NetScreen Concepts & Examples
ScreenOS Reference Guide

Volume 4: Attack Detection
and Defense Mechanisms

ScreenOS 5.0.0
P/N 093-0927-000
Rev. B
Copyright Notice

Copyright © 2003 NetScreen Technologies, Inc. All rights reserved.

NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of NetScreen Technologies, Inc. NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC, and NetScreen ScreenOS 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.
# Contents

**Preface** ................................................................. V  
Conventions .......................................................... vi  
  CLI Conventions .................................................. vi  
WebUI Conventions ................................................ vii  
Illustration Conventions .................................. ix  
Naming Conventions and Character Types .......... x  
NetScreen Documentation .................................. xi  

**Chapter 1  Protecting a Network** ................................. 1  
  Stages of an Attack .............................................. 2  
  Detection and Defense Mechanisms ....................... 3  
  Exploit Monitoring ............................................. 5  
  Example: Monitoring Attacks  from the Untrust Zone .... 6  

**Chapter 2  Reconnaissance Deterrence** ...................... 7  
  IP Address Sweep ............................................... 8  
  Port Scanning ................................................... 10  
  Network Reconnaissance Using IP Options .......... 12  
  Operating System Probes ..................................... 16  
    SYN and FIN Flags Set .................................... 16  
    FIN Flag without ACK Flag ............................. 18  
    TCP Header without Flags Set ......................... 20  
  Evasion Techniques ........................................... 22  
  FIN Scan ....................................................... 22  

**Chapter 3  Denial-of-Service Attack Defenses** ............ 35  
  Firewall DoS Attacks .......................................... 36  
  Session Table Flood ........................................... 36  
    Source- and Destination-Based Session Limits ........ 36  
    Example: Source-Based Session Limiting .......... 39  
    Example: Destination-Based Session Limiting ....... 40  
    Aggressive Aging ............................................ 40  
    Example: Aggressively Aging Out Sessions .......... 42  
  SYN-ACK-ACK Proxy Flood .................................. 43  
  Network DoS Attacks .......................................... 45  
    SYN Flood .................................................... 45  
    Example: SYN Flood Protection ......................... 52  
    ICMP Flood .................................................. 59  
    UDP Flood ................................................... 61  
    Land Attack .................................................. 63  
  OS-Specific DoS Attacks .................................... 65  
    Ping of Death ............................................... 65  
    Teardrop Attack ............................................. 67  
    WinNuke ....................................................... 69  

IP Spoofing .................................................................. 22  
  Example: L3 IP Spoof Protection ......................... 25  
  Example: L2 IP Spoof Protection ......................... 29  
IP Source Route Options .................................... 31
Chapter 4  Content Monitoring and Filtering .......... 71
  Fragment Reassembly ...................................... 72
  Malicious URL Protection ................................... 72
  Application Layer Gateway .................................. 73
    Example: Blocking Malicious URLs in Packet Fragments ................... 74
  Antivirus Scanning ........................................ 76
  Internal AV Scanning ...................................... 77
    Enabling Internal AV Scanning ............................... 81
    Updating the Pattern File Automatically or Semi-Automatically ........... 82
    Example: Automatic Pattern Update .......................... 83
    Example: Semi-Automatic Pattern Update ....................... 83
    Configuring Content Processing ............................ 84
    Example: Internal AV Scanning for SMTP ...................... 84
    Example: Internal AV Scanning for SMTP and HTTP ............... 85
    Configuring Decompression and Maximum Content Size .................. 85
    Example: Dropping Large Files .............................. 86
    Applying Internal AV Scanning ............................. 87
    Example: Internal AV Scanning (POP3) ....................... 87
  External AV Scanning ...................................... 90
    Defining AV Objects ....................................... 93
    Example: Defining Three AV Objects ........................ 99
    Applying External AV Scanning ............................. 102
    Example: Antivirus with One AV Object ....................... 103
    Example: Antivirus with Two AV Objects ..................... 106
  URL Filtering ............................................. 113
    Example: URL Filtering Configuration ....................... 119

Chapter 5  Deep Inspection ................................. 123
  Deep Inspection Overview ................................ 124
  Attack Object Database Server ............................ 128
    Example: Immediate Update ................................ 129
    Example: Automatic Updates ............................... 130
    Example: Automatic Notification and Immediate Update ............... 132
    Example: Manual Update .................................. 134
  Attack Objects and Groups ................................ 136
    Stateful Signatures ....................................... 138
    TCP Stream Signatures .................................... 139
    Protocol Anomalies ....................................... 139
    Attack Object Groups .................................... 140
      Changing Severity Levels ................................. 140
  Attack Actions ............................................ 142
    Example: Attack Actions – Close Server, Close, Close Client .......... 143
  Mapping Custom Services to Applications .................... 152
    Example: Mapping an Application to a Custom Service ............... 153
  Customized Attack Objects and Groups ..................... 156
    User-Defined Stateful Signature Attack Objects .................. 156
      Contexts ................................................ 156
      Signatures ............................................. 157
    Example: User-Defined Stateful Signature Attack Objects .......... 160
    TCP Stream Signature Attack Objects ........................ 164
      Example: User-Defined Stream Signature Attack Object .............. 164
Contents

Granular Blocking of HTTP Components .............. 167
   ActiveX Controls ............................................. 167
   Java Applets ................................................ 168
   EXE Files ..................................................... 168
   ZIP Files ..................................................... 168
      Example: Blocking Java Applets
      and .exe Files .............................................. 169

Chapter 6  Suspicious Packet Attributes .............. 171

ICMP Fragments ............................................... 172
   Large ICMP Packets ....................................... 174
   Bad IP Options .............................................. 176
   Unknown Protocols ....................................... 178
   IP Packet Fragments ..................................... 180
   SYN Fragments ............................................. 182

Index ................................................................. IX--I
Volume 4, “Attack Detection and Defense Mechanisms” describes the network security options available in ScreenOS. Many of these are SCREEN options that you can enable at the security zone level. Screen options apply to traffic reaching the NetScreen device through any interface bound to a zone for which you have enabled such options. SCREEN options offer protection against IP address and port scans, denial-of-service (DoS) attacks, and other kinds of malicious activity. You can apply other network security options, such as URL filtering, antivirus checking, and intrusion detection and prevention (IDP), at the policy level. These options only apply to traffic under the jurisdiction of the policies in which they are enabled.

**Note:** The subject of policies is only presented in this volume peripherally, as it applies to the network security options that you can enable at the policy level. For a complete examination of policies, see “Policies” on page 2-197.

The material within this volume is organized as follows:

- **Chapter 1, “Protecting a Network”** outlines the basic stages of an attack and the firewall options available to combat the attacker at each stage.
- **Chapter 2, “Reconnaissance Deterrence”** describes the options available for blocking IP address sweeps, port scans, and attempts to discover the type of operating system (OS) of a targeted system.
- **Chapter 3, “Denial-of-Service Attack Defenses”** explains firewall, network, and OS-specific DoS attacks and how NetScreen mitigates such attacks.
- **Chapter 4, “Content Monitoring and Filtering”** describes how to protect Hypertext Transfer Protocol (HTTP) and File Transfer Protocol (FTP) users from malicious uniform resource locators (URLs) and how to configure the NetScreen device to work with third party products to provide antivirus scanning and URL filtering.
- **Chapter 5, “Deep Inspection”** describes how to configure the NetScreen device to obtain IDP attack object updates, how to create user-defined attack objects and attack object groups, and how to apply IDP at the policy level.
- **Chapter 6, “Suspicious Packet Attributes”** presents several SCREEN options that protect network resources from potential attacks indicated by unusual IP and ICMP packet attributes.
This document contains several types of conventions, which are introduced in the following sections:

- “CLI Conventions”
- “WebUI Conventions” on page vii
- “Illustration Conventions” on page ix
- “Naming Conventions and Character Types” on page x

**CLI Conventions**

The following conventions are used when presenting the syntax of a command line interface (CLI) command:

- Anything inside square brackets [ ] is optional.
- Anything inside braces { } is required.
- If there is more than one choice, each choice is separated by a pipe ( | ). For example,
  
  ```
  set interface { ethernet1 | ethernet2 | ethernet3 } manage
  ```
  
  means “set the management options for the ethernet1, ethernet2, or ethernet3 interface”.

- Variables appear in *italic*. For example:
  
  ```
  set admin user *name* password
  ```

When a CLI command appears within the context of a sentence, it is in **bold** (except for variables, which are always in *italic*). For example: “Use the **get system** command to display the serial number of a NetScreen device.”

**Note:** When typing a keyword, you only have to type enough letters to identify the word uniquely. For example, typing **set adm u joe j12fmt54** is enough to enter the command **set admin user joe j12fmt54**. Although you can use this shortcut when entering commands, all the commands documented here are presented in their entirety.
WebUI Conventions

Throughout this book, a chevron (>) is used to indicate navigation through the WebUI by clicking menu options and links. For example, the path to the address configuration dialog box is presented as **Objects > Addresses > List > New**. This navigational sequence is shown below.

1. Click **Objects** in the menu column. The Objects menu option expands to reveal a subset of options for Objects.

2. (Applet menu) Hover the mouse over **Addresses**. (DHTML menu) Click **Addresses**. The Addresses option expands to reveal a subset of options for Addresses.

3. Click **List**. The address book table appears.

4. Click the **New** link. The new address configuration dialog box appears.

---

Throughout this book, a chevron (>) is used to indicate navigation through the WebUI by clicking menu options and links. For example, the path to the address configuration dialog box is presented as **Objects > Addresses > List > New**. This navigational sequence is shown below.

1. Click **Objects** in the menu column. The Objects menu option expands to reveal a subset of options for Objects.

2. (Applet menu) Hover the mouse over **Addresses**. (DHTML menu) Click **Addresses**. The Addresses option expands to reveal a subset of options for Addresses.

3. Click **List**. The address book table appears.

4. Click the **New** link. The new address configuration dialog box appears.
To perform a task with the WebUI, you must first navigate to the appropriate dialog box where you can then define objects and set parameters. The set of instructions for each task is divided into two parts: a navigational path and configuration details. For example, the following set of instructions includes the path to the address configuration dialog box and the settings for you to configure:

**Objects > Addresses > List > New:** Enter the following, and then click **OK**:

- **Address Name:** addr_1
- **IP Address/Domain Name:**
  - **IP/Netmask:** (select), 10.2.2.5/32
- **Zone:** Untrust

**Note:** Because there are no instructions for the Comment field, leave it as it is.

![Address Configuration Dialog Box](image.png)
Illustration Conventions

The following graphics make up the basic set of images used in illustrations throughout this book:

- **Generic NetScreen Device**
- **Virtual Routing Domain**
- **Security Zone**
- **Security Zone Interfaces**
  - White = Protected Zone Interface (example: Trust Zone)
  - Black = Outside Zone Interface (example: Untrust Zone)
- **Tunnel Interface**
- **VPN Tunnel**
- **Router Icon**
- **Switch Icon**
- **Local Area Network (LAN) with a Single Subnet**
  (example: 10.1.1.0/24)
- **Internet**
- **Dynamic IP (DIP) Pool**
- **Desktop Computer**
- **Laptop Computer**
- **Generic Network Device**
  (examples: NAT server, Access Concentrator)
- **Server**
ScreenOS employs the following conventions regarding the names of objects—such as addresses, admin users, auth servers, IKE gateways, virtual systems, VPN tunnels, and zones—defined in ScreenOS configurations.

- If a name string includes one or more spaces, the entire string must be enclosed within double quotes (" "); for example, `set address trust "local LAN" 10.1.1.0/24`.
- NetScreen trims any spaces leading or trailing text within a set of double quotes; for example, `" local LAN "` becomes `"local LAN"`.
- NetScreen treats multiple consecutive spaces as a single space.
- Name strings are case sensitive, although many CLI key words are case insensitive. For example, `"local LAN"` is different from `"local lan"`.

ScreenOS supports the following character types:

- Single-byte character sets (SBCS) and multiple-byte character sets (MBCS). Examples of SBCS are ASCII, European, and Hebrew. Examples of MBCS—also referred to as double-byte character sets (DBCS)—are Chinese, Korean, and Japanese.

> **Note:** A console connection only supports SBCS. The WebUI supports both SBCS and MBCS, depending on the character sets that your Web browser supports.

- ASCII characters from 32 (0x20 in hexadecimals) to 255 (0xff), except double quotes (" "), which have special significance as an indicator of the beginning or end of a name string that includes spaces.
NETSCREEN DOCUMENTATION

To obtain technical documentation for any NetScreen product, visit www.netscreen.com/resources/manuals/.

To obtain the latest software version, visit www.netscreen.com/services/download_soft. Select a category of software product from the dropdown list, then follow the displayed instructions. (You must be a registered user to download NetScreen software.)

If you find any errors or omissions in the following content, please contact us at the e-mail address below:

technical@netscreen.com
Protecting a Network

There can be many reasons for invading a protected network. The following list contains some common objectives:

- Gathering the following kinds of information about the protected network:
  - The topology of the network
  - The IP addresses of active hosts
  - The numbers of active ports on active hosts
  - The operating systems of active hosts
- Overwhelming a host on a protected network with bogus traffic to induce a Denial-of-Service (DoS)
- Overwhelming the protected network with bogus traffic to induce a network-wide DoS
- Overwhelming a firewall with bogus traffic, and thereby inducing a DoS for the network behind it
- Causing damage to and stealing data from a host on the protected network
- Gaining access to a host on the protected network to obtain information
- Gaining control of a host to launch other exploits
- Gaining control of a firewall to control access to the network that it protects

ScreenOS provides detective and defensive tools to uncover and thwart the efforts of attackers to achieve the above objectives when they attempt to target a network protected by a NetScreen device.

This chapter first presents an overview of the main stages of an attack and of the various defense mechanisms that you can employ to thwart an attack at each stage:

- “Stages of an Attack” on page 2
- “Detection and Defense Mechanisms” on page 3
- “Exploit Monitoring” on page 5
STAGES OF AN ATTACK

Each attack typically progresses in two major stages. In the first stage, the attacker gathers information, and in the second stage he or she launches the attack.

1. Perform reconnaissance.
   1. Map the network and determine which hosts are active (IP address sweep).
   2. Discern which ports are active (port scans) on the hosts discovered by the IP address sweep.
   3. Determine the operating system (OS), which might expose a weakness in the OS or suggest an attack to which that particular OS is susceptible.

2. Launch the attack.
   1. Conceal the origin of the attack.
   2. Perform the attack.
   3. Remove or hide evidence.
**Detection and Defense Mechanisms**

An exploit can be an information-gathering probe or an attack to compromise, disable, or harm a network or network resource. In some cases, the distinction between the two objectives of an exploit can be unclear. For example, a barrage of TCP SYN segments might be an IP address sweep with the intent of triggering responses from active hosts, or it might be a SYN flood attack with the intent of overwhelming a network so that it can no longer function properly. Furthermore, because an attacker usually precedes an attack by performing reconnaissance on the target, we can consider information-gathering efforts as a precursor to an impending attack—that is, they constitute the first stage of an attack. Thus, the term “exploit” encompasses both reconnaissance and attack activities, and the distinction between the two is not always clear cut.

NetScreen provides various detection methods and defense mechanisms at the zone and policy levels to combat exploits at all stages of their execution:

- SCREEN options at the zone level
- Firewall policies at the inter-, intra-, and super-zone policy levels. (“super-zone” meaning global policies, where no security zones are referenced)

To secure all connection attempts, NetScreen devices use a dynamic packet filtering method known as stateful inspection. Using this method, the NetScreen device notes various components in the IP packet and TCP segment headers—source and destination IP addresses, source and destination port numbers, and packet sequence numbers—and maintains the state of each TCP session and pseudo UDP session traversing the firewall. (The NetScreen device also modifies session states based on changing elements such as dynamic port changes or session termination.) When a responding TCP packet arrives, the NetScreen device compares the information reported in its header with the state of its associated session stored in the inspection table. If they match, the responding packet is allowed to pass the firewall. If the two do not match, the packet is dropped.

NetScreen SCREEN options secure a zone by inspecting, and then allowing or denying, all connection attempts that require crossing an interface bound to that zone. The NetScreen device then applies firewall policies, which can contain content filtering and intrusion detection and prevention (IDP) components, to the traffic that passes the SCREEN filters.

---

1. Although the VLAN and MGT zones are function zones and not security zones, you can set SCREEN options for them. The VLAN zone supports the same set of SCREEN options as a Layer 3 security zone. (Layer 2 security zones support an additional SYN flood option that Layer 3 zones do not: Drop Unknown MAC). Because the following SCREEN options do not apply to the MGT zone, they are not available for that zone: SYN flood protection, SYN-ACK-ACK proxy flood protection, HTTP component blocking, and WinNuke attack protection.
The sets of defense mechanisms that a NetScreen firewall provides for network protection are outlined below:

Network Protection Options

- Reconnaissance
  - IP Address Sweep
  - Port Scanning
  - Operating System Probes
  - Evasion Techniques

- Deterrence

- Content Monitoring and Filtering
  - Fragment Reassembly
  - Antivirus Scanning
  - URL Filtering

- Deep Inspection
  - Stateful Signatures
  - Protocol Anomalies
  - Granular Blocking of HTTP Components

- Denial-of-Service Attack Defenses
  - Firewall DoS Attacks
    - Session Table Flood
    - SYN-ACK-ACK Proxy Flood
  - Network DoS Attacks
    - SYN Flood
    - ICMP Flood
    - UDP Flood
    - Land Attack
  - OS-Specific DoS Attacks
    - Ping of Death
    - Teardrop Attack
    - WinNuke

- Suspicious Packet Attributes
  - ICMP Fragments
  - Large ICMP Packets
  - Bad IP Options
  - Unknown Protocols
  - IP Packet Fragments
  - SYN Fragments
As previously stated, NetScreen network protection settings operate at two levels: security zone and policy. The NetScreen device performs reconnaissance deterrence and DoS attack defenses at the security zone level. In the area of content monitoring and filtering, the NetScreen device applies fragment reassembly at the zone level and antivirus (AV) scanning and uniform resource locator (URL) filtering at the policy level. The NetScreen device applies IDP at the policy level, except for the detection and blocking of HTTP components, which occurs at the zone level. Zone-level firewall settings are SCREEN options. A network protection option set in a policy is a component of that policy.

**Exploit Monitoring**

Although you typically want the NetScreen device to block exploits, there might be times when you want to gather intelligence about them. You might want to learn specifically about a particular exploit—to discover its intention, its sophistication, and possibly (if the attacker is careless or unsophisticated) its source.

If you want to gather information about an exploit, you can let it occur, monitor it, analyze it, perform forensics, and then respond as delineated in a previously prepared incident response plan. You can instruct the NetScreen device to notify you of an exploit, but instead of taking action, the NetScreen device allows the exploit to transpire. You can then study what occurred, and try to understand the attacker’s method, strategy, and objectives. Increased understanding of the threat to the network can then allow you to better fortify your defenses. Although a smart attacker can conceal his or her location and identity, you might be able to gather enough information to discern where the attack originated. You also might be able to estimate the attacker’s capabilities. This kind of information allows you to gauge your response.
Example: Monitoring Attacks from the Untrust Zone

In this example, IP spoofing attacks from the Untrust zone have occurred on a daily basis, usually between 9:00 PM and 12:00 AM. Instead of dropping the packets with the spoofed source IP addresses, you want the NetScreen device to notify you of their arrival but allow them to pass, perhaps directing them to a honeypot that you have connected on the DMZ interface connection. At 8:55 PM, you change the firewall behavior from notification and rejection of packets belonging to a detected attack to notification and acceptance. When the attack occurs, you can then use the honeypot to monitor the attacker’s activity after crossing the firewall. You might also work in cooperation with the upstream ISP to begin tracking the source of the packets back to their source.

**WebUI**

Screening > Screen (Zone: Untrust): Enter the following, and then click **Apply**:

Generate Alarms without Dropping Packet: (select)

IP Address Spoof Protection: (select)

**CLI**

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

---

2. A honeypot is a decoy network server that is designed to lure attackers and then record their actions during an attack.
Reconnaissance Deterrence

Attackers can better plan their attack when they first know the layout of the targeted network (which IP addresses have active hosts), the possible entry points (which port numbers are active on the active hosts), and the constitution of their victims (which operating system the active hosts are running). To gain this information, attackers must perform reconnaissance. NetScreen provides several SCREEN options to deter attackers’ reconnaissance efforts and thereby hinder them from obtaining valuable information about the protected network and network resources.

- “IP Address Sweep” on page 8
- “Port Scanning” on page 10
- “Network Reconnaissance Using IP Options” on page 12
- “Operating System Probes” on page 16
  - “SYN and FIN Flags Set” on page 16
  - “FIN Flag without ACK Flag” on page 18
  - “TCP Header without Flags Set” on page 20
- “Evasion Techniques” on page 22
  - “FIN Scan” on page 22
  - “IP Spoofing” on page 22
  - “IP Source Route Options” on page 31
IP ADDRESS SWEEP

An address sweep occurs when one source IP address sends 10 ICMP packets to different hosts within a defined interval (5000 microseconds is the default). The purpose of this scheme is to send ICMP packets—typically echo requests—to various hosts in the hopes that at least one replies, thus uncovering an address to target. The NetScreen device internally logs the number of ICMP packets to different addresses from one remote source. Using the default settings, if a remote host sends ICMP traffic to 10 addresses in 0.005 seconds (5000 microseconds), NetScreen flags this as an address sweep attack, and rejects the 11th and all further ICMP packets from that host for the remainder of that second.

Source: 2.2.2.5
(Most likely a spoofed address or a zombie agent)

Untrust

ethernet3
1.1.1.1/24

ethernet2
1.2.2.1/24

DMZ

ICMP Packets

<table>
<thead>
<tr>
<th>Src addr</th>
<th>Dst addr</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.2.5</td>
<td>1.2.2.5</td>
</tr>
<tr>
<td>2.2.2.5</td>
<td>1.2.2.160</td>
</tr>
<tr>
<td>2.2.2.5</td>
<td>1.2.2.84</td>
</tr>
<tr>
<td>2.2.2.5</td>
<td>1.2.2.211</td>
</tr>
<tr>
<td>2.2.2.5</td>
<td>1.2.2.10</td>
</tr>
<tr>
<td>2.2.2.5</td>
<td>1.2.2.20</td>
</tr>
<tr>
<td>2.2.2.5</td>
<td>1.2.2.21</td>
</tr>
<tr>
<td>2.2.2.5</td>
<td>1.2.2.240</td>
</tr>
<tr>
<td>2.2.2.5</td>
<td>1.2.2.17</td>
</tr>
<tr>
<td>2.2.2.5</td>
<td>1.2.2.123</td>
</tr>
</tbody>
</table>

Rejected 2.2.2.5 1.2.2.6

Note: A zombie agent is a compromised host under the covert control of an attacker.
Consider enabling this SCREEN option for a security zone only if there is a policy permitting ICMP traffic from that zone. Otherwise, you do not need to enable it. The lack of such a policy denies all ICMP traffic from that zone, precluding an attacker from successfully performing an IP address sweep anyway.

To block IP address sweeps originating in a particular security zone, do either of the following:

**WebUI**

Screening > Screen (Zone: select a zone name): Enter the following, and then click **Apply**:

- IP Address Sweep Protection: (select)
- Threshold: (enter a value to trigger IP address sweep protection)

**CLI**

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

---

1. The value unit is microseconds. The default value is 5000 microseconds.
PORT SCANNING

A port scan occurs when one source IP address sends IP packets containing TCP SYN segments to 10 different ports at the same destination IP address within a defined interval (5000 microseconds is the default). The purpose of this scheme is to scan the available services in the hopes that at least one port will respond, thus identifying a service to target. The NetScreen device internally logs the number of different ports scanned from one remote source. Using the default settings, if a remote host scans 10 ports in 0.005 seconds (5000 microseconds), NetScreen flags this as a port scan attack, and rejects all further packets from the remote source (regardless of the destination IP address) for the remainder of that second.

Source: 2.2.2.5
(Most likely a spoofed address or a zombie agent)

Untrust
ethernet3 1.1.1.1/24
ethernet2 1.2.2.1/24
DMZ
destination: 1.2.2.5

IP Packets with TCP SYN Segments

<table>
<thead>
<tr>
<th>Dst addr:port</th>
<th>Dst addr:port</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.2.5:17820</td>
<td>1.2.2.5:21</td>
</tr>
<tr>
<td>2.2.2.5:42288</td>
<td>1.2.2.5:23</td>
</tr>
<tr>
<td>2.2.2.5:22814</td>
<td>1.2.2.5:53</td>
</tr>
<tr>
<td>2.2.2.5:15401</td>
<td>1.2.2.5:80</td>
</tr>
<tr>
<td>2.2.2.5:13373</td>
<td>1.2.2.5:111</td>
</tr>
<tr>
<td>2.2.2.5:33811</td>
<td>1.2.2.5:113</td>
</tr>
<tr>
<td>2.2.2.5:17821</td>
<td>1.2.2.5:129</td>
</tr>
<tr>
<td>2.2.2.5:19003</td>
<td>1.2.2.5:123</td>
</tr>
<tr>
<td>2.2.2.5:26450</td>
<td>1.2.2.5:137</td>
</tr>
<tr>
<td>2.2.2.5:38087</td>
<td>1.2.2.5:138</td>
</tr>
<tr>
<td>2.2.2.5:24111</td>
<td>1.2.2.5:139</td>
</tr>
</tbody>
</table>

The NetScreen device makes an entry in its session table for the first 10 connection attempts from 2.2.2.5 to 1.2.2.5 and does a route lookup and policy lookup for these. If no policy permits these connection attempts, the NetScreen device tags these as invalid and removes them from the session table in the next “garbage sweep”, which occurs every two seconds. After the tenth attempt, the NetScreen device rejects all further connection attempts from 2.2.2.5.
To block port scans originating in a particular security zone, do either of the following:

**WebUI**

Screening > Screen (Zone: select a zone name): Enter the following, and then click **Apply**:

- Port Scan Protection: (select)
- Threshold: (enter a value to trigger protection against port scans²)

**CLI**

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

---

² The value unit is microseconds. The default value is 5000 microseconds.
**NETWORK RECONNAISSANCE USING IP OPTIONS**

The Internet Protocol standard “RFC 791, Internet Protocol” specifies a set of options to provide special routing controls, diagnostic tools, and security. These options appear after the destination address in an IP packet header.

**IP Header**

<table>
<thead>
<tr>
<th>Version</th>
<th>Header Length</th>
<th>Type of Service</th>
<th>Total Packet Length (in Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Identification</td>
<td>0 D M</td>
<td>Fragment Offset</td>
</tr>
<tr>
<td></td>
<td>Time to Live (TTL)</td>
<td>Protocol</td>
<td>Header Checksum</td>
</tr>
<tr>
<td></td>
<td>Source Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Destination Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Options</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Payload</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

RFC 791 admits that these options are “unnecessary for the most common communications” and, in reality, they rarely appear in IP packet headers. When they do appear, they are frequently being put to some nefarious use. The following is a list of all the IP options and their accompanying attributes:

<table>
<thead>
<tr>
<th>Type</th>
<th>Class</th>
<th>Number</th>
<th>Length</th>
<th>Intended Use</th>
<th>Nefarious Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>End of Options</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Indicates the end of one or more IP options.</td>
<td>None</td>
</tr>
<tr>
<td>No Options</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>Indicates that there are no IP options in the header.</td>
<td>None</td>
</tr>
<tr>
<td>Type</td>
<td>Class</td>
<td>Number</td>
<td>Length</td>
<td>Intended Use</td>
<td>Nefarious Use</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------</td>
<td>--------</td>
<td>--------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Security</td>
<td>0</td>
<td>2</td>
<td>11 bits</td>
<td>Provides a way for hosts to send security, compartmentation, TCC (closed user group) parameters, and Handling Restriction Codes compatible with Department of Defense (DoD) requirements. (This option, as specified in RFC 791 and RFC 1038, is obsolete.)</td>
<td>Unknown, but because it is obsolete, its presence in an IP header is suspect.</td>
</tr>
<tr>
<td>Loose Source Route</td>
<td>0</td>
<td>3</td>
<td>Varies</td>
<td>Specifies a partial route list for a packet to take on its journey from source to destination. The packet must proceed in the order of addresses specified, but it is allowed to pass through other routers in between those specified.</td>
<td>Evasion. The attacker can use the specified routes to hide the true source of a packet or gain access to a protected network. (See “IP Source Route Options” on page 31.)</td>
</tr>
<tr>
<td>Record Route</td>
<td>0</td>
<td>7</td>
<td>Varies</td>
<td>Records the IP addresses of the network devices along the path that the IP packet travels. The destination machine can then extract and process the route information. (Due to the size limitation of 40 bytes for both the option and storage space, this can only record up to 9 IP addresses.)</td>
<td>Reconnaissance. If the destination host is a compromised machine in the attacker’s control, he or she can glean information about the topology and addressing scheme of the network through which the packet passed.</td>
</tr>
<tr>
<td>Stream ID</td>
<td>0</td>
<td>8</td>
<td>4 bits</td>
<td>(Obsolete) Provided a way for the 16-bit SATNET stream identifier to be carried through networks that did not support the stream concept.</td>
<td>Unknown, but because it is obsolete, its presence in an IP header is suspect.</td>
</tr>
</tbody>
</table>
The following SCREEN options detect IP options that an attacker can use for reconnaissance or for some unknown but suspect purpose:

- **Record Route**: The NetScreen device detects packets where the IP option is 7 (Record Route) and records the event in the SCREEN counters list for the ingress interface.
- **Timestamp**: The NetScreen device detects packets where the IP option list includes option 4 (Internet Timestamp) and records the event in the SCREEN counters list for the ingress interface.
- **Security**: The NetScreen device detects packets where the IP option is 2 (security) and records the event in the SCREEN counters list for the ingress interface.
- **Stream ID**: The NetScreen device detects packets where the IP option is 8 (Stream ID) and records the event in the SCREEN counters list for the ingress interface.
To detect packets with the above IP options set, do either of the following, where the specified security zone is the one from which the packets originate:

**WebUI**

Screening > Screen (Zone: select a zone name): Enter the following, and then click **Apply**:

- IP Record Route Option Detection: (select)
- IP Timestamp Option Detection: (select)
- IP Security Option Detection: (select)
- IP Stream Option Detection: (select)

**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
```
Operating System Probes

Before launching an exploit, an attacker might try to probe the targeted host to learn its operating system (OS). With that knowledge, he can better decide which attack to launch and which vulnerabilities to exploit. A NetScreen device can block reconnaissance probes commonly used to gather information about OS types.

SYN and FIN Flags Set

Both the SYN and FIN control flags are not normally set in the same TCP segment header. The SYN flag synchronizes sequence numbers to initiate a TCP connection. The FIN flag indicates the end of data transmission to finish a TCP connection. Their purposes are mutually exclusive. A TCP header with the SYN and FIN flags set is anomalous TCP behavior, causing various responses from the recipient, depending on the OS.

TCP Header

<table>
<thead>
<tr>
<th>16-bit Source Port Number</th>
<th>16-bit Destination Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>32-bit Sequence Number</td>
</tr>
<tr>
<td></td>
<td>32-bit Acknowledgement Number</td>
</tr>
<tr>
<td>4-bit Header Length</td>
<td>Reserved (6 bits)</td>
</tr>
<tr>
<td></td>
<td>SYN</td>
</tr>
<tr>
<td></td>
<td>FIN</td>
</tr>
<tr>
<td></td>
<td>S</td>
</tr>
<tr>
<td></td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>N</td>
</tr>
<tr>
<td></td>
<td>F</td>
</tr>
<tr>
<td></td>
<td>I</td>
</tr>
<tr>
<td></td>
<td>N</td>
</tr>
</tbody>
</table>

16-bit Window Size

An attacker can send a segment with both flags set to see what kind of system reply is returned and thereby determine what kind of OS is on the receiving end. The attacker can then use any known system vulnerabilities for further attacks.
When you enable this SCREEN option, the NetScreen device checks if the SYN and FIN flags are set in TCP headers. If it discovers such a header, it drops the packet.

To block packets with both the SYN and FIN flags set, do either of the following, where the specified security zone is the one from which the packets originate:

**WebUI**

Screening > Screen (Zone: select a zone name): Select **SYN and FIN Bits Set Protection**, and then click **Apply**.

**CLI**

```
set zone zone screen syn-fin
```
FIN Flag without ACK Flag

TCP segments with the FIN control flag set (to signal the conclusion of a session and terminate the connection) normally also have the ACK flag set (to acknowledge the previous packet received). Because a TCP header with the FIN flag set but not the ACK flag is anomalous TCP behavior, there is no uniform response to this. The OS might respond by sending a TCP segment with the RST flag set. Another might completely ignore it. The victim’s response can provide the attacker with a clue as to its OS. (Other purposes for sending a TCP segment with the FIN flag set are to evade detection while performing address and port scans and to evade defenses on guard for a SYN flood by performing a FIN flood instead. For information about FIN scans, see “FIN Scan” on page 22.)

TCP Header

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>16-bit Source Port Number</td>
<td></td>
</tr>
<tr>
<td>16-bit Destination Port Number</td>
<td></td>
</tr>
<tr>
<td>32-bit Sequence Number</td>
<td></td>
</tr>
<tr>
<td>32-bit Acknowledgement Number</td>
<td></td>
</tr>
<tr>
<td>4-bit Header Length</td>
<td>Reserved (6 bits)</td>
</tr>
<tr>
<td>16-bit Window Size</td>
<td></td>
</tr>
<tr>
<td>URG ACK PSH RST SYN F IN</td>
<td>Options (if any)</td>
</tr>
<tr>
<td>16-bit TCP Checksum</td>
<td>16-bit Urgent Pointer</td>
</tr>
</tbody>
</table>

Only the FIN flag is set.

When you enable this SCREEN option, the NetScreen device checks if the FIN flag is set but not the ACK flag in TCP headers. If it discovers a packet with such a header, it drops the packet.

---

3. Vendors have interpreted RFC 793 “Transmission Control Protocol” variously when designing their TCP/IP implementations. When a TCP segment arrives with the FIN flag set but not the ACK flag, some implementations send RST segments. Some drop the packet without sending a RST.
To block packets with the FIN flag set but not the ACK flag, do either of the following, where the specified security zone is the one from which the packets originate:

**WebUI**

Screening > Screen (Zone: select a zone name): Select **FIN Bit with No ACK Bit in Flags Protection**, and then click **Apply**.

**CLI**

```
set zone zone screen fin-no-ack
```
TCP Header without Flags Set

A normal TCP segment header has at least one flag control set. A TCP segment with no control flags set is an anomalous event. Because different operating systems respond differently to such anomalies, the response (or lack of response) from the targeted device can provide a clue as to the type of OS it is running.

TCP Header

<table>
<thead>
<tr>
<th>16-bit Source Port Number</th>
<th>16-bit Destination Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>32-bit Sequence Number</td>
<td></td>
</tr>
<tr>
<td>32-bit Acknowledgement Number</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4-bit Header Length</th>
<th>Reserved (6 bits)</th>
<th>U</th>
<th>R</th>
<th>A</th>
<th>C</th>
<th>K</th>
<th>P</th>
<th>R</th>
<th>S</th>
<th>T</th>
<th>S</th>
<th>Y</th>
<th>N</th>
<th>F</th>
<th>I</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>16-bit Window Size</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16-bit TCP Checksum</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16-bit Urgent Pointer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Options (if any)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data (if any)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

None of the flags are set.

When you enable the NetScreen device to detect TCP segment headers with no flags set, the NetScreen device drops all TCP packets with a missing or malformed flags field.
To block packets with no flags set, do either of the following, where the specified security zone is the one from which the packets originate:

**WebUI**

Screening > Screen (Zone: select a zone name): Select **TCP Packet without Flag Protection**, and then click **Apply**.

**CLI**

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

Whether gathering information or launching an attack, it generally behooves the attacker to avoid detection. Although some IP address and port scans are blatant and easily detectable, more wily attackers use a variety of means to conceal their activity. Such techniques as using FIN scans instead of SYN scans—which attackers know most firewalls and intrusion detection programs detect—indicate an evolution of reconnaissance and exploit techniques to evade detection and successfully accomplish their tasks. (to elicit a RST and thereby discover the IP address of an active host)

FIN Scan

A FIN scan sends TCP segments with the FIN flag set in the attempt to provoke a response (a TCP segment with the RST flag set) and thereby discover an active host or an active port on a host. An attacker might use this approach rather than perform an address sweep with ICMP echo requests or an address scan with SYN segments because he or she knows that many firewalls typically guard against the latter two approaches—but not necessarily against FIN segments. The use of TCP segments with the FIN flag set might evade detection and thereby help the attacker succeed in his or her reconnaissance efforts.

The packet flow behavior for a NetScreen device is to reject TCP segments with non-SYN flags set unless they belong to an established session. NetScreen devices never allow such unsolicited segments to reach a protected host. In addition, you can enable the SCREEN option that specifically blocks TCP segments with the FIN flag set but not the ACK flag, which is anomalous for a TCP segment.

IP Spoofing

One method of attempting to gain access to a restricted area of the network is to insert a bogus source address in the packet header to make the packet appear to come from a trusted source. This technique is called IP spoofing. NetScreen has two IP spoofing detection methods, both of which accomplish the same task: determining that the packet came from a location other than that indicated in its header. The method that a NetScreen device uses depends if it is operating at Layer 3 or Layer 2 in the OSI model.
Layer 3 – When interfaces on the NetScreen device are operating in Route or NAT mode, the mechanism to detect IP spoofing relies on route table entries. If, for example, a packet with source IP address 10.1.1.6 arrives at ethernet3, but the NetScreen device has a route to 10.1.1.0/24 through ethernet1, IP spoof checking notes that this address arrived at an invalid interface—as defined in the route table, a valid packet from 10.1.1.6 can only arrive via ethernet1, not ethernet3. Therefore, the device concludes that the packet has a spoofed source IP address and discards it.

If the source IP address in a packet does not appear in the route table, by default the NetScreen device allows that packet to pass (assuming that a policy exists permitting it). Using the following CLI command—where the specified security zone is the one from which the packets originate—you can instruct the NetScreen device to drop any packet whose source IP address is not in the route table:

```
set zone Trust Zone screen ip-spoofing drop-no-rpf-route
```

1. An IP packet arrives at ethernet3. Its source IP address is 10.1.1.6.
2. Because IP spoof protection is enabled in the Untrust zone, the NetScreen device checks if 10.1.1.6 is a valid source IP address for a packet arriving on ethernet3.
3. When the route table lookup reveals that 10.1.1.6 is not a valid source IP address for a packet arriving on ethernet3, the NetScreen device rejects the packet.
Layer 2 – When interfaces on the NetScreen device are operating in Transparent mode, the IP spoof checking mechanism makes use of the address book entries. For example, you define an address for “serv A” as 1.2.2.5/32 in the V1-DMZ zone. If a packet with source IP address 1.2.2.5 arrives at a V1-Untrust zone interface (ethernet3), IP spoof checking notes that this address arrived at an invalid interface. The address belongs to the V1-DMZ zone, not to the V1-Untrust zone, and is accepted only at ethernet2, which is bound to V1-DMZ. The device concludes that packet has a spoofed source IP address and discards it.

1. An IP packet arrives from the V1-Untrust zone. Its source IP address is 1.2.2.5.

2. Because IP spoof protection is enabled in the V1-Untrust zone, the NetScreen device checks if 1.2.2.5 is a valid source IP address for a packet arriving from the V1-Untrust zone.

3. When the address book lookup reveals that 1.2.2.5 is not a valid source IP address for a packet arriving from the V1-Untrust zone, the NetScreen device rejects the packet.

Be careful when defining addresses for the subnet that straddles multiple security zones. In the above illustration, 1.2.2.0/24 belongs to both the V1-Untrust and V1-DMZ zones. If you configure the NetScreen device as follows, the device will block traffic from the V1-DMZ zone that you want it to permit:

- You define an address for 1.2.2.0/24 in the V1-Untrust zone.
- You have a policy permitting traffic from any address in the V1-DMZ zone to any address in the V1-Untrust zone (**set policy from v1-dmz to v1-untrust any any any permit**).
- You enable IP spoof checking.

Because addresses in the V1-DMZ zone are also in the 1.2.2.0/24 subnet, when traffic from these addresses reaches ethernet2, the IP spoof check refers to the address book and finds 1.2.2.0/24 in the V1-Untrust zone. Consequently, the NetScreen device blocks the traffic.
Example: L3 IP Spoof Protection

In this example, you enable IP spoof protection for the Trust, DMZ, and Untrust zones for a NetScreen device operating at Layer 3. By default, the NetScreen device automatically makes entries in the route table for the subnets specified in interface IP addresses. In addition to these automatic route table entries you manually enter the following three routes:

<table>
<thead>
<tr>
<th>Destination:</th>
<th>Egress Interface:</th>
<th>Next Gateway:</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.2.0/24</td>
<td>ethernet1</td>
<td>10.1.1.250</td>
</tr>
<tr>
<td>1.2.3.0/24</td>
<td>ethernet2</td>
<td>1.2.2.250</td>
</tr>
<tr>
<td>0.0.0.0/0</td>
<td>ethernet3</td>
<td>1.1.1.250</td>
</tr>
</tbody>
</table>

If you enable the IP spoof protection SCREEN option but do not enter the above three routes, the NetScreen device will drop all traffic from the addresses in the “Destination” column and enter alarms in the event log. For example, if a packet with the source address 10.1.2.5 arrives at ethernet1 and there is no route to the 10.1.2.0/24 subnet via ethernet1, the NetScreen device will determine that that packet has arrived at an invalid interface and drop it.

All the security zones in this example are in the trust-vr routing domain.
WebUI

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click Apply:

Zone Name: Trust
Static IP: (select this option when present)
IP Address/Netmask: 10.1.1.1/24

Enter the following, and then click OK:
Interface Mode: NAT

Network > Interfaces > Edit (for ethernet2): Enter the following, and then click OK:

Zone Name: DMZ
Static IP: (select this option when present)
IP Address/Netmask: 1.2.2.1/24

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click OK:

Zone Name: Untrust
Static IP: (select this option when present)
IP Address/Netmask: 1.1.1.1/24

2. Routes

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click OK:

Network Address/Netmask: 10.1.2.0/24
Gateway: (select)
   Interface: ethernet1
Gateway IP Address: 10.1.1.250
Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click OK:

- Network Address/Netmask: 1.2.3.0/24
- Gateway: (select)
  - Interface: ethernet2
  - Gateway IP Address: 1.2.2.250

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click OK:

- Network Address/Netmask: 0.0.0.0/0
- Gateway: (select)
  - Interface: ethernet3
  - Gateway IP Address: 1.1.1.250

3. **IP Spoof Protection**

Screening > Screen ( Zone: Trust): Select IP Address Spoof Protection, and then click Apply.
Screening > Screen ( Zone: DMZ): Select IP Address Spoof Protection, and then click Apply.
Screening > Screen ( Zone: Untrust): Select IP Address Spoof Protection, and then click Apply.
CLI

1. Interfaces
   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. Routes
   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 Spoof Protection
   set zone trust screen ip-spoofing
   set zone dmz screen ip-spoofing
   set zone untrust screen ip-spoofing
   save
Example: L2 IP Spoof Protection

In this example, you protect the V1-DMZ zone from IP spoofing on traffic originating in the V1-Untrust zone. First, you define the following addresses for three Web servers in the V1-DMZ zone:

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

You then enable IP spoofing in the V1-Untrust zone. If an attacker in the V1-Untrust zone attempts to spoof the source IP address using any of the three addresses in the V1-DMZ zone, the NetScreen device checks the address against those in the address books. When it finds that the source IP address on a packet coming from the V1-Untrust zone belongs to a defined address in the V1-DMZ zone, the NetScreen device rejects the packet.

WebUI

1. Addresses

Objects > Addresses > List > New: Enter the following, and then click OK:

- Address Name: servA
- IP Address/Domain Name:
  - IP/Netmask: (select), 1.2.2.10/32
- Zone: V1-DMZ

Objects > Addresses > List > New: Enter the following, and then click OK:

- Address Name: servB
- IP Address/Domain Name:
  - IP/Netmask: (select), 1.2.2.20/32
- Zone: V1-DMZ
Objects > Addresses > List > New: Enter the following, and then click OK:

Address Name: servC
IP Address/Domain Name:
   IP/Netmask: (select), 1.2.2.30/32
Zone: V1-DMZ

2. **IP Spoof Protection**

Screening > Screen (Zone: V1-Trust): Select **IP Address Spoof Protection**, and then click **Apply**.

**CLI**

1. **Addresses**

   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 Spoof Protection**

   set zone v1-untrust screen ip-spoofing
   save
Source routing was designed to allow the user at the source of an IP packet transmission to specify the IP addresses of the routers (also referred to as “hops”) along the path that he or she wants an IP packet to take on its way to its destination. The original intent of the IP source route options was to provide routing control tools to aid diagnostic analysis. If, for example, the transmission of a packet to a particular destination meets with irregular success, you might first use either the record route or timestamp IP option to discover the addresses of routers along the path or paths that the packet takes. You can then use either the loose or strict source route option to direct traffic along a specific path, using the addresses you learned from the results that the record route or timestamp options produced. By changing router addresses to alter the path and sending several packets along different paths, you can note changes that either improve or lessen the success rate. Through analysis and the process of elimination, you might be able to deduce where the trouble lies.

Transmission from A to B is successful 50% of the time using routers 1 and 3.

Using IP source routing, A sends traffic through routers 2 and 3. Transmission from A to B remains successful only 50% of the time.

Using IP source routing, A sends traffic through routers 1 and 4. Transmission from A to B is successful 100% of the time. Therefore, we can conclude that the trouble lies in router #3.
Although the uses of IP source route options were originally benign, attackers have learned to put them to more devious uses. They can use IP source route options to hide their true address and access restricted areas of a network by specifying a different path. For an example showing how an attacker can put both deceptions to use, consider the following scenario.

The NetScreen firewall only allows traffic 2.2.2.0/24 if it comes through ethernet1, an interface bound to the Untrust zone. Routers 3 and 4 enforce access controls but routers 1 and 2 do not. Furthermore, router 2 does not check for IP spoofing. The attacker spoofs the source address, and by using the loose source route option, directs the packet through router 2 to the 2.2.2.0/24 network and from there out router 1. Router 1 forwards it to router 3, which forwards it to the NetScreen device. Because the packet came from the 2.2.2.0/24 subnet and has a source address from that subnet, it seems to be valid. However, one remnant of the earlier chicanery remains: the loose source route option. In this example, you have enabled the “Deny IP Source Route Option” SCREEN option for the Untrust zone. When the packet arrives at ethernet3, the NetScreen device rejects it.
You can enable the NetScreen device to either block any packets with loose or strict source route options set or detect such packets and then record the event in the counters list for the ingress interface. The SCREEN options are as follows:

- **Deny IP Source Route Option:** Enable this option to block all IP traffic that employs the loose or strict source route option. Source route options can allow an attacker to enter a network with a false IP address.

- **Detect IP Loose Source Route Option:** The NetScreen device detects packets where the IP option is 3 (Loose Source Routing) and records the event in the SCREEN counters list for the ingress interface. This option specifies a partial route list for a packet to take on its journey from source to destination. The packet must proceed in the order of addresses specified, but it is allowed to pass through other routers in between those specified.

- **Detect IP Strict Source Route Option:** The NetScreen device detects packets where the IP option is 9 (Strict Source Routing) and records the event in the SCREEN counters list for the ingress interface. This option specifies the complete route list for a packet to take on its journey from source to destination. The last address in the list replaces the address in the destination field.

(For more information about all the IP options, see “Network Reconnaissance Using IP Options” on page 12.)

To block packets with either a loose or strict source route option set, do either of the following, where the specified security zone is the one from which the packets originate:

**WebUI**

Screening > Screen (Zone: select a zone name): Select **IP Source Route Option Filter**, and then click **Apply**.

---

**CLI**

```
set zone zone screen ip-filter-src
```
To detect and record (but not block) packets with a loose or strict source route option set, do either of the following, where the specified security zone is the one from which the packets originate:

**WebUI**

Screening > Screen (Zone: select a zone name): Enter the following, and then click **Apply**:

- IP Loose Source Route Option Detection: (select)
- IP Strict Source Route Option Detection: (select)

**CLI**

```
set zone zone screen ip-loose-src-route
set zone zone screen ip-strict-src-route
```
Denial-of-Service Attack Defenses

The intent of a denial-of-service (DoS) attack is to overwhelm the targeted victim with a tremendous amount of bogus traffic so that the victim becomes so preoccupied processing the bogus traffic that it is unable to process legitimate traffic. The target can be the NetScreen firewall, the network resources to which the firewall controls access, or the specific hardware platform or operating system (OS) of an individual host.

If a DoS attack originates from multiple source addresses, it is known as a distributed denial-of-service (DDoS) attack. Typically, the source address of a DoS attack is spoofed. The source addresses in a DDoS attack might be spoofed or the actual addresses of hosts that the attacker has previously compromised and which he or she is now using as “zombie agents” from which to launch the attack.

The NetScreen device can defend itself and the resources it protects from DoS and DDoS attacks. The following sections describe the various defense options available:

- **“Firewall DoS Attacks” on page 36**
  - “Session Table Flood” on page 36
  - “SYN-ACK-ACK Proxy Flood” on page 43
- **“Network DoS Attacks” on page 45**
  - “SYN Flood” on page 45
  - “ICMP Flood” on page 59
  - “UDP Flood” on page 61
  - “Land Attack” on page 63
- **“OS-Specific DoS Attacks” on page 65**
  - “Ping of Death” on page 65
  - “Teardrop Attack” on page 67
  - “WinNuke” on page 69
FIREWALL DO\textit{S} ATTACKS

If an attacker discovers the presence of the NetScreen firewall, he or she might launch a denial-of-service (DoS) attack against it instead of the network behind it. A successful DoS attack against a firewall amounts to a successful DoS attack against the protected network in that it thwarts attempts of legitimate traffic to traverse the firewall. This section explains two methods that an attacker might use to fill up the session table of a NetScreen device and thereby produce a DoS: “Session Table Flood” on page 36 and “SYN-ACK-ACK Proxy Flood” on page 43.

Session Table Flood

A successful DoS attack overwhelms its victim with such a massive barrage of ersatz traffic that it becomes unable to process legitimate connection requests. DoS attacks can take many forms—SYN flood, SYN-ACK-ACK flood, UDP flood, ICMP flood, and so on—but they all seek the same objective: to fill up their victim’s session table. When the session table is full, that host cannot create any new sessions and begins rejecting new connection requests.

The following SCREEN options help mitigate such attacks:

- “Source- and Destination-Based Session Limits”
- “Aggressive Aging” on page 40

Source- and Destination-Based Session Limits

In addition to limiting the number of concurrent sessions from the same source IP address, you can also limit the number of concurrent sessions to the same destination IP address. One benefit of setting a source-based session limit is that it can stem an attack such as the Nimda virus (which is actually both a virus and a worm) that infects a server and then begins generating massive amounts of traffic from that server. Because all the virus-generated traffic originates from the same IP address, a source-based session limit ensures that the NetScreen firewall can curb such excessive amounts of traffic.
Another benefit of source-based session limiting is that it can mitigate attempts to fill up the NetScreen session table—if all the connection attempts originate from the same source IP address. However, a wily attacker can launch a distributed denial-of-service (DDoS) attack. In a DDoS attack, the malicious traffic can come from hundreds of hosts, known as “zombie agents”, that are surreptitiously under the control of an attacker. In addition to the SYN, UDP, and ICMP flood detection and prevention SCREEN options, setting a destination-based session limit can ensure that the NetScreen device allows only an acceptable number of concurrent connection requests—no matter what the source—to reach any one host.
Determining what constitutes an acceptable number of connection requests requires a period of observation and analysis to establish a baseline for typical traffic flows. You also need to consider the maximum number of concurrent sessions required to fill up the session table of the particular NetScreen platform you are using. To see the maximum number of sessions that your session table supports, use the CLI command `get session`, and then look at the first line in the output, which lists the number of current (allocated) sessions, the maximum number of sessions, and the number of failed session allocations:

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

The default maximum for both source- and destination-based session limits is 128 concurrent sessions, a value that might need adjustment to suit the needs of your network environment and the platform.

Source-Based Session Limiting:
Denial-of-Service Attack

Attacker
Nonexistent host
Src IP: 6.6.6.6

Untrust Zone
DMZ Zone
Web Server

When the number of concurrent sessions from 6.6.6.6 surpasses the maximum limit, the NetScreen device begins blocking further connection attempts from that IP address.

Destination-Based Session Limiting:
Distributed Denial-of-Service Attack

Attacker
Untrust Zone
Zombie Agents
DMZ Zone
Web Server

When the number of concurrent sessions to the Web server surpasses the maximum limit, the NetScreen device begins blocking further connection attempts to that IP address.
Example: Source-Based Session Limiting

In this example, you want to limit the amount of sessions that any one server in the DMZ and Trust zones can initiate. Because the DMZ zone only contains Web servers, none of which should initiate traffic, you set the source-session limit at the lowest possible value: 1 session. On the other hand, the Trust zone contains personal computers, servers, printers, and so on, many of which do initiate traffic. For the Trust zone, you set the source-session limit maximum to 80 concurrent sessions.

**WebUI**

Screening > Screen (Zone: DMZ): Enter the following, and then click **OK**:

- Source IP Based Session Limit: (select)
- Threshold: 1 Sessions

Screening > Screen (Zone: Trust): Enter the following, and then click **OK**:

- Source IP Based Session Limit: (select)
- 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
```
Example: Destination-Based Session Limiting

In this example, you want to limit the amount of traffic to a Web server at 1.2.2.5. The server is in the DMZ zone. After observing the traffic flow from the Untrust zone to this server for a month, you have determined that the average number of concurrent sessions it receives is 2000. Based on this information, you decide to set the new session limit at 4000 concurrent sessions. Although your observations show that traffic spikes sometimes exceed that limit, you opt for firewall security over occasional server inaccessibility.

**WebUI**

Screening > Screen (Zone: Untrust): Enter the following, and then click **OK**:

- Destination IP Based Session Limit: (select)
- Threshold: 4000 Sessions

**CLI**

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

**Aggressive Aging**

By default, an initial TCP session 3-way handshake takes 20 seconds to time out (that is, to expire because of inactivity). After a TCP session has been established, the timeout value changes to 30 minutes. For HTTP and UDP sessions, the session timeouts are 5 minutes and 1 minute respectively. The session timeout counter begin when a session starts and is refreshed every 10 seconds if the session is active. If a session becomes idle for more than 10 seconds, the timeout counter begins to decrement.
NetScreen provides a mechanism to accelerate the timeout process when the number of sessions in the session table surpasses a specified high-watermark threshold. When the number of sessions dips below a specified low-watermark threshold, the timeout process returns to normal. During the period when the aggressive aging out process is in effect, a NetScreen device ages out the oldest sessions first, using the aging out rate that you specify. These aged-out sessions are tagged as invalid and are removed in the next “garbage sweep”, which occurs every 2 seconds.

The aggressive ageout option shortens default session timeouts by the amount you enter\(^1\). The aggressive ageout value can be between 2 and 10 units, where each unit represents a 10-second interval (that is, the aggressive ageout setting can be between 20 and 100 seconds). The default setting is 2 units, or 20 seconds. If you define the aggressive ageout setting at 100 seconds, for example, you shorten the TCP and HTTP session timeouts as follows:

- **TCP**: The session timeout value shortens from 1800 seconds (30 minutes) to 1700 seconds (28:20 minutes) during the time when the aggressive aging process is in effect. During that period, the NetScreen device automatically deletes all TCP sessions whose timeout value has passed 1700 seconds, beginning with the oldest sessions first.

<table>
<thead>
<tr>
<th>Default TCP Session Timeout: 30 Mins (1800 Secs)</th>
<th>Mins 30 25 20 15 10 5 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggressive Ageout = 10 (-100 Secs from Default): 28:20 Mins (1700 Secs)</td>
<td>Secs 1800 1500 1200 900 600 300 0</td>
</tr>
</tbody>
</table>

- **HTTP**: The session timeout value shortens from 300 seconds (5 minutes) to 200 seconds (3:20 minutes) during the time when the aggressive aging process is in effect. During that period, the NetScreen device automatically deletes all HTTP sessions whose timeout value has passed 200 seconds, beginning with the oldest sessions first.

<table>
<thead>
<tr>
<th>Default HTTP Session Timeout: 5 Mins (300 Secs)</th>
<th>Mins 5 4 3 2 1 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggressive Ageout = 10 (-100 Secs from Default): 3:20 Mins (200 Secs)</td>
<td>Secs 300 240 180 120 60 0</td>
</tr>
</tbody>
</table>

- **UDP**: Because the default UDP session timeout is 60 seconds, defining an early ageout setting at 100 seconds causes all UDP sessions to ageout and be marked for deletion in the next garbage sweep.

---

1. When you set and enable the aggressive ageout option, the normal session timeout value displayed in the configuration remains unchanged—1800 seconds for TCP, 300 seconds for HTTP, and 60 seconds for UDP sessions. However, when the aggressive ageout period is in effect, these sessions time out earlier—by the amount you specify for early ageout—instead of counting down all the way to zero.
Example: Aggressively Aging Out Sessions

In this example, you set the aggressive aging out process to commence when traffic exceeds a high-watermark of 80% and cease when it retreats below a low-watermark of 70%. You specify 40 seconds for the aggressive age-out interval. When the session table is more than 80% full (the high-mark threshold), the NetScreen device decreases the timeout for all sessions by 40 seconds and begins aggressively aging out the oldest sessions until the number of sessions in the table is under 70% (the low-mark threshold).

WebUI

Note: You must use the CLI to configure the aggressive age-out settings.

CLI

set flow aging low-watermark 70
set flow aging high-watermark 80
set flow aging early-ageout 4
save
SYN-ACK-ACK Proxy Flood

When an authentication user initiates a Telnet or FTP connection, the user sends a SYN segment to the Telnet or FTP server. The NetScreen device intercepts the SYN segment, creates an entry in its session table, and proxies a SYN-ACK segment to the user. The user then replies with an ACK segment. At that point, the initial 3-way handshake is complete. The NetScreen device sends a login prompt to the user. If the user, with malicious intent, does not log in, but instead continues initiating SYN-ACK-ACK sessions, the NetScreen session table can fill up to the point where the device begins rejecting legitimate connection requests.

1. Client sends a SYN segment to the server.
2. The NetScreen device proxies a SYN/ACK segment.
3. Client responds with an ACK segment.
4. The NetScreen device prompts the client (auth user) to log in.
5. Client ignores the login prompt and keeps repeating steps 1–4 until the NetScreen session table is full.
6. Because the session table is full, the NetScreen device must reject all further connection requests.

To thwart such an attack, you can enable the SYN-ACK-ACK proxy protection SCREEN option. After the number of connections from the same IP address reaches the SYN-ACK-ACK proxy threshold, the NetScreen device rejects further connection requests from that IP address. By default, the threshold is 512 connections from any single IP address. You can change this threshold (to any number between 1 and 2,500,000) to better suit the requirements of your network environment.

To enable protection against a SYN-ACK-ACK proxy flood, do either of the following, where the specified zone is that in which the attack originates:

**WebUI**

Screening > Screen (Zone: select a zone name): Enter the following, and then click **Apply**:

- SYN-ACK-ACK Proxy Protection: (select)
- Threshold: (enter a value to trigger SYN-ACK-ACK proxy flood protection²)

**CLI**

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

---

2. The value unit is connections per source address. The default value is 512 connections from any single address.
A denial-of-service (DoS) attack directed against one or more network resources floods the target with an overwhelming number of SYN, ICMP, or UDP packets, or with an overwhelming number of SYN fragments. Depending on the attacker’s purpose and the extent and success of previous intelligence gathering efforts, the attacker might single out a specific host, such as a router or server; or he or she might aim at random hosts across the targeted network. Either approach has the potential of upsetting service to a single host or to the entire network, depending on how critical the role of the victim is to the rest of the network.

**SYN Flood**

A SYN flood occurs when a host becomes so overwhelmed by SYN segments initiating uncompletable connection requests that it can no longer process legitimate connection requests.

Two hosts establish a TCP connection with a triple exchange of TCP segments known as a three-way handshake: A sends a SYN segment to B; B responds with a SYN/ACK segment; and A responds with an ACK segment. A SYN flood attack inundates a site with SYN segments containing forged (“spoofed”) IP source addresses with nonexistent or unreachable addresses. B responds with SYN/ACK segments to these addresses and then waits for responding ACK segments. Because the SYN/ACK segments are sent to nonexistent or unreachable IP addresses, they never elicit responses and eventually time out.

---

**Diagram Description:**

- **Actual IP Address:** 2.2.2.5
- **Non-existent or Unreachable IP Addresses:**
  - 3.3.3.5
  - 4.4.4.20
  - 5.5.5.10
  - 6.6.6.3

- **Host at 2.2.2.5 sends SYN segments in IP packets with spoofed source addresses.**

- **If a policy permits the inbound traffic, the NetScreen device permits the SYN segments. The victim responds by sending SYN/ACK segments to the spoofed source IP address, and waits for a response until the effort times out.**

- **Protected LAN**

- **The memory buffer in the victim begins filling up.**
By flooding a host with uncompletable TCP connections, the attacker eventually fills the memory buffer of the victim. Once this buffer is full, the host can no longer process new TCP connection requests. The flood might even damage the victim’s operating system. Either way, the attack disables the victim and its normal operations.

**SYN Flood Protection**

NetScreen devices can impose a limit on the number of SYN segments permitted to pass through the firewall per second. You can base the attack threshold on the destination address and port, the destination address only, or the source address only. When the number of SYN segments per second exceeds one of these thresholds, the NetScreen device starts proxying incoming SYN segments, replying with SYN/ACK segments and storing the incomplete connection requests in a connection queue. The incomplete connection requests remain in the queue until the connection is completed or the request times out. In the following illustration, the SYN attack threshold has been passed and the NetScreen device has started proxying SYN segments.
In the next illustration, the proxied connection queue has completely filled up, and the NetScreen device is rejecting new incoming SYN segments. This action shields hosts on the protected network from the bombardment of incomplete three-way handshakes.

The NetScreen device starts receiving new SYN packets when the proxy queue drops below the maximum limit.

**Note:** The procedure of proxying incomplete SYN connections above a set threshold pertains only to traffic permitted by existing policies. Any traffic for which a policy does not exist is automatically dropped.
To enable the SYN flood protection SCREEN option and define its parameters, do either of the following, where the specified zone is that in which a flood might originate:

**WebUI**

Screening > Screen (Zone: select a zone name): Enter the following, and then click **Apply**:

- **SYN Flood Protection**: (select to enable)
- **Threshold**: (enter the number of SYN packets—that is, TCP segments with the SYN flag set—per second required to activate the SYN proxying mechanism)
- **Alarm Threshold**: (enter the number of proxied TCP connection requests required to write an alarm in the event log)
- **Source Threshold**: (enter the number SYN packets per second from a single IP address required to activate SYN proxying)
- **Destination Threshold**: (enter the number SYN packets per second to a single IP address required to activate SYN proxying)
- **Timeout Value**: (enter the length of time in seconds that the NetScreen device holds an incomplete TCP connection attempt in the proxied connection queue)
- **Queue Size**: (enter the number of proxied TCP connection requests held in the proxied connection queue before the NetScreen device starts rejecting new connection requests)

---

3. For more details on each of these parameters, see the descriptions in the following CLI section.
To enable SYN flood protection.

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

You can set the following parameters for proxying uncompleted TCP connection requests:

**Attack Threshold:** The number of SYN segments (that is, TCP segments with the SYN flag set) to the same destination address and port number per second required to activate the SYN proxying mechanism. Although you can set the threshold at any number, you need to know the normal traffic patterns at your site to set an appropriate threshold for it. For example, if it is an e-business site that normally gets 20,000 SYN segments per second, you might want to set the threshold at 30,000/second. If a smaller site normally gets 20 SYN segments/second, you might consider setting the threshold at 40.

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

**Alarm Threshold:** The number of proxied, half-complete TCP connection requests per second after which the NetScreen device enters an alarm in the event log. The value you set for an alarm threshold triggers an alarm when the number of proxied, half-completed connection requests to the same destination address and port number per second exceeds that value. For example, if you set the SYN attack threshold at 2000 SYN segments per second and the alarm at 1000, then a total of 3001 SYN segments to the same destination address and port number per second is required to trigger an alarm entry in the log. More precisely:

1. The firewall passes the first 2000 SYN segments per second that meet policy requirements.
2. The firewall proxies the next 1000 SYN segments in the same second.
3. The 1001st proxied connection request (or 3001st connection request in that second) triggers the alarm.

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

For each SYN segment to the same destination address and port number in excess of the alarm threshold, the attack detection module generates a message. At the end of the second, the logging module compresses all similar messages into a single log entry that indicates how many SYN segments to the same destination address and port number arrived after exceeding the alarm threshold. If the attack persists beyond the first second, the event log enters an alarm every second until the attack stops.
**Source Threshold:** This option allows you to specify the number of SYN segments received per second from a single source IP address—regardless of the destination IP address and port number—before the NetScreen device executes the SYN proxying mechanism.

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

Tracking a SYN flood by source address uses different detection parameters from tracking a SYN flood by destination address and destination port number. When you set a SYN attack threshold and a source threshold, you put both the basic SYN flood protection mechanism and the source-based SYN flood tracking mechanism in effect.

**Destination Threshold:** This option allows you to specify the number of SYN segments received per second for a single destination IP address before the NetScreen device executes the SYN proxying mechanism. If a protected host runs multiple services, you might want to set a threshold based on destination IP address only—regardless of the destination port number.

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

When you set a SYN attack threshold and a destination threshold, you put both the basic SYN flood protection mechanism and the destination-based SYN flood tracking mechanism in effect.

Tracking a SYN flood by destination address uses different detection parameters from tracking a SYN flood by destination address and destination port number. Consider the following case where the NetScreen device has policies permitting FTP requests (port 21) and HTTP requests (port 80) to the same server. If the SYN flood attack threshold is 1000 packets per second (pps) and an attacker sends 999 FTP packets and 999 HTTP packets per second, neither set of packets (where a set is defined as having the same destination address and port number) activates the SYN proxying mechanism. The basic SYN flood attack mechanism tracks destination address and port number, and neither set exceeds the attack threshold of 1000 pps. However, if the destination threshold is 1000 pps, the NetScreen device treats both FTP and HTTP packets with the same destination address as members of a single set. The 1001st packet—FTP or HTTP—to the same destination address triggers the SYN proxying mechanism.
**Timeout:** The maximum length of time before a half-completed connection is dropped from the queue. The default is 20 seconds, and you can set the timeout from 0–50 seconds. You might try decreasing the timeout value to a shorter length until you begin to see any dropped connections during normal traffic conditions. Twenty seconds is a very conservative timeout for a threeway-handshake ACK response.

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

**Queue size:** The number of proxied connection requests held in the proxied connection queue before the NetScreen device starts rejecting new connection requests. The longer the queue size, the longer the NetScreen device needs to scan the queue to match a valid ACK response to a proxied connection request. This can slightly slow the initial connection establishment; however, because the time to begin data transfer is normally far greater than any minor delays in initial connection setup, users would not see a noticeable difference.

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

**Drop Unknown MAC:** When a NetScreen device detects a SYN attack, it proxies all TCP connection requests. However, a NetScreen device in Transparent mode cannot proxy a TCP connection request if the destination MAC address is not in its MAC learning table. By default, a NetScreen device in Transparent mode that has detected a SYN attack passes SYN packets containing unknown MAC addresses. You can use this option to instruct the device to drop SYN packets containing unknown destination MAC addresses instead of letting them pass.

```
set zone zone screen syn-flood drop-unknown-mac
```
Example: SYN Flood Protection

In this example, you protect four Web servers in the DMZ zone from SYN flood attacks originating in the Untrust zone by enabling the SYN flood protection SCREEN option for the Untrust zone.

**Note:** NetScreen recommends that you augment the SYN flood protection that the NetScreen device provides with device-level SYN flood protection on each of the Web servers. In this example, the Web servers are running UNIX, which also provides some SYN flood defenses, such as adjusting the length of the connection request queue and changing the timeout period for incomplete connection requests.

---

To configure the SYN flood protection parameters with appropriate values for your network, you must first establish a baseline of typical traffic flows. For one week, you run a sniffer\(^4\) on ethernet3—the interface bound to the Untrust zone—to monitor the number of new TCP connection requests arriving every second for the four Web servers in the DMZ\(^5\). Your analysis of the data accumulated from one week of monitoring produces the following statistics:

- Average number of new connection requests per server: 250/second
- Average peak number of new connection requests per server: 500/second

---

4. A sniffer is a network analyzing device that captures packets on the network segment to which you attach it. Most sniffers allow you to define filters to collect only the type of traffic that interests you. Later, you can view and evaluate the accumulated information. In this example, you want the sniffer to collect all TCP packets with the SYN flag set arriving at ethernet3 and destined for one of the four Web servers in the DMZ.

5. You might want to continue running the sniffer at regular intervals to see if there are traffic patterns based on the time of day, days of the week, the time of month, or the season of the year. For example, traffic might increase dramatically during the Christmas season. Significant changes probably warrant adjusting the various thresholds.
Based on this information, you set the following SYN flood protection parameters for the Untrust zone:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
<th>Reason for Each Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Threshold</td>
<td>625 packets per second (pps)</td>
<td>This is 25% higher than the average peak number of new connection requests per second per server, which is unusual for this network environment. When the number of SYN packets per second for any one of the four Web servers exceeds this number, the NetScreen device begins proxying new connection requests to that server. (In other words, beginning with the 626th SYN packet to the same destination address and port number in one second, the NetScreen device begins proxying connection requests to that address and port number.)</td>
</tr>
<tr>
<td>Alarm Threshold</td>
<td>250 pps</td>
<td>250 pps is 1/4 of the queue size (1000 proxied, half-completed connection requests). When the NetScreen device proxies 251 new connection requests in one second, it makes an alarm entry in the event log. By setting the alarm threshold somewhat higher than the attack threshold, you can avoid alarm entries for traffic spikes that only slightly exceed the attack threshold.</td>
</tr>
<tr>
<td>Source Threshold</td>
<td>25 pps</td>
<td>When you set a source threshold, the NetScreen device tracks the source IP address of SYN packets, regardless of the destination address and port number. (Note that this source-based tracking is separate from the tracking of SYN packets based on destination address and destination port number that constitutes the basic SYN flood protection mechanism.) In the one week of monitoring activity, you observed that no more than 1/25 of new connection requests for all servers came from any one source within a one-second interval. Therefore, connection requests exceeding this threshold are unusual and provide sufficient cause for the NetScreen device to execute its proxying mechanism. (25 pps is 1/25 of the attack threshold, which is 625 pps.)</td>
</tr>
</tbody>
</table>
Network > Interfaces > Edit (for ethernet2): Enter the following, and then click **OK**:

- **Zone Name:** DMZ
- **Static IP:** (select this option when present)
  - **IP Address/Netmask:** 1.2.2.1/24

---

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
<th>Reason for Each Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Threshold</td>
<td>0 pps</td>
<td>When you set a destination threshold, the NetScreen device runs a separate tracking of only the destination IP address, regardless of the destination port number. Because the four Web servers only receive HTTP traffic (destination port 80)—no traffic to any other destination port number reaches them—setting a separate destination threshold offers no additional advantage.</td>
</tr>
<tr>
<td><strong>Timeout</strong></td>
<td>20 seconds</td>
<td>Because the queue size is relatively short (1000 proxied connection requests), the default value of 20 seconds is a reasonable length of time to hold incomplete connection requests in the queue for this configuration.</td>
</tr>
<tr>
<td><strong>Queue Size</strong></td>
<td>1000 proxied, half-completed connections</td>
<td>1000 proxied, half-completed connection requests is twice the average peak number of new connection requests (500 pps). The NetScreen device proxies up to 1000 requests per second before dropping new requests. Proxying twice the average peak number of new connection requests provides a conservative buffer for legitimate connection requests to get through.</td>
</tr>
</tbody>
</table>

* Half-completed connection requests are incomplete three-way handshakes. A three-way handshake is the initial phase of a TCP connection. It consists of a TCP segment with the SYN flag set, a response with the SYN and ACK flags set, and a response to that with the ACK flag set. For a complete description, see “Glossary” in Volume 1, “Overview”.

**WebUI**

1. **Interfaces**

   Network > Interfaces > Edit (for ethernet2): Enter the following, and then click **OK**:
   - Zone Name: DMZ
   - Static IP: (select this option when present)
   - IP Address/Netmask: 1.2.2.1/24
Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:  
Zone Name: Untrust  
Static IP: (select this option when present)  
IP Address/Netmask: 1.1.1.1/24

2. **Addresses**  
Objects > Addresses > List > New: Enter the following, and then click **OK**:  
Address Name: ws1  
IP Address/Domain Name:  
IP/Netmask: (select), 1.2.2.10/32  
Zone: DMZ  

Objects > Addresses > List > New: Enter the following, and then click **OK**:  
Address Name: ws2  
IP Address/Domain Name:  
IP/Netmask: (select), 1.2.2.20/32  
Zone: DMZ  

Objects > Addresses > List > New: Enter the following, and then click **OK**:  
Address Name: ws3  
IP Address/Domain Name:  
IP/Netmask: (select), 1.2.2.30/32  
Zone: DMZ
Objects > Addresses > List > New: Enter the following, and then click **OK**:
- **Address Name**: ws4
- **IP Address/Domain Name**:
  - IP/Netmask: (select), 1.2.2.40/32
- **Zone**: DMZ

Objects > Addresses > Group > (for Zone: DMZ) New: Enter the following group name, move the following addresses, and then click **OK**:
- **Group Name**: web_servers
  - Select **ws1** and use the << button to move the address from the Available Members column to the Group Members column.
  - Select **ws2** and use the << button to move the address from the Available Members column to the Group Members column.
  - Select **ws3** and use the << button to move the address from the Available Members column to the Group Members column.
  - Select **ws4** and use the << button to move the address from the Available Members column to the Group Members column.

3. **Policy**

Policies > (From: Untrust, To: DMZ) New: Enter the following, and then click **OK**:
- **Source Address**:
  - Address Book Entry: (select), Any
- **Destination Address**:
  - Address Book Entry: (select), web_servers
- **Service**: HTTP
- **Action**: Permit
4. SCREEN

Screening > Screen (Zone: Untrust): Enter the following, and then click **Apply**:

- **SYN Flood Protection**: (select)
  - Threshold: 625
  - Alarm Threshold: 250
  - Source Threshold: 25
  - Destination Threshold: 0
  - Timeout Value: $20^6$
  - Queue Size: 1000

---

6. Because 20 seconds is the default setting, you do not have to set the timeout to 20 seconds unless you have previously set it to another value.
CLI

1. Interfaces
   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. Addresses
   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. Policy
   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
   set zone untrust screen syn-flood queue-size 1000
   set zone untrust screen syn-flood
   save

7. Because 20 seconds is the default setting, you do not have to set the timeout to 20 seconds unless you have previously set it to another value.
ICMP Flood

An ICMP flood occurs when ICMP echo requests overload its victim with so many requests that it expends all its resources responding until it can no longer process valid network traffic. When enabling the ICMP flood protection feature, you can set a threshold that once exceeded invokes the ICMP flood attack protection feature. (The default threshold value is 1000 packets per second.) If the threshold is exceeded, the NetScreen device ignores further ICMP echo requests for the remainder of that second plus the next second as well.

The attacker sends ICMP echo requests with spoofed source addresses.

The NetScreen device passes the echo requests only if a policy permits them.

ICMP echo requests from a variety of spoofed IP addresses

— Maximum Limit of ICMP Echo Requests per Second —

After the ICMP threshold is reached, the NetScreen device rejects further ICMP echo requests from all addresses in the same security zone for the remainder of the current second and the next second as well.

Legitimate ICMP echo request from an address in the same security zone
To enable ICMP flood protection, do either of the following, where the specified zone is that in which a flood might originate:

**WebUI**

Screening > Screen (Zone: select a zone name): Enter the following, and then click **Apply**:
- ICMP Flood Protection: (select)
- Threshold: (enter a value to trigger ICMP flood protection)

**CLI**

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

---

8. The value unit is ICMP packets per second. The default value is 1000 packets per second.
UDP Flood

Similar to the ICMP flood, UDP flooding occurs when an attacker sends IP packets containing UDP datagrams with the purpose of slowing down the victim to the point that it can no longer handle valid connections. After enabling the UDP flood protection feature, you can set a threshold that once exceeded invokes the UDP flood attack protection feature. (The default threshold value is 1000 packets per second.) If the number of UDP datagrams from one or more sources to a single destination exceeds this threshold, the NetScreen device ignores further UDP datagrams to that destination for the remainder of that second plus the next second as well.

The attacker sends UDP datagrams in IP packets with spoofed source addresses.

The datagrams are targeting a DNS server at 1.2.2.5:53.

After the UDP flood threshold is reached, the NetScreen device rejects further UDP datagrams from all addresses in the same security zone for the remainder of the current second and the next second as well.

The NetScreen device passes the UDP datagrams only if a policy permits them.

Legitimate UDP datagram from an address in the same security zone

UDP datagrams inside IP packets from a variety of spoofed IP addresses

— Maximum Limit of UDP Datagrams per Second —

DNS Server
IP: 1.2.2.5
Port: 53 (UDP)
To enable UDP flood protection, do either of the following, where the specified zone is that in which a flood might originate:

**WebUI**

Screening > Screen (Zone: select a zone name): Enter the following, and then click **Apply**:

- UDP Flood Protection: (select)
- Threshold: (enter a value to trigger UDP flood protection\(^9\))

**CLI**

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

---

9. The value unit is UDP packets per second. The default value is 1000 packets per second.
Land Attack

Combining a SYN attack with IP spoofing, a Land attack occurs when an attacker sends spoofed SYN packets containing the IP address of the victim as both the destination and source IP address. The receiving system responds by sending the SYN-ACK packet to itself, creating an empty connection that lasts until the idle timeout value is reached. Flooding a system with such empty connections can overwhelm the system, causing a DoS.

When you enable the SCREEN option to block Land attacks, the NetScreen device combines elements of the SYN flood defense and IP spoofing protection to detect and block any attempts of this nature.
To enable protection against a Land attack, do either of the following, where the specified zone is that in which the attack originates:

**WebUI**

Screening > Screen (Zone: select a zone name): Select **Land Attack Protection**, and then click **Apply**.

**CLI**

```
set zone zone screen land
```
**OS-Specific DoS Attacks**

If an attacker not only identifies the IP address and responsive port numbers of an active host but also its operating system (OS), instead of resorting to brute-force attacks, he or she can launch more elegant attacks that can produce one- or two-packet “kills”. The attacks presented in this section can cripple a system with minimum effort. If your NetScreen device is protecting hosts susceptible to these attacks, you can enable the NetScreen device to detect these attacks and block them before they reach their target.

**Ping of Death**

The maximum allowable IP packet size is 65,535 bytes, including the packet header, which is typically 20 bytes long. An ICMP echo request is an IP packet with a pseudo header, which is 8 bytes long. Therefore, the maximum allowable size of the data area of an ICMP echo request is 65,507 bytes (65,535 - 20 - 8 = 65,507).

However, many ping implementations allow the user to specify a packet size larger than 65,507 bytes. A grossly oversized ICMP packet can trigger a range of adverse system reactions such as denial of service (DoS), crashing, freezing, and rebooting.

When you enable the Ping of Death SCREEN option, the NetScreen device detects and rejects such oversized and irregular packet sizes even when the attacker hides the total packet size by purposefully fragmenting it.

![Table of Ping of Death Packet Sizes](image)

<table>
<thead>
<tr>
<th>Original, Unfragmented Packet</th>
<th>20 Bytes</th>
<th>8 Bytes</th>
<th>65,510 Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Header</td>
<td>ICMP Header</td>
<td>ICMP Data</td>
<td></td>
</tr>
</tbody>
</table>

The size of this packet is 65,538 bytes. It exceeds the size limit prescribed by RFC 791, “Internet Protocol”, which is 65,535 bytes. As the packet is transmitted, it becomes broken into numerous fragments. The reassembly process might cause the receiving system to crash.

---

10. For information about IP specifications, see RFC 791, “Internet Protocol”.
11. For more information about ICMP specifications, see RFC 792, “Internet Control Message Protocol”.

---

Note: For information about Ping of Death, see [http://www.insecure.org/sploits/ping-o-death.html](http://www.insecure.org/sploits/ping-o-death.html).
To enable protection against a Ping of Death attack, do either of the following, where the specified zone is that in which the attack originates:

**WebUI**

Screening > Screen (Zone: select a zone name): Select **Ping of Death Attack Protection**, and then click **Apply**.

**CLI**

```
set zone zone screen ping-death
```
Teardrop Attack

Teardrop attacks exploit the reassembly of fragmented IP packets. In the IP header, one of the fields is the fragment offset field, which indicates the starting position, or “offset”, of the data contained in a fragmented packet relative to the data of the original unfragmented packet.

When the sum of the offset and size of one fragmented packet differ from that of the next fragmented packet, the packets overlap, and the server attempting to reassemble the packet can crash, especially if it is running an older operating system that has this vulnerability.
Fragment Discrepancy

<table>
<thead>
<tr>
<th>Fragmented Packet #1</th>
<th>20 Bytes</th>
<th>800 Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Header</td>
<td></td>
<td>Data</td>
</tr>
<tr>
<td>Offset = 0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Length = 820</td>
<td></td>
<td></td>
</tr>
<tr>
<td>More Fragments = 1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fragmented Packet #2</th>
<th>20 Bytes</th>
<th>600 Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Header</td>
<td></td>
<td>Data</td>
</tr>
<tr>
<td>Offset = 800</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Length = 620</td>
<td></td>
<td></td>
</tr>
<tr>
<td>More Fragments = 0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The second fragment purports to begin 20 bytes earlier (at 800) than the first fragment ends (at 820). The offset of fragment #2 is not in accord with the packet length of fragment #1. This discrepancy can cause some systems to crash during the reassembly attempt.

After you enable the Teardrop Attack SCREEN option, whenever the NetScreen detects this discrepancy in a fragmented packet, it drops it.

To enable protection against a Teardrop attack, do either of the following, where the specified zone is that in which the attack originates:

**WebUI**

Screening > Screen (Zone: select a zone name): Select **Teardrop Attack Protection**, and then click **Apply**.

**CLI**

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

WinNuke is a DoS attack targeting any computer on the Internet running Windows. The attacker sends a TCP segment—usually to NetBIOS port 139 with the urgent (URG) flag set—to a host with an established connection. This introduces a NetBIOS fragment overlap, which causes many machines running Windows to crash. After rebooting the attacked machine, the following message appears, indicating that an attack has occurred:

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 Attack Indicators

TCP Header

<table>
<thead>
<tr>
<th>Source Port Number</th>
<th>Destination Port: 139</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sequence Number</td>
<td></td>
</tr>
<tr>
<td>Acknowledgement Number</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Header Length</th>
<th>Reserved</th>
<th>TCP Checksum</th>
<th>Urgent Pointer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>U R G A C K</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- The destination port is 139.
- The URG flag is set.
If you enable the WinNuke attack defense SCREEN option, the NetScreen device scans any incoming Microsoft NetBIOS session service (port 139) packets. If the NetScreen device observes that the URG flag is set in one of those packets, it unsets the URG flag, clears the URG pointer, forwards the modified packet, and makes an entry in the event log noting that it has blocked an attempted WinNuke attack.

To enable protection against a WinNuke attack, do either of the following, where the specified zone is that in which the attack originates:

**WebUI**

Screening > Screen (Zone: select a zone name): Select **WinNuke Attack Protection**, and then click **Apply**.

**CLI**

```
set zone zone screen winnuke
```
NetScreen provides broad protection and control of network activity through ScreenOS features and the pairing of NetScreen with Websense and Trend Micro products.

NetScreen provides some content monitoring and filtering capabilities within ScreenOS in its malicious URL protection SCREEN option. Furthermore, through the fragment reassembly feature, the NetScreen device can detect URLs even among fragmented TCP segments and fragmented IP packets.

For antivirus (AV) protection, you have a choice on some NetScreen devices to obtain an advanced license key and an AV license key and use an internal AV scanning feature. You can also configure NetScreen devices to work with up to three external Trend Micro AV scanners (after you have first obtained and loaded the two license keys). For URL filtering, you can configure a NetScreen device to work with one or more Websense servers.

This chapter examines how to configure the NetScreen device to perform segment and packet reassembly, monitor HTTP and FTP traffic for malicious URLs, and communicate with other devices to perform AV scanning and URL filtering. The chapter is organized into the following sections:

- “Fragment Reassembly” on page 72
  - “Malicious URL Protection” on page 72
  - “Application Layer Gateway” on page 73
- “Antivirus Scanning” on page 76
  - “Internal AV Scanning” on page 77
  - “External AV Scanning” on page 90
- “URL Filtering” on page 113
**Fragment Reassembly**

Typically, a network forwarding device such as a router or switch does not reassemble fragmented packets that it receives. It is the responsibility of the destination host to reconstruct the fragmented packets when they all arrive. Because the purpose of forwarding devices is the efficient delivery of traffic, queuing fragmented packets, reassembling them, then refragmenting them, and forwarding them is unnecessary and inefficient. However, passing fragmented packets through a firewall is insecure. An attacker can intentionally break up packets to conceal traffic strings that the firewall otherwise would detect and block.

ScreenOS allows you to enable fragment reassembly on a per zone basis. Doing so allows the NetScreen device to expand its ability to detect and block malicious URL strings, and to improve its ability to provide an application layer gateway (ALG) to check the data portions of packets.

**Malicious URL Protection**

In addition to the URL filtering feature explained later in this chapter (see “URL Filtering” on page 113), you can define up to 16 malicious URL string patterns, each of which can be up to 24 characters long, for malicious URL protection at the zone level. With the Malicious URL blocking feature enabled, the NetScreen device examines the data payload of all HTTP and FTP packets. If it locates a URL and detects that the beginning of its string—up to a specified number of characters—matches the pattern you defined, the NetScreen device blocks that packet from passing the firewall.

A resourceful attacker, realizing that the string is known and might be guarded against, can deliberately fragment the IP packets or TCP segments and thereby make the pattern unrecognizable during a packet-by-packet inspection. For example, if the malicious URL string is `120.3.4.5/level/50/exec`, IP fragmentation might break up the string into the following sections:

- First packet: `120`
- Second packet: `3.4.5/level/50`
- Third packet: `/exec`

Individually, the fragmented strings can pass undetected through the NetScreen device, even if you have the string defined as `120.3.4.5/level/50/exec` with a length of 20 characters. The string in the first packet—"120."—matches the first part of the defined pattern, but it is shorter than the required length of 20 matching characters. The strings in the second and third packets do not match the beginning of the defined pattern, and so too pass without impedance.
However, if the packets are reassembled, the fragments combine to form a recognizable string that the NetScreen device can block. Using the Fragment Reassembly feature, the NetScreen device can buffer fragments in a queue, reassemble them into a complete packet, and then inspect that packet for a malicious URL. Depending on the results of this reassembly process and subsequent inspection, the NetScreen device performs one of the following steps:

- If the NetScreen device discovers a malicious URL, it drops the packet and enters the event in the log.
- If the NetScreen device cannot complete the reassembly process, a time limit is imposed to age out and discard fragments.
- If the NetScreen device determines that the URL is not malicious but the reassembled packet is too big to forward, the NetScreen device fragments that packet into multiple packets and forwards them.
- If the NetScreen device determines that the URL is not malicious and does not need to fragment it, it then forwards the packet.

**Application Layer Gateway**

NetScreen provides an application layer gateway (ALG) for a number of protocols, such as DNS, FTP, H.323, and HTTP. Of these, fragment reassembly can be an important component in the enforcement of policies involving FTP and HTTP services. The ability of the NetScreen firewall to screen packets for protocols such as FTP-Get and FTP-Put requires it to examine not only the packet header but also the data in the payload. For example, there might be two policies, one denying FTP-put from the Untrust to DMZ zones, and another permitting FTP-get from the Untrust to the DMZ zones:

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

To distinguish the two types of traffic, the NetScreen firewall examines the payload. If it reads `RETR filename`, the FTP client has sent a request to get (or “retrieve”) the specified file from the FTP server, and the NetScreen device allows the packet to pass. If the NetScreen device finds `STOR filename`, the client has sent a request to put (or “store”) the specified file on the server, and the NetScreen device blocks the packet.

To get around this defense, an attacker can deliberately fragment a single FTP-put packet into two packets that contain the following text in their respective payloads: packet 1: `ST`; packet 2: `OR filename`. When the NetScreen device inspects each packet individually, it does not find the string `STOR filename`, and consequently allows them both to pass.
However, if the packets are reassembled, the fragments combine to form a recognizable string upon which the NetScreen device can act. Using the Fragment Reassembly feature, the NetScreen device buffers the FTP fragments in a queue, reassembles them into a complete packet, and then inspects that packet for the complete FTP request. Depending on the results of this reassembly process and subsequent inspection, the NetScreen device performs one of the following steps:

- If the NetScreen device discovers an FTP-put request, it drops the packet and enters the event in the log.
- If the NetScreen device cannot complete the reassembly process, a time limit is imposed to age out and discard fragments.
- If the NetScreen device discovers an FTP-get request but the reassembled packet is too big to forward, the NetScreen device fragments that packet into multiple packets and forwards them.
- If the NetScreen device discovers an FTP-get request and does not need to fragment it, it then forwards the packet.

**Example: Blocking Malicious URLs in Packet Fragments**

In this example, you define the following three malicious URL strings and enable the malicious URL blocking option:

- **Malicious URL #1**
  - ID: Perl
  - Pattern: scripts/perl.exe
  - Length: 14

- **Malicious URL #2**
  - ID: CMF
  - Pattern: cgi-bin/phf
  - Length: 11

- **Malicious URL #3**
  - ID: DLL
  - Pattern: 210.1.1.5/msadcs.dll
  - Length: 18

The values for “length” indicate the number of characters in the pattern that must be present in a URL—starting from the first character—for a positive match. Note that for #1 and #3, not every character is required.
You then enable fragment reassembly for the detection of the URLs in fragmented HTTP and FTP traffic arriving at an Untrust zone interface.

**WebUI**

Screening > Mal-URL (Zone: Untrust): Enter the following, and then click **OK**:

ID: perl
Pattern: /scripts/perl.exe
Length: 14

Screening > Mal-URL (Zone: Untrust): Enter the following, and then click **OK**:

ID: cmf
Pattern: cgi-bin/phf
Length: 11

Screening > Mal-URL (Zone: Untrust): Enter the following, and then click **OK**:

ID: dll
Pattern: 210.1.1.5/msadcs.dll
Length: 18

Screening > Mal-URL (Zone: Untrust): Select the **IP/TCP Reassembly for ALG** check box, and then click **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
```
ANTIVIRUS SCANNING

A virus is an executable code that infects or attaches itself to other executable code so that it can reproduce itself. Some viruses are malicious, erasing files or locking up systems. Others present a problem merely in the act of infecting other files, as their propagation may overwhelm the infected host or network with excessive amounts of bogus data.

In conjunction with Trend Micro antivirus (AV) technology, NetScreen provides two AV solutions:

- Internal AV scanning
- External AV scanning

With internal AV scanning, the AV scanner is inside the NetScreen device as part of ScreenOS. Using a NetScreen device that supports internal AV simplifies deployment and management. It is a cost-effective choice for remote sites, small offices, retail outlets, and telecommuters. For information on configuring the internal AV scanning feature, see “Internal AV Scanning” on page 77.

With external AV scanning, the AV scanner is a separate device to which the NetScreen device forwards traffic that requires scanning. Using a NetScreen device that supports one or more external AV scanners provides a flexible and scalable approach. You can begin with one AV scanner, but if the protected network grows, you can add more scanners (up to three total) to process increased traffic loads. For information on configuring the external AV scanning feature, see “External AV Scanning” on page 90.
Internal AV Scanning

Some NetScreen devices provide antivirus (AV) scanning for specific application-layer transactions using an internal AV scanner developed by Trend Micro. To use the internal AV scanner to scan network traffic for viruses, you reference the internal AV scanner in your security policy.

You can configure the internal AV scanner to examine network traffic from several protocols including Simple Mail Transfer Protocol (SMTP), Hypertext Transfer Protocol (HTTP), and Post Office Protocol - version 3 (POP3). After verifying that it has received the entire content of the SMTP, HTTP or POP3 packet, the internal AV scanner examines the data for viruses. It does this by referencing a virus pattern file to identify virus signatures. When the internal AV scanner detects a virus, the NetScreen device drops the content and sends a message to the client indicating that the content is infected. If the scanner does not detect a virus, the NetScreen device forwards the content to its intended destination.

For SMTP traffic scanning, the NetScreen device redirects traffic from a local SMTP client to the internal AV scanner before sending it to the local mail server.

SMTP Antivirus Scanning

1. A remote mail server forwards an e-mail message via SMTP to the local mail server.
2. The NetScreen device intercepts the e-mail message and passes the data to the internal AV scanner, which scans it for viruses.
3. After completing the scan, the NetScreen device follows one of two courses:
   - If there is no virus, it forwards the message to the local server.
   - If there is a virus, it sends a message reporting the infection to the remote server.
A. An SMTP client sends an e-mail message to a local mail server.
B. The NetScreen device intercepts the e-mail message and passes the data to the internal AV scanner, which scans it for viruses.
C. After completing the scan, the NetScreen device follows one of two courses:
   - If there is no virus, it forwards the message to the local server.
   - If there is a virus, it sends a message reporting the infection to the client.
For POP3 traffic scanning, the NetScreen device redirects traffic from a local mail server to the internal AV scanner before sending it to the local POP3 client.

A. The POP3 client downloads an e-mail message from the local mail server.
B. The NetScreen device intercepts the e-mail message and passes the data to the internal AV scanner, which scans it for viruses.
C. After completing the scan, the NetScreen device follows one of two courses:
   - If there is no virus, it forwards the message to the client.
   - If there is a virus, it sends a message reporting the infection to the client.
For HTTP traffic scanning, the NetScreen device redirects replies from a Web server responding to the client that made HTTP requests to the internal AV scanner before forwarding the traffic to the client.

**HTTP Antivirus Scanning**

1. A local HTTP client sends an HTTP request to a remote Web server, which the NetScreen device permits.
2. The NetScreen device intercepts the inbound HTTP reply and passes the HTTP data to its internal AV scan engine, which scans it for viruses.
3. After completing the scan, the NetScreen device follows one of two courses:
   - If there is no virus, it forwards the message to the client.
   - If there is a virus, it drops the message, and sends a message reporting the infection to the client.

**Note:** The internal AV scanner examines HTTP downloads; that is, HTTP data in replies from a Web server to HTTP requests from a client. The internal AV scanner does not scan uploads, such as when an HTTP client completes a questionnaire on a Web server or when a client writes a message in an e-mail originating on a Web server.
For HTTP webmail traffic scanning, the NetScreen device redirects replies from a Web server responding to the client that made HTTP web-mail requests to the internal AV scanner before forwarding the traffic to the client.

HTTP Web-Mail Antivirus Scanning

1. A local HTTP client sends an HTTP web-mail request to a remote Web server, which the NetScreen device permits.
2. The NetScreen device intercepts the inbound HTTP reply and passes the HTTP data to its internal AV scan engine, which scans it for viruses.
3. After completing the scan, the NetScreen device follows one of two courses:
   - If there is no virus, it forwards the message to the client.
   - If there is a virus, it drops the message, and sends a message reporting the infection to the client.
Enabling Internal AV Scanning

Internal AV scanning requires that you load a database of AV patterns onto the NetScreen device and update the pattern file periodically. To do so, you must register the device and purchase a subscription for the AV signature service. The subscription allows you to load the current version of the database and update it as newer versions become available for the life of the subscription. The procedure for initiating the AV signature service varies:

- If you purchased a NetScreen device with AV functionality, you can load an AV pattern file for a short period of time after the initial purchase. You must, however, register the device and purchase a subscription for AV signatures to continue receiving pattern updates.

- If you are upgrading a current NetScreen device to use internal AV scanning, you must register the device and purchase a subscription for AV signatures before you can begin loading the AV pattern file. After completing the registration process, you must wait for a period of up to 4 hours before initiating the AV pattern file download.

**Note:** For more information about the AV signature service, see “Registration and Activation of Signature Services” on page 2-538.

The process of updating the AV pattern file is as follows:

1. From the NetScreen device, specify the URL address of the external pattern file server to retrieve a server initialization file called server.ini.

2. If pattern file version is out of date, the update server returns the server.ini file.

**URL:** http://5gt-t.activeupdate.trendmicro.com/activeupdate/server.ini
2. After the NetScreen device downloads the server initialization file, it parses it to obtain information about the updated pattern file including the pattern file version and size, and the location of the external pattern file server.

**Note:** ScreenOS contains a CA certificate for authenticating communication with the pattern file server.

3. If the current pattern file is out of date, the NetScreen device retrieves the updated pattern file from the external pattern file server automatically.

4. After the NetScreen device downloads the pattern file, it verifies that the AV subscription is still valid. If the AV signature service subscription is valid, the pattern file is updated. If the subscription is expired, the pattern file update fails and an error message appears indicating that the AV subscription is expired.

**Note:** The total estimated time to complete a pattern update is approximately 3 minutes. This time may vary depending upon the pattern file size and existing network traffic. After completing the pattern file update, the NetScreen device re-initializes the internal AV scanner in order to use the new pattern.

**Updating the Pattern File Automatically or Semi-Automatically**

Updates to the pattern file are added as new viruses propagate. You can configure the NetScreen device to update the pattern file either automatically on a regular basis or semi-automatically.

**Note:** Once your subscription expires, the update server no longer permits you to update the AV pattern file.
Example: Automatic Pattern Update

In this example, you configure the NetScreen device to update the pattern file automatically every 15 minutes. (The default AV pattern update interval is 60 minutes.) The pattern update server is located at the following URL address: http://5gt-t.activeupdate.trendmicro.com/activeupdate/server.ini

**WebUI**

Screening > Antivirus > Scan Manager: Enter the following, and then click **OK**:

Pattern Update Server:
http://5gt-t.activeupdate.trendmicro.com/activeupdate/server.ini
Auto Pattern Update: (select), 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

Example: Semi-Automatic Pattern Update

In this example, you configure the NetScreen device to update the pattern file semi-automatically. The pattern update server is located at the following URL address:
http://5gt-t.activeupdate.trendmicro.com/activeupdate/server.ini

**WebUI**

Screening > Antivirus > Scan Manager: Enter the following, and then click **OK**:

Pattern Update Server:
http://5gt-t.activeupdate.trendmicro.com/activeupdate/server.ini
Update Now: (select)
**CLI**

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

**Configuring Content Processing**

The internal AV scanner examines SMTP, HTTP (webmail-only) and POP3 traffic by default.

*Note: The internal AV scanner examines specific HTTP webmail patterns only. The patterns for Yahoo!, Hotmail, and AOL mail services are pre-defined.*

You can change the default behavior so that the internal AV scanner examines specific network traffic only.

**Example: Internal AV Scanning for SMTP**

In this example, you configure the internal AV scanner to examine SMTP traffic only.

**WebUI**

Screening > Antivirus > Scan Manager: Enter the following, and then click OK:

- Protocols to be scanned:
  - SMTP: (select)

**CLI**

set av scan-mgr content smtp timeout 20
save
Example: Internal AV Scanning for SMTP and HTTP

In this example, you configure the internal AV scanner to examine all SMTP and HTTP traffic.

**WebUI**

Screening > Antivirus > Scan Manager: Enter the following, and then click **OK**:

- Protocols to be scanned:
  - SMTP: (select)
  - HTTP: (select); ALL HTTP: (select)

**CLI**

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

Configuring Decompression and Maximum Content Size

When it receives content, the internal AV scanner decompresses any compressed files. It decompresses up to 2 layers of compressed files by default. For example, if the scanner receives a file with an attachment, and the attachment is a compressed file layered within another compressed file, the scanner may decompress both layers in order to detect any viruses. You can configure the internal AV scanner to decompress up to 20 compressed files layered within another.

The internal AV scanner examines a maximum of 8 messages and 16 MB of “decompressed” file content at any specific time. If the total number of messages or size of the content received concurrently exceeds these limits, the scanner passes the content without checking for viruses by default. For example, the scanner can receive and examine four 4-MB messages concurrently. If the scanner receives nine 2-MB messages concurrently, it passes the content without scanning it. You can change this default behavior so that the internal AV scanner drops traffic instead of passing it.
Example: Dropping Large Files

In this example, you configure the internal AV scanner to decompress up to 10 files layered within another. You also configure the scanner to drop content if either the total number of messages received concurrently exceeds 4 messages or the total “decompressed” size of the content exceeds 12 MB.

WebUI

Screening > Antivirus > Scan Manager: Enter the following, and then click OK:

File decompression: 10 layers (1~4)
Drop: (select) file if it exceeds 3000 KB (4000~20000)
Drop: (select) 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
Applying Internal AV Scanning

To apply internal AV scanning to SMTP, HTTP, or POP3 network traffic, you must reference the pre-defined internal AV scanner in policies.

Example: Internal AV Scanning (POP3)

In this example, you reference the internal AV scanner in a firewall policy permitting POP3 traffic from addresses in the Trust zone to the mail server (“mailsrv1”, 1.2.2.5) in the DMZ zone. All zones are in the trust-vr routing domain.

WebUI

1. Interfaces

   Network > Interfaces > Edit (for ethernet1): Enter the following, and then click Apply:
   - Zone Name: Trust
   - Static IP: (select this option when present)
   - IP Address/Netmask: 10.1.1.1/24

   Enter the following, and then click OK:
   - Interface Mode: NAT

   Network > Interfaces > Edit (for ethernet2): Enter the following, and then click OK:
   - Zone Name: DMZ
   - Static IP: (select this option when present)
   - IP Address/Netmask: 1.2.2.1/24

   Network > Interfaces > Edit (for ethernet3): Enter the following, and then click OK:
   - Zone Name: Untrust
   - Static IP: (select this option when present)
   - IP Address/Netmask: 1.1.1.1/24
2. **Address**
   Objects > Addresses > List > New: Enter the following, and then click **OK**:
   - Address Name: mailsrv1
   - IP Address/Domain Name:
     - IP/Netmask: (select), 1.2.2.5/32
   - Zone: DMZ

3. **POP3 Internal AV Scanning**
   Screening > Antivirus > Scan Manager: Enter the following, and then click **OK**:
   - Protocols to be scanned:
     - POP3: (select)

4. **Route**
   Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:
   - Network Address/Netmask: 0.0.0.0/0
   - Gateway: (select)
     - Interface: ethernet3
   - Gateway IP Address: 1.1.1.250

5. **Policy**
   Policies > (From: Trust, To: DMZ) New: Enter the following, and then click **OK**:
   - Source Address:
     - Address Book Entry: (select), Any
   - Destination Address:
     - Address Book Entry: (select), mailsrv1
   - Service: POP3
Action: Permit

> Advanced: Move the following AV objects, and then click Return to set the advanced options and return to the basic configuration page:

Select scan-mgr and use the << button to move the AV object from the Available AV Object Names column to the Attached AV Object Names column.

**CLI**

1. **Interfaces**
   - 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. **Address**
   - set address dmz mailsvr1 1.2.2.5/32

3. **POP3 Internal AV Scanning**
   - set av-scan-mgr content pop3 timeout 20

4. **Route**
   - set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250

5. **Policy**
   - set policy from trust to dmz any mailsvr1 pop3 permit av scan-mgr
   - save
External AV Scanning

Most NetScreen devices can interoperate with an external antivirus (AV) scanner produced by Trend Micro called InterScan VirusWall Edition 3.6. You can configure the NetScreen device to forward Simple Mail Transfer Protocol (SMTP) and Hypertext Transfer Protocol (HTTP) traffic to the VirusWall AV scanner. The protocol for communication between the NetScreen device and the VirusWall scanner is called Content Scanning Protocol (CSP), version 1.5.

**Note:** NetScreen does not support AV for virtual systems. On systems that support both virtual systems and AV, AV is only available at the root level.

When the VirusWall scanner receives the entire content of an SMTP or HTTP packet, it examines the data for viruses. It has a database of virus patterns that it uses to identify virus signatures. If it finds anything amiss, the VirusWall quarantines the infected data for further study and returns the SMTP or HTTP file—without the infected data—to the NetScreen device. The NetScreen device then forwards the file to the intended recipient.

Whenever the VirusWall detects a virus, both the NetScreen device and the VirusWall make an event log entry identifying the detected virus.

**Note:** To learn how to configure the Trend Micro InterScan VirusWall to communicate with the NetScreen device, as well as how to configure other settings, refer to the Trend Micro product documentation.
For SMTP traffic scanning, the NetScreen device can redirect traffic from a remote mail server or from a local SMTP client to the VirusWall antivirus scanner before sending it to the local mail server.

**SMTP Antivirus Scanning**

1. A remote mail server forwards an e-mail message to the local mail server.
2. The NetScreen device intercepts the e-mail message and passes the data to the antivirus scanner, which scans it for viruses.
3. After completing the scan (and possibly modifying or deleting content if it finds a virus), the scanner returns the data to the NetScreen device, which then forwards it to the mail server.

A. The SMTP client sends an e-mail message to the local mail server.
B. The NetScreen device intercepts the e-mail message and passes the data to the antivirus scanner, which scans it for viruses.
C. After completing the scan (and possibly modifying or deleting content if it finds a virus), the scanner returns the data to the NetScreen device, which then forwards it to the mail server.
For HTTP traffic scanning, the NetScreen device can redirect replies from a Web server responding to the client that made HTTP requests to an antivirus scanner before forwarding the traffic to the client.

HTTP Antivirus Scanning

1. A local HTTP client sends an HTTP request to a remote Web server, which the NetScreen device permits.
2. The NetScreen device intercepts the inbound HTTP reply and passes the HTTP data to the antivirus server, which scans it for viruses.
3. After completing the scan (and possibly modifying or deleting content if it finds a virus), the antivirus server returns the data to the NetScreen device, which then forwards it to the client.

**Note:** The antivirus scanner scans HTTP downloads; that is, HTTP data in replies from a Web server to HTTP requests from a client. The antivirus scanner does not scan uploads, such as when an HTTP client completes a questionnaire on a Web server or when a client writes a message in an e-mail originating on a Web server.
Defining AV Objects

An antivirus object (AV object) is the term NetScreen uses to refer to an external antivirus scanner. You can define up to three AV objects to increase bandwidth capacity. When you create an AV object, you must define the following three components:

- AV object name
- IP address or domain name (resolved to an IP address by DNS) of the antivirus scanner
- Content type: HTTP, or SMTP, or both

When you define only one or two of the above components, the state of the AV object is considered incomplete. When you define all three, it is considered complete. For example:

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

The AV object is **incomplete** because it has a name ("scanner1") and an address (1.2.2.25) but not a content type.

```
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
```

The AV object is **complete** because it has a name, an address, and a content type (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
```
There are a few optional parameters that you can set for an AV object:

- **Port number:** By default, the port number that Content Scanning Protocol (CSP) uses for communication between a NetScreen device and a Trend Micro InterScan VirusWall is 3300. You can change this number on a per-AV object basis.
  
  ```
  set av name_str server-name { ip_addr | domain_name } port number
  unset av name_str server-name { ip_addr | domain_name } port
  ```

  The above `unset av` command returns the port number to the default (3300).

- **Timeout value (in seconds):** By default, a CSP connection times out after 180 seconds of inactivity. You can change this value on a per-AV object basis. The range is 1 to 1800 seconds.
  
  ```
  set av name_str content { http | smtp } timeout number
  unset av name_str content { http | smtp } timeout number
  ```

  The above `unset av` command returns the timeout value to the default (180 seconds).

In addition to the above options that you can set per AV object, you can also set the following parameters, which apply to the antivirus feature at large:

- **Maximum simultaneous TCP connections:** This specifies the maximum number of simultaneous TCP connections between the NetScreen device and all AV objects as a group, not between the NetScreen device and each individual AV object. The default value varies from platform to platform. (Refer to the NetScreen marketing literature for information relevant to your platform.)

  ```
  WebUI
  ```

  Screening > Antivirus: Enter a number in the Maximum Number of TCP Connections field, and then click **Apply**.

  ```
  CLI
  ```

  ```
  set av all max-connections number
  unset av all max-connections
  ```
- **CSP resources per source:** A malicious user might simultaneously send a large number of SMTP or HTTP traffic to consume all available Content Scanning Protocol (CSP) resources and thereby hinder the ability of the NetScreen device to forward any other traffic to the AV scanner. To prevent such activity from succeeding, the NetScreen device can impose a maximum percentage of CSP resources that traffic from a single source can consume at any one time. The default maximum percentage is 70%. You can change this setting to any value between 1% and 100%, where 100% does not impose any restriction on the amount of CSP resources that traffic from a single source can consume.

**WebUI**

Screening > Antivirus: Enter a number in the Maximum AV Resources Allowed per AV Client field, and then click **Apply**.

**CLI**

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

The above **unset av** command returns the maximum percentage of CSP resources per source to the default (70%).

- **Fail mode behavior:** Fail mode is the behavior that the NetScreen device applies when it loses connectivity with the VirusWall scanner—either permit the unexamined traffic or block it. By default, if a NetScreen device cannot reach a VirusWall scanner, it blocks HTTP and SMTP traffic that a policy with antivirus checking enabled permits. You can change the default behavior from block to permit.

**WebUI**

Screening > Antivirus: Select the Fail Mode Traffic Permit check box to permit unexamined traffic, or clear the check box to block it, and then click **Apply**.

**CLI**

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

The above **unset av** command returns the fail mode behavior to the default (block unexamined traffic).
- **Fail mode threshold:** Fail mode is the state when a number of consecutive failed connection attempts to an AV object exceeds a threshold. By default, that threshold is 150, and it applies to all AV objects. If the number of consecutive failed attempts exceeds this threshold, the NetScreen device waits for a defined interval of time (five minutes) before renewing its connection efforts. You can change the threshold if the default setting seems too high or too low for your needs.

**WebUI**

Screening > Antivirus: Enter a number in the Fail Mode Scanner Threshold field, and then click **Apply**.

**CLI**

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

If you want the NetScreen device to resume its efforts to connect to a particular AV object before the wait interval has elapsed, you can enter the following command:

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

This command clears the failure status so that when the next SMTP or HTTP traffic arrives, the NetScreen device immediately attempts to connect to the AV scanner. If it is successful, the NetScreen device resumes forwarding files for virus scanning to the AV scanner. If its connection attempts are unsuccessful, the status returns to fail mode.

- **HTTP keep-alive:** By default, the NetScreen device uses the HTTP “close” connection option for indicating the end of data transmission. (If necessary, the NetScreen device changes the token in the connection header field from “keep-alive” to “close”.) In this method, when the HTTP server completes its data transmission, it sends a TCP FIN to close the TCP connection and thereby indicate that it has finished sending data. When the NetScreen device receives a TCP FIN, it has all the HTTP data from the server and can instruct the AV scanner to begin scanning.
You can change the default behavior of the NetScreen device to use the HTTP “keep-alive” connection option, which does not send a TCP FIN to indicate the termination of data transmission. The HTTP server must indicate that it has sent all the data in another way, such as by sending the content length in the HTTP header or by some form of encoding. (The method that a server uses varies by server type.) This method keeps the TCP connection open while the antivirus examination occurs, which decreases latency and improves CPU performance. However, it is not as secure as the “close” connection method. You can change this behavior if you find that HTTP connections are timing out during the antivirus examination.

**WebUI**

Screening > Antivirus: Select the Keep Alive check box to use the “keep-alive” connection option, or clear the check box to use the “close” connection option, and then click **Apply**.

**CLI**

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

- **HTTP trickling**: HTTP trickling is the forwarding of specified amounts of unscanned HTTP traffic to the requesting HTTP client to prevent the browser window from timing out while the VirusWall examines downloaded HTTP files. (The NetScreen device forwards small amounts of data in advance of transferring an entire scanned file.) By default, HTTP trickling is disabled. To enable it and use the default HTTP trickling parameters, do either of the following:

  **WebUI**

  Screening > Antivirus: Select the Trickling Default check box, and then click **Apply**.

  **CLI**

  ```
  set av http trickling default
  ```

With the default parameters, the NetScreen device employs trickling if the size of an HTTP file is 3 megabytes or larger. Then it forwards 500 bytes of content for every 1 megabyte sent for scanning.
To change the parameters for HTTP trickling, do either of the following:

**WebUI**

Screening > Antivirus: Enter the following, and then click **Apply**:

- **Trickling:**
  - **Custom:** (select)
  - Minimum Length to Start Trickling: Enter `number1`.
  - Trickle Size: Enter `number2`.
  - Trickle for Every MB Sent for Scanning: Enter `number3`.

**CLI**

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

The three number variables have the following meanings:

- `number1`: The minimum size (in megabytes) of an HTTP file to trigger trickling
- `number2`: The size (in bytes) of unscanned traffic that the NetScreen device forwards
- `number3`: The size (in megabytes) of a block of traffic to which the NetScreen device applies trickling

**Note:** *Data trickled to the client’s hard drive appears as a small, unusable file. Because trickling works by forwarding a small amount of data to a client without scanning it, virus code might be among the data that the NetScreen device has trickled to the client. NetScreen advises users to delete such files.*

You can disable HTTP trickling in the WebUI (Screening > Antivirus: Click **Disable** in the Trickling section.) or with the CLI command `set av http trickling 0 0 0`. However, if a file being downloaded is larger than eight megabytes and HTTP trickling is disabled, the browser window will most likely time out.
Example: Defining Three AV Objects

In this example, you define the following AV objects:

- **AV Object 1**
  - Name: scanner1
  - IP address: 1.2.2.20
  - Port number for Content Scanning Protocol (CSP): 3300 (default)
  - Content: HTTP
  - Timeout: 180 seconds (default)

- **AV Object 2**
  - Name: scanner2
  - IP address: 1.2.2.30
  - Port number for CSP: 6830
  - Content: SMTP
  - Timeout: 200 seconds

- **AV Object 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

The NetScreen device accesses the above addresses through ethernet2, which has IP address 1.2.2.1/24 and is bound to the DMZ zone.
WebUI

1. **AV Object 1**
   Objects > Antivirus > New: Enter the following, and then click **OK**:
   - AV Object Name: scanner1
   - Scan Server Name/IP: 1.2.2.20
   - Scan Server Port: 3300
   - Contents:
     HTTP: (select), Timeout: 180 Seconds

2. **AV Object 2**
   Objects > Antivirus > New: Enter the following, and then click **OK**:
   - AV Object Name: scanner2
   - Scan Server Name/IP: 1.2.2.30
   - Scan Server Port: 6830
   - Contents:
     SMTP: (select), Timeout: 200 Seconds

3. **AV Object 3**
   Objects > Antivirus > New: Enter the following, and then click **OK**:
   - AV Object Name: scanner3
   - Scan Server Name/IP: 1.2.2.40
   - Scan Server Port: 6840
   - Contents:
     HTTP: (select), Timeout: 120 Seconds
     SMTP: (select), Timeout: 200 Seconds
**CLI**

1. **AV Object 1**
   
   ```
   set av scanner1 server-name 1.2.2.20
   set av scanner1 content http
   ```

2. **AV Object 2**
   
   ```
   set av scanner2 server-name 1.2.2.30 port 6830
   set av scanner2 content smtp timeout 200
   ```

3. **AV Object 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`
Applying External AV Scanning

After you create one or more AV objects, you can reference them in policies to apply antivirus scanning to HTTP and SMTP traffic. A single AV object can scan HTTP traffic or SMTP traffic or both kinds of traffic. If you reference two or three AV objects in the same policy, then the NetScreen device sends traffic appropriate for scanning to those objects in a sequence that provides load balancing.

The order in which you reference the three AV objects in the policy configuration defines the order in which the NetScreen device sends HTTP and SMTP traffic to them. The AV object that you reference first is the one to which the NetScreen device sends the first file, such as an e-mail message or an HTTP reply, for scanning. In other words, the first AV object has the highest priority. The AV object that you reference second is the one to which the NetScreen device sends a second file if the first AV object is currently scanning another file. It has the second highest priority. The AV object that you reference in the policy configuration third gets a third file if the first two AV objects are both scanning other files. It has the lowest priority.

For example, if you create three AV objects “scanner1”, “scanner2”, and “scanner3” and then reference them in a policy in the following order,

```
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
```

then the order for sending files to each scanner proceeds as follows:

1. The NetScreen device sends the first file for scanning to scanner1.
2. When a second file to be scanned arrives, the NetScreen device sends it to scanner1 or scanner2 under the following conditions:
   - scanner1 if it has completed its scan of the first file
   - scanner2 if scanner1 is still scanning the first file
3. When a third file arrives, the NetScreen sends it to one of the three AV objects under the following conditions:
   - scanner1 if it is not scanning a file
   - scanner2 if scanner1 is scanning a file but scanner2 is not
   - scanner3 if scanner1 and scanner2 are both scanning files
The above sequence continues when all the scanners are busy scanning multiple files. If all scanners are scanning
the same number of files, the NetScreen device sends the next file to scanner1. If scanner1 is scanning fewer files
than scanner2 and scanner3, the NetScreen device sends the next file to scanner1. If scanner2 is scanning fewer
files than scanner1 and scanner3, the NetScreen device sends the next file to scanner2. If scanner3 is scanning
fewer files than scanner1 and scanner2, then the NetScreen device sends the next file to scanner3.

**Example: Antivirus with One AV Object**

In this example, you create a single AV object named “scanner1” to perform virus scanning on HTTP replies from
Web servers in the Untrust zone to clients in the Trust zone. The antivirus scanner is also in the Trust zone.
Although you enable antivirus checking for HTTP traffic between the Trust and Untrust zones, no additional policy is
necessary to permit CSP traffic between the NetScreen device and scanner1. All zones are in the trust-vr routing
domain.

*WebUI*

1. **Interfaces**

   Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:
   - Zone Name: Trust
   - Static IP: (select this option when present)
   - IP Address/Netmask: 10.1.1.1/24

   Enter the following, and then click **OK**:
   - Interface Mode: NAT

   Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:
   - Zone Name: Untrust
   - Static IP: (select this option when present)
   - IP Address/Netmask: 1.1.1.1/24
2. **AV Object**
   Objects > Antivirus > New: Enter the following, and then click **OK**:
   - AV Object Name: scanner1
   - Scan Server Name/IP: 1.2.2.20
   - Scan Server Port: 3300
   - Contents:
     - HTTP: (select), Timeout: 180 Seconds

3. **Route**
   Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:
   - Network Address/Netmask: 0.0.0.0/0
   - Gateway: (select)
   - Interface: ethernet3
   - Gateway IP Address: 1.1.1.250

4. **Policy**
   Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:
   - Source Address:
     - Address Book Entry: (select), Any
   - Destination Address:
     - Address Book Entry: (select), Any
   - Service: HTTP
   - Action: Permit
   > Advanced: Move the following AV object, and then click **Return** to set the advanced options and return to the basic configuration page:
   
   Select **scanner1** and use the << button to move the AV object from the Available AV Object Names column to the Attached AV Object Names column.
**CLI**

1. **Interfaces**
   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. **AV Object**
   set av scanner1 server-name 1.2.2.20
   set av scanner1 content http

3. **Route**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250

4. **Policy ID 1**
   set policy id 1 from trust to untrust any any http permit av scanner1
   save
Example: Antivirus with Two AV Objects

In this example, you define two AV objects named “scanner1” and “scanner2” for scanning HTTP and SMTP traffic. You then reference the AV objects in policies permitting HTTP between the Trust and Untrust zones and SMTP traffic from addresses in the Untrust and Trust zones to the mail server in the DMZ zone. To balance the traffic load sent to the two AV objects, you set up the distribution of antivirus scanning requests to them as follows:

- The NetScreen device redirects all HTTP antivirus scanning replies to the two AV objects. The two policies permitting HTTP traffic each reference both AV objects.

  1. First HTTP reply -> scanner1
  2. Second HTTP reply -> scanner2 (if scanner1 has not finished scanning the first HTTP reply; if scanner1 is free, then the NetScreen device redirects the second HTTP reply to scanner1)

- The NetScreen device sends antivirus scanning requests to scanner1 for all SMTP traffic from the remote mail server (named “r-mail”) in the Untrust zone to the local mail server (named “mailsvr1”) in the DMZ. The NetScreen device sends antivirus scanning requests to scanner2 for all SMTP traffic from the Trust zone.

  From the Untrust zone
  All SMTP traffic -> scanner1
  From the Trust zone
  All SMTP traffic -> scanner2
Both AV objects are in the Trust zone. Although you enable antivirus checking on traffic at the policy level, no additional policy is necessary to permit CSP traffic between the NetScreen device and the antivirus scanners. All zones are in the trust-vr routing domain.

WebUI

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:
   - Zone Name: Trust
   - Static IP: (select this option when present)
   - IP Address/Netmask: 10.1.1.1/24

   Enter the following, and then click **OK**:
   - Interface Mode: NAT

Network > Interfaces > Edit (for ethernet2): Enter the following, and then click **OK**:
   - Zone Name: DMZ
   - Static IP: (select this option when present)
   - IP Address/Netmask: 1.2.2.1/24

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:
   - Zone Name: Untrust
   - Static IP: (select this option when present)
   - IP Address/Netmask: 1.1.1.1/24
2. **AV Object 1**
   Objects > Antivirus > New: Enter the following, and then click **OK**:
   - AV Object Name: scanner1
   - Scan Server Name/IP: 10.1.1.20
   - Scan Server Port: 3300
   - Contents:
     - HTTP: (select), Timeout: 180 Seconds
     - SMTP: (select), Timeout: 180 Seconds

3. **AV Object 2**
   Objects > Antivirus > New: Enter the following, and then click **OK**:
   - AV Object Name: scanner2
   - Scan Server Name/IP: 10.1.1.30
   - Scan Server Port: 3300
   - Contents:
     - HTTP: (select), Timeout: 180 Seconds
     - SMTP: (select), Timeout: 180 Seconds

4. **Addresses**
   Objects > Addresses > List > New: Enter the following, and then click **OK**:
   - Address Name: mailsrv1
   - IP Address/Domain Name:
     - IP/Netmask: (select), 1.2.2.6/32
   - Zone: DMZ
Objects > Addresses > List > New: Enter the following, and then click **OK**:  
Address Name: r-mail  
IP Address/Domain Name:  
   IP/Netmask: (select), 2.2.2.5/32  
Zone: Untrust

5. **Route**  
Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:  
Network Address/Netmask: 0.0.0.0/0  
Gateway: (select)  
   Interface: ethernet3  
   Gateway IP Address: 1.1.1.250

6. **Policy ID 1**  
Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:  
Source Address:  
   Address Book Entry: (select), Any  
Destination Address:  
   Address Book Entry: (select), Any  
Service: HTTP  
Action: Permit  
> Advanced: Move the following AV objects, and then click **Return** to set the advanced options and return to the basic configuration page:  
   Select **scanner1** and use the << button to move the AV object from the Available AV Object Names column to the Attached AV Object Names column.
Select **scanner2** and use the << button to move the AV object from the Available AV Object Names column to the Attached AV Object Names column.

7. **Policy ID 2**
   Policies > (From: Untrust, To: DMZ) New: Enter the following, and then click **OK**:
   
   **Source Address:**
   
   Address Book Entry: (select), r-mail
   
   **Destination Address:**
   
   Address Book Entry: (select), mailsrv1
   
   **Service:** MAIL
   
   **Action:** Permit
   
   > Advanced: Move the following AV objects, and then click **Return** to set the advanced options and return to the basic configuration page:
   
   Select **scanner1** and use the << button to move the AV object from the Available AV Object Names column to the Attached AV Object Names column.

8. **Policy ID 3**
   Policies > (From: Trust, To: DMZ) New: Enter the following, and then click **OK**:
   
   **Source Address:**
   
   Address Book Entry: (select), Any
   
   **Destination Address:**
   
   Address Book Entry: (select), mailsrv1
   
   **Service:** MAIL
   
   **Action:** Permit
Advanced: Move the following AV objects, and then click Return to set the advanced options and return to the basic configuration page:

Select scanner2 and use the << button to move the AV object from the Available AV Object Names column to the Attached AV Object Names column.

**CLI**

1. **Interfaces**
   
   ```
   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. **AV Object 1**
   
   ```
   set av scanner1 server-name 10.1.1.20
   set av scanner1 content http
   set av scanner1 content smtp
   ```

3. **AV Object 2**
   
   ```
   set av scanner1 server-name 10.1.1.30
   set av scanner1 content http
   set av scanner1 content smtp
   ```

4. **Addresses**
   
   ```
   set address dmz mailsvr1 1.2.2.6/32
   set address untrust r-mail 2.2.2.5/32
   ```

5. **Route**
   
   ```
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
   ```
6. **Policy 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. **Policy ID 2**
   
   set policy id 2 from untrust to dmz r-mail mailsr1 mail permit av scanner1

8. **Policy ID 3**
   
   set policy id 3 from trust to dmz any mailsr1 mail permit av scanner2
   save
**URL Filtering**

NetScreen supports URL filtering using the Websense Enterprise Engine, which enables you to block or permit access to different sites based on their URLs, domain names, and IP addresses. With the Websense API built directly into the NetScreen firewall, the NetScreen device can link directly to a Websense URL-filtering server.

The following illustration shows the basic sequence of events when a host in the Trust zone attempts an HTTP connection to a server in the Untrust zone. However, URL filtering determines that the requested URL is prohibited.

**A Blocked URL**

NetScreen device intercepts and buffers the HTTP GET Request. It then sends the requested URL to the URL-filtering server. The URL-filtering server replies with a “block” message.

The NetScreen device drops the HTTP packet and closes the connection, sending a TCP RST to the source and destination addresses. It also sends the source a “blocked URL” message.
If the URL-filtering server permits access to the URL, the sequence of events in the HTTP connection attempt proceeds as follows:

A **Permitted** URL

1. **TCP Three-Way Handshake**
2. **HTTP Get Request**
3. **URL Filter Request**
4. **URL Filter Reply: “permit”**
5. **Forwards HTTP GET Request**
6. **Further HTTP GET Requests without URL Filter Checks**

The NetScreen device intercepts and buffers the HTTP GET Request. It then sends the requested URL to the URL-filtering server. The URL filtering-server replies with a “permit” message.

The NetScreen device forwards the buffered HTTP packet to the destination address. It also permits further HTTP GET requests in the same session without doing further URL filtering.
Using Websense, the administrator can do the following:

- Alter the URL-filtering database to block or allow access to selected sites
- Schedule different URL filtering profiles for different times of the day
- Download Websense Reporter logs of blocked or viewed URLs

**Note:** For additional information about Websense, visit www.websense.com.

NetScreen devices with virtual systems support up to eight different URL-filtering servers—one server reserved for the root system, and which can be shared with an unrestricted number of virtual systems; and seven URL-filtering servers for private use by the virtual systems. A root-level admin can configure the URL-filtering module at the root and virtual system (vsys) levels. A vsys-level admin can configure the URL module for his or her own vsys if that vsys has its own dedicated URL-filtering server. If the vsys-level admin uses the root URL-filtering server settings, that admin can see—but not modify—the root-level URL-filtering settings.

To configure a NetScreen device for URL filtering, you must perform the following tasks:

1. Set up communications with up to eight URL-filtering servers.
2. Define some system-level behavioral parameters. One set of parameters can apply to the root system and any vsys that shares the URL filtering configuration with the root system. Other sets can apply to virtual systems that have their own dedicated URL filtering server.
3. Activate URL filtering at the root and vsys levels.
4. Enable URL filtering in individual policies.

Details of these tasks are provided below.

1. **Device-to-Device Communications**

   You first define settings for the Websense server and parameters for the behavior that you want the NetScreen device to take when applying URL filtering. If you configure these settings in the root system, they also apply to any virtual system that shares the URL-filtering configuration with the root system. For a vsys that has its own dedicated URL-filtering server, the root admin or vsys admin must configure the settings separately for that vsys.
The URL-filtering settings that you must define at the system level for device-to-device communications are as follows:

- **Websense Server Name**: The IP address or fully qualified domain name (FQDN) of the computer running the Websense server.

- **Websense Server Port**: The default port for Websense is 15868. If you have changed the default port on the Websense server you must also change it on the NetScreen device. Please see your Websense documentation for full details.

- **Source Interface**: The source from which the NetScreen device initiates URL filter requests to a Websense server when sending them through a VPN tunnel. (Note that the source interface is different from the outgoing interface, which is the egress interface for VPN traffic.) Typically, the URL-filtering server belongs in the Trust zone. However, if you want several NetScreen devices to access a single URL-filtering server, you might configure VPN tunnels from each remote device to the local NetScreen device protecting the server. From the remote peers’ perspective, the server is in their Untrust zones, and they send URL filter requests to it through the tunnels.

- **Communication Timeout**: The time interval, in seconds, that the NetScreen device waits for a response from the Websense filter. If Websense does not respond within the time interval, the NetScreen device either blocks the request or allows it, as you choose (see below).

You can use the following CLI command to configure these settings:

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

In the WebUI, enter these settings in their respective fields on the Screening > URL Filtering page.

2. **System-Level Behavioral Parameters**

Second, you define the behavior parameters that you want the system—root or vsys—to take when applying URL filtering. The behavior options are as follows:

- **Fail/Pass Mode**: If the NetScreen device loses contact with the Websense server, you can specify whether to **Block** or **Permit** all HTTP requests.
– **Blocked URL Message Type:** The source of the message the user receives when Websense blocks a site. If you select NetPartners Websense, the NetScreen device forwards the message it receives in the “block” response from the Websense server. When you select NetScreen, the NetScreen device sends the message that you have previously entered in the NetScreen Blocked URL Message field.

*Note: If you select NetScreen, some of the functionality that Websense provides, such as redirection, are suppressed.*

– **NetScreen Blocked URL Message:** This is the message the NetScreen device returns to the user after blocking a site. You can use the message sent from the Websense server, or create a message (up to 500 characters) to be sent from the NetScreen device.

You can use the following CLI commands to configure these settings:

```
set url fail-mode { block | permit }
set url type { NetScreen | Websense }
set url message string
```

In the WebUI, enter these settings in their respective fields on the Screening > URL Filtering page.

3. **System-Level Activation**

When you complete the configuration, you must enable URL filtering at the system level. For a NetScreen device hosting virtual systems, you must enable URL filtering for each system that in which you want to apply it. For example, if you want the root system and a vsys to apply URL filtering, you must enable URL filtering in both the root system and that vsys.

You can use the following CLI command to activate and deactivate URL filtering at the system level:

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

In the WebUI, select or clear the **Enable URL Filtering via Websense Server** check box on the Screening > URL Filtering page.
When you enable URL filtering at the system level, the NetScreen device checks all HTTP traffic to which policies (defined in that system) that require URL filtering apply by redirecting the HTTP requests to a Websense server. If you disable URL filtering at the system level, the NetScreen device ignores the URL filtering component in policies and treats them as simple “permit” policies.

4. **Policy-Level Application**

Finally, you configure the NetScreen device to contact the URL-filtering server on a per-policy basis. You can use the following CLI command to enable URL filtering in a policy:

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

In the WebUI, select the **URL Filter** check box on the Advanced policy configuration page for the policy to which you want to apply URL filtering.

**Note:** The NetScreen device reports the status of the Websense server. To update the status report, click the Server Status icon on the Screening > URL Filtering page in the WebUI.
Example: URL Filtering Configuration

In this example, you configure the NetScreen device to work with a URL-filtering server at IP address 10.1.2.5, with port number 15868 (default). The URL-filtering server is in the Trust zone. You want to do URL filtering on all outbound HTTP traffic from hosts in the Trust zone to hosts in the Untrust zone. If the NetScreen device loses connectivity with the URL-filtering server, you want the NetScreen device to permit outbound HTTP traffic. When an HTTP client requests access to a prohibited URL, you want the NetScreen device to send the following message: “We’re sorry, but the requested URL is prohibited. If this prohibition appears to be in error, contact ntksec@mycompany.com.”

The interface for the Untrust zone is ethernet3 and has IP address 1.1.1.1/24. The interface for the Trust zone is ethernet1 and has IP address 10.1.1.1/24. Both zones are in the trust-vr routing domain. Because the URL-filtering server is not in the immediate subnet of one of the NetScreen device interfaces, you add a route to it through ethernet1 and the internal router at 10.1.1.250.

WebUI

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click Apply:
   - Zone Name: Trust
   - Static IP: (select this option when present)
   - IP Address/Netmask: 10.1.1.1/24

Enter the following, and then click OK:
   - Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click OK:
   - Zone Name: Untrust
   - Static IP: (select this option when present)
   - IP Address/Netmask: 1.1.1.1/24
2. **URL-Filtering Server**

   Screening > URL Filtering: Enter the following, and then click **Apply**:
   - Enable URL Filtering via Websense Server: (select)
   - Websense Server Name: 10.1.2.5
   - Websense Server Port: 15868
   - Communication Timeout: 10 (seconds)
   - 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. **Routes**

   Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:
   - Network Address/Netmask: 0.0.0.0/0
   - Gateway: (select)
     - Interface: ethernet3
     - Gateway IP Address: 1.1.1.250
   
   Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:
   - Network Address/Netmask: 10.1.2.0/24
   - Gateway: (select)
     - Interface: ethernet1
     - Gateway IP Address: 10.1.1.250
4. **Policy**

   Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

   - **Source Address:**
     - Address Book Entry: (select), Any
   - **Destination Address:**
     - Address Book Entry: (select), Any
   - **Service:** HTTP
   - **Action:** Permit

   > **Advanced:** Select the **URL Filter** check box, and then click **Return** to set the advanced options and return to the basic configuration page.

---

**CLI**

1. **Interfaces**

   - `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-Filtering Server**

   - `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. **Routes**

   - `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. **Policy**

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

You can enable Deep Inspection (DI) in policies to examine permitted traffic and take action if the DI module in ScreenOS finds attack signatures or protocol anomalies. The following sections in this chapter present the Deep Inspection elements that appear in policies and explains how to configure them:

- “Deep Inspection Overview” on page 124
- “Attack Object Database Server” on page 128
- “Attack Objects and Groups” on page 136
  - “Stateful Signatures” on page 138
  - “TCP Stream Signatures” on page 139
  - “Protocol Anomalies” on page 139
  - “Attack Object Groups” on page 140
- “Attack Actions” on page 142
- “Mapping Custom Services to Applications” on page 152
- “Customized Attack Objects and Groups” on page 156
  - “User-Defined Stateful Signature Attack Objects” on page 156
  - “TCP Stream Signature Attack Objects” on page 164

You can also enable Deep Inspection at the security zone level for HTTP components. These SCREEN options are explained in the final section of this chapter:

- “Granular Blocking of HTTP Components” on page 167
  - “ActiveX Controls” on page 167
  - “Java Applets” on page 168
  - “EXE Files” on page 168
  - “ZIP Files” on page 168
**DEEP INSPECTION OVERVIEW**

Deep Inspection (DI) is a mechanism for filtering the traffic permitted by the NetScreen firewall. Deep Inspection examines Layer 3 and 4 packet headers and Layer 7 application content and protocol characteristics in an effort to detect and prevent any attacks or anomalous behavior that might be present.

When the NetScreen device receives the first packet of a session, it inspects the source and destination IP addresses in the IP packet header (Layer 3 inspection) and the source and destination port numbers and protocol in

---

1. NetScreen detects anomalous traffic patterns at Layers 3 and 4 (IP and TCP) via SCREEN options set at the zone level, not the policy level. Examples of IP and TCP traffic-anomaly detection are “IP Address Sweep” on page 8, “Port Scanning” on page 10, and the various flood attacks described in “Network DoS Attacks” on page 45.
the TCP segment or UDP datagram header (Layer 4 inspection). If the Layer 3 and 4 components match the criteria specified in a policy, the NetScreen device then performs the specified action on the packet—permit, deny, or tunnel\(^2\). When the NetScreen device receives a packet for an established session, it compares it with the state information maintained in the session table to determine if it indeed belongs to the session.

If you have enabled Deep Inspection in the policy that applies to this packet and the policy action is “permit” or “tunnel”, then the NetScreen device further inspects it and its associated data stream for attack objects. Attack objects can be attack signatures or protocol anomalies, which you can either define yourself or download to the NetScreen device from an attack object database server\(^3\). (For more information, see “Attack Objects and Groups” on page 136 and “Customized Attack Objects and Groups” on page 156.) Based on the attack objects specified in the policy, the NetScreen device might perform the following inspections:

- Examine header values and payload data for stateful attack signatures
- Compare the format of the transmitted protocol with the standards specified in the RFCs and RFC extensions for that protocol to determine if someone has altered it, possibly for malicious purposes

\(^2\) If the specified action is tunnel, the notion of permission is implied. Note that if you enable Deep Inspection (DI) in a policy whose action is tunnel, the NetScreen device performs the specified DI operations before encrypting an outbound packet and after decrypting an inbound packet.

\(^3\) The ability to download attack objects from the attack object database server requires that you first subscribe for the service. For more information, see “Registration and Activation of Signature Services” on page 2-538.
If the NetScreen device detects an attack object, it performs the action specified in the DI component of the policy: close, close-client, close-server, drop, drop-packet, ignore, or none. If it does not find one of the specified attack objects, it forwards the packet. (For more information about attack actions, see “Attack Actions” on page 142.)

The following set policy command includes a DI component:

```
set policy id 1 from untrust to dmz any websrv1 http permit attack HIGH:HTTP:ANOM action close
```

The above command directs the NetScreen device to permit HTTP traffic from any address in the Untrust zone to the destination address “websrv1” in the DMZ zone. It also instructs the NetScreen device to inspect all HTTP traffic permitted by this policy. If it finds any attack objects defined in the attack object group “HIGH:HTTP:ANOM”, the NetScreen device closes the connection by dropping the packet and sending TCP RST notifications to the source and destination.

You can conceptually separate a set policy command into two parts—the core section and the DI component:

- The core section contains the source and destination zones, source and destination addresses, one or more services, and an action.
- The DI component instructs the NetScreen device to inspect traffic permitted by the core section of the policy for attack objects contained in one or more specified attack object groups. If the NetScreen device detects an attack object the NetScreen device then performs the action stated in the DI component.

4. You can optionally add other extensions to the core component of a set policy command: VPN and L2TP tunnel references, a schedule reference, address translation specifications, user authentication specifications, antivirus checking, logging, counting, and traffic management settings. Whereas these extensions are optional, the elements that constitute the core of a policy—source and destination zones, source and destination addresses, service (or services), and action—are required. (An exception to this is a global policy, in which no source and destination zones are specified: set policy global src_addr dst_addr service action. For more information about global policies, see “Global Policies” on page 2-201.)
It is possible to enter the context of an existing policy by using its ID number. For example:

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

**Note:** The command prompt changes to signal that a subsequent command is within a particular context.

Entering a policy context is convenient if you want to enter several commands related to a single policy. For example, the following set of commands creates a policy that permits HTTP and HTTPS traffic from the any address in the Untrust to websrv1 and websrv2 in the DMZ zone and looks for medium, high, and critical HTTP stateful signature and protocol anomaly attacks:

```
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
```

The above configuration permits both HTTP and HTTPS traffic, but only looks for attacks in HTTP traffic. To be able to add attack object groups with a policy context, you must first specify a DI attack and action in the top-level command. In the above example, you can add CRITICAL:HTTP:SIGS, HIGH:HTTP:ANOM, and HIGH:HTTP:SIGS attack object groups because you first configured the policy for Deep Inspection with the CRITICAL:HTTP:ANOM group.

**Note:** You can specify only one attack action per policy. For information about the seven attack actions, see “Attack Actions” on page 142.
ATTACK OBJECT DATABASE SERVER

The attack object database contains all the predefined attack objects, organized into attack object groups by protocol and severity level. NetScreen stores the attack object database on a server at https://services.netscreen.com/restricted/sigupdates. To use the predefined attack objects, you must download the database from this server, load it on your NetScreen device, and then reference specific attack object groups in policies. To gain access to the attack object database server, you must first subscribe to the DI signature service for your NetScreen device. (For information on how to do that, see “Registration and Activation of Signature Services” on page 2-538.)

Note: ScreenOS contains a CA certificate for authenticating communication with the attack object database server.

There are four ways to update the database:

- **Immediate Update**: With this option, you update the attack object database on the NetScreen device immediately with the database stored on the attack object database server. For this operation to work, you must first configure the attack object database server settings. (For an example, see “Example: Immediate Update” on page 129.)

  Note: Before performing an immediate database update, you can use the exec attack-db check command to check if the attack object database on the server is more recent than the one on the NetScreen device.

- **Automatic Update**: With this option, the NetScreen device downloads the attack object database directly to the NetScreen device at user-scheduled times if the database on the server is a newer version than that previously loaded on the NetScreen device. NetScreen updates the database on a regular basis with newly discovered attack patterns. Therefore, because of its changing nature, it behooves you to update your NetScreen device regularly too. For this operation to work, you must first configure the attack object database server settings. (For an example, see “Example: Automatic Updates” on page 130.)

- **Automatic Notification and Immediate Update**: With this option, the NetScreen device checks at user-scheduled times if the data on the attack object database server is more recent than that on the NetScreen device. If the data on the server is more recent, a notice appears on the Home page in the WebUI, and in the CLI after you log in to the NetScreen device. You can then enter the exec attack-db
update command or click the Update Now button on the Configuration > Update > Attack Signature page in the WebUI to save the database from the server to the NetScreen device. For the server-checking operation semi-automatic procedure to work, you must first configure the attack object database server settings. (For an example, see “Example: Automatic Notification and Immediate Update” on page 132.)

- **Manual Update:** With this option, you first use a Web browser to download the attack object database to a local directory or TFTP server directory. You can then load the database on the NetScreen device using either the WebUI (from the local directory) or CLI (from the TFTP server directory). (For an example, see “Example: Manual Update” on page 134.)

**Example: Immediate Update**

In this example, you save the attack object database (the attacks.bin file) from the attack object database server to the NetScreen device immediately. You use the default URL: https://services.netscreen.com/restricted/sigupdates. You do not have to set this URL for the database server. The NetScreen device uses it by default.

You do not set a schedule for updating the database on the NetScreen device. Instead you save the database from the server to the NetScreen device immediately.

**Note:** This example assumes that you have already obtained and activated a subscription for the DI signature service for the NetScreen device. (For information about subscriptions, see “License Keys” on page 2-536.)
**WebUI**

Configuration > Update > Attack Signature: Click the **Update Now** button.

**CLI**

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

**Example: Automatic Updates**

In this example, you set a schedule to update the database on the NetScreen device every Monday at 4:00 AM. At that scheduled time, the NetScreen device compares the version of the database on the server with that on the NetScreen device. If the version on the server is more recent, the NetScreen device automatically replaces its database with the newer version.

**Note:** This example assumes that you have already obtained and activated a subscription for the DI signature service for the NetScreen device. (For information about subscriptions, see “License Keys” on page 2-536.)

You use the default URL: https://services.netscreen.com/restricted/sigupdates. You do not have to set this URL for the database server. The NetScreen device uses it by default.
**WebUI**

Configuration > Update > Attack Signature: Enter the following, and then click **OK**:  
- Database Server: (leave empty)  
- Update Mode: Automatic Update  
- Schedule:  
  - Weekly on: Monday  
- Time (hh:mm): 04:00

**CLI**

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

---

5. If you schedule updates on a monthly basis and the date you choose does not occur in a month (for example, 31 does not occur in several months), the NetScreen device uses the last possible date of the month in its place.
Example: Automatic Notification and Immediate Update

In this example, you set a schedule to check the database on the NetScreen device on a daily basis at 7:00 AM. When you receive a notice that the database on the server has been updated, you click the Update Now button on the Configuration > Update > Attack Signature page in the WebUI or enter the exec attack-db update command to save the database from the server to the NetScreen device.

**Note:** This example assumes that you have already obtained and activated a subscription for the DI signature service for the NetScreen device. (For information about subscriptions, see “License Keys” on page 2-536.)

You use the default URL: https://services.netscreen.com/restricted/sigupdates. You do not have to set this URL for the database server. The NetScreen device uses it by default.

**WebUI**

1. **Scheduled Database Checking**

   Configuration > Update > Attack Signature: Enter the following, and then click OK:
   - Database Server: (leave empty)
   - Update Mode: Automatic Notification
   - Schedule:
     - Daily
   - Time (hh:mm): 07:00
2. **Immediate Database Update**

When you receive a notice that the attack database on the server is more current than the one on the NetScreen device, do the following:

Configuration > Update > Attack Signature: Click the **Update Now** button.

**CLI**

1. **Scheduled Database Checking**

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

2. **Immediate Database Update**

When you receive a notice that the attack database on the server is more current than the one on the NetScreen device, do the following:

exec attack-db update
Example: Manual Update

In this example, you manually save the latest attack object database to the local directory “C:\netscreen\attacks-db” (if you want to use the WebUI to load the database) or C:\Program Files\TFTP Server (if you want to use the CLI to load it). You then load the database on the NetScreen device from your local directory.

For an automatic update, the NetScreen device automatically adds the following elements to the URL:

- Serial number of the NetScreen device
- Number of the major ScreenOS version running on the device
- Platform type

When you manually update the database, you must add these elements yourself. In this example, the serial number is 0043012001000213, the ScreenOS version is 5.0, and the platform is NetScreen-208 (ns200). Consequently, the resulting URL is:

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

**Note:** This example assumes that you have already obtained and activated a subscription for the DI signature service for the NetScreen device. (For information about subscriptions, see “License Keys” on page 2-536.)

6. After downloading the attack object database, you can also post it on a local server and set it up for other NetScreen devices to access. The admins for the other devices must then change the database server URL to that of the new location. They can either enter the new URL in the Database Server field on the Configuration > Update > Attack Signature page or use the following CLI command: `set attack db server url_string`. 
1. **Database Download**

   Enter the following URL in the address field of your Web browser:

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

   Save `attacks.bin` to the local directory “C:\netscreen\attacks-db” (for loading via the WebUI) or to your TFTP server directory C:\Program Files\TFTP Server (when you want to use the CLI to load it).

   **WebUI**

   2. **Database Update**

      Configuration > Update > Attack Signature: Enter the following, and then click **OK**:

      Deep Inspection Signature Update:

      Load File: Enter C:\netscreen\attacks-db\attacks.bin, or click **Browse** and navigate to that directory, select `attacks.bin`, and then click **Open**.

   **CLI**

   2. **Database Update**

      ```
      save attack-db from tftp 10.1.1.5 attacks.bin to flash
      ```
**Attack Objects and Groups**

Attack objects are stateful signatures and protocol anomalies that a NetScreen device uses to detect attacks aimed at compromising one or more hosts on a network. Attack objects are in groups organized by protocol type and then by severity. When you add Deep Inspection (DI) to a policy, the NetScreen device inspects the traffic that the policy permits for any patterns matching those in the referenced attack object group (or groups).

Set policy from untrust to dmz any webserv1 http permit attack HIGH:HTTP:SIGS action close

Remote Host
1.1.1.3:25611

NetScreen
Untrust: ethernet3 1.1.1.1/24; DMZ: ethernet2 1.2.2.1/24

Untrust Zone
SYN
ACK
SRC IP DST IP SRC PT DST PT PROTO
1.1.1.3 1.2.2.5 25611 80 HTTP
Payload: ... revlog/.

DMZ Zone
SYN/ACK
RST

Webserv1
1.2.2.5:80

The NetScreen device detects an attack object in the packet. It drops the packet and closes the connection by sending TCP RST notifications to the source and destination.

Payload: revlog/.

Match!
The attack object groups that you reference in the DI component must target the same service type that the policy permits. For example, if the policy permits SMTP traffic, the attack object group must aim at attacks on SMTP traffic. The following policy exemplifies a valid configuration:

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

The next policy is erroneous because the policy permits SMTP traffic, but the attack object group is for POP3 traffic:

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

The second policy is misconfigured and, if implemented, would cause the NetScreen device to expend unnecessary resources inspecting SMTP traffic for POP3 attack objects that it could never find. If policy 2 permits both SMTP and POP3 traffic, you can configure the DI component to check for SMTP attack objects, POP3 attack objects, or for both.

```net
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
```

If the NetScreen device has access to http://help.netscreen.com/sigupdates/english, you can see the contents of all the predefined attack object groups and descriptions of the predefined attack objects. Open your Web browser, and enter one of the following URLs in the Address field:


Each of the above URLs links to an HTML page containing a list of all the predefined attack objects—organized in groups by severity—for a particular protocol. To see a description of an attack object, click its name.
An attack signature is a pattern that exists when a particular exploit is in progress. The signature can be a Layer 3 or 4 traffic pattern, such as when one address sends lots of packets to different port numbers at another address (port scan), or a textual pattern, such as when a malicious URL string appears in the data payload of a single HTTP or FTP packet. The string can also be a specific segment of code or a specific value in the packet header. However, when searching for a textual pattern, the Deep Inspection (DI) module in a NetScreen device looks for more than just a signature in a packet; it looks for the signature in a particular portion of the packet (even if fragmented or segmented), in packets sent at a particular time in the life of the session, and sent by either the connection initiator or the responder.

When the DI module checks for a textual pattern, it considers the roles of the participants as client or server and monitors the state of the session to narrow its search to just those elements relevant to the exploit for which attackers use the pattern. Using contextual information to refine packet examination greatly reduces false alarms—or “false positives”—and avoids unnecessary processing. The term “stateful signatures” conveys this concept of looking for signatures within the context of the participants’ roles and session state.

To see the advantage of considering the context in which a signature occurs, note the way the NetScreen DI module examines packets when enabled to detect the EXPN Root attack. Attackers use the EXPN Root attack to expand and expose mailing lists on a mail server. To detect the EXPN Root attack, the NetScreen device searches for the signature “expn root” in the control portion of a Simple Mail Transfer Protocol (SMTP) session. The NetScreen device examines only the control portion because that is only where the attack can occur. If “expn root” occurs in any other portion of the session, it is not an attack.

Using a simple textual packet signature detection technique, the signature “expn root” triggers an alarm even if it appears in the data portion of the SMTP connection; that is, in the body of an e-mail message. If, for example, you were writing to a colleague about EXPN Root attacks, a simple packet signature detector would regard this as an attack. Using stateful signatures, the NetScreen DI module can distinguish between text strings that signal attacks and those that are harmless occurrences.

---

7. Because the NetScreen DI module supports regular expressions, it can use wildcards when searching for patterns. Thus, a single attack signature definition can apply to multiple attack pattern variations.
TCP Stream Signatures

Like a stateful signature, a TCP stream signature is a pattern that exists when an exploit is in progress. However, when the DI module examines traffic for stateful signatures, it searches only within specific contexts. When the DI module examines traffic for TCP stream signatures, it does so without regard for contexts. Another distinction between the two types of signatures is that although stateful signatures can be predefined or user-defined, TCP stream signatures must be user-defined. After you add a stream signature attack object to an attack object group, you can then reference that group in a policy that applies Deep Inspection. (For more about TCP stream signatures, see “TCP Stream Signature Attack Objects” on page 164.)

Note: You can define TCP stream signatures on NetScreen-5000 series systems only.

Protocol Anomalies

Attack objects that search for protocol anomalies detect traffic that deviates from the standards defined in RFCs and common RFC extensions. With signature attack objects, you must use a predefined pattern or create a new one; therefore, they can only detect known attacks. Protocol anomaly detection is particularly useful for catching new attacks or those attacks that cannot be defined by a textual pattern. ScreenOS supports protocol anomaly attack objects for the following protocols:

- DNS
- FTP
- HTTP
- IMAP
- POP3
- SMTP
Attack Object Groups

Predefined attack object groups contain attack objects for a specific protocol. For each protocol, the groups are separated into protocol anomalies and stateful signatures, and then roughly organized by severity. The three attack object group severity levels are critical, high, and medium:

**Critical:** Contains attack objects matching exploits that attempt to evade detection, cause a network device to crash, or gain system-level privileges.

**High:** Contains attack objects matching exploits that attempt to disrupt a service, gain user-level access to a network device, or activate a Trojan horse previously loaded on a device.

**Medium:** Contains attack objects matching exploits that detect reconnaissance efforts attempting to access vital information through directory traversal or information leaks.

Changing Severity Levels

Although attack object groups are classified by protocol and severity level (critical, high, medium), each attack object has its own specific severity level:

- Critical
- Very High
- High
- Medium
- Low
- Info

These severity levels are meaningful for NetScreen-Security Manager (NSM).

It is possible to override the default severity level of all attack objects in one or more attack object groups referenced in a policy. You do this at the policy level by entering the context of an existing policy and then assigning a new severity level.
The following shows how to change the severity level of the attack object groups referenced in a policy through the WebUI and CLI:

**WebUI**

Policies > Edit (for an existing policy): Do the following, and then click OK:

> Deep Inspection: Select a severity option in the Severity drop-down list, and then click OK.

**CLI**

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

To return the severity level for each attack object to its original setting, you again enter the context of a policy and issue the following **unset policy** command:

**WebUI**

Policies > Edit (for an existing policy): Do the following, and then click OK:

> Deep Inspection: Select Default in the Severity drop-down list, and then click OK.

**CLI**

```
ns-> set policy id number
ns(policy: number)-> unset policy id number severity
```
**ATTACK ACTIONS**

When the NetScreen Deep Inspection (DA) module detects an attack, it then performs the action that you specify. The seven possibilities are as follows:

- **Close** (severs connection and sends RST to client and server)
  
  Use this option for TCP connections. The NetScreen device drops the connection and sends a TCP RST to both the client (source) and server (destination). Because the delivery of RST notifications is unreliable, by sending a RST to both client and server, there is a greater chance that at least one gets the RST and closes the session.

- **Close Client** (severs connection and sends RST to client)
  
  Use this option for outbound TCP connections from a protected client to an untrusted server. If, for example, the server sends a malicious URL string, the NetScreen device drops the connection and sends a RST only to the client for it to clear its resources while the server is left hanging.

- **Close Server** (severs connection and sends RST to server)
  
  Use this option for inbound TCP connections from an untrusted client to a protected server. If the client tries to launch an attack, the NetScreen device drops the connection and sends a TCP RST only to the server for it to clear its resources while the client is left hanging.

- **Drop** (severs connection without sending anyone a RST)
  
  Use this option for UDP or other non-TCP connections, such as DNS. The NetScreen device drops all packets in a session, but does not send a TCP RST.

- **Drop Packet** (drops a particular packet, but does not sever connection)
  
  This option drops the packet in which an attack signature or protocol anomaly occurs but does not terminate the session itself. Use this option to drop malformed packets without disrupting the entire session. For example, if the NetScreen device detects an attack signature or protocol anomaly from an AOL proxy, dropping everything would disrupt all AOL service. Instead, dropping just the packet stops the problem packet without stopping the flow of all the other packets.

---

8. The client is always the initiator of a session; that is, the source address in a policy. The server is always the responder, or the destination address.
• **Ignore** (after detecting an attack signature or anomaly, the NetScreen device makes a log entry and stops checking—or ignores—the remainder of the connection)

If the NetScreen device detects an attack signature or protocol anomaly, it makes an event log entry but does not sever the session itself. Use this option to tweak false positives during the initial setup phase of your Deep Inspection (DI) implementation. Also, use this option when a service uses a standard port number for nonstandard protocol activities; for example, Yahoo Messenger uses port 25 (SMTP port) for non-SMTP traffic. The NetScreen device logs the occurrence once per session (so that it does not fill the log with false positives), but takes no action.

• **None** (no action)

It is useful when first identifying attack types during the initial setup phase of your DI implementation. When the NetScreen device detects an attack signature or protocol anomaly, it makes an entry in the event log but takes no action on the traffic itself. The NetScreen device continues to check subsequent traffic in that session and make log entries if it detects other attack signatures and anomalies.

**Example: Attack Actions – Close Server, Close, Close Client**

In this example, there are three zones: Trust, Untrust, and DMZ. You have finished analyzing attacks and have concluded you need the following three policies:

• **Policy ID 1:** Permit HTTP, HTTPS, PING, and FTP-GET traffic from any address in the Untrust zone to the Web servers (websrv1 and websrv2) in the DMZ.

**Attack Settings for Policy ID 1:**

– CRITICAL:HTTP:ANOM, CRITICAL:HTTP:SIGS
– HIGH:HTTP:ANOM, HIGH:HTTP:SIGS
– MEDIUM:HTTP:ANOM, MEDIUM:HTTP:SIGS
– CRITICAL:FTP:SIGS
– Action: Close Server

You choose to drop the connection and send a TCP RST notification only to the protected Web servers so they can terminate sessions and clear resources. You anticipate attacks coming from the Untrust zone.
• **Policy ID 2:** Permit HTTP, HTTPS, PING, and FTP traffic from any address in the Trust zone to the Web servers (websrv1 and websrv2) in the DMZ

**Attack Settings for Policy ID 2:**
- CRITICAL:HTTP:ANOM, CRITICAL:HTTP:SIGS
- HIGH:HTTP:ANOM, HIGH:HTTP:SIGS
- MEDIUM:HTTP:ANOM, MEDIUM:HTTP:SIGS
- CRITICAL:FTP:SIGS
- Action: Close

You choose to drop the connection and send a TCP RST notification to both the protected clients and servers so they both can terminate their sessions and clear their resources regardless of the severity level of the attack.

• **Policy ID 3:** Permit FTP-GET, HTTP, HTTPS, PING traffic from any address in the Trust zone to any address in the Untrust zone

**Attack Settings for Policy ID 3:**
- CRITICAL:HTTP:ANOM, CRITICAL:HTTP:SIGS
- HIGH:HTTP:ANOM, HIGH:HTTP:SIGS
- MEDIUM:HTTP:ANOM, MEDIUM:HTTP:SIGS
- CRITICAL:FTP:SIGS
- Action: Close Client

You choose to drop the connection and send a TCP RST notification to the protected clients so they both can terminate their sessions and clear their resources. In this case, you anticipate an attack coming from an untrusted HTTP or FTP server.

Although the policies permit HTTP, HTTPS, Ping, and FTP-Get or FTP, the NetScreen device activates Deep Inspection only for HTTP and FTP traffic. All zones are in the trust-vr routing domain.
**WebUI**

1. **Interfaces**
   Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:
   
   Zone Name: Trust
   Static IP: (select this option when present)
   IP Address/Netmask: 10.1.1.1/24

   Enter the following, and then click **OK**:
   Interface Mode: NAT
   Service Options:
   Management Services: (select all)
   Other services: Ping
Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

- Zone Name: Untrust
- Static IP: (select this option when present)
- IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > Edit (for ethernet2): Enter the following, and then click **OK**:

- Zone Name: DMZ
- Static IP: (select this option when present)
- IP Address/Netmask: 1.2.2.1/24

2. **Addresses**

Objects > Addresses > List > New: Enter the following, and then click **OK**:

- Address Name: websrv1
- IP Address/Domain Name:
  - IP/Netmask: (select), 1.2.2.5/32
- Zone: DMZ

Objects > Addresses > List > New: Enter the following, and then click **OK**:

- Address Name: websrv2
- IP Address/Domain Name:
  - IP/Netmask: (select), 1.2.2.6/32
- Zone: DMZ

3. **Route**

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

- Network Address/Netmask: 0.0.0.0/0
- Gateway: (select)
  - Interface: ethernet3
  - Gateway IP Address: 1.1.1.250
4. **Policy ID 1**

Policies > (From: Untrust, To: DMZ) New: Enter the following, and then click **OK**:

**Source Address:**
- Address Book Entry: (select), Any

**Destination Address:**
- Address Book Entry: (select), webserv1

> Click **Multiple**, select **webserv2**, and then click **OK** to return to the basic policy configuration page.

**Service:** HTTP

> Click **Multiple**, select **FTP-GET**, **HTTPS**, **PING**, and then click **OK** to return to the basic policy configuration page.

**Action:** Permit

> Click **Deep Inspection**, enter the following, and then click **OK** to return to the basic policy configuration page:

**Action:** Close Server

Use the **<<** button to move the following attack groups from the Available Members column to the Selected Members column:

- **CRITICAL**: HTTP:ANOM
- **CRITICAL**: HTTP:SIGS
- **HIGH**: HTTP:ANOM
- **HIGH**: HTTP:SIGS
- **MEDIUM**: HTTP:ANOM
- **MEDIUM**: HTTP:SIGS
- **CRITICAL**: FTP:SIGS
5. Policy ID 2

Policies > (From: Trust, To: DMZ) New: Enter the following, and then click OK:

Source Address:
   Address Book Entry: (select), Any

Destination Address:
   Address Book Entry: (select), websrv1

> Click Multiple, select websrv2, and then click OK to return to the basic policy configuration page.

Service: HTTP

> Click Multiple, select FTP-GET, HTTPS, PING, and then click OK to return to the basic policy configuration page.

Action: Permit

> Click Deep Inspection, enter the following, and then click OK to return to the basic policy configuration page:

   Action: Close

   Use the << button to move the following attack groups from the Available Members column to the Selected Members column:

   CRITICAL:HTTP:ANOM
   CRITICAL:HTTP:SIGS
   HIGH:HTTP:ANOM
   HIGH:HTTP:SIGS
   MEDIUM:HTTP:ANOM
   MEDIUM:HTTP:SIGS
   CRITICAL:FTP:SIGS
6. **Policy ID 3**

   Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

   Source Address:
   - Address Book Entry: (select), Any
   Destination Address:
   - Address Book Entry: (select), Any
   Service: HTTP

   > Click **Multiple**, select **FTP-GET, HTTPS, PING**, and then click **OK** to return to the basic policy configuration page.

   Action: Permit

   > Click **Deep Inspection**, enter the following, and then click **OK** to return to the basic policy configuration page:

       Action: Close Client

   Use the << button to move the following attack groups from the Available Members column to the Selected Members column:

       CRITICAL:HTTP:ANOM
       CRITICAL:HTTP:SIGS
       HIGH:HTTP:ANOM
       HIGH:HTTP:SIGS
       MEDIUM:HTTP:ANOM
       MEDIUM:HTTP:SIGS
       CRITICAL:FTP:SIGS
**CLI**

1. **Interfaces**
   
   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. **Addresses**
   
   set address dmz websrv1 1.2.2.5/32
   set address dmz websrv2 1.2.2.6/32

3. **Route**
   
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250

4. **Policy 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. **Policy 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. **Policy 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
When using a custom service in a policy with a Deep Inspection (DI) component, you must explicitly specify the application that is running on that service so that the DI module can function properly. For example, if you create a custom service for FTP running on the nonstandard port number 2121, you can reference that custom service in a policy as follows:

```
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
```

However, if you add a DI component to a policy that references a custom service, the DI module cannot recognize the application because it is using a nonstandard port number.

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

To avoid this problem, you must inform the DI module that the FTP application is running on port 2121. Essentially, you must map the protocol in the Application Layer to a specific port number in the Transport Layer. You can do this binding at the policy level:

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

When you map the FTP application to the custom service “custom-ftp” and configure DI to examine FTP traffic for the attacks defined in the CRITICAL:FTP:SIGS attack object group in a policy that references custom-ftp, the DI module perform its inspection on port 2121.
Example: Mapping an Application to a Custom Service

In this example, you define a custom service named “HTTP1” that uses destination port 8080. You map the HTTP application to the custom service for a policy permitting HTTP1 traffic from any address in the Untrust zone to a Web server named “server1” in the DMZ zone.

**WebUI**

1. **Custom Service**
   - Objects > Services > Custom > New: Enter the following, and then click **OK**:
     - **Service Name**: HTTP1
     - **Transport Protocol**: TCP (select)
     - **Source Port Low**: 0
     - **Source Port High**: 65535
     - **Destination Port Low**: 8080
     - **Destination Port High**: 8080
2. Address

Objects > Addresses > List > New: Enter the following, and then click **OK**:
- Address Name: server1
- IP Address/Domain Name:
  - IP/Netmask: 1.2.2.5/32
- Zone: DMZ

3. Policy

Policies > (From: Untrust, To: DMZ) New: Enter the following, and then click **OK**:
- Source Address:
  - Address Book Entry: (select), Any
- Destination Address:
  - Address Book Entry: (select), server1
- Service: HTTP1
- Application: HTTP
- Action: Permit

> Click **Deep Inspection**, enter the following, and then click **OK** to return to the basic policy configuration page:

  - Action: Close Server

Use the << button to move the following attack groups from the Available Members column to the Selected Members column:

- CRITICAL:HTTP:ANOM
- CRITICAL:HTTP:SIGS
- HIGH:HTTP:ANOM
- HIGH:HTTP:SIGS
- MEDIUM:HTTP:ANOM
- MEDIUM:HTTP:SIGS
**CLI**

1. **Custom Service**
   
   ```
   set service HTTP1 protocol tcp src-port 0-65535 dst-port 8080-8080
   ```

2. **Address**
   
   ```
   set address dmz server1 1.2.2.5/32
   ```

3. **Policy**
   
   ```
   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
   ```
CUSTOMIZED ATTACK OBJECTS AND GROUPS

You can define new attack objects and object groups to customize the Deep Inspection (DI) application to best meet your needs. The attack objects can be stateful signatures or—on the NetScreen-5000—TCP stream signatures.

User-Defined Stateful Signature Attack Objects

You can create a stateful signature attack object for FTP, HTTP, and SMTP. When creating an attack object, you perform the following steps:

- Name the attack object. (All user-defined attack objects must begin with “CS:”.)
- Set the context for the Deep Inspection search.
- Define the signature.
- Assign the attack object a severity level.

The following subsections examine the topics of contexts and signatures. For information on severity levels, which are used by NetScreen Security Manager 2004, see “Changing Severity Levels” on page 140.

Contexts

The context defines the location in the packet where the NetScreen DI module searches for a signature matching the attack object pattern. You can specify any of the following contexts:

- FTP Command: Sets the context as one of the FTP commands specified in RFC 959, “File Transfer Protocol (FTP)”
- FTP User Name: Sets the context as the name that a user enters when logging in to an FTP server
- HTTP URL Parsed: Sets the context as the “normalized” text string decoded from a unicode string
- SMTP Header From: Sets the context as the SMTP “From:” header
- SMTP Header To: Sets the context as the SMTP “To:” header
- SMTP Mail From: Sets the context as the SMTP ‘MAIL FROM’ command line
- SMTP Recipient: Sets the context as the SMTP ‘RCPT TO’ command line

You must then put a user-defined attack object in a user-defined attack object group for use in policies.
**Note:** A user-defined attack object group can only contain user-defined attack objects. You cannot mix predefined and user-defined attack objects in the same attack object group.

### Signatures

When entering the text string for a signature, you can enter an alphanumeric string of ordinary characters to search for an exact character-to-character match, or you can use regular expressions to broaden the search for possible matches to sets of characters. ScreenOS supports the following regular expressions:

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Metacharacters</th>
<th>Example</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct binary match (octal)</td>
<td>\O octal_number</td>
<td>\0162</td>
<td>Matches: 162</td>
</tr>
<tr>
<td>Direct binary match (hexadecimal)</td>
<td>\X hexadecimal_number\X</td>
<td>\X01 A5 00 00\X</td>
<td>Matches: 01 A5 00 00</td>
</tr>
<tr>
<td>Case-insensitive matches</td>
<td>[characters]</td>
<td>[cat]</td>
<td>Matches: Cat, cAt, caT CAT, CaT, CAT cat, cAt</td>
</tr>
<tr>
<td>Match any character</td>
<td>.</td>
<td>c . t</td>
<td>Matches: cat, cbt, cct, … czt cAt, cBt, cCt, … cZt c1t, c2t, c3t, … c9t</td>
</tr>
<tr>
<td>Purpose</td>
<td>Metacharacters</td>
<td>Example</td>
<td>Meaning</td>
</tr>
<tr>
<td>---------</td>
<td>----------------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>Match the previous character 0 or more times, instead of only once</td>
<td>*</td>
<td>a*b+c</td>
<td>Match 0, 1, or multiple occurrences of “a”, followed by 1 or more occurrences of “b”, followed by one occurrence of “c”.</td>
</tr>
<tr>
<td>Match the previous character 1 or more times</td>
<td>+</td>
<td>a+b+c</td>
<td>Match 1 or more occurrences of “a”, followed by 1 or more occurrences of “b”, followed by one occurrence of “c”.</td>
</tr>
<tr>
<td>Match the previous character 0 times or 1 time</td>
<td>?</td>
<td>drop-?packet</td>
<td>Match either “drop-packet” or “droppacket”.</td>
</tr>
<tr>
<td>Group expressions</td>
<td>( )</td>
<td>(drop</td>
<td>packet)</td>
</tr>
</tbody>
</table>

Purpose

**Metacharacters**

- `*` Match the previous character 0 or more times, instead of only once.
- `+` Match the previous character 1 or more times.
- `?` Match the previous character 0 times or 1 time.
- `()` Group expressions — typically used with `()`.
- `|` Either the previous or the following character — typically used with `()`.

**Example**

- `a*b+c`
- `a+b+c`
- `drop-?packet`
- `(drop | packet)`
<table>
<thead>
<tr>
<th>Purpose</th>
<th>Metacharacters</th>
<th>Example</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Character range</td>
<td>[start-end]</td>
<td>[c-f]a(d</td>
<td>t)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Matches: cad, cat dad, dat ead, eat fad, fat</td>
<td></td>
</tr>
<tr>
<td>Negation of the following</td>
<td>^[character]</td>
<td>^0-9A-Z</td>
<td>Match lowercase letters.</td>
</tr>
<tr>
<td>character</td>
<td></td>
<td>Matches: a, b, c, d, e, … z</td>
<td></td>
</tr>
</tbody>
</table>

1 Octal is a base-8 number system that uses only the digits 0-7.

1 Hexadecimal is a base-16 number system that uses digits 0–9 as usual, and then the letters A–F representing hexadecimal digits with decimal values of 10-15.
Example: User-Defined Stateful Signature Attack Objects

In this example, you have an FTP server, a Web server, and a mail server in the DMZ zone. You define the following attack objects for the following uses:

<table>
<thead>
<tr>
<th>Attack Object Name</th>
<th>You can use it to</th>
</tr>
</thead>
<tbody>
<tr>
<td>cs:ftp-stor</td>
<td>stop someone from putting files on your FTP server.</td>
</tr>
<tr>
<td>cs:ftp-user-dm</td>
<td>deny FTP access to the user with the login name “dmartin”.</td>
</tr>
<tr>
<td>cs:url-index</td>
<td>block HTTP packets with a defined URL in any HTTP request.</td>
</tr>
<tr>
<td>cs:spammer</td>
<td>block e-mail from any e-mail address at “spam.com”.</td>
</tr>
</tbody>
</table>

You then organize them into a user-defined attack object group named “DMZ DI”, which you reference in a policy permitting traffic from the Untrust zone to the servers in the DMZ zone.

**WebUI**

1. **Attack Object 1: ftp-stor**
   Objects > Attacks > Custom > New: Enter the following, and then click **OK**:
   - Attack Name: cs:ftp-stor
   - Attack Context: FTP Command
   - Attack Severity: Medium
   - Attack Pattern: stor

2. **Attack Object 2: ftp-user-dm**
   Objects > Attacks > Custom > New: Enter the following, and then click **OK**:
   - Attack Name: cs:ftp-user-dm
   - Attack Context: FTP User Name
   - Attack Severity: Low
   - Attack Pattern: dmartin
3. **Attack Object 3: url-index**
   Objects > Attacks > Custom > New: Enter the following, and then click **OK**:
   - Attack Name: cs:url-index
   - Attack Context: HTTP URL Parsed
   - Attack Severity: High
   - Attack Pattern: .*index.html.*

4. **Attack Object 4: url-index**
   Objects > Attacks > Custom > New: Enter the following, and then click **OK**:
   - Attack Name: cs:spammer
   - Attack Context: SMTP From
   - Attack Severity: Info
   - Attack Pattern: .@spam.com

5. **Attack Object Group**
   Objects > Attacks > Custom Group > New: Enter the following group name, move the following custom
   attack objects, and then click **OK**:
   - Group Name: CS:DMZ DI
   - Select **cs:ftp-stor** and use the << button to move the address from the
     Selected Members column to the Selected Members column.
   - Select **cs:ftp-user-dm** and use the << button to move the address from the
     Available Members column to the Selected Members column.
   - Select **cs:url-index** and use the << button to move the address from the
     Available Members column to the Selected Members column.
   - Select **cs:spammer** and use the << button to move the address from the
     Available Members column to the Selected Members column.
6. Policy

Policies > (From: Untrust, To: DMZ) New: Enter the following, and then click OK:

Source Address:
  Address Book Entry: (select), Any
Destination Address:
  Address Book Entry: (select), Any
Service: HTTP
> Click Multiple, select FTP, and then click OK to return to the basic policy configuration page.

Action: Permit
> Click Deep Inspection, enter the following, and then click OK to return to the basic policy configuration page:

  Action: Close Server

Use the << button to move the following attack groups from the Available Members column to the Selected Members column,

CS:DMZ DI
CLI

1. **Attack Object 1: ftp-stor**
   
   set attack cs:ftp-stor ftp-command stor severity medium

2. **Attack Object 2: ftp-user-dm**
   
   set attack cs:ftp-user-dm ftp-username dmartin severity low

3. **Attack Object 3: url-index**
   
   set attack cs:url-index http-url-parsed index.html severity high

4. **Attack Object 4: url-index**
   
   set attack cs:spammer smtp-from .@spam.com severity info

5. **Attack Object Group**
   
   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. **Policy**
   
   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 Stream Signature Attack Objects

The stateful signatures are context-based within specific applications, such as an FTP user name or an SMTP header field. TCP stream signatures look for patterns anywhere in any kind of TCP traffic regardless of the application protocol in use.

**Note:** You can define TCP stream signatures on NetScreen-5000 series systems only.

Because there are no predefined TCP stream signature attack objects, you must define them. When creating a signature attack object, you define the following components:

- Attack object name (All user-defined attack objects must begin with “CS:”.)
- Object type ("stream")
- Pattern definition
- Severity level

**Example of a TCP Stream Signature Attack Object**

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

**Example: User-Defined Stream Signature Attack Object**

In this example, you define a stream signature object ".*satori.*". You name it “CS:A1” and define its severity level as critical. Because a policy can reference only attack object groups, you create a group named “CS:Gr1”, and then add this object to it. Finally, you define a policy that references CS:Gr1 and that instructs the NetScreen device to sever the connection and send TCP RST to the client if the pattern appears in any traffic to which the policy applies.


**WebUI**

1. **Stream Signature Attack Object**
   Objects > Attacks > Custom > New: Enter the following, and then click **OK**:
   - Attack Name: CS:A1
   - Attack Context: Stream
   - Attack Severity: Critical
   - Attack Pattern: .*satori.*

2. **Stream Signature Attack Object Group**
   Objects > Attacks > Custom Group > New: Enter the following, and then click **OK**:
   - Group Name: CS:Gr1
   Select **CS:A1** in the Available Members column and then click **<<** to move it to the Selected Members column.

3. **Policy**
   Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:
   - Source Address:
     - Address Book Entry: (select), Any
   - Destination Address:
     - Address Book Entry: (select), Any
   - Service: ANY
   - Action: Permit
   > Click **Deep Inspection**, enter the following, and then click **OK** to return to the basic policy configuration page:
     - Action: Close Client
   Select **CS:Gr1** in the Available Members column and then click **<<** to move it to the Selected Members column.
CLI

1. Stream Signature Attack Object
   set attack "CS:A1" stream ".*satori.*" severity critical

2. Stream Signature Attack Group
   set attack group "CS:Gr1"
   set attack group "CS:Gr1" add "CS:A1"

3. Policy
   set policy from trust to untrust any any any any permit attack CS:Gr1 action close-client
   save
**Granular Blocking of HTTP Components**

A NetScreen device can selectively block ActiveX controls, Java applets, .zip files, and .exe files sent via HTTP. The danger that these components pose to the security of a network is that they provide a means for an untrusted party to load and then control an application on hosts in a protected network.

When you enable the blocking of one or more of these components in a security zone, the NetScreen device examines every HTTP header that arrives at an interface bound to that zone. It checks if the content type listed in the header indicates that any of the targeted components are in the packet payload. If the content type is Java, .exe, or .zip and you have configured the NetScreen device to block those HTTP component types, the NetScreen device blocks the packet. If the content type lists only “octet stream” instead of a specific component type, then the NetScreen device examines the file type in the payload. If the file type is Java, .exe, or .zip and you have configured the NetScreen device to block those component types, the NetScreen device blocks the packet.

When you enable the blocking of ActiveX controls, the NetScreen device blocks all HTTP packets containing any type of HTTP component in its payload—ActiveX controls, Java applets, .exe files, or .zip files.

**Note:** When ActiveX-blocking is enabled, the NetScreen device blocks Java applets, .exe files, and .zip files whether they are contained within an ActiveX control or not.

**ActiveX Controls**

Microsoft ActiveX technology provides a tool for Web designers to create dynamic and interactive Web pages. ActiveX controls are components that allow different programs to interact with each other. For example, ActiveX allows your Web browser to open a spreadsheet or display your personal account from a backend database. ActiveX components might also contain other components such as Java applets, or files such as .exe and .zip files.

When you visit an ActiveX-enabled Web site, the site prompts you to download ActiveX controls to your computer. Microsoft provides a pop-up message displaying the name of the company or programmer who authenticated the ActiveX code that is offered for download. If you trust the source of the code, you can proceed to download the controls. If you distrust the source, you can refuse them.

If you download an ActiveX control to your computer, it can then do whatever its creator designed it to do. If it is malicious code, it can now reformat your hard drive, delete all your files, send all your personal e-mail to your boss, and so on.
Java Applets

Serving a similar purpose as ActiveX, Java applets also increase the functionality of Web pages by allowing them to interact with other programs. You download Java applets to a Java Virtual Machine (VM) on your computer. In the initial version of Java, the VM did not allow the applets to interact with other resources on your computer. Starting with Java 1.1, some of these restrictions were relaxed to provide greater functionality. As a result, Java applets can now access local resources outside the VM. Because an attacker can program Java applets to operate outside the VM, they pose the same security threat as ActiveX controls do.

EXE Files

If you download and run an executable file (that is, a file with a .exe extension) obtained off the Web, you cannot guarantee that the file is uncontaminated. Even if you trust the site from which you downloaded it, it is possible that somebody sniffing download requests from that site has intercepted your request and responded with a doctored .exe file that contains malicious code.

ZIP Files

A zip file (that is, a file with a .zip extension) is a type of file containing one or more compressed files. The danger of downloading a .exe file presented in the previous section about .exe files applies to .zip files, because a .zip file can contain one or more .exe files.
Example: Blocking Java Applets and .exe Files

In this example, you block any HTTP traffic containing Java applets and .exe files in packets arriving at an Untrust zone interface.

**WebUI**

Screening > Screen (Zone: Untrust): Select **Block Java Component** and **Block EXE Component**, and then click **Apply**.

**CLI**

```
set zone untrust screen java
set zone untrust screen exe
save
```
As shown in the other chapters in this volume, attackers can craft packets to perform reconnaissance or launch denial-of-service (DoS) attacks. Sometimes it is unclear what the intent of a crafted packet is, but the very fact that it is crafted suggests that it is being put to some kind of insidious use. All of the SCREEN options presented in this chapter block suspicious packets that might contain hidden threats:

- “ICMP Fragments” on page 172
- “Large ICMP Packets” on page 174
- “Bad IP Options” on page 176
- “Unknown Protocols” on page 178
- “IP Packet Fragments” on page 180
- “SYN Fragments” on page 182
### ICMP Fragments

Internet Control Message Protocol (ICMP) provides error reporting and network probe capabilities. Because ICMP packets contain very short messages, there is no legitimate reason for ICMP packets to be fragmented. If an ICMP packet is so large that it must be fragmented, something is amiss. When you enable the ICMP Fragment Protection SCREEN option, the NetScreen device blocks any ICMP packet with the More Fragments flag set, or with an offset value indicated in the offset field.

![ICMP Packet Header Diagram](image)

<table>
<thead>
<tr>
<th>IP Header</th>
<th>Version</th>
<th>Header Length</th>
<th>Type of Service</th>
<th>Total Packet Length (in Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification</td>
<td>0</td>
<td>D</td>
<td>M</td>
<td>Fragment Offset</td>
</tr>
<tr>
<td>Time to Live (TTL)</td>
<td>Protocol (ICMP = 1)</td>
<td>Header Checksum</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source Address</td>
<td>Destination Address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICMP Header (IP Packet Payload)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Options</td>
<td>Type</td>
<td>Code</td>
<td>Checksum</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Identifier</td>
<td></td>
<td>Sequence Number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If the protocol type is 1 for ICMP, and the More Fragments flag is set, or there is a non-zero value in the Fragment Offset field, the NetScreen device blocks the packet.
To block fragmented ICMP packets, do either of the following, where the specified security zone is the one from which the fragments originate:

**WebUI**

Screening > Screen (Zone: select a zone name): Select **ICMP Fragment Protection**, and then click **Apply**.

**CLI**

```
set zone zone screen icmp-fragment
```
LARGE ICMP PACKETS

As stated in the previous section “ICMP Fragments” on page 172, Internet Control Message Protocol (ICMP) provides error reporting and network probe capabilities. Because ICMP packets contain very short messages, there is no legitimate reason for large ICMP packets. If an ICMP packet is unusually large, something is wrong. For example, the Loki program uses ICMP as a channel for transmitting covert messages. The presence of large ICMP packets might expose a compromised machine acting as a Loki agent. It might also indicate some other kind of shifty activity.

When you enable the Large Size ICMP Packet Protection SCREEN option, the NetScreen device checks drops ICMP packets with a length greater than 1024 bytes.
To block large ICMP packets, do either of the following, where the specified security zone is the one from which the ICMP packets originate:

**WebUI**

Screening > Screen (Zone: select a zone name): Select **Large Size ICMP Packet (Size > 1024)** Protection, and then click **Apply**.

**CLI**

```plaintext
set zone zone screen icmp-large
```
BAD IP OPTIONS

The Internet Protocol standard “RFC 791, Internet Protocol” specifies a set of eight options that provide special routing controls, diagnostic tools, and security. Although the original, intended uses for these options served worthy ends, people have figured out ways to twist these options to accomplish less commendable objectives. (For a summary of the exploits that attackers can wreak from IP options, see “Network Reconnaissance Using IP Options” on page 12.)

Either intentionally or accidentally, attackers sometimes misconfigure IP options, producing either incomplete or malformed fields. Regardless of the intentions of the person who crafted the packet, the misformatting is anomalous and potentially harmful to the intended recipient.

<table>
<thead>
<tr>
<th>IP Header</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
</tr>
<tr>
<td>Identification</td>
</tr>
<tr>
<td>Time to Live (TTL)</td>
</tr>
<tr>
<td>Source Address</td>
</tr>
<tr>
<td>Destination Address</td>
</tr>
<tr>
<td>Options</td>
</tr>
<tr>
<td>Payload</td>
</tr>
</tbody>
</table>

If the IP options are misformatted, the NetScreen device records the event in the SCREEN counters for the ingress interface.

When you enable the Bad IP Option Protection SCREEN option, the NetScreen device blocks packets when any IP option in the IP packet header is incorrectly formatted. The NetScreen device records the event in the event log.
To detect and block IP packets with incorrectly formatted IP options, do either of the following, where the specified security zone is the one from which the packets originate:

**WebUI**

Screening > Screen (Zone: select a zone name): Select **Bad IP Option Protection**, and then click **Apply**.

**CLI**

```
set zone zone screen ip-bad-option
```
**UNKNOWN PROTOCOLS**

These protocol types with ID numbers of 135 or greater are reserved and undefined at this time. Precisely because these protocols are undefined, there is no way to know in advance if a particular unknown protocol is benign or malicious. Unless your network makes use of a non-standard protocol with an ID number of 135 or greater, a cautious stance is to block such unknown elements from entering your protected network.

When you enable the Unknown Protocol Protection SCREEN option, the NetScreen device drops packets when the protocol field is contains a protocol ID number of 135 or greater.
To drop packets using an unknown protocol, do either of the following, where the specified security zone is the one from which the packets originate:

**WebUI**

Screening > Screen (Zone: select a zone name): Select **Unknown Protocol Protection**, and then click **Apply**.

**CLI**

```
set zone zone screen unknown-protocol
```
**IP PACKET FRAGMENTS**

As packets traverse different networks, it is sometimes necessary to break a packet into smaller pieces (fragments) based upon the maximum transmission unit (MTU) of each network. IP fragments might contain an attacker’s attempt to exploit the vulnerabilities in the packet reassembly code of specific IP stack implementations. When the victim receives these packets, the results can range from processing the packets incorrectly to crashing the entire system.

When you enable the NetScreen device to deny IP fragments on a security zone, the device blocks all IP packet fragments that it receives at interfaces bound to that zone.
To drop fragmented IP packets, do either of the following, where the specified security zone is the one from which the fragments originate:

**WebUI**

Screening > Screen (Zone: select a zone name): Select **Block Fragment Traffic**, and then click **Apply**.

**CLI**

```
set zone zone screen block-frag
```
SYN FRAGMENTS

The Internet Protocol (IP) encapsulates a Transmission Control Protocol (TCP) SYN segment in the IP packet that initiates a TCP connection. Because the purpose of this packet is to initiate a connection and invoke a SYN/ACK segment in response, the SYN segment typically does not contain any data. Because the IP packet is small, there is no legitimate reason for it to be fragmented. A fragmented SYN packet is anomalous, and as such suspect. To be cautious, block such unknown elements from entering your protected network.

When you enable the SYN Fragment Detection SCREEN option, the NetScreen device detects packets when the IP header indicates that the packet has been fragmented and the SYN flag is set in the TCP header. The NetScreen device records the event in the SCREEN counters list for the ingress interface.

To drop IP packets containing SYN fragments, do either of the following, where the specified security zone is the one from which the packets originate:

**WebUI**

Screening > Screen (Zone: select a zone name): Select **SYN Fragment Protection**, and then click **Apply**.

**CLI**

```
set zone zone screen syn-frag
```
### TCP Header

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>16-bit Source Port Number</td>
<td></td>
</tr>
<tr>
<td>16-bit Destination Port Number</td>
<td></td>
</tr>
<tr>
<td>32-bit Sequence Number</td>
<td></td>
</tr>
<tr>
<td>32-bit Acknowledgement Number</td>
<td></td>
</tr>
</tbody>
</table>

#### IP Header

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td></td>
</tr>
<tr>
<td>Header Length</td>
<td></td>
</tr>
<tr>
<td>Type of Service</td>
<td></td>
</tr>
<tr>
<td>Total Packet Length (in Bytes)</td>
<td></td>
</tr>
<tr>
<td>Identification</td>
<td></td>
</tr>
<tr>
<td>Time to Live (TTL)</td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td></td>
</tr>
<tr>
<td>Source Address</td>
<td></td>
</tr>
<tr>
<td>Destination Address</td>
<td></td>
</tr>
<tr>
<td>Options (if any)</td>
<td></td>
</tr>
<tr>
<td>4-bit Header Length</td>
<td></td>
</tr>
<tr>
<td>Reserved (6 bits)</td>
<td></td>
</tr>
<tr>
<td>URG</td>
<td></td>
</tr>
<tr>
<td>ACK</td>
<td></td>
</tr>
<tr>
<td>PSH</td>
<td></td>
</tr>
<tr>
<td>RST</td>
<td></td>
</tr>
<tr>
<td>SYN</td>
<td></td>
</tr>
<tr>
<td>FIN</td>
<td></td>
</tr>
<tr>
<td>16-bit Window Size</td>
<td></td>
</tr>
<tr>
<td>16-bit Urgent Pointer</td>
<td></td>
</tr>
<tr>
<td>Options (if any)</td>
<td></td>
</tr>
<tr>
<td>Data (if any)</td>
<td></td>
</tr>
</tbody>
</table>

*If the More Fragments flag is set ... or there is a non-zero value is in the Fragment Offset field, ...*

*... and the SYN flag is set ... ... then the NetScreen device drops the packet.*
## Index

### A
- ActiveX controls, blocking 167
- address sweep 8
- aggressive aging 40–42
- ALG 73
- antivirus objects  See AV objects
- antivirus scanning  See AV scanning
- application layer gateway  See ALG
- attack actions 142–151  
  - close 142  
  - close client 142  
  - close server 142  
  - drop 142  
  - drop packet 142  
  - ignore 143  
  - none 143
- attack object database 128–135  
  - auto notification and manual update 128, 132  
  - automatic update 128, 130  
  - changing the default URL 134  
  - immediate update 128, 129  
  - manual update 129, 134
- attack object groups 140  
  - changing severity 140  
  - severity levels 140
- attack objects 125  
  - protocol anomalies 139  
  - stateful signatures 138  
  - TCP stream signatures 164
- attack protection  
  - policy level 5  
  - security zone level 5
- attacks  
  - common objectives 1  
  - detection and defense options 3–5  
  - ICMP flood 59  
  - ICMP fragments 172  
  - IP packet fragments 180
- Land attack 63  
  - large ICMP packets 174  
  - Ping of Death 65  
  - stages of 2  
  - SYN flood 45–51  
  - SYN fragments 182–183  
  - Teardrop 67  
  - UDP flood 61  
  - unknown MAC addresses 51  
  - unknown protocols 178  
  - WinNuke 69
- AV objects 93–101  
  - port number 94  
  - states 93  
  - timeout 94
- AV scanning 76–112  
  - application 102  
  - AV objects 93–101  
  - decompression 85  
  - external AV scanner 90–112  
  - external, CSP resources 95  
  - external, HTTP 92  
  - external, SMTP 91  
  - fail-mode 95  
  - fail-mode threshold 96  
  - HTTP keep-alive 96  
  - HTTP trickling 97  
  - HTTP webmail 80  
  - internal AV scanner 77–89  
  - internal, HTTP 79  
  - internal, POP3 78  
  - internal, SMTP 77  
  - internal, subscription 81  
  - InterScan VirusWall 90  
  - max TCP connections 94  
  - multiple AV objects 106
- content filtering 71–121  
  - Content Scanning Protocol  
    - See CSP
- conventions  
  - CLI vi  
  - illustration ix  
  - names x  
  - WebUI vii
- CSP 90

### D
- DDoS 35  
  - decompression, AV scanning 85
- Deep Inspection 140–163  
  - attack actions 142–151  
  - attack object database 128–135  
  - attack object groups 140  
  - attack objects 125  
  - changing severity 140  
  - context 156  
  - custom attack objects 156  
  - custom services 152–155  
  - custom signatures 157–163  
  - protocol anomalies 139  
  - regular expressions 157–159  
  - stateful signatures 138
- Denial-of-Service  
  - See DoS
- DoS 35–70  
  - firewall 36–44  
  - network 45–63  
  - OS-specific 65–70  
  - session table flood 36  
  - drop-no-rpf-route 23  
  - dynamic packet filtering 3

### E
- evasion 22–33
- exe files, blocking 168
Index

exploits
See attacks

F
fail/pass mode, URL filtering 116
fail-mode 95
  threshold 96
FIN scan 22
FIN without ACK flag 18
fragment reassembly 72–75

H
high-watermark threshold 41
HTTP
  blocking components 167–169
  keep-alive 96
  session timeout 41
  trickling 97

I
ICMP
  fragments 172
  large packets 174
ICMP flood 59
illustration
  conventions ix
InterScan VirusWall 90
IP
  packet fragments 180
IP options 12–14
  attributes 12–14
  incorrectly formatted 176
  loose source route 13, 31–33
  record route 13, 14
  security 13, 14
  source route 31
  stream ID 13, 14
  strict source route 14, 31–33
  timestamp 14
IP spoofing 22–30
  drop-no-rpf-route 23
Layer 2 24, 29
Layer 3 23, 25

J
Java applets, blocking 168

L
Land attack 63
loose source route IP option 13, 31–33
low-watermark threshold 41

M
malicious URL protection 72–75

N
names
  conventions x

P
Ping of Death 65
policies
  context 127
  core section 126
  URL filtering 118
port scan 10
probes
  network 8
  open ports 10
  operating systems 16–20
protocol anomalies 139

R
reconnaissance 7–33
  address sweep 8
  FIN scan 22
  IP options 12
  port scan 10
  SYN and FIN flags set 16
  TCP packet without flags 20
  record route IP option 13, 14
  regular expressions 157–159

S
SCREEN
  address sweep 8
  bad IP options, drop 176
  drop unknown MAC addresses 51
  FIN with no ACK 22
  FIN without ACK flag, drop 18
  ICMP flood 59
  ICMP fragments, block 172
  IP options 12
  IP packet fragments, block 180
  IP spoofing 22–30
  Land attack 63
  large ICMP packets, block 174
  loose source route IP option, detect 33
  Ping of Death 65
  port scan 10
  source route IP option, deny 33
  strict source route IP option, detect 33
  SYN and FIN flags set 16
  SYN flood 45–51
  SYN fragments, detect 182–183
  SYN-ACK-ACK proxy flood 43
  TCP packet without flags, detect 20
  Teardrop 67
  UDP flood 61
  unknown protocols, drop 178
  VLAN and MGT zones 3
  WinNuke attack 69
security IP option 13, 14
services
  custom 152
  session limits 36–40
    destination based 37, 40
    source based 36, 39
  session table flood 36
  session timeout
    HTTP 41
    TCP 41
    UDP 41
stateful inspection 3
stateful signatures 138
  definition 138
stream ID IP option 13, 14
  strict source route IP option 14, 31–33
  SYN and FIN flags set 16
Index

SYN flood 45–51
  alarm threshold 49
  attack 45
  attack threshold 49
  destination threshold 50
  drop unknown MAC addresses 51
  queue size 51
  source threshold 50
  threshold 46
  timeout 51
SYN fragments 182–183
SYN-ACK-ACK proxy flood 43

T
  TCP
    max simultaneous connections 94
    packet without flags 20

  session timeout 41
  stream signatures 164
  Teardrop attack 67
  three-way handshake 45
  timestamp IP option 14
  Transparent mode
    drop unknown MAC addresses 51

U
  UDP
    session timeout 41
    UDP flood 61
    unknown protocols 178
    URL filtering 113–121
      blocked URL message type 117
      communication timeout 116
      device-level activation 117
    fail/pass mode 116
    NetScreen blocked URL message 117
    policy-level application 118
    routing 119
    server status 118
    servers per vsys 115
    Websense server name 116
    Websense server port 116

W
  Websense 113
  WinNuke attack 69

Z
  zip files, blocking 168
  zombie agent 35, 37