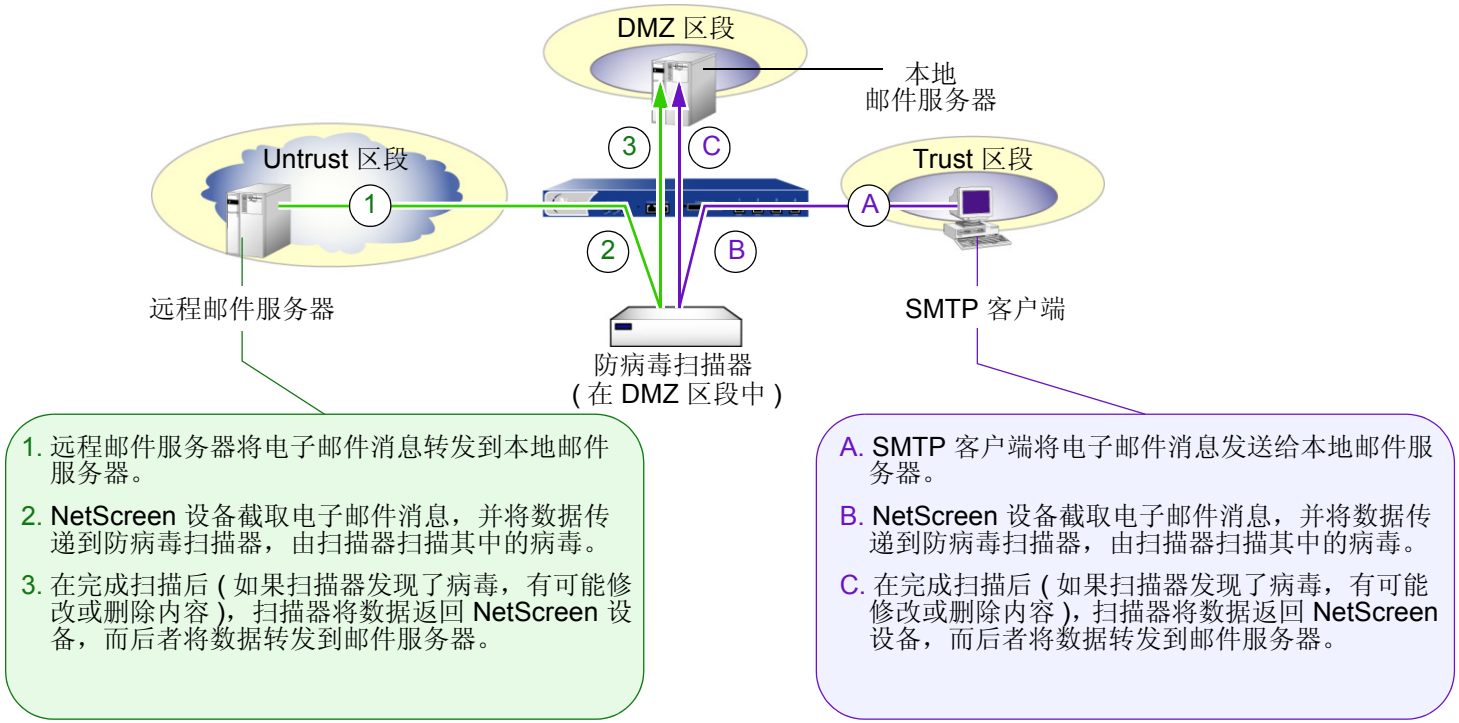
当接收到 SMTP 或 HTTP 封包的整个内容时， VirusWall 扫描器将检查数据中的病毒。扫描器拥有用于识别病毒特征的病毒模式数据库。如果扫描器发现有问题， VirusWall 将隔离受感染的数据以供进一步研究，并将 SMTP 或 HTTP 文件 (不含受感染的数据) 返回到 NetScreen 设备。然后 NetScreen 设备将该文件转发到预定接收者。

每当 VirusWall 检测到病毒时， NetScreen 设备和 VirusWall 都将生成标识所检测到的病毒的事件日志条目。

***注意：** 要了解如何配置 Trend Micro InterScan VirusWall 使其与 NetScreen 设备进行通信，以及如何配置其它设置，请参阅 Trend Micro 产品文档。*

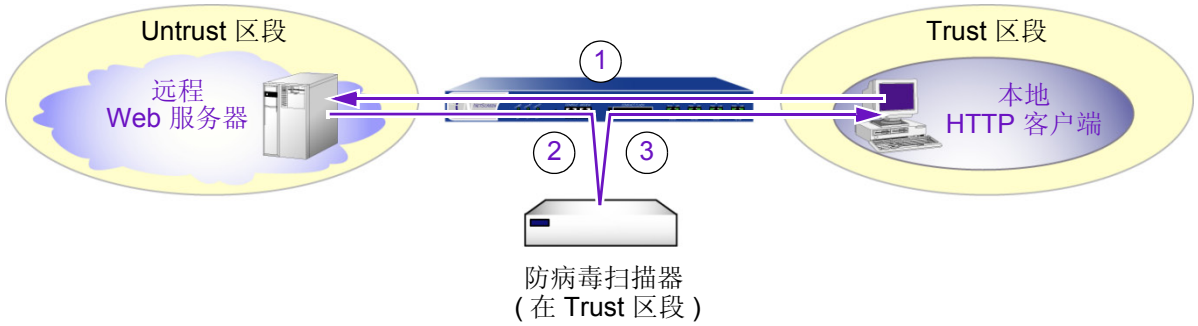
在扫描 SMTP 信息流时，将信息流发送到本地邮件服务器之前， NetScreen 设备会将来自远程邮件服务器或本地 SMTP 客户端的信息流改发到内部 VirusWall 防病毒扫描器。

SMTP 防病毒扫描



在扫描 HTTP 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 请求的客户端的响应回复改发到防病毒扫描器。

HTTP 防病毒扫描



1. 本地 HTTP 客户端将 HTTP 请求发送给 NetScreen 设备允许的远程 Web 服务器。
2. NetScreen 设备截取入站的 HTTP 回复，并将 HTTP 数据传递到防病毒服务器，由服务器扫描其中的病毒。
3. 在完成扫描后 (如果服务器发现了病毒，有可能修改或删除内容)，防病毒服务器将数据返回 NetScreen 设备，而后者将数据转发到客户端。

***注意：** 防病毒扫描器检查 HTTP 下载内容，也就是针对来自客户端的 HTTP 请求， Web 服务器所发送的回复中的 HTTP 数据。防病毒扫描器不扫描上载内容，例如，当 HTTP 客户端完成 Web 服务器上的调查问卷时，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。*

定义防病毒对象

防病毒对象 (防病毒对象) 是 NetScreen 用以引用外部防病毒扫描器的术语。您最多可以定义三个防病毒对象以增加带宽容量。在创建防病毒对象时，必须定义下列三个部分 :

- 防病毒对象名称
- 防病毒扫描器的 IP 地址或域名 (由 DNS 解析为 IP 地址)
- 内容类型 : HTTP 和 / 或 SMTP

当您仅定义了上面一个或两个部分时，防病毒对象的状态被认为是不完整的。在定义了所有三个部分信息后，才会认为是完整的。例如 :

```
set av scanner1 server-name 1.2.2.25
```

此防病毒对象是**不完整的**，因为它有名称 (“scanner1”) 和地址 (1.2.2.25) 但没有内容类型。

```
ns208A_5.0.0_beta3-> get av scanner1
<AV object scanner1>
     scanner name:     1.2.2.25
     scanner ip:       1.2.2.25
     scanner port:     3300
     status:           incomplete
     applications:     0
     scanned bytes:    0
     policy ref cnt:   0
```

```
set av scanner1 server-name 1.2.2.25
set av scanner1 content http
```

此防病毒对象是**完整的**，因为它有名称、地址和内容类型 (HTTP)。

```
get av scanner1
<AV object scanner1>
     scanner name:     1.2.2.25
     scanner ip:       1.2.2.25
     scanner port:     3300
     HTTP:             timeout 180 seconds
     status:           complete
     applications:     0
     scanned bytes:    0
     policy ref cnt:   0
```

还可以为防病毒对象设置下面几个可选参数 :

- **端口号 :** 在缺省情况下，“内容扫描协议” (CSP) 用于 NetScreen 设备和 Trend Micro InterScan VirusWall 之间通信的端口号是 3300。可以对每个防病毒对象更改此数值。

```
set av name_str server-name { ip_addr | domain_name } port number
unset av name_str server-name { ip_addr | domain_name } port
```

上面的 **unset av** 命令将端口号还原为缺省值 (3300)。

- **超时值 (单位为秒):** 在缺省情况下， 180 秒无活动之后， CSP 连接超时。可以对每个防病毒对象更改此值。值的范围是 1 到 1800 秒。

```
set av name_str content { http | smtp } timeout number
unset av name_str content { http | smtp } timeout number
```

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

除了可以对防病毒对象设置上述选项之外，也可以设置下列参数，它们普遍适用于防病毒功能 :

- **最大同步 TCP 连接数 :** 此参数指定 NetScreen 设备与作为一个整体的所有防病毒对象之间的最大同步 TCP 连接数，而不是指 NetScreen 设备与每个防病毒对象之间的连接数。缺省值因平台而异。 (有关平台的信息，请参阅 NetScreen 营销文献。)

WebUI

Screening > Antivirus: 在 Maximum Number of TCP Connections 字段中输入数值，然后单击 **Apply**。

CLI

```
set av all max-connections number
unset av all max-connections
```

- **每个来源的 CSP 资源：** 恶意的用户可能会同时发送大量的 SMTP 或 HTTP 信息流，以消耗掉所有可用的“内容扫描协议” (CSP) 资源，从而阻止 NetScreen 设备将任何其它信息流转发到防病毒扫描器中。为了防止这类活动的成功，对于任一时刻来自单个来源的信息流可消耗的 CSP 资源， NetScreen 设备可以规定一个最大的百分比。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 CSP 资源不施加任何限制。

  ### *WebUI*

  Screening > Antivirus: 在 Maximum AV Resources Allowed per AV Client 字段中输入数值，然后单击 **Apply**。

  ### *CLI*

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

  上述 **unset av** 命令将每个来源的最大 CSP 资源百分比恢复为缺省值 (70%)。

- **失败模式行为：**失败模式是 NetScreen 设备失去与 VirusWall 扫描器的连接时的行为 — 或者允许未经检查的信息流，或者封锁它。在缺省情况下，如果无法访问 VirusWall 扫描器， NetScreen 设备将封锁启用了防病毒检查的策略所允许的 HTTP 和 SMTP 信息流。可以将缺省行为从封锁改为允许。

  ### *WebUI*

  Screening > Antivirus: 选择 Fail Mode Traffic Permit 复选框以允许未经检查的信息流，或者清除该复选框以封锁信息流，然后单击 **Apply**。

  ### *CLI*

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

  上面的 **unset av** 命令将失败模式还原为缺省值 (封锁未经检查的信息流)。

- **失败模式临界值：** 失败模式是当到防病毒对象的很多连续的连接尝试失败超过临界值时的状态。在缺省情况下，该临界值是 150，并且适用于所有防病毒对象。如果连续的失败尝试次数超过此临界值，则 NetScreen 设备在重新开始连接尝试之前，将等待指定的一段时间 (5 分钟)。如果缺省设置对您的需要来说显得太高或太低，则可以更改此临界值。

WebUI

Screening > Antivirus: 在 Fail Mode Scanner Threshold 字段中输入数值，然后单击 **Apply**。

CLI

```
set av all fail-mode scanner threshold number
unset av all fail-mode scanner
```

如果希望 NetScreen 设备在达到等待时间之前恢复对特定防病毒对象的连接尝试，可以输入以下命令：

```
clear av name_str fail-mode
```

此命令清除失败状态，使得当下一个 SMTP 或 HTTP 信息流到达时，NetScreen 设备立即尝试连接到防病毒扫描器。如果连接成功，则 NetScreen 设备重新开始将要扫描病毒的文件转发到防病毒扫描器。如果连接尝试失败，则状态恢复为失败模式。

- **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 设备将连接标题字段中的标记从 “keep-alive” 更改为 “close”。) 在此方法中，当完成其数据传输时， HTTP 服务器发送 TCP FIN 以关闭 TCP 连接，并因此表明已发送完数据。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保持打开 TCP 连接，这样就会减少等待时间和改进 CPU 性能。但是，它没有 “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: 选择 Keep Alive 复选框以使用 “keep-alive”连接选项，或清除该复选框以使用 “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转发小量的数据)。在缺省情况下禁用 HTTP trickling。要启用 HTTP trickling 并使用缺省的 HTTP trickling 参数，请执行下列操作 :

WebUI

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

CLI

```
set av http trickling default
```

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

要更改 HTTP trickling 的参数，请执行下列操作：

WebUI

Screening > Antivirus: 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
```

三个数值变量有下列含义：

- *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 设备应用了 trickling 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 trickling 是通过不加扫描地转发小量数据到客户端来实现的，因此病毒代码有可能包含在 NetScreen 设备细流到客户端的数据中。 NetScreen 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 8MB，并且禁用了 HTTP 细流，则浏览器窗口将极有可能会超时。

范例：定义三个防病毒对象

在本例中，定义下列防病毒对象：

- 防病毒对象 1
  - Name: scanner1
  - IP address: 1.2.2.20
  - Port number for Content Scanning Protocol (CSP): 3300 (缺省值)
  - Content: HTTP
  - Timeout: 180 seconds (缺省值)
- 防病毒对象 2
  - Name: scanner2
  - IP address: 1.2.2.30
  - Port number for CSP: 6830
  - Content: SMTP
  - Timeout: 200 seconds
- 防病毒对象 3
  - Name: scanner3
  - IP address: 1.2.2.40
  - Port number for CSP: 6840
  - Content: HTTP and SMTP
  - HTTP Timeout: 120 seconds
  - SMTP Timeout: 200 seconds

NetScreen 设备通过 ethernet2 访问上述地址， ethernet2 的 IP 地址为 1.2.2.1/24，并绑定到 DMZ 区段上。

WebUI

1. 防病毒对象 1

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

   AV Object Name: scanner1

   Scan Server Name/IP: 1.2.2.20

   Scan Server Port: 3300

   Contents:

   HTTP: (选择), Timeout: 180 Seconds

2. 防病毒对象 2

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

   AV Object Name: scanner2

   Scan Server Name/IP: 1.2.2.30

   Scan Server Port: 6830

   Contents:

   SMTP: (选择), Timeout: 200 Seconds

3. 防病毒对象 3

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

   AV Object Name: scanner3

   Scan Server Name/IP: 1.2.2.40

   Scan Server Port: 6840

   Contents:

   HTTP: (选择), Timeout: 120 Seconds

   SMTP: (选择), Timeout: 200 Seconds

CLI

1. 防病毒对象 1

```
set av scanner1 server-name 1.2.2.20
set av scanner1 content http
```

2. 防病毒对象 2

```
set av scanner2 server-name 1.2.2.30 port 6830
set av scanner2 content smtp timeout 200
```

3. 防病毒对象 3

```
set av scanner3 server-name 1.2.2.40 port 6840
set av scanner3 content http timeout 120
set av scanner3 content smtp timeout 200
save
```

应用外部防病毒扫描

在创建一个或多个防病毒对象后，可以在策略中引用它们，以便对 HTTP 和 SMTP 信息流应用防病毒扫描。单个防病毒对象可以扫描 HTTP 信息流或 SMTP 信息流，或同时扫描两种信息流。如果在相同的策略中引用两个或三个防病毒对象，则 NetScreen 设备按照提供负载平衡的顺序，将要进行扫描的信息流发送到那些对象中。

在策略配置中引用三个防病毒对象的顺序，规定了 NetScreen 设备向防病毒对象发送 HTTP 和 SMTP 信息流的顺序。首先引用的防病毒对象是 NetScreen 设备发送要扫描的第一个文件 (如电子邮件消息或 HTTP 回复) 的对象。换句话说，第一个防病毒对象拥有最高的优先级。如果第一个防病毒对象目前正在扫描其它文件，则第二个引用的防病毒对象是 NetScreen 设备发送第二个文件的对象。它拥有次高的优先级。如果前两个防病毒对象都在扫描其它文件，则在策略配置中第三个引用的防病毒对象将获得第三个文件。它的优先级最低。

例如，如果创建了三个防病毒对象 “scanner1”、“scanner2” 和 “scanner3”，则在策略中以下列顺序引用它们，

```
set policy id 1 from trust to untrust any any http permit av scanner1
set policy id 1
ns(policy:1)-> set av scanner2
ns(policy:1)-> set av scanner3
```

然后按照如下顺序将文件发送到每个扫描器 :

1. NetScreen 设备将第一个要扫描的文件发送到 scanner1。
2. 当第二个要扫描的文件到达时，在下列条件下 NetScreen 设备将其发送到 scanner1 或 scanner2:
   - 如果 scanner1 已完成第一个文件的扫描，则发送到 scanner1
   - 如果 scanner1 仍在扫描第一个文件，则发送到 scanner2
3. 当第三个文件到达时， NetScreen 按照下列条件将其发送到三个防病毒对象之一 :
   - scanner1，如果 scanner1 没有正在扫描文件
   - scanner2，如果 scanner1 正在扫描文件，但 scanner2 没有正在扫描
   - scanner3，如果 scanner1 和 scanner2 都正在扫描文件

当所有扫描器都在忙于扫描多个文件时，则继续上述顺序。如果所有扫描器都在扫描相同数目的文件，则 NetScreen 设备将下一个文件发送到 scanner1。如果 scanner1 正在扫描的文件比 scanner2 和 scanner3 要少，则 NetScreen 设备将下一个文件发送到 scanner1。如果 scanner2 正在扫描的文件比 scanner1 和 scanner3 要少，则 NetScreen 设备将下一个文件发送到 scanner2。如果 scanner3 正在扫描的文件比 scanner1 和 scanner2 要少，则 NetScreen 设备将下一个文件发送到 scanner3。

范例：用防病毒对象防病毒

在本例中，创建名称为 “scanner1”的单个防病毒对象，对从位于 Untrust 区段的 Web 服务器发给 Trust 区段中客户端的 HTTP 回复，执行病毒扫描。防病毒扫描器也位于 Trust 区段中。尽管您对 Trust 和 Untrust 区段之间的 HTTP 信息流启用了防病毒检查，但却不需要附加的策略来允许 NetScreen 设备与 scanner1 之间的 CSP 信息流。所有区段都在 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: (有此选项时将其选定)

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: (有此选项时将其选定)

IP Address/Netmask: 1.1.1.1/24

2. 防病毒对象

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

AV Object Name: scanner1

Scan Server Name/IP: 1.2.2.20

Scan Server Port: 3300

Contents:

HTTP: (选择), Timeout: 180 Seconds

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

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

> Advanced: 移动下列防病毒对象，然后单击 **Return** 以设置高级选项并返回基本配置页 :

选择 **scanner1**，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 ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. 防病毒对象

```
set av scanner1 server-name 1.2.2.20
set av scanner1 content http
```

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 trust to untrust any any http permit av scanner1
save
```

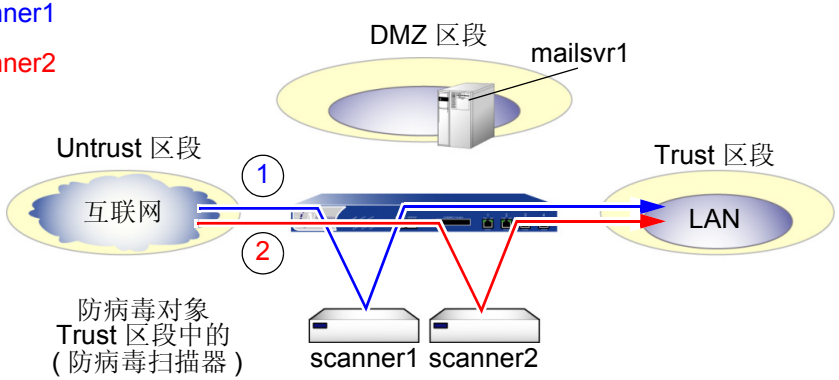
范例：用两个防病毒对象防病毒

在本例中，定义名称为 “scanner1” 和 “scanner2” 的两个防病毒对象来扫描 HTTP 和 SMTP 信息流。然后在策略中引用这些防病毒对象，允许 Trust 和 Untrust 区段之间的 HTTP 信息流，并允许从 Untrust 和 Trust 区段中的地址发到 DMZ 区段中邮件服务器的 SMTP 信息流。为了平衡发送到两个防病毒对象的信息流负载，按照如下方式设置向防病毒对象发送的防病毒扫描请求的分布：

- NetScreen 设备将所有 HTTP 防病毒扫描回复改发到两个防病毒对象。这两个允许 HTTP 信息流的策略每个都引用两个防病毒对象。

1. 第一个 HTTP 回复 -> scanner1

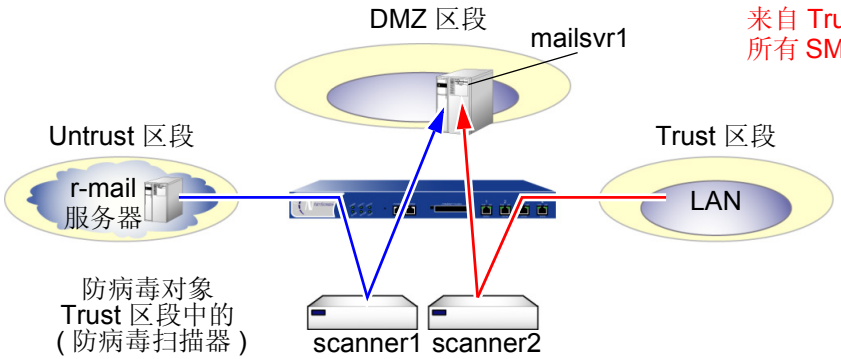
2. 第二个 HTTP 回复 -> scanner2
(如果 scanner1 还未完成
第一个 HTTP 回复的扫描；
如果 scanner1 是空闲的，
则 NetScreen 设备将第二个
HTTP 回复改发到 scanner1)



- 对于从 Untrust 区段中的远程邮件服务器 (名称为 “r-mail”) 发向 DMZ 中的本地邮件服务器 (名称为 “mailsvr1”) 的 SMTP 信息流， NetScreen 设备将防病毒扫描请求发送到 scanner1。对于来自 Trust 区段的所有 SMTP 信息流， NetScreen 设备将防病毒扫描请求发送到 scanner2。

来自 Untrust 区段
所有 SMTP 信息流 -> scanner1

来自 Trust 区段
所有 SMTP 信息流 -> scanner2



两个防病毒对象都在 Trust 区段中。尽管对信息流启用了策略级的防病毒检查，但不需要附加的策略来允许 NetScreen 设备与防病毒扫描器之间的 CSP 信息流。所有区段都在 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: (有此选项时将其选定)

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: (有此选项时将其选定)

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: (有此选项时将其选定)

IP Address/Netmask: 1.1.1.1/24

2. 防病毒对象 1

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

AV Object Name: scanner1

Scan Server Name/IP: 10.1.1.20

Scan Server Port: 3300

Contents:

HTTP: (选择), Timeout: 180 Seconds

SMTP: (选择), Timeout: 180 Seconds

3. 防病毒对象 2

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

AV Object Name: scanner2

Scan Server Name/IP: 10.1.1.30

Scan Server Port: 3300

Contents:

HTTP: (选择), Timeout: 180 Seconds

SMTP: (选择), Timeout: 180 Seconds

4. 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), 1.2.2.6/32

Zone: DMZ

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

Address Name: r-mail

IP Address/Domain Name:

IP/Netmask: (选择), 2.2.2.5/32

Zone: Untrust

5. 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

6. 策略 ID 1

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

> Advanced: 移动下列防病毒对象，然后单击 **Return** 以设置高级选项并返回基本配置页：

选择 **scanner1**，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。

选择 **scanner2**，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。

7. 策略 ID 2

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

Source Address:

Address Book Entry: (选择), r-mail

Destination Address:

Address Book Entry: (选择), mailsrv1

Service: MAIL

Action: Permit

> Advanced: 移动下列防病毒对象，然后单击 **Return** 以设置高级选项并返回基本配置页：

选择 **scanner1**，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。

8. 策略 ID 3

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: MAIL

Action: Permit

> Advanced: 移动下列防病毒对象，然后单击 **Return** 以设置高级选项并返回基本配置页：

选择 **scanner2**，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 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. 防病毒对象 1

```
set av scanner1 server-name 10.1.1.20
set av scanner1 content http
set av scanner1 content smtp
```

3. 防病毒对象 2

```
set av scanner1 server-name 10.1.1.30
set av scanner1 content http
set av scanner1 content smtp
```

4. 地址

```
set address dmz mailsvr1 1.2.2.6/32
set address untrust r-mail 2.2.2.5/32
```

5. 路由

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

6. 策略 ID 1

```
ns-> set policy id 1 from trust to untrust any any http permit av scanner1
ns-> set policy id 1
ns(policy:1)-> set av scanner2
ns(policy:1)-> exit
ns->
```

7. 策略 ID 2

```
set policy id 2 from untrust to dmz r-mail mailsvr1 mail permit av scanner1
```

8. 策略 ID 3

```
set policy id 3 from trust to dmz any mailsvr1 mail permit av scanner2
save
```

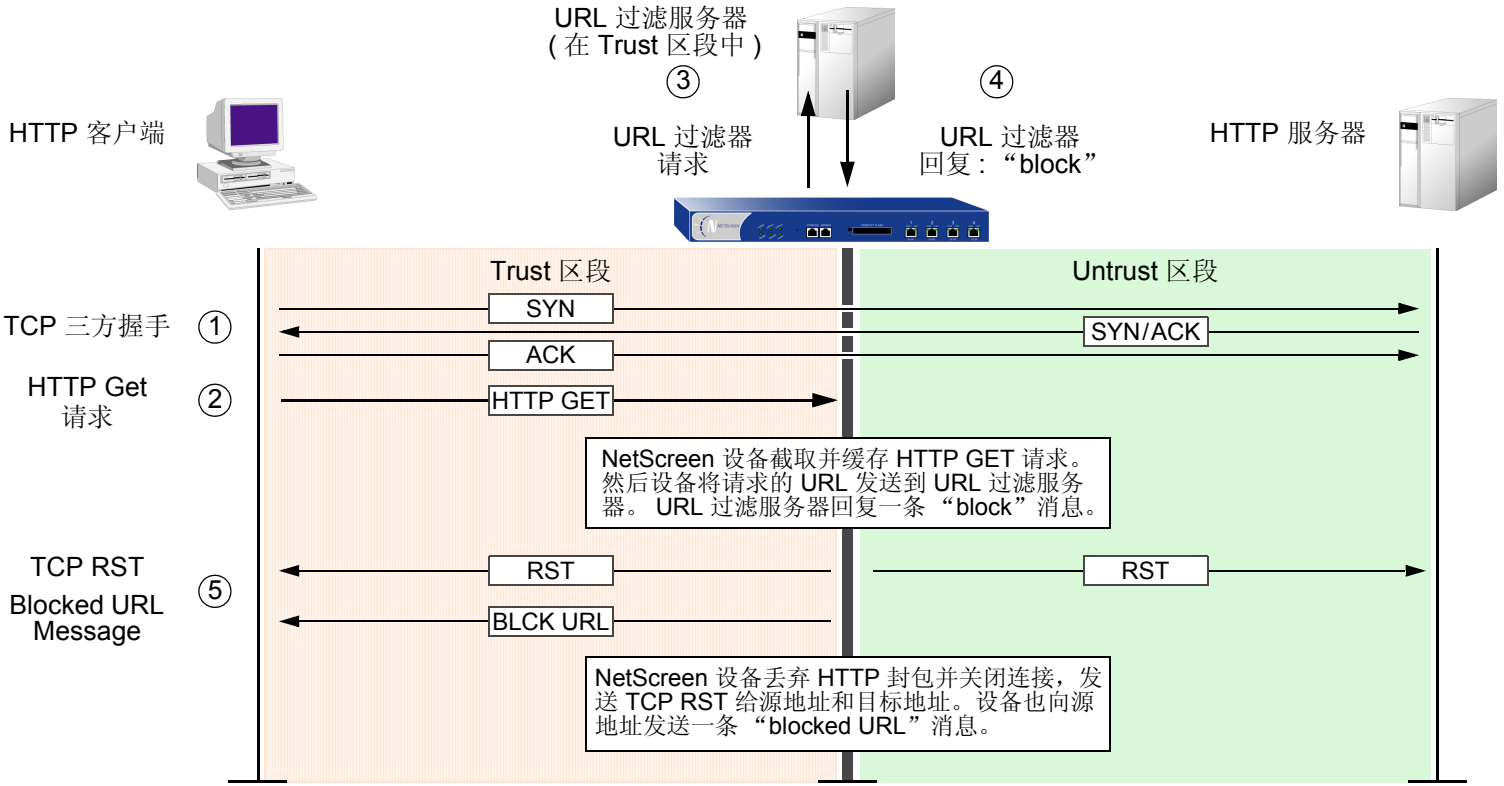
URL 过滤

NetScreen 利用 Websense Enterprise Engine 支持 URL 过滤，根据站点的 URL、域名和 IP 地址， Websense Enterprise Engine 可以阻止或允许访问不同的站点。使用直接嵌入在 NetScreen 防火墙中的 Websense API，NetScreen 设备可以直接链接到 Websense URL 过滤服务器。

当 Trust 区段中的主机试图建立与 Untrust 区段中的服务器的 HTTP 连接时，下图说明了事件的基本顺序。但是，URL 过滤过程确定所请求的 URL 是被禁止的。

Blocked URL

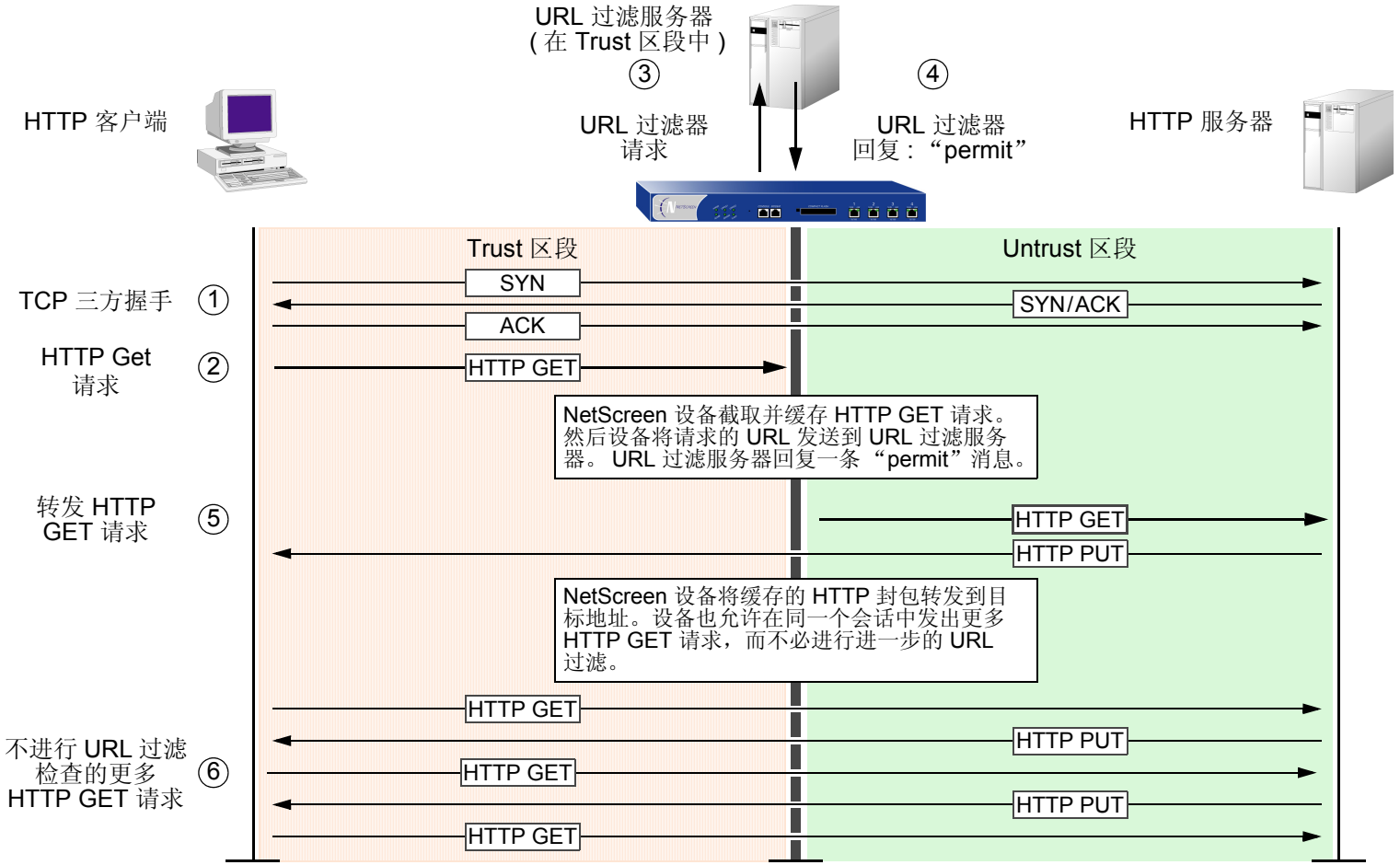
set policy from trust to untrust any any http permit url-filter



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：

Permitted URL

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



利用 Websense，管理员可以执行下列操作 :

- 修改 URL 过滤数据库，以阻止或允许访问所选的站点
- 为一天中的不同时间安排不同的 URL 过滤配置文件
- 下载被封锁或查看的 URL 的 Websense Reporter 日志

***注意：**有关 Websense 的详细信息，请访问 www.websense.com。*

带有虚拟系统的 NetScreen 设备最多支持八个不同的 URL 过滤服务器 — 保留一个服务器供根系统使用，此服务器可与任何数目的虚拟系统共享；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 URL 过滤，必须执行下列任务 :

1. 建立与最多八个 URL 过滤服务器的通信。
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。其它参数组可应用到已定义了专用 URL 过滤服务器的虚拟系统。
3. 激活根级和 vsys 级的 URL 过滤。
4. 在各个策略中启用 URL 过滤。

下面提供这些任务的详细信息。

1. 设备到设备的通信

首先定义 Websense 服务器的设置，并定义应用 URL 过滤时希望 NetScreen 设备采取的行为的参数。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 :

- **Websense Server Name:** 运行 Websense 服务器的计算机的 IP 地址或完全合格的域名 (FQDN)。
- **Websense Server Port:** Websense 的缺省端口是 15868。如果更改了 Websense 服务器的缺省端口，还必须更改 NetScreen 设备上的端口。有关完整信息，请参阅 Websense 文档。
- **Source Interface:** 在将 URL 过滤请求通过 VPN 通道发送到 Websense 服务器时， NetScreen 设备发起这些请求的来源。 (注意源接口不同于外向接口，后者是用于 VPN 信息流的出口接口)。通常情况下， URL 过滤服务器属于 Trust 区段。但是，如果希望几个 NetScreen 设备访问单个 URL 过滤服务器，则可以配置从每个远程设备通往保护该服务器的本地 NetScreen 设备的 VPN 通道。从远程对等方看来，该服务器位于 Untrust 区段中，并且它们通过这些通道向该服务器发送 URL 过滤请求。
- **Communication Timeout:** NetScreen 设备等待 Websense 过滤器响应的时间间隔 (以秒为单位)。如果 Websense 在该时间间隔内没有响应，您可以选择让 NetScreen 设备阻止或允许该请求 (参见下文)。

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 页面上的各个字段中输入这些设置。

2. 系统级行为参数

其次，定义在应用 URL 过滤时希望 (根或 vsys) 系统采用的行为参数。行为选项如下 :

- **Fail/Pass Mode:** 如果 NetScreen 设备与 Websense 服务器失去联系，您可以指定 **Block** 或 **Permit** 所有 HTTP 请求。

– **Blocked URL Message Type:** 当 Websense 封锁某站点时，用户接收的消息源。如果选择 **NetPartners Websense**， NetScreen 设备转发从 Websense 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 发来的消息，也可以创建一条要从 NetScreen 设备发送的消息 (最多 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 | Websense }
set url message string
```

在 WebUI 中，在 Screening > URL Filtering 页面上的各个字段中输入这些设置。

3. 系统级激活

在完成配置后，必须在系统级启用 URL 过滤。对于以 NetScreen 设备为主机的虚拟系统，必须在要应用 URL 过滤的每个系统中启用 URL 过滤。例如，如果希望根系统和 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 命令来在系统级激活或禁用 URL 过滤 :

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

在 WebUI 上，选择或清除 Screening > URL Filtering 页面上的 **Enable URL Filtering via Websense Server** 复选框。

当在系统级启用 URL 过滤时， NetScreen 设备将通过将 HTTP 请求改发到 Websense 服务器，检查 (该系统中定义的) 策略要求应用 URL 过滤的所有 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 过滤部分，并将其当作简单 “permit” 策略。

4. 策略级应用

最后，配置 NetScreen 设备，使其根据策略来连接 URL 过滤服务器。

可以使用一些 CLI 命令来在策略中启用 URL 过滤 :

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

在 WebUI 中，在 Advanced 策略配置页面上，为要应用 URL 过滤的策略选择 **URL Filter** 复选框。

注意 : *NetScreen 设备报告 Websense 服务器的状态。要更新状态报告，请在 WebUI 中单击 Screening > URL Filtering 页面上的 Server Status 图标。*

范例 : URL 过滤配置

在本例中，配置 NetScreen 设备，使之用端口号 15868 (缺省值) 与 IP 地址为 10.1.2.5 的 URL 过滤服务器协同工作。 URL 过滤服务器位于 Trust 区段中。您要对从 Trust 区段的主机发往 Untrust 区段的主机的所有出站 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 且拥有 IP 地址 1.1.1.1/24。 Trust 区段的接口是 ethernet1 且拥有 IP 地址 10.1.1.1/24。两个区段都位于 trust-vr 路由域中。由于该 URL 过滤服务器不在其中任一个 NetScreen 设备接口的直接子网中，因此为过滤服务器添加一个通过 ethernet1 和位于 10.1.1.250 的路由器的路由。

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: (有此选项时将其选定)

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: (有此选项时将其选定)

IP Address/Netmask: 1.1.1.1/24

2. URL 过滤服务器

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

Enable URL Filtering via Websense Server: (选择)

Websense Server Name: 10.1.2.5

Websense Server Port: 15868

Communication Timeout: 10 (秒)

If connectivity to the Websense 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. If this prohibition appears to be in error, 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

> Advanced: 选择 **URL Filter**复选框，然后单击 **Return** 以设置高级选项并返回基本配置页。

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 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. If this
    prohibition appears to be in error, 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

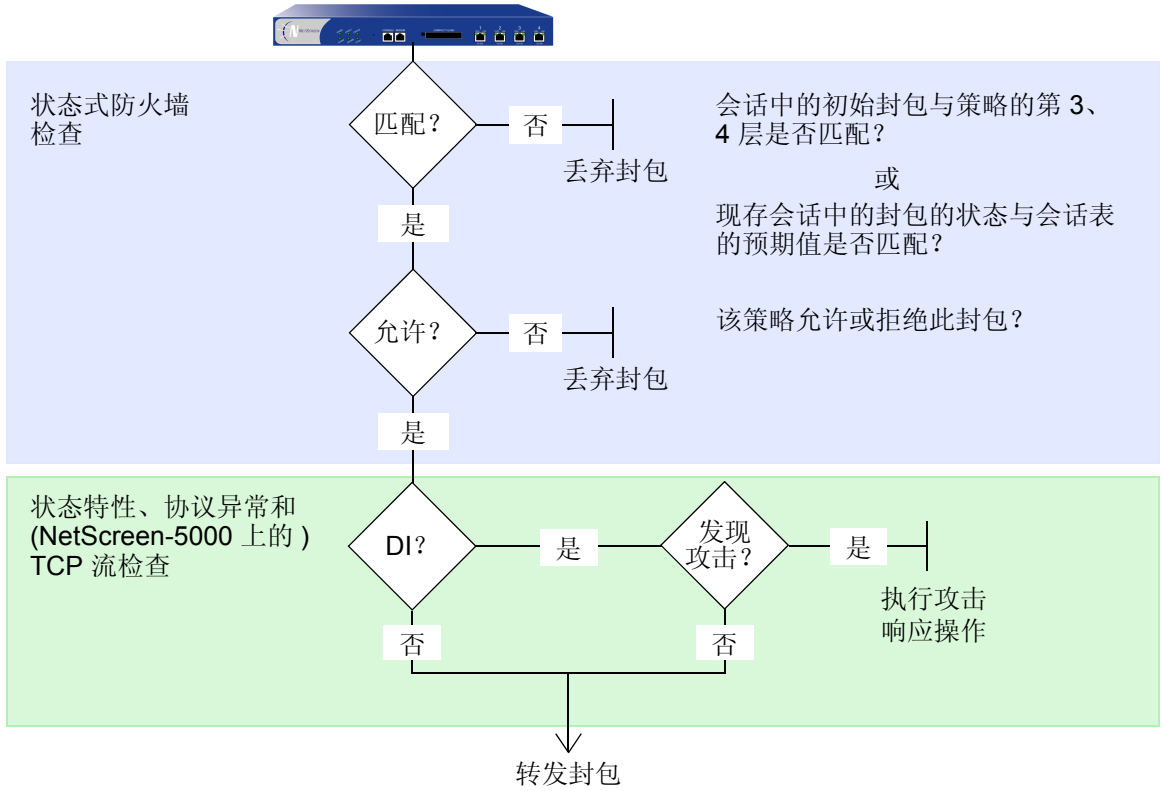
深层检测

您可以在策略中启用 “深层检测” (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 “深层检测” 原理，并说明如何配置它们：

也可以在安全区级为 HTTP 组件启用 “深层检测”。本章最后一节介绍 SCREEN 选项。

深层检测概述

“深层检测”(DI) 是过滤 NetScreen 防火墙允许的信息流的机制。深层检测第 3、4 层封包包头和第 7 层内容和协议特性，以努力检测和防止可能出现的任何攻击或异常行为[1]。



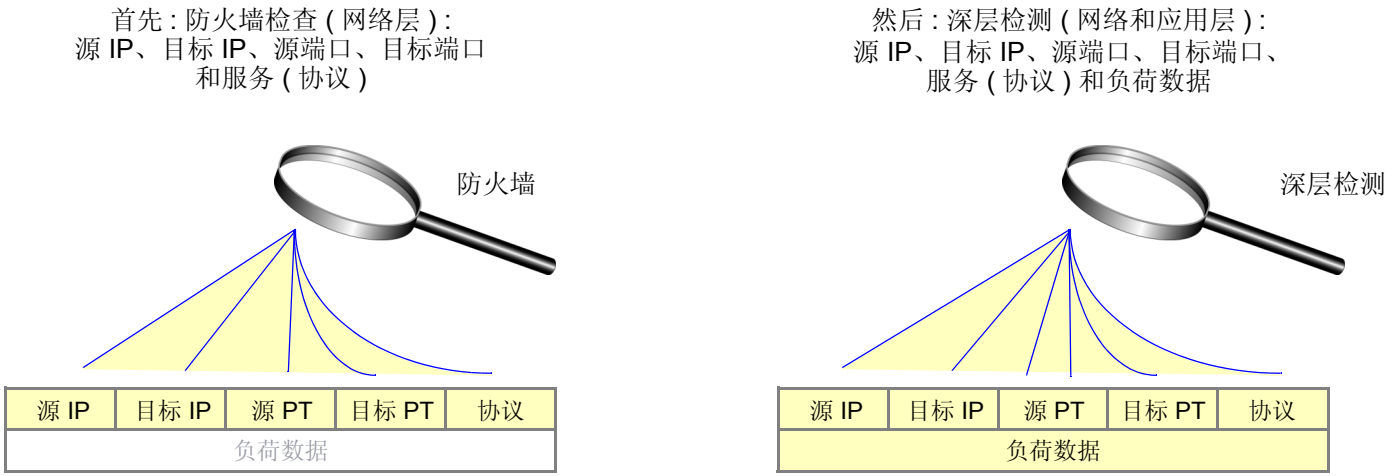
当设备接收到会话的第一个封包时， NetScreen 将检查 IP 封包包头中的源和目标 IP 地址 (检查第 3 层)，并检查 TCP 片段或 UDP 数据报报头中的源和目标端口号与协议 (检查第 4 层)。如果第 3 层和第 4 层组件的信息与策略中

1. NetScreen 通过在区段级 (而非策略级) 设置的 SCREEN 选项，来检查第 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。

指定的标准相匹配，则 NetScreen 设备对该封包执行指定的操作 — permit、 deny 或 tunnel[2]。当接收到已建立的会话的封包时， NetScreen 设备会将该封包与会话表中的状态信息进行比较，以确定其是否确实属于该会话。

如果您在应用到此封包上的策略中启用了 “深层检测”，并且策略操作是 “permit” 或 “tunnel”，则 NetScreen 将进一步检查该封包及其关联的数据流中的攻击对象。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 140 页上的 “攻击对象和组”和第 160 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

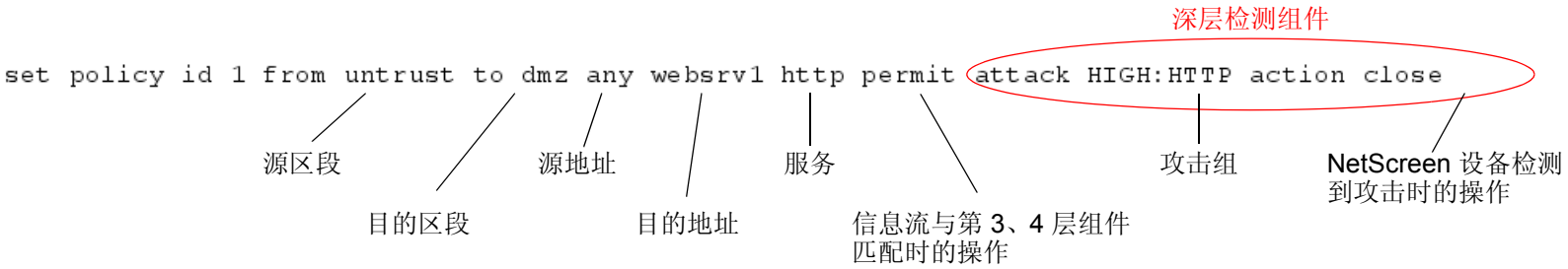


2. 如果指定的操作是 tunnel，则暗指允许概念。注意，如果您在操作为 tunnel 的策略中启用 “深层检测” (DI)，则 NetScreen 设备将在加密出站封包之前和解密入站封包之后，执行指定的 DI 操作。

3. 您需要先预订服务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**-554 页上的 “签名服务的注册与激活”。

如果检测到攻击对象，则 NetScreen 设备将执行策略的 DI 组件中指定的操作 : 关闭、关闭客户端、关闭服务器、丢弃、丢弃封包、忽略或无。如果没有发现所指定的攻击对象，则设备转发封包。 (有关攻击操作的详细信息，请参阅第 146 页上的 “攻击操作”。)

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。它也指示 NetScreen 设备检查该策略允许的所有 HTTP 信息流。如果发现了攻击对象组 “HIGH:HTTP:ANOM” 中定义的任何攻击对象，则 NetScreen 将丢弃封包并发送 TCP RST 通知给源和目标，从而关闭连接。

可以概念性地将一个 **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、以及操作[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，以查找一个或多个指定的攻击对象组中包含的攻击对象。如果检测到攻击对象，则 NetScreen 设备将执行 DI 组件中声明的操作。

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、服务和操作 — 是必须的。 (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**-217 页上的 “全局策略”。)

可以通过使用 ID number 来输入现有策略的上下文。例如：

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

注意：命令提示发生变化，说明后续命令位于特定环境内。

如果要输入与单个策略相关的几个命令，则输入策略上下文将会很方便。例如，下列命令集创建一个策略，允许从 Untrust 中的任何地址发出的 HTTP 和 HTTPS 信息流发送到 DMZ 中的 websrv1 和 websrv2，并查找中级、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
ns(policy:1)-> set attack HIGH:HTTP:ANOM
ns(policy:1)-> set attack HIGH:HTTP:SIGS
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。为了能够用策略上下文添加攻击对象组，首先必须在顶级命令中指定 DI 攻击和操作。在上例中，可以添加 CRITICAL:HTTP:SIGS、HIGH:HTTP:ANOM 和 HIGH:HTTP:SIGS 攻击对象组，因为您首先配置对 CRITICAL:HTTP:ANOM 组进行 “深层检测” 的策略。

注意：可以为每个策略只指定一个攻击操作。有关七个攻击操作的详细信息，请参阅第 146 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。 NetScreen 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。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** -554 页上的 “签名服务的注册与激活”。)

***注意：** ScreenOS 含有用于认证与攻击对象数据库服务器通信的 CA 证书。*

有四个方法可更新数据库 :

- **立即更新 ：**选定此选项时，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，首先必须配置攻击对象数据库服务器设置。 (有关的范例，请参阅第 133 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 设备上的更新一些。*

- **自动更新 ：**选定此选项时，如果服务器上的数据库版本比先前在 NetScreen 设备上装载的数据库版本更新，则 NetScreen 设备将在用户预定的时间将攻击对象数据库直接下载到设备中。 NetScreen 定期用新发现的攻击模式更新数据库。因此，由于数据库不断变化的特性，也要求您定期更新 NetScreen 设备。为了执行此操作，首先必须配置攻击对象数据库服务器设置。(有关的范例，请参阅第 134 页上的 “范例 : 自动更新”。)
- **自动通知和立即更新：**选定此选项时， 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 的主页上出现通知，也会在 CLI 中出现通知。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。 (有关的范例，请参阅第 136 页上的 “范例 : 自动通知和立即更新”。)

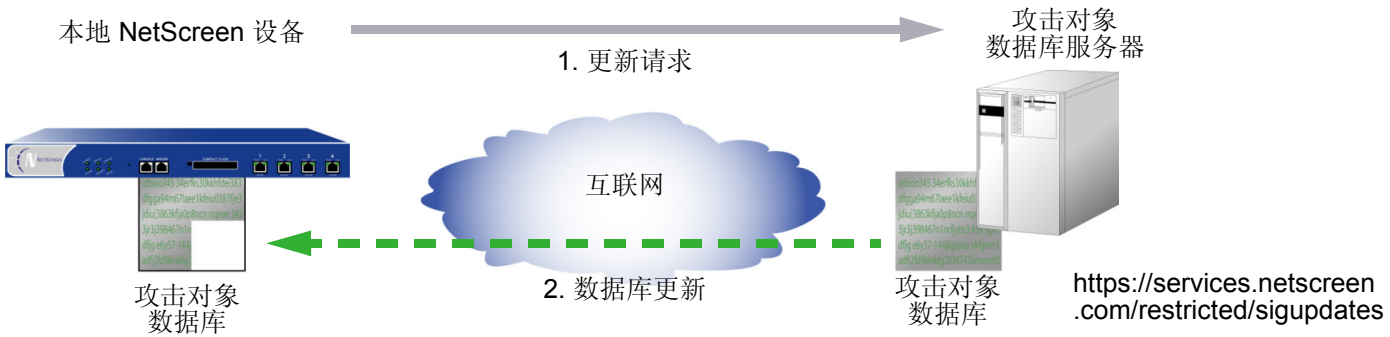
- **手动更新：**选定此选项时，首先使用 Web 浏览器将攻击对象数据库下载到本地目录或 TFTP 服务器目录中。然后可使用 WebUI (从本地目录) 或 CLI (从 TFTP 服务器目录) 在 NetScreen 设备上加载数据库。(有关的范例，请参阅第 138 页上的 “范例：手动更新”。)

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。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。

请勿设置在 NetScreen 设备上更新数据库的时间表。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 设备获得并激活对 DI 签名服务的预订。(有关预订的信息，请参阅第 **2**-552 页上的 “许可密钥”。)*



WebUI

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

CLI

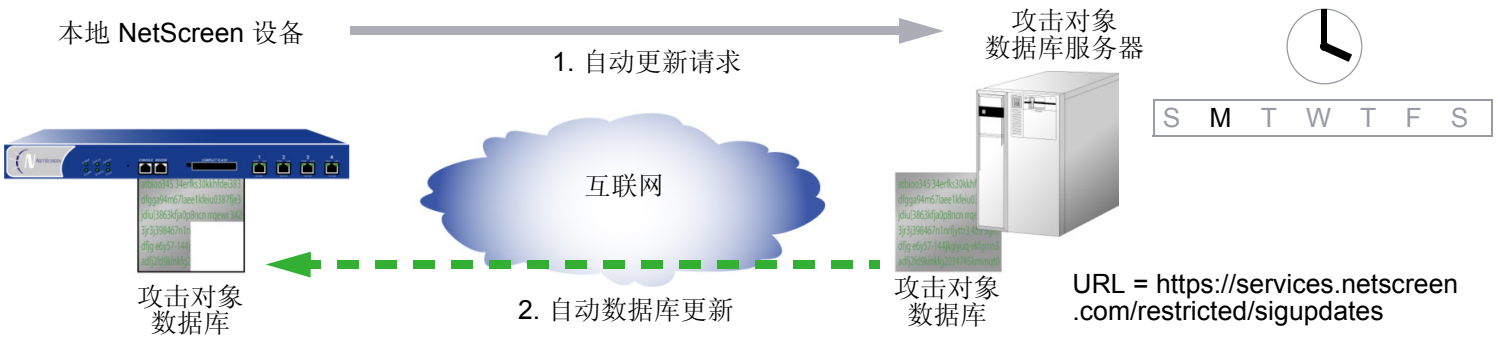
```
ns-> exec attack-db update
Loading attack database.............
Done.
Done.
Switching attack database...Done
Saving attack database to flash...Done.
ns->
```

范例：自动更新

在本例中，将设置一个时间表，使得每星期一上午 4:00 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 设备获得并激活对 DI 签名服务的预订。(有关预订的信息，请参阅第 **2**-552 页上的“许可密钥”。)*

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[5]

Time (hh:mm): 04:00

CLI

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

5. 如果您预定每月执行更新，而在某个月份中并没有您所选择的日期 (例如，多个月份中没有 31 日)，则 NetScreen 设备将在该月使用可能的最后日期。

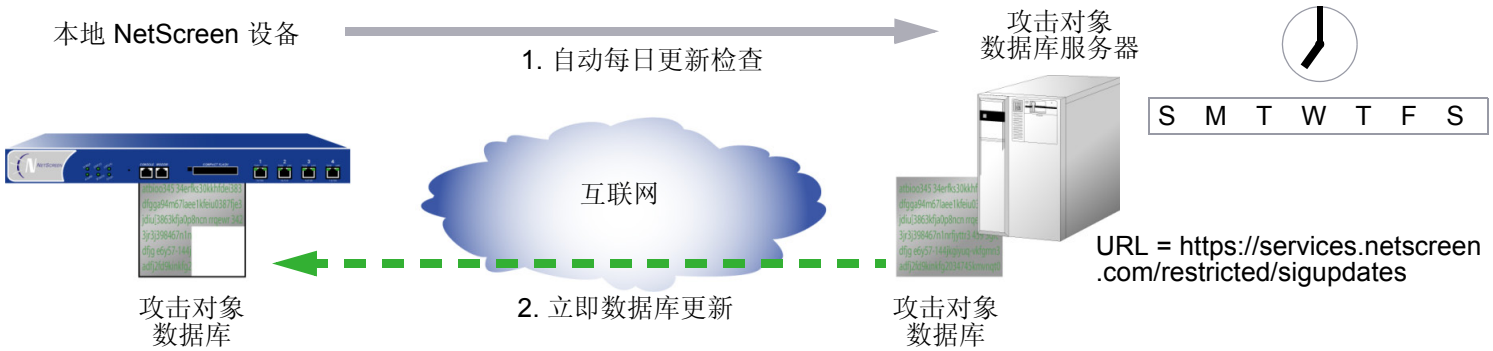
范例：自动通知和立即更新

在本例中，将设置时间表，使得每天上午 7:00 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 设备获得并激活对 DI 签名服务的预订。(有关预订的信息，请参阅第 **2**-552 页上的 “许可密钥”。)*

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，说明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，说明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，您手动地将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)。然后从本地目录装载 NetScreen 设备上的数据库[6]。

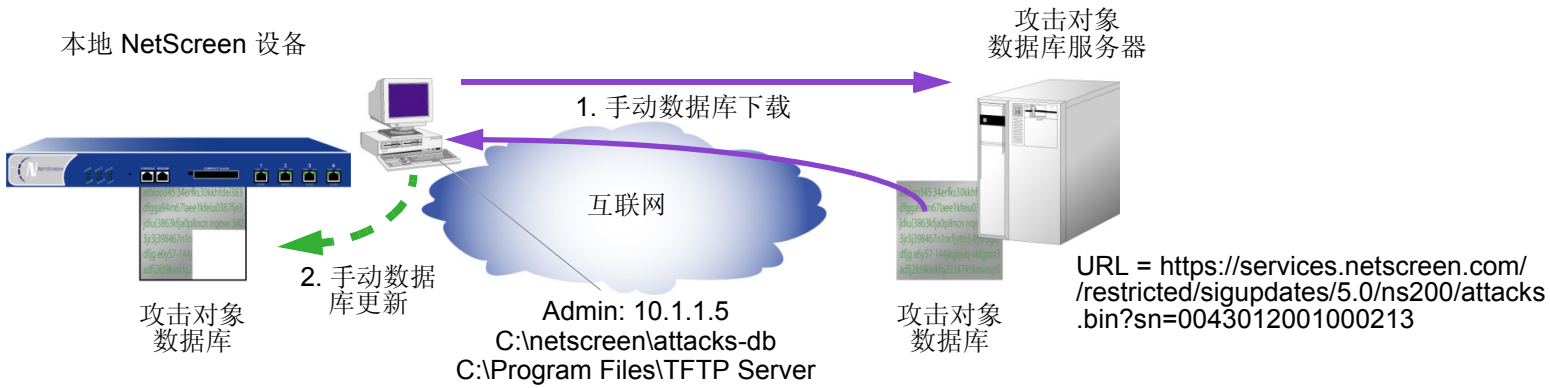
对于自动更新， NetScreen 设备自动向 URL 添加下列元素 :

- 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 5.0，平台是 NetScreen-208 (ns200)。因此，产生的 URL 是 :

https://services.netscreen.com//restricted/sigupdates/5.0/ns200/attacks.bin?sn=0043012001000213

注意 : *此范例假定您已经为 NetScreen 设备获得并激活对 DI 签名服务的预订。(有关预订的信息，请参阅第* ***2****-552 页上的 “许可密钥”。)*



6. 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，或者可使用下列 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/5.0/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 装载)，或者保存到 TFTP 服务器目录 C:\Program Files\TFTP Server (如果要使用 CLI 装载)。

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**。

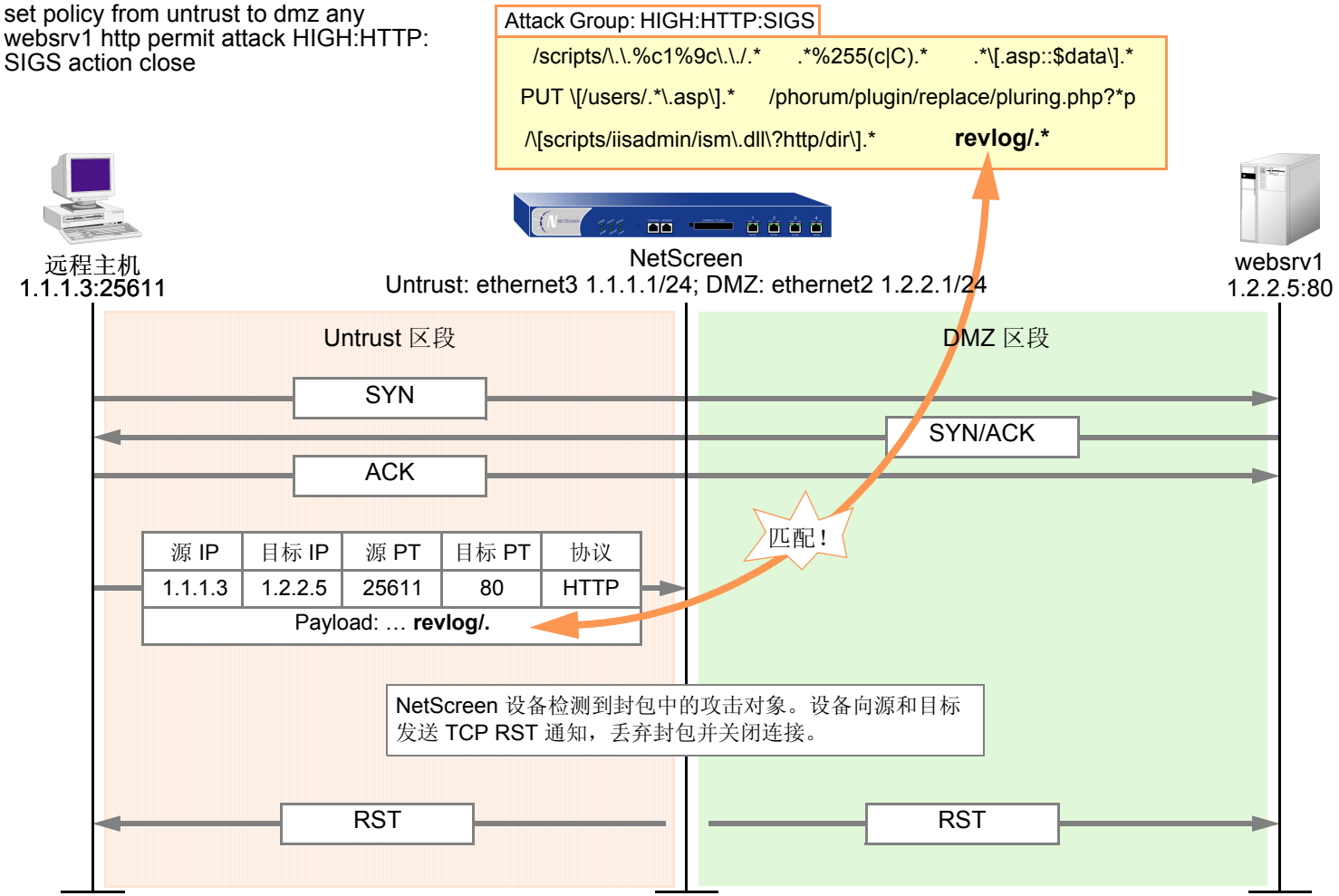
CLI

1. 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和协议异常，它们被 NetScreen 设备用以检测旨在损害网络上的主机的攻击。攻击对象先按照协议类型再按照严重性编排成组。当您将 “深层检测” (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。



DI 组件中引用的攻击对象组的目标服务类型，必须与策略允许的服务类型相同。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 信息流中其永远不可能找到的 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 组件以检查 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
```

如果 NetScreen 设备拥有对 http://help.netscreen.com/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 Address 栏中输入下列 URL 之一：

http://help.netscreen.com/sigupdates/english/DNS.html

http://help.netscreen.com/sigupdates/english/FTP.html

http://help.netscreen.com/sigupdates/english/HTTP.html

http://help.netscreen.com/sigupdates/english/IMAP.html

http://help.netscreen.com/sigupdates/english/POP3.html

http://help.netscreen.com/sigupdates/english/SMTP.html

以上每个 URL 都链接到 HTML 页面，其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[7]。该签名可以是第 3 或 4 层信息流模式，例如当某个地址发送很多封包到位于另一个地址处的不同端口号时 (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 封包的数据负荷中时。该字符串也可以是特殊的代码段或封包包头中的特定值。但是，在搜索文本模式时，NetScreen 设备中的“深层检测”(DI) 模块不仅查找封包中的签名，也在封包的特定部分中查找该签名 (即便是封包碎片或片段)，在会话生存期内的特定时间发送的封包内查找，以及在由连接发起方或响应方发送的封包内查找。

当检查文本模式时， DI 模块会考虑参与者作为客户端或服务器时的角色，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该模式的攻击相关的那些元素。使用上下文信息来改进封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”表达了这样一个概念 : 在参与者的角色和会话状态的环境内查找签名。

为了看到考虑出现签名的环境的优点，在启用 NetScreen DI 模块检测 EXPN Root 攻击时，请注意模块检查封包的方式。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。

利用简单的文本封包签名检测技术，即使签名 “expn root”出现在 SMTP 连接的数据部分，也就是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，则单个封包签名检测器会将此邮件当作一次攻击。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。

7. 由于支持规则表达式， NetScreen DI 模块可以在搜索模式时使用通配符。因此，单个攻击签名定义可以适用于多种攻击模式的变体。

TCP 流式签名

像状态式签名一样， 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 : 尽管状态式签名可以是预定义的或用户定义的， TCP 流式签名却必须是用户定义的。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 “深层检测” 的策略中引用该组。 (有关 TCP 流式签名的更多信息，请参阅第 168 页上的 “TCP 流式签名攻击对象”。)

注意 : *只能在 NetScreen-5000 Series 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。协议异常检查对于捕捉新攻击或不能用文本模式定义的那些攻击特别有用。 ScreenOS 支持适用于下列协议的协议异常攻击对象 :

- DNS
- FTP
- HTTP
- IMAP
- POP3
- SMTP

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，这些组分为协议异常组和状态式签名组，然后粗略地按照严重性加以组织。三个攻击对象组严重性级别是关键、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 : 试图破坏设备、获得对网络设备的用户级访问权、或者激活以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 : 检测侦查尝试、试图通过目录遍历或信息漏洞来访问关键信息。

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 (关键、高级、中级) 进行分类的，但每个攻击对象都有其本身的特定严重性级别 : Critical (关键) 、 High (高级)、 Medium (中级)、 Low (低级)、 Info (信息)。这些攻击对象严重性级别与事件日志条目严重性级别的对应关系如下 :

攻击对象严重性级别	– 对应 –	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 设备检测到严重性级别为 “中级”的攻击对象，则在事件日志中出现的相应条目具有严重性级别 “Warning”。

可以覆盖策略中引用的攻击对象组中的所有攻击对象的缺省严重性级别。通过输入现有策略的上下文，然后给策略引用的所有攻击对象组指定新的严重性级别，即可在策略级执行此操作。

下面说明如何通过 WebUI 和 CLI 更改策略中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 下拉列表中选择严重性选项，然后单击 **OK**。

CLI

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

如要将每个攻击对象的严重性级别恢复为其原始设置，可以再次输入策略的上下文，并执行下列 **unset policy** 命令 :

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
```

攻击操作

当检测到攻击时， NetScreen “深层检测” (DI) 模块将执行指定的操作。七个可能的操作如下：

- **Close** (服务器连接，并将 RST 发送给客户端和服务器[8])

  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，通过向客户端和服务器都发送 RST，更有可能让至少一方获得该 RST 并关闭会话。

- **Close Client** (服务器连接，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。

- **Close Server** (服务器连接，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。

- **Drop** (服务器连接而不向任一方发送 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封包，但不发送 TCP RST。

- **Drop Packet** (丢弃特定的封包，但不切断连接)

  此选项丢弃出现攻击签名或协议异常的封包，但不终止会话本身。使用此选项丢弃残缺的封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，仅丢弃封包将停止有问题的封包，而不会停止所有其它封包的流动。

8. 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** (在检测到攻击签名或异常后， NetScreen 设备编写一个日志条目，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 设备生成一个事件日志条目，但不切断会话本身。在实现“深层检测” (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 设备对每个会话发记录一次 (使其不会用主动错误信息填写日志)，但不采取措施。

- **None** (无操作)

  在实现 “深层检测” (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 设备在事件日志中写入一个条目，但不对信息流本身采取措施。 NetScreen 设备继续检查该会话中的后续信息流，并且如果检测到其它攻击签名和异常，则记录日志条目。

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

在本例中有三个区段 : Trust、 Untrust 和 DMZ。您已完成了对攻击的分析，并断定您需要下列三个策略 :

- **策略 ID 1:** 允许从 Untrust 区段中的任何地址发向 DMZ 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
  – Action: Close Server

  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向 DMZ 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
  – Action: Close

  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，他们都能终止会话和清除资源。

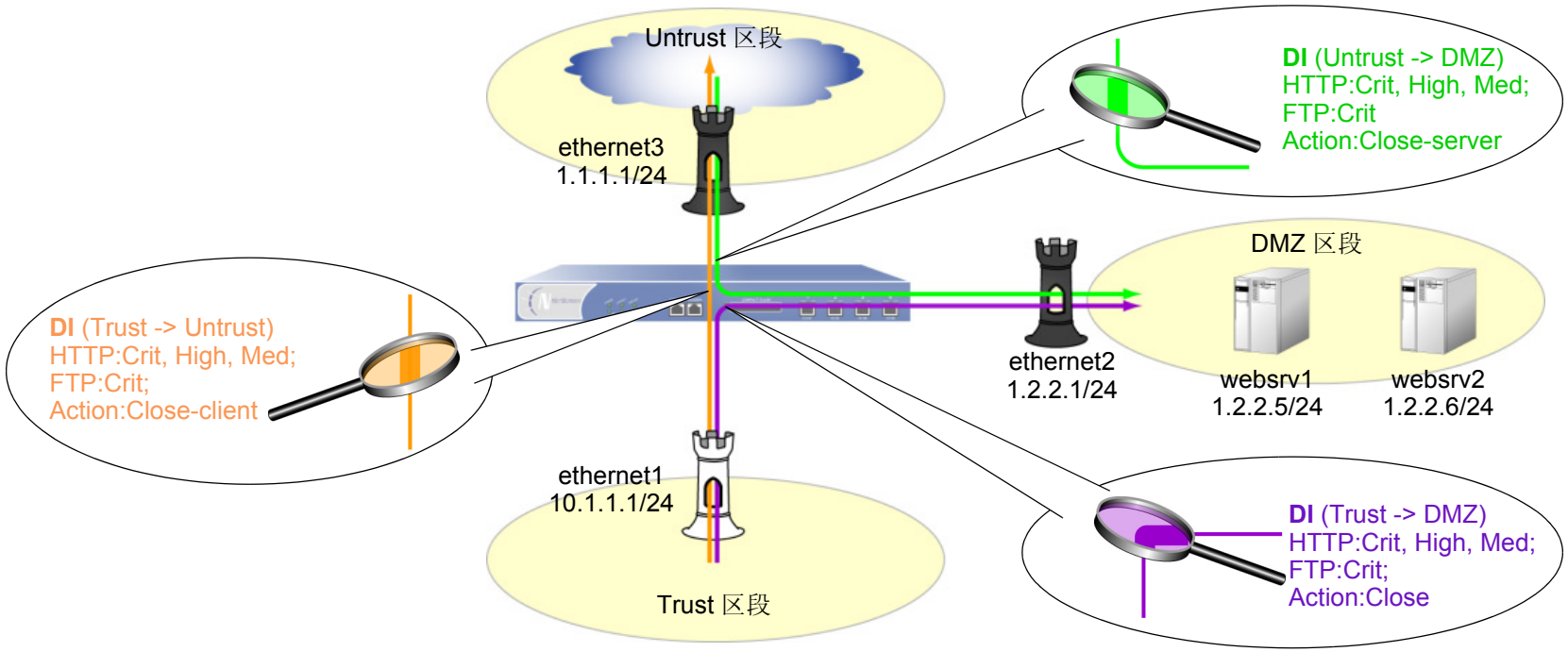
- **策略 ID 3:** 允许从 Trust 区段的任何地址发送到 Untrust 区段的任何地址的 FTP-GET、 HTTP、 HTTPS、PING 信息流。

  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
  – Action: Close Client

  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“深层检测”。所有区域都在 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: (有此选项时将其选定)

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: (有此选项时将其选定)

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: (有此选项时将其选定)

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**，输入下列信息，然后单击 **OK** 以返回基本策略配置页 :

Action: Close Server

使用 **<<** 按钮将下列攻击组从 Available Members 列移动到 Selected Members 栏中 :

CRITICAL:HTTP:ANOM

CRITICAL:HTTP:SIGS

HIGH:HTTP:ANOM

HIGH:HTTP:SIGS

MEDIUM:HTTP:ANOM

MEDIUM:HTTP:SIGS

CRITICAL:FTP:SIGS

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**，输入下列信息，然后单击 **OK** 以返回基本策略配置页 :

Action: Close

使用 **<<** 按钮将下列攻击组从 Available Members 列移动到 Selected Members 栏中 :

CRITICAL:HTTP:ANOM

CRITICAL:HTTP:SIGS

HIGH:HTTP:ANOM

HIGH:HTTP:SIGS

MEDIUM:HTTP:ANOM

MEDIUM:HTTP:SIGS

CRITICAL:FTP:SIGS

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**，输入下列信息，然后单击 **OK** 以返回基本策略配置页 :

Action: Close Client

使用 **<<** 按钮将下列攻击组从 Available Members 列移动到 Selected Members 栏中 :

CRITICAL:HTTP:ANOM

CRITICAL:HTTP:SIGS

HIGH:HTTP:ANOM

HIGH:HTTP:SIGS

MEDIUM:HTTP:ANOM

MEDIUM:HTTP:SIGS

CRITICAL:FTP:SIGS

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
ns(policy:1)-> set attack HIGH:HTTP:ANOM
ns(policy:1)-> set attack HIGH:HTTP:SIGS
ns(policy:1)-> set attack MEDIUM:HTTP:ANOM
ns(policy:1)-> set attack MEDIUM:HTTP:SIGS
ns(policy:1)-> set attack CRITICAL:FTP:SIGS
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
ns(policy:2)-> set attack HIGH:HTTP:ANOM
ns(policy:2)-> set attack HIGH:HTTP:SIGS
ns(policy:2)-> set attack MEDIUM:HTTP:ANOM
ns(policy:2)-> set attack MEDIUM:HTTP:SIGS
ns(policy:2)-> set attack CRITICAL:FTP:SIGS
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
ns(policy:3)-> set attack HIGH:HTTP:ANOM
ns(policy:3)-> set attack HIGH:HTTP:SIGS
ns(policy:3)-> set attack MEDIUM:HTTP:ANOM
ns(policy:3)-> set attack MEDIUM:HTTP:SIGS
ns(policy:3)-> set attack CRITICAL:FTP:SIGS
ns(policy:3)-> exit
save
```

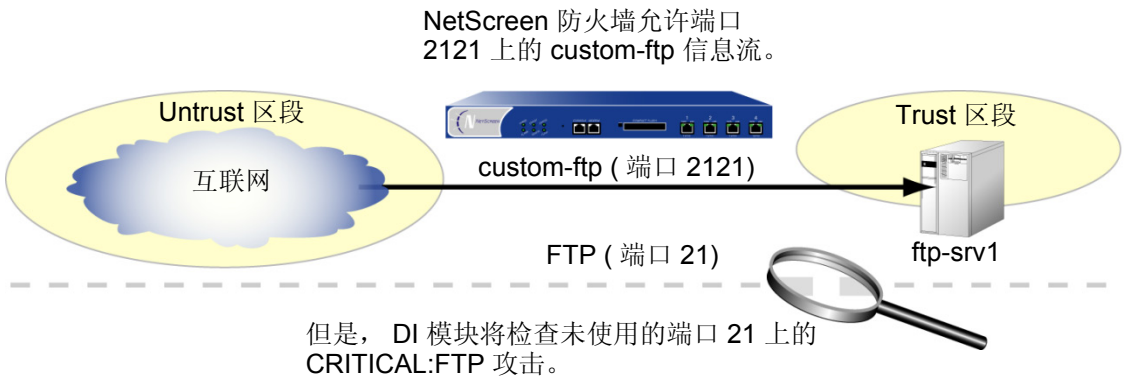
将定制服务映射到应用程序

当在含 “深层检测” (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，如果您正在为 FTP 创建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 组件添加到引用定制服务的策略中，则此 DI 组件将不能识别应用程序，因为该应用程序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
```



为了避免这个问题，您必须通知 DI 模块，该 FTP 应用程序正在运行在端口 2121 上。实际上，您必须将 “应用层” 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，使其检查引用 custom-ftp 的策略中的 CRITICAL:FTP:SIGS 攻击对象组定义的攻击时， DI 模块在端口 2121 上执行检查。

```
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，定义名为 “HTTP1” 的定制服务，使用目标端口 8080。对于允许将 HTTP1 信息流从 Untrust 区段的任何地址发送到 DMZ 区段中名为 “server1” 的 Web 服务器的策略，将 HTTP 应用程序映射到该定制服务上。

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**，输入下列信息，然后单击 **OK** 以返回基本策略配置页 :

Action: Close Server

使用 **<<** 按钮将下列攻击组从 Available Members 列移动到 Selected Members 栏中 :

CRITICAL:HTTP:ANOM

CRITICAL:HTTP:SIGS

HIGH:HTTP:ANOM

HIGH:HTTP:SIGS

MEDIUM:HTTP:ANOM

MEDIUM:HTTP:SIGS

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
ns(policy:1)-> set attack HIGH:HTTP:ANOM
ns(policy:1)-> set attack HIGH:HTTP:SIGS
ns(policy:1)-> set attack MEDIUM:HTTP:ANOM
ns(policy:1)-> set attack MEDIUM:HTTP:SIGS
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 “深层检测” (DI) 应用程序来最好地满足自己的需要。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。

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。在创建攻击对象时，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:” 开始。)
- 选择 “深层检测” 搜索的环境。
- 定义签名。
- 给攻击对象分配严重性级别。

以下各小节讨论有关环境和签名的主题。有关 NetScreen-Security Manager 2004 所使用的严重性级别的信息，请参阅第 144 页上的 “更改严重性级别”。

环境

环境定义封包中的位置，从中 NetScreen DI 模块搜索与攻击对象模式相匹配的签名。可以指定下列环境中的任一个 :

- FTP 命令 : 将环境设置为 RFC 959 “File Transfer Protocol” (FTP) 中指定的 FTP 命令之一
- FTP 用户名 : 将环境设置为在登录到 FTP 服务器时用户输入的名称
- 已分析的 HTTP URL: 将环境设置为从 unicode 字符串解码的 “规格化” 文本字符串
- SMTP 包头发送者 : 将环境设置为 SMTP “发送者 :” 包头
- SMTP 包头接收者 : 将环境设置为 SMTP “接收者 :” 包头
- SMTP 邮件发送者 : 将环境设置为 SMTP “MAIL FROM” 命令行
- SMTP 收件人 : 将环境设置为 SMTP “RCPT TO” 命令行

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。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。*

签名

在输入签名的文本字符串时，可以输入由普通字符组成的字母数字字符串，按照字符搜索精确的匹配，或者可使用规则表达式来将搜索范围扩大到可能匹配的字符集。 ScreenOS 支持以下规则表达式：

目的	元字符	范例	含义
直接二进制匹配（八进制）*	\O*octal_number*	\0162 匹配： 162	精确匹配此八进制数：“162”。
直接二进制匹配（十六进制）†	\X*hexadecimal_number*\X	\X01 A5 00 00\X 匹配： 01 A5 00 00	精确匹配这五个十六进制数：“01 A5 00 00”。
不区分大小写的匹配	\[*characters*\]	\[cat\] 匹配： 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： cat, cbt, cct, … czt cAt, cBt, cCt, … cZt c1t, c2t, c3t, … c9t	匹配“c- 任何字符 -t”。

目的	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： bc bbc abc aaabbbbc	匹配“a”0 次、1 次或多次，后面“b”1 次或多次，最后“c”1 次。
1 次或多次匹配前一个字符	+	a+b+c 匹配： abc aabc aaabbbbc	匹配“a”1 次或多次，后面“b”1 次或多次，最后“c”1 次。
0 次或 1 次匹配前一个字符	?	drop-?packet 匹配： drop-packet droppacket	匹配“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： drop packet	匹配“drop”或“packet”。

目的	元字符	范例	含义
字符范围	[*start-end*]	[c-f]a(d | t) 匹配： cad, cat dad, dat ead, eat fad, fat	匹配所有以“c”、“d”、“e”或“f”开头、以字母“d”或“t”结尾而且中间含字母“a”的所有字符串。
下列字符的相反值	[^*character*]	[^0-9A-Z] 匹配： a, b, c, d, e, … z	匹配小写字母。

* 八进制是以 8 为基数的记数系统，只使用数字 0-7。

† 十六进制是以 16 为基数的记数系统，使用通常的 0-9 数字，并使用字母 A-F 表示十进制值为 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，您拥有 DMZ 区域中的一个 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	停止让某人在 FTP 服务器上放文件。
cs:ftp-user-dm	拒绝登录名为 “dmartin” 的用户的 FTP 访问。
cs:url-index	在任何 HTTP 请求中，封锁含有已定义的 URL 的 HTTP 封包。
cs:spammer	封锁从含有 “spam.com” 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，允许从 Untrust 区段发到 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: url-index

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**，输入下列信息，然后单击 **OK** 以返回基本策略配置页 :

Action: Close Server

使用 **<<** 按钮将下列攻击组从 Available Members 栏移动到 Selected Members 栏中，

CS:DMZ DI

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: url-index

```
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

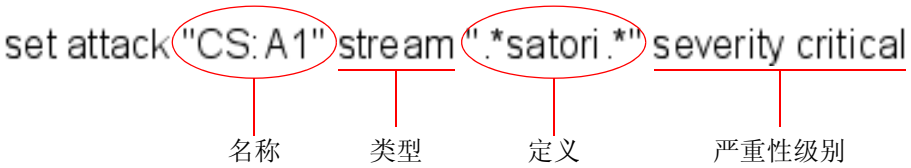
状态式签名在特定应用中是基于环境的，如 FTP 用户名或 SMTP 包头字段。 TCP 流式签名查找任何种类的 TCP 信息流中所有位置的模式，而不管所使用的应用协议是什么。

注意：*只能在 NetScreen-5000 Series 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，您必须定义它们。在创建签名攻击对象时，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:” 开始。)
- 对象类型 (“流”)
- 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，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，创建名为 “CS:Gr1” 的一个组，然后将该对象添加到该组中。最后，定义引用 CS:Gr1 的一个策略，并且指示 NetScreen 设备：如果该模式出现在此策略所适用的任何信息流中，则切断连接并将 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**，输入下列信息，然后单击 **OK** 以返回基本策略配置页：

   Action: Close Client

   选择 Available Members 栏中的 **CS:Gr1**，然后单击 **<<** 将其移动到 Selected Members 栏中。

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
```

HTTP 组件的点状封锁

NetScreen 设备可以选择性地封锁通过 HTTP 发送的 ActiveX 控件、 Java applet、 .zip 文件和 .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手段，使其有可能载入然后控制受保护网络中的主机上的应用程序。

当在安全区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，看看其是否指示封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 设备将封锁封包。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 设备将封锁封包。

当启用 ActiveX 控件的封锁时， NetScreen 设备将封锁负荷中包含任何类型 HTTP 组件 (ActiveX 控件、 Java applets、 .exe 文件或 .zip 文件) 的所有 HTTP 封包。

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 Web 页面的工具。 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目。 ActiveX 组件也可以包含其它组件 (如 Java applet) 或文件 (如 .exe 和 .zip 文件)。

当您访问启用了 ActiveX 的网站时，网站提示您将 ActiveX 控件下载到计算机中。 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 控件下载到计算机中，则该控件将实现其创建者设计的任何功能。如果这是恶意代码，该控件现在可以重新格式化硬盘、删除所有文件、将您所有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 Java applet 来在 VM 外部运行，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 (即带有 .exe 扩展名的文件)，并不能保证该文件未受感染。即使您信任下载文件的网站，嗅探该网站下载请求的某人可能已截取了您的请求，并用修改过的包含恶意代码的 .exe 文件做出响应。

ZIP 文件

zip 文件 (即带有 .zip 扩展名的文件) 是包含一个或多个压缩文件的一类文件。前一部分介绍的有关下载 .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，在到达 Untrust 区段接口的封包中，封锁包含 Java applet 和 .exe 文件的任何 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
```

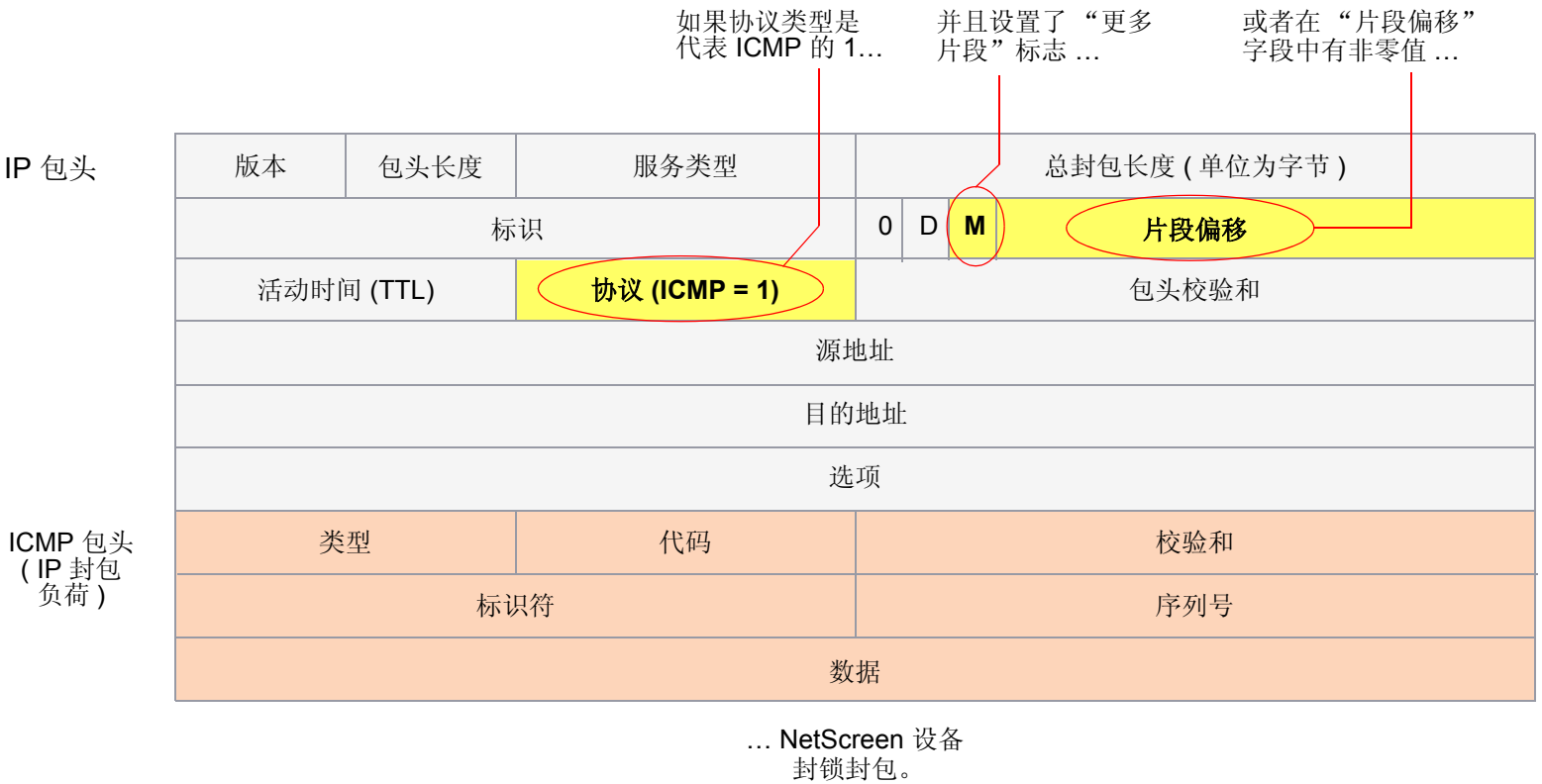
6

可疑封包属性

如本卷其它章所述，攻击者可以通过精心设计封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封包的意图，但由于其是精心设计的，这就暗示其会被用到某些类型的阴险用途中。本章中介绍的所有 SCREEN 选项都能封锁可能包含隐藏威胁的封包：

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 封包只包含很短的信息，因此没有合法理由将 ICMP 封包分为碎片。如果 ICMP 封包太大，必须分为碎片，则可能有一些问题。当启用 ICMP Fragment Protection SCREEN 选项时， NetScreen 设备将封锁设置了 “更多片段” 标志的任何 ICMP 封包，或者含有偏移字段中指示的偏移值的任何 ICMP 封包。



要封锁 ICMP 封包碎片，请执行以下任一操作，其中指定的安全区是封包碎片始发的区段 :

WebUI

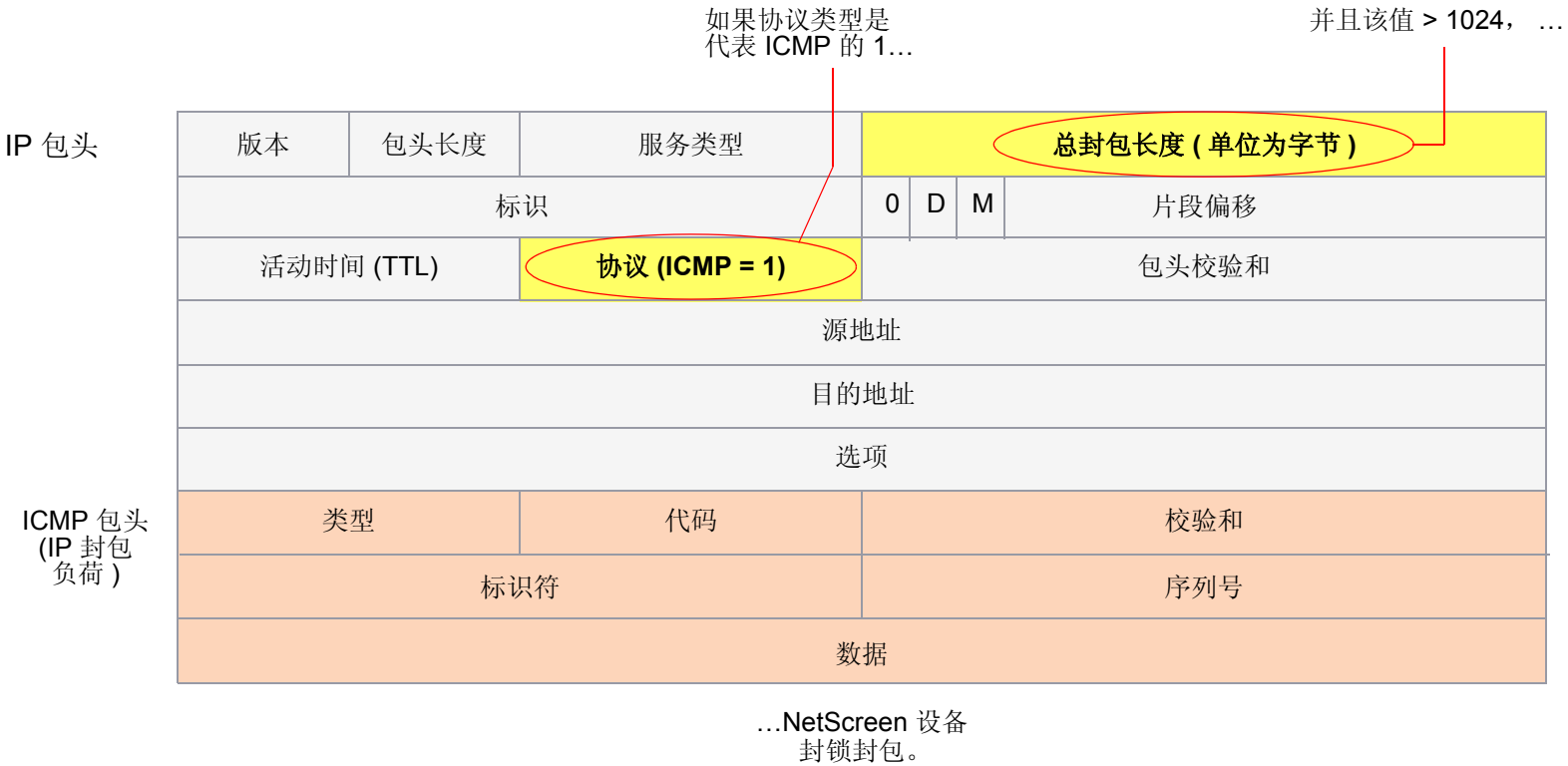
Screening > Screen (Zone: 选择区段名称): 选择 **ICMP Fragment Protection**，然后单击 **Apply**。

CLI

```
set zone zone screen icmp-fragment
```

大的 ICMP 封包

如上节第 176 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 封包只包含很短的信息，因此没有合法理由适用于大的 ICMP 封包。如果 ICMP 封包异常地大，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 ICMP 封包的存在可能会使作为 Loki 代理的受损机器暴露。也可能指示出某些类型的变化活动。



当启用 Large Size ICMP Packet Protection SCREEN 选项时，NetScreen 设备检查丢弃长度大于 1024 字节的 ICMP 封包。

要封锁大的 ICMP 封包，请执行以下任一操作，其中指定的安全区是 ICMP 封包始发的区段 :

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

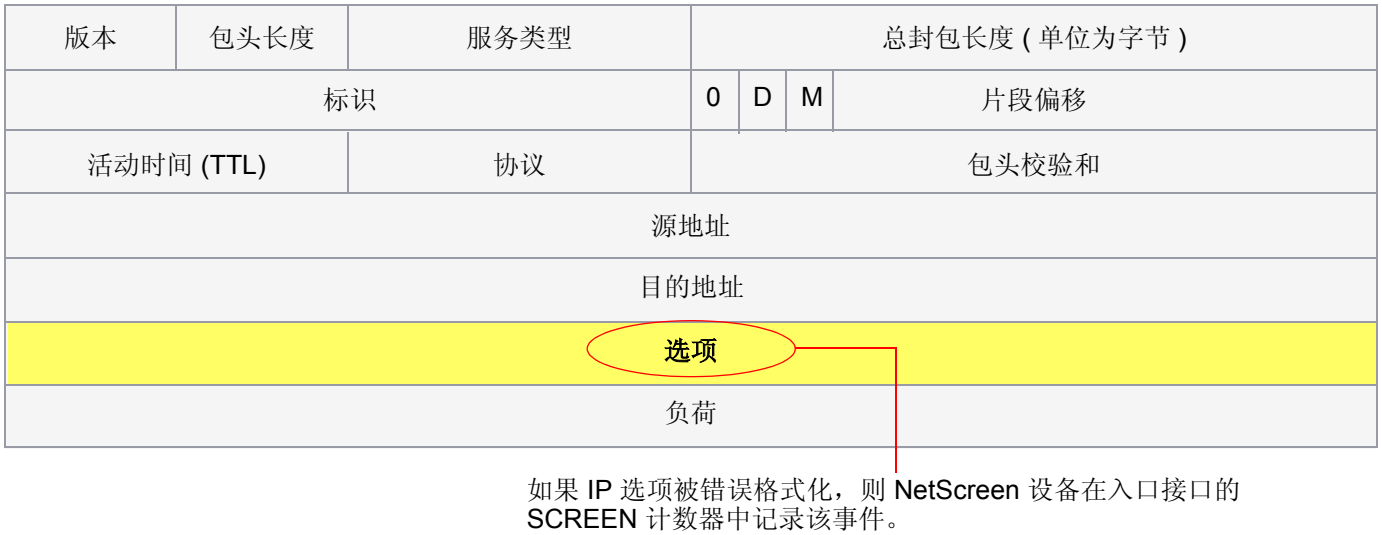
```
set zone zone screen icmp-large
```

坏的 IP 选项

互联网协议标准 “RFC 791, Internet Protocol” 指定了一组八个选项以提供特殊路由控制、诊断工具和安全性。尽管这些选项的原来预期用途发挥了作用，但某些人已想出了歪曲这些选项的方法，以达到不可告人的目的。 (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”。)

或是故意或是偶然，攻击者有时会错误配置 IP 选项，产生不完整或残缺的字段。不管精心设计该封包的人的目的是什么，错误格式化都是反常的，并且对预定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，那么，当 IP 封包包头中的任何 IP 选项被不正确格式化时，NetScreen 设备将封锁这些封包。 NetScreen 设备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 封包，请执行以下任一操作，其中指定的安全区是封包始发的区段 :

WebUI

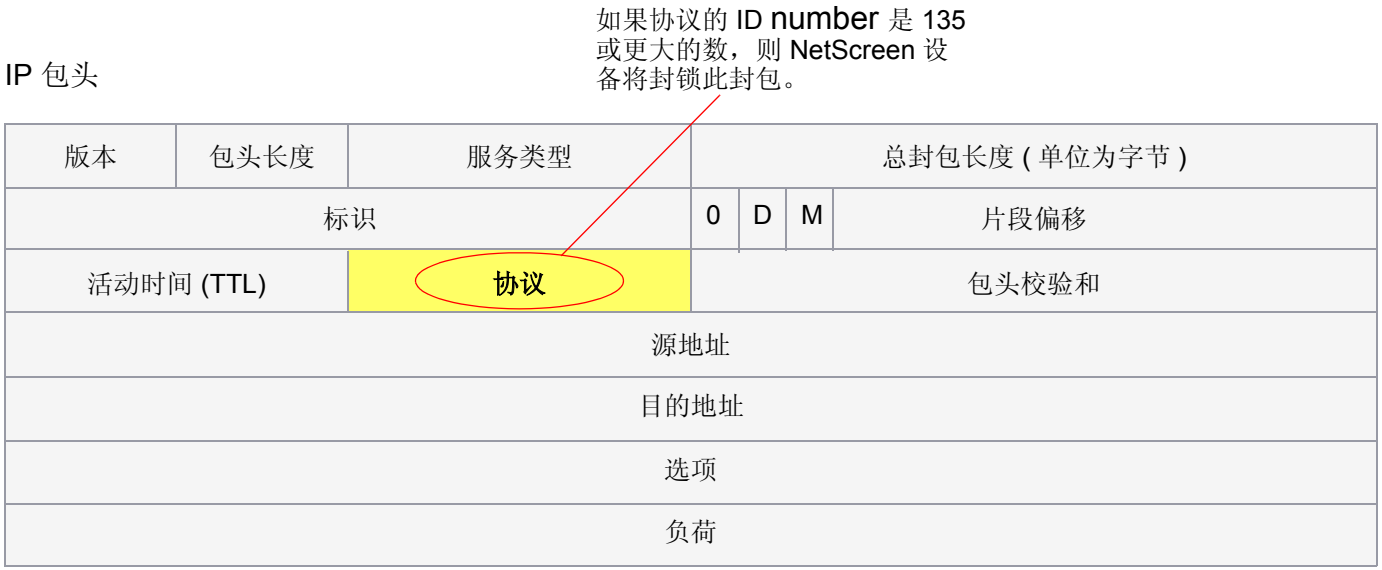
Screening > Screen (Zone: 选择区段名称): 选择 **Bad IP Option Protection**，然后单击 **Apply**。

CLI

```
set zone zone screen ip-bad-option
```

未知协议

目前，这些 ID number 为 135 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，就没有办法事先知道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 number 为 135 或更大的非标准协议，否则谨慎的立场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，那么，当协议字段包含 ID number 为 135 或更大数的协议时， NetScreen 设备将丢弃这些封包。

要丢弃采用未知协议的封包，请执行以下任一操作，其中指定的安全区是封包始发的区段 :

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 封包碎片

封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)，将封包分成更小的部分 (片段)。攻击者可能会利用 IP 栈实现方案的封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封包时，造成的结果小到无法正确处理封包，大到使整个系统崩溃。

如果允许 NetScreen 设备拒绝安全区上的 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 封包碎片。

要丢弃 IP 封包碎片，请执行以下任一操作，其中指定的安全区是封包碎片始发的区段 :

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 封包中，封装了 “传输控制协议” (TCP) SYN 片段。由于这种封包的用途是发起连接和在响应时调用 SYN/ACK 片段，因此 SYN 片段通常不包含任何数据。因为 IP 封包很小，没有必要将其分为片段。分为片段的 SYN 封包是不正常的，要引起怀疑。为了小心起见，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 包头表明封包已分为碎片，并且在 TCP 包头中设置了 SYN 标志时， NetScreen 设备将会检测到这些封包。 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 封包，请执行以下任一操作，其中指定的安全区是封包始发的区段 :

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 “更多片段” 标志 …
或者在 “片段偏移” 字段中有非零值 …
IP 包头
TCP 包头
版本
包头长度
服务类型
总封包长度 (单位为字节)
标识
0
D
M
片段偏移
活动时间 (TTL)
协议
包头校验和
源地址
目的地址
选项 (如果有)
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 …
… 然后 NetScreen 设备丢弃封包。

索引

I

J

L

M

N

P

S

T

U

W

X

Y

Z