



FORTINET™

FortiGate NIDS Guide

FortiGate User Manual Volume 4

Version 2.50 MR2

8 August 2003

© Copyright 2003 Fortinet Inc. All rights reserved.

No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet Inc.

FortiGate NIDS Guide

Version 2.50 MR2

8 August 2003

Trademarks

Products mentioned in this document are trademarks or registered trademarks of their respective holders.

Regulatory Compliance

FCC Class A Part 15 CSA/CUS

For technical support, please visit <http://www.fortinet.com>.

Send information about errors or omissions in this document or any Fortinet technical documentation to techdoc@fortinet.com.

Table of Contents

Overview	5
NIDS Modules.....	5
Detecting intrusions with the NIDS Detection module	5
Preventing intrusions with the NIDS Prevention module	6
Managing messages with the NIDS Response module.....	6
NIDS detection and prevention features	6
Denial of Service (DoS) attacks	6
Reconnaissance	7
Exploits	7
NIDS evasion	7
About this document	8
What's new in Version 2.50	8
Document conventions	9
Fortinet documentation	10
Comments on Fortinet technical documentation.....	10
Customer service and technical support.....	11
Detecting attacks	13
Signature Groups.....	13
Signature Examples.....	15
General configuration steps	18
NIDS general configuration.....	18
Selecting the interfaces to monitor.....	18
Disabling the NIDS.....	18
Configuring checksum verification	19
Managing attack detection signatures	19
Viewing the signature list	20
Disabling attack detection signatures	20
Using signatures to view detailed attack information	21
Updating attack definitions.....	21
Creating user-defined signatures.....	23
Creating user-defined attack detection signatures.....	24
User-defined signature notes.....	25
General configuration steps	25
User-defined attack detection signature syntax.....	25
Syntax conventions.....	26
Complete signature syntax	26
Detailed signature syntax.....	27

Managing user-defined signatures.....	33
Uploading a user-defined signature list.....	33
Downloading a user-defined signature list	34
Preventing attacks	35
General configuration steps	36
Enabling NIDS attack prevention	36
Enabling attack prevention signatures.....	37
Configuring signature threshold values.....	38
Configuring synflood signature values	40
Example: NIDS configuration.....	41
Preventing TCP and UDP attacks.....	41
NIDS messaging.....	45
Managing the attack log.....	45
Logging attack messages to the attack log	45
Viewing attack messages	46
Attack message example	46
Managing alert emails.....	47
Configuring the FortiGate unit to send alert emails.....	47
Enabling the FortiGate unit to send alert emails for intrusions	47
Customizing alert email messages	48
Alert email example	48
Using alert emails to view detailed attack information	48
Reducing the number of NIDS attack log and email messages.....	49

Overview

The FortiGate NIDS is a real-time network intrusion detection sensor that uses attack signature definitions to both detect and prevent a wide variety of suspicious network traffic and direct network-based attacks. Also, whenever an attack occurs, the FortiGate NIDS can record the event in a log plus send an alert email to the system administrator.

NIDS Modules

The NIDS consists of three software modules designed to detect, prevent and respond to attacks. For an overview of the NIDS modules, see:

- [Detecting intrusions with the NIDS Detection module](#)
- [Preventing intrusions with the NIDS Prevention module](#)
- [Managing messages with the NIDS Response module](#)

Detecting intrusions with the NIDS Detection module

The NIDS Detection module detects a wide variety of suspicious network traffic and network-based attacks.

Attack signatures are the core of the FortiGate NIDS Detection module. Signatures are transmission patterns and other codes that indicate that a system might be under attack. Functionally, signatures are similar to virus definitions, with each signature designed to detect a particular type of attack.

The FortiGate NIDS uses over 1,000 attack signatures. To ensure that you have the latest attack signatures, you need to update the attack definitions file periodically. You can configure the FortiGate unit to automatically check for and download updated attack definitions containing the latest signatures, or you can manually download updated attack definitions. For details, see the *FortiGate Installation and Configuration Guide*.

You can also create custom signatures. For more information on creating custom signatures see [“Creating user-defined signatures” on page 23](#). After creating a signature, you can upload it to the FortiGate unit. User-defined signatures should only be configured by IT specialists.

You can enable the FortiGate NIDS to generate attack messages. You can configure the FortiGate unit to record the attack messages in the attack log, and to send the attack messages in alert emails to up to 3 email addresses.

Preventing intrusions with the NIDS Prevention module

The FortiGate unit is capable of doing more than simply detecting attacks—it can also prevent them. The NIDS Prevention module allows you to prevent common TCP, ICMP, UDP, and IP attacks from disrupting network operations. You can enable the NIDS Prevention module to prevent a set of default attacks with default threshold values, and you can enable individual attack signatures and change the threshold values. When the NIDS detects an intrusion which matches a definition, access is denied or packets are dropped thereby avoiding costly network disruptions.

Like the NIDS Detection module, the NIDS Prevention module uses signatures to detect attacks, and it generates attack messages which can be logged or emailed. However, although the NIDS Prevention module and the NIDS Detection module operate similarly, they use unique signatures and generate unique messages.

The signatures listed in the NIDS Prevention module are updated when the FortiGate unit receives a firmware upgrade. New signatures cannot be downloaded from Fortinet or created by users.

Managing messages with the NIDS Response module

Whenever an attack is detected or prevented, the NIDS Response module generates a message which can be added to the attack log or emailed to up to three destinations. System administrators can use this information to respond to threats in a timely fashion.

NIDS detection and prevention features

The NIDS detects and prevents the following types of attacks:

- [Denial of Service \(DoS\) attacks](#)
- [Reconnaissance](#)
- [Exploits](#)
- [NIDS evasion](#)

Denial of Service (DoS) attacks

Denial of Service attacks attempt to deny access to a service or a computer by overloading network links, overloading the CPU, or filling up disks. The attacker is not trying to gain information, but to interfere with access to network resources. The FortiGate NIDS detects the following common DoS attacks:

- Packet floods, including Smurf flood, TCP SYN flood, UDP flood, and ICMP flood
- Incorrectly formed packets, including Ping of Death, Chargen, Tear drop, land, and WinNuke

Reconnaissance

Reconnaissance attacks attempt to gain information about a computer network in preparation for an attempt to break into it. Using the information gained, an attacker can identify and attack specific vulnerabilities. The FortiGate NIDS detects the following common reconnaissance attacks:

- Fingerprinting
- Ping sweeps
- Port scans
- Buffer overflows, including SMTP, FTP and POP3
- Account scans
- OS identification

Exploits

Exploits are attempts to take advantage of features or bugs to gain unauthorized access to a computer or network. The FortiGate NIDS detects the following common exploits:

- Brute Force attack
- CGI Scripts, including Phf, EWS, info2www, TextCounter, GuestBook, Count.cgi, handler, webdist.cgi,php.cgi, files.pl, nph-test-cgi, nph-publish, AnyForm, and FormMail
- Web Server attacks
- Web Browser attacks, including URL, HTTP, HTML, JavaScript, Frames, Java, and ActiveX
- SMTP (SendMail) attack
- IMAP/POP attack
- Buffer overflow
- DNS attacks, including BIND and Cache
- IP spoofing
- Trojan Horse attacks, including BackOrifice 2K, IniKiller, Netbus, NetSpy, Priority, Ripper, Striker, and SubSeven

NIDS evasion

As attackers become more sophisticated, they are developing techniques to evade NIDS systems. The FortiGate NIDS detects the following NIDS evasion techniques:

- Signature spoofing
- Signature encoding
- IP fragmentation
- TCP/UDP disassembly

About this document

This guide contains general configuration steps, web-based manager and CLI procedures, and configuration examples in the following chapters:

- [Detecting attacks](#) describes how to configure the general NIDS settings and how to configure the signature list to enable the FortiGate unit to detect attacks.
- [Creating user-defined signatures](#) describes how you can program your own signatures and add them to the FortiGate unit. After they are added, these signatures can be used to detect attacks.
- [Preventing attacks](#) describes how to use signatures to prevent attacks.
- [NIDS messaging](#) describes how to configure the NIDS to log and email the messages that are generated when an attack occurs.
- The [Glossary](#) defines many of the terms used in this document.

What's new in Version 2.50

The following features are new in Version 2.50.

NIDS attack ID numbers

Each NIDS attack has an ID number that also appears in email alerts and attack log messages generated by the NIDS when the attack is detected. This makes it easier to reference the NIDS attacks that are generating email alerts or attack log messages. See [“Viewing the signature list” on page 20](#).

Signature groups

In the NIDS Detection module, attack signatures are now arranged into groups. When you enable a group, the signatures contained within it will be used to detect a variety of network-based attacks. When you disable a group, the signatures will not detect attacks. You cannot enable or disable individual signatures. See [“Detecting attacks” on page 13](#).

Intrusion prevention

In earlier releases the NIDS could only detect attacks, not prevent them. Now the NIDS can be configured to prevent common TCP, ICMP, UDP, and IP attacks from disrupting network operations. See [“Preventing attacks” on page 35](#).

New CLI commands

The command line interface has been extensively changed for v2.50. Command syntax has been changed to be easier to use and more effective, many command names and keywords have changed, and CLI help has been improved.

Document conventions

This guide uses the following conventions to describe command syntax.

- angle brackets < > to indicate variable keywords

For example:

```
execute restore config <filename_str>
```

You enter `restore config myfile.bak`

<xxx_str> indicates an ASCII string variable.

<xxx_integer> indicates an integer variable.

<xxx_ip> indicates an IP address variable.

<xxx_hex> indicates a hexadecimal variable.

- vertical bar and curly brackets { | } to separate alternative, mutually exclusive required keywords

For example:

```
set system opmode {nat | transparent}
```

You can enter `set system opmode nat` or `set system opmode transparent`

- square brackets [] to indicate that a keyword is optional

For example:

```
get firewall ipmacbinding [dhcpiamac]
```

You can enter `get firewall ipmacbinding` or `get firewall ipmacbinding dhcpiamac`

- a space to separate options that can be entered in any combination and must be separated by spaces

For example:

```
set system interface internal config allowaccess  
    {ping https ssh snmp http telnet}
```

You can enter any of the following:

```
set system interface internal config allowaccess ping
```

```
set system interface internal config allowaccess ping https  
    ssh
```

```
set system interface internal config allowaccess https ping  
    ssh
```

```
set system interface internal config allowaccess snmp
```

Fortinet documentation

Information about FortiGate products is available from the following sources:

- *FortiGate Installation and Configuration Guide*
Describes installation and basic configuration for the FortiGate unit. Also describes how to use FortiGate firewall policies to control traffic flow through the FortiGate unit and how to use firewall policies to apply antivirus protection, web content filtering, and email filtering to HTTP, FTP and email content passing through the FortiGate unit.
- *FortiGate VPN Guide*
Contains in-depth information about FortiGate IPsec VPN using certificates, pre-shared keys and manual keys for encryption. Also contains basic configuration information for the Fortinet Remote VPN Client, detailed configuration information for FortiGate PPTP and L2TP VPN, and VPN configuration examples.
- *FortiGate Content Protection Guide*
Describes how to configure antivirus protection, web content filtering, and email filtering to protect content as it passes through the FortiGate unit.
- *FortiGate NIDS Guide*
Describes how to configure the FortiGate NIDS to detect and protect the FortiGate unit from network-based attacks.
- *FortiGate Logging and Message Reference Guide*
Describes how to configure FortiGate logging and alert email. Also contains the FortiGate log message reference.
- *FortiGate CLI Reference Guide*
Describes the FortiGate CLI and contains a reference to all FortiGate CLI commands.
- FortiGate web-based manager online help
FortiGate online help contains procedures for using the FortiGate web-based manager to configure and manage your FortiGate unit.

Comments on Fortinet technical documentation

You can send information about errors or omissions in this document or any Fortinet technical documentation to techdoc@fortinet.com.

Customer service and technical support

For antivirus and attack definition updates, firmware updates, updated product documentation, technical support information, and other resources, please visit the Fortinet technical support web site at <http://support.fortinet.com>.

You can also register FortiGate Antivirus Firewalls from <http://support.fortinet.com> and modify your registration information at any time.

Fortinet email support is available from the following addresses:

- | | |
|----------------------------------|---|
| amer_support@fortinet.com | For customers in the United States, Canada, Mexico, Latin America and South America. |
| apac_support@fortinet.com | For customers in Japan, Korea, China, Hong Kong, Singapore, Malaysia, all other Asian countries, and Australia. |
| eu_support@fortinet.com | For customers in the United Kingdom, Scandinavia, Mainland Europe, Africa, and the Middle East. |

For information on Fortinet telephone support, see <http://support.fortinet.com>.

When requesting technical support, please provide the following information:

- Your name
- Company name
- Location
- Email address
- Telephone number
- FortiGate unit serial number
- FortiGate model
- FortiGate FortiOS firmware version
- Detailed description of the problem

Detecting attacks

The NIDS Detection module detects a wide variety of suspicious network traffic and network-based attacks.

This chapter describes how to configure the general NIDS settings and the NIDS Detection module Signature List. For the general NIDS settings, you need to select which interfaces will be monitored for network-based attacks. You also need to decide whether to enable checksum verification. Checksum verification tests the integrity of packets received at the monitored interface(s).

For the Signature List, you need to enable and disable signature groups. Each group contains a number of signatures, or attack definitions. When you enable a signature group, the signatures contained within it will be used to detect a variety of network-based attacks. When you disable a group, the signatures will not detect attacks.

Whenever an attack is detected, a NIDS response message is generated. You can add this message to the attack log and email it to up to three destinations. For details, see [“NIDS messaging” on page 45](#).

This chapter describes:

- [Signature Groups](#)
- [Signature Examples](#)
- [General configuration steps](#)
- [NIDS general configuration](#)
- [Managing attack detection signatures](#)
- [Updating attack definitions](#)

Signature Groups

The NIDS Detection module uses over 1,000 signatures. These signatures are arranged into groups, with each group detecting a different type of attack. The groups are listed by name in alphabetical order within the NIDS Detection module. If you choose to view the details for a particular group, you will see the complete list of signatures contained within it.

By default, all groups are enabled. You have the option to disable a group so that the signatures in that group no longer detect attacks. You do not have the option to enable or disable individual signatures.

By disabling a signature group, you can improve system performance and reduce the number of log messages and alert emails that the NIDS generates. For example, the NIDS detects a large number of web server attacks. If you do not provide access to a web server behind your firewall, you might want to disable all web server attack signatures.

Table 1: NIDS signature groups

Signature group name	Description
backdoor	Detect attacks that use back door techniques to bypass system protection mechanisms.
compromised	Detect attacks that violate the system security policy.
ddos	Detect Distributed Denial of Service attacks.
dns	Detect attacks that use DNS.
dos	Detect Denial of Service attacks.
exploit	Detect exploit-based attacks.
finger	Detect attacks that use the Finger protocol.
ftp	Detect attacks that use the FTP protocol.
icmp	Detect attacks that use the ICMP protocol.
imap	Detect attacks that use the IMAP protocol.
misc-traffic	Detect attacks that use miscellaneous and bad traffic techniques.
netbios	Detect attacks that use the NETBIOS protocol.
pop2	Detect attacks that use the POP2 protocol.
pop3	Detect attacks that use the POP3 protocol.
rlogin	Detect attacks that use remote login to gain information about a computer network.
rpc	Detect attacks that use the RPC protocol.
scan	Detect various types of Port Scan and related reconnaissance attacks.
shellcode	Detect attacks involving the shell code of various operating systems.
smtp	Detect attacks that use the SMTP protocol.
snmp	Detect attacks that use the SNMP protocol.
sql	Detect attacks that exploit SQL vulnerabilities. Enable this signature group if the FortiGate unit protects a web server or other application that runs MS-SQL or MS-SQL/SMB.
telnet	Detect attacks that use the Telnet protocol.
tftp	Detect attacks that use the TFTP protocol.

Table 1: NIDS signature groups (Continued)

Signature group name	Description
web-apache web-attacks web-cgi web-client web-coldfusion web-domino web-frontpage web-iis web-misc web-netscape web-php web-tomcat	Detect web-based attacks, including attacks that exploit vulnerabilities in CGI, ColdFusion, FrontPage, IIS, client, and PHP.
portscan	Detect attacks that send client requests to a range of server port addresses on a host, to find an active port and exploit the vulnerabilities of that service.
httpdecode	Detect attacks that use the HTTP protocol.
backorifice	Detect attacks that use the Back Orifice trojan horse to monitor or tamper with computers with MicroSoft Windows operating systems.
rpcdecode	Detect attacks that involve RPC records.
tcpassembly	Detect attacks that use the TCP protocol.
ipdefragmentation	Detect attacks that use fragmented IP packets.
packetformat	Detect attacks that use packets with non-standard header and packet lengths.
user-defined	Detect attacks that are new and that use a user-defined signature. See “Creating user-defined signatures” on page 23 .

Signature Examples

The individual signatures are contained within signature groups. If you view the details for a particular group, you will see the complete list of signatures for that group. Each signature has an ID number, name and revision number.

Examples of some signatures are contained in the following tables:

- [Table 2](#) lists examples of signatures that can detect denial of service (DoS) attacks.
- [Table 3](#) lists examples of signatures that can detect reconnaissance attacks.
- [Table 4](#) lists examples of signatures that can detect exploit attacks.



Note: The values contained in the tables are examples only. To review the complete, current list of signature groups and the signatures contained within them, see an operational FortiGate unit.

Table 2: DoS signature examples

Attack type	Signature group name	Example signature ID	Example signature rule name
Denial of Service	ddos	17563649	DDOS TFN Probe
	dos	917505	DOS Jolt attack
	misc-traffic	101974020	Misc. traffic Source Port 20 to <1024
	ipdefragmentation	7405573	Duplicate first fragments
	packetformat	7602271	UDP Header Truncated
	rpcdecode	6946820	Incomplete RPC segment

Table 3: Reconnaissance signature examples

Attack type	Signature group name	Example signature ID	Example signature rule name
Reconnaissance	finger	101711873	Finger overflow(>128) attempt
	icmp	17956865	ICMP ISS Pinger
	rlogin	102236167	rlogin root
	rpc	286851134	RPC portmap request status
	scan	102367236	SCAN Squid Proxy attempt
	shellcode	1769486	Shell code linux shellcode
	portscan	6553602	(spp_portscan) portscan status
	tcpassembly	7274504	STEALTH ACTIVITY (FIN scan) detection

Table 4: Exploit attack signatures

Attack type	Signature group name	Example signature ID	Example signature rule name
Exploits	backdoor	101318672	Back door subseven 22
	compromised	101384193	Successful gobbles ssh exploit (GOBBLE)
	dns	286064641	Solaris tsig exploit packet
	exploit	101646338	Exploit ssh CRC32 overflow /bin/sh
	ftp	101777411	FTP command STAT with ?
	netbios	102039554	NETBIOS nimda .eml
	rpc	102301722	RPC snmpXdmi overflow attempt
	smtp	102498305	SMTP sendmail 8.6.9 exploit
	sql	102629377	MS-SQL/SMB sp_start_job - program execution
	telnet	102694920	Telnet login incorrect
	tftp	287309825	TFTP GET Admin.dll
	web-attacks	102891521	Web-Attacks ps command attempt
	web-cgi	102957107	Web-CGI bnbform.cgi access
	web-coldfusion	103088129	Web-ColdFusion cfcache.map access
	web-frontpage	103219201	Web-FrontPage rad overflow attempt
	web-iis	103284737	Web-IIS repost.asp access
	web-misc	103350273	Web-Misc. cross site scripting attempt
	httpdecode	6684678	(spp_http_decode) Illegal URL hex encoding
backorifice	6881281	(spo_bo) Back Orifice Traffic detected	

General configuration steps

To configure the NIDS to detect network-based attacks, you must complete two basic procedures. First you must configure the general NIDS settings. Then you must review the signature list and decide which groups you want to enable in order to detect attacks. By default, all signature groups are enabled.

To configure the NIDS to detect attacks:

- 1 Configure the general NIDS settings. After selecting the interfaces that you want the NIDS to monitor, you have the option to enable checksum verification for those interfaces. See [“NIDS general configuration” on page 18](#).
- 2 Select the signature groups that you want NIDS to use to detect network-based attacks. See [“Managing attack detection signatures” on page 19](#).
- 3 Optionally, you can configure the FortiGate unit to automatically check for new versions of the attack definitions. See [“Updating attack definitions” on page 21](#).

NIDS general configuration

To enable the FortiGate NIDS, you must select at least one interface to monitor for network-based attacks. To disable the FortiGate NIDS, you must deselect all monitored interfaces.



Note: A maximum of four interfaces can be monitored. (The FortiGate-50 is limited to one monitored interface.)

Selecting the interfaces to monitor

To select interfaces to monitor for attacks:

- 1 Go to **NIDS > Detection > General**.
- 2 Select the interfaces to monitor for network attacks.
You can select one or more interfaces.
- 3 Select Apply.

Using the CLI:

```
set nids detection interface <name_str> status enable
```

Disabling the NIDS

To de-select interfaces to monitor for attacks:

- 1 Go to **NIDS > Detection > General**.
- 2 Deselect all monitored interfaces.
- 3 Select Apply.

Using the CLI:

```
set nids detection interface <name_str> status disable
```

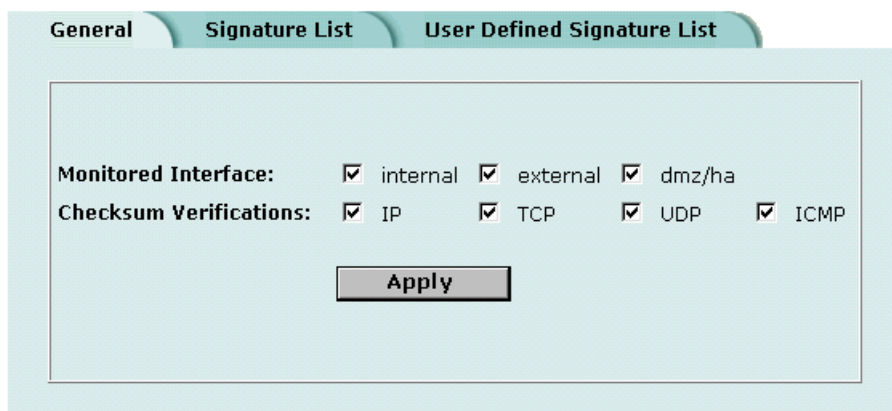
Configuring checksum verification

Checksum verification tests files passing through the FortiGate unit to make sure that they have not been changed in transit. The NIDS can run checksum verification on IP, TCP, UDP, and ICMP traffic. For maximum detection, you can turn on checksum verification for all types of traffic. However, if the FortiGate unit does not need to run checksum verification, you can turn it off for some or all types of traffic to improve system performance. For example, you might not need to run checksum verification if your FortiGate unit is installed behind a router that also does checksum verification.

To configure checksum verification:

- 1 Go to **NIDS > Detection > General**.
- 2 Check the type of traffic on which to run Checksum Verifications.
- 3 Select Apply.

Figure 1: Example NIDS detection configuration for a FortiGate-300 unit



Using the CLI:

```
set nids detection checksum {none | ip,tcp,udp,icmp}
```

Managing attack detection signatures

The NIDS Detection module uses over 1,000 signatures arranged into groups. By default, all groups are enabled.

To optimize system performance, you can disable some groups. If you disable a group, the FortiGate NIDS will no longer use the signatures contained within it to detect intrusion attempts. You cannot enable or disable individual signatures within groups.

Each signature includes an attack ID, a name and a revision number. You can use the ID to view detailed information about the attack that a signature is designed to detect.

- [Viewing the signature list](#)
- [Disabling attack detection signatures](#)
- [Using signatures to view detailed attack information](#)

Viewing the signature list

To display the current list of NIDS signature groups and to view the member signatures of a signature group:

- 1 Go to **NIDS > Detection > Signature List**.
- 2 View the names and status of the signature groups in the list.
The NIDS detects attacks listed in all the signature groups that are checked in the Enable column.



Note: The user-defined signature group is the last item in the signature list. See “[Creating user-defined signatures](#)” on page 23.


- 3 Select View Details  to display the member signatures of a signature group. The Signature Group Members list displays the attack ID, Rule Name, and Revision number for each group member.

Figure 2: Example signature group members list

exploit		
ID	Rule Name	Revision
101646337	gobbles SSH exploit attempt	16
101646338	ssh CRC32 overflow /bin/sh	16
101646339	ssh CRC32 overflow NOOP	16
101646340	ssh CRC32 overflow	16
101646341	x86 linux samba overflow	16
101646342	Solaris x86 nlps overflow attempt	16
101646343	nlps x86 solaris overflow	16
101646344	LPRng overflow	16
101646345	redhat 7.0 lprd overflow	16

Disabling attack detection signatures



By default, all signature groups are enabled. Disabling unnecessary NIDS attack signature groups can improve system performance and reduce the number of log messages and alert emails that the NIDS generates. For example, the NIDS detects a large number of web server attacks. If you do not provide access to a web server behind your firewall, you might want to disable all web server attack signatures.



Note: To save your NIDS attack signature settings, Fortinet recommends that you back up the FortiGate configuration before updating the firmware. You can then restore the saved configuration after the update.

To disable NIDS attack signatures:

- 1 Go to **NIDS > Detection > Signature List**.
- 2 Scroll down the signature list to find the signature group to disable.
Attack ID numbers and rule names in attack log messages and alert email match those in the signature group members list. You can scroll through a signature group members list to locate specific attack signatures by ID number and name.
- 3 Uncheck the Enable check box.
- 4 Select OK.

- 5 Repeat steps 2 to 4 for each NIDS attack signature group that you want to disable.
Select Check All  to enable all NIDS attack signature groups in the signature list.
Select Uncheck All  to disable all NIDS attack signature groups in the signature list.



Note: Attack messages can be recorded in the attack log and emailed to system administrators. See “NIDS messaging” on page 45.


Using the CLI:

```
set nids rule <group_str> status {enable | disable}
```

Using signatures to view detailed attack information

Fortinet provides online information for all NIDS attacks. To view the FortiResponse Attack Analysis web page for an attack listed on the signature list:

To view the Attack Analysis web page for an attack:

- 1 Go to **NIDS > Detection > Signature List**.
- 2 Select View Details  to display the members of a signature group.
Select a signature and copy its attack ID.

- 3 Open a web browser and enter this URL:

```
http://www.fortinet.com/ids/ID<attack-ID>
```

Remember to include the attack ID.

For example, to view the Fortinet Attack Analysis web page for the `ssh CRC32 overflow /bin/sh` attack (ID 101646338), use the following URL:

```
http://www.fortinet.com/ids/ID101646338
```



Note: You can also use alert emails to view detailed information about attacks. For details, see “Using alert emails to view detailed attack information” on page 48.

Updating attack definitions

You can configure the FortiGate unit to automatically check for new versions of the attack definitions. If it finds new versions, the FortiGate unit automatically downloads and installs the updated definitions. You can also update attack definitions manually.

For detailed information about configuring attack definition updates, see the *FortiGate Installation and Configuration Guide*.



Note: Updating the attack definitions only updates attack detection signatures, not attack prevention signatures.

Creating user-defined signatures

Signatures are transmission patterns and other codes that indicate that a system might be under attack.

You can add a user-defined attack signature rule to the FortiGate NIDS to detect attacks not included in the current attack definitions file.

You use the syntax described in this chapter to create user-defined signature rules in a text file. You then upload the text file to the FortiGate unit. The FortiGate unit assigns a unique ID to each rule in the file, and adds the signatures to the User Defined Signature group on the signature groups list.

Once you have created and uploaded a user-defined signature list, you can then download the user-defined signature list from the FortiGate unit to a backup file on the management computer. You can edit or add new signature rules to the user-defined signature list and upload it again to the FortiGate unit.



Note: User-defined signatures are an advanced feature and should only be created and added to the FortiGate unit by IT specialists who are familiar with programming concepts and with network intrusion detection systems.

This chapter describes:

- [Creating user-defined attack detection signatures](#)
- [General configuration steps](#)
- [User-defined attack detection signature syntax](#)
- [Managing user-defined signatures](#)

Creating user-defined attack detection signatures

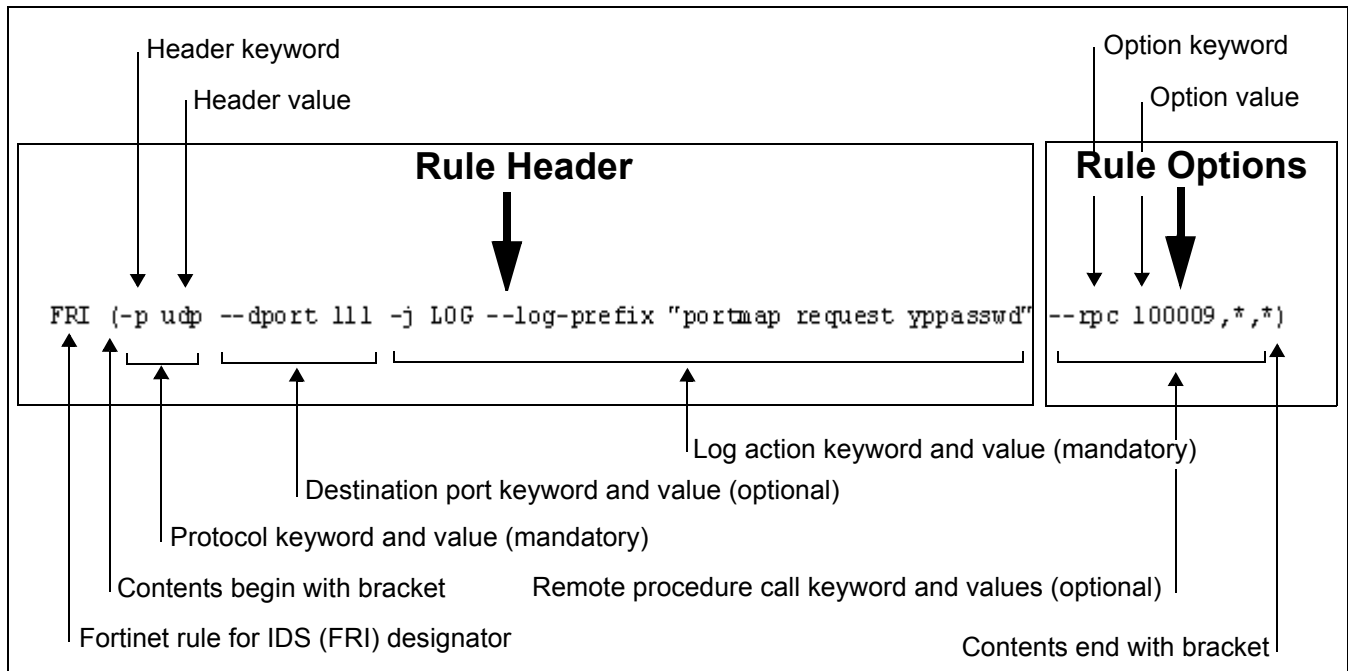
You use a simple, lightweight rules description language to create user-defined signatures.

There are some guidelines to remember when using the rules description language:

- The user-defined signature can itself be looked upon as a rule.
- Each signature must be entered on a single line. The Fortinet rules parser does not know how to read rules on multiple lines.
- A signature consists of two logical segments, the rule header and the rule options. The rule header contains an action (which is always to log the threat and send an alert message) and basic match elements. The basic match elements include the protocol and optional source and destination IP addresses and port numbers. The rule options section contains additional, more specific match elements used to detect threats in packets.
- All of the elements that make up a signature must be true for the threat to be detected and the action (to log the threat and send an alert) to be taken.
- The elements in a single signature form a logical AND statement. The collection of signatures in a signature file form a logical OR statement.

Figure 3 illustrates the various elements of a user-defined signature.

Figure 3: Example user-defined signature



User-defined signature notes

- Each signature must begin with the FRI (Fortinet rule for IDS) designator.
- The contents of the signature (the portion that follows FRI) must be enclosed in brackets ().
- A single hyphen - introduces one-character keywords (for example, -p), and a double hyphen -- introduces full-name keywords (for example, --log-prefix).
- A space separates the signature elements (keyword and value combinations).
- A comma , separates options that can be entered in any combination and must be separated by commas.
- Double quotes " " enclose character strings. A string enclosed in double quotes can include spaces.
- An asterisk (*) matches any character, any number of times. A question mark (?) matches a single character. An exclamation mark (!) inverts the match (matches all values except the values specified).
- As a minimum, each signature must include two elements: protocol and log action. All other elements are optional. For example:

```
FRI (-p <protocol_str> -j LOG --log-prefix "prefix_str")
```
- The traffic direction is from source to destination unless you include the --bi-dir option in the rule header section.

General configuration steps

To configure user-defined signatures:

- 1 Use the syntax described in this guide in order to create a text file containing user-defined signatures. See ["User-defined attack detection signature syntax" on page 25](#).
- 2 Upload the user-defined signature text file from the management computer to the FortiGate unit. See ["Managing user-defined signatures" on page 33](#).

User-defined attack detection signature syntax

This section explains the syntax to use when creating user-defined attack detection signatures. This section is divided into three parts:

- [Syntax conventions](#) explains the conventions used in this chapter.
- [Complete signature syntax](#) provides a complete example of the syntax without any description.
- [Detailed signature syntax](#) provides a detailed description of each syntax element.

Syntax conventions

This guide uses the following conventions to describe the signature syntax:

- Angle brackets < > indicate variable keywords or values.
- A vertical bar and curly brackets { | } separate alternative, mutually exclusive keywords or values.
- Square brackets [] indicate that a keyword or value is optional.

Complete signature syntax

The following syntax contains all of the available elements required to create user-defined signatures.

```
FRI
(
-p <protocol_str>
[-s <source-ip_range/netmask>]
[-d <dest-ip_range/netmask>]
[--sport <start-port_integer:end-port_integer>]
[--dport <start-port_integer:end-port_integer>]
[--bi-dir]
-j LOG --log-prefix "prefix_str"
[--rev <rev_integer>]
[--reference <system_str><id_str>]
[--content "content_str"]
[--offset <offset_integer>]
[--depth <depth_integer>]
[--uri "URI_str"]
[--nc --regex]
[--sameip]
[--fragment <bitvalue_str>]
[-ttl <ttl_integer>]
[-tos <tos_integer> -id <id_integer>]
[-ip-option <ipoption_str>]
[-dsize [<>><size_integer>[<><size_integer>]]]
[--tcp-flags <flag_str>[,<mask_str>]]
[--tcp-seq <sequence_integer>]
[--tcp-ack <ack_integer>]
[--tcp-session <session_integer>]
[--rpc <appl_integer> [,<proc_integer> | *]
[,<version_integer> | *]]
[--icmp-type <type_integer>]
[--icmp-code <code_integer> --icmp-id <id_integer>]
[--icmp-seq <seq_integer>]
)
```

Detailed signature syntax

The following section contains detailed descriptions of all the available elements required to create user-defined attack detection signatures. The tables are divided into two sections: rule header elements and rule options elements.

Rule header elements

In addition to basic match elements (protocol and optional source and destination IP addresses and ports), the rule header contains an action element that defines what the Fortinet rules parser does if it intercepts a packet that matches the signature rule criteria.

- [Table 5 on page 28](#) describes the syntax for the basic match elements. Only the protocol element is mandatory.
- [Table 6 on page 29](#) describes the syntax for the action element. The Fortinet rules parser can perform only one action, which is to log the threat and send an alert email message. In addition to enabling this action, you must specify a message prefix. Optionally, you can add a rule revision number and reference to an external attack classification system ID.

Rule options elements

The rule options elements determine which parts of the packet the Fortinet rules parser inspects to determine if an attack is occurring. These elements are optional; they are not specifically required by any rule, but provide more specific definition of packets to detect.

- [Table 7 on page 30](#) describes the syntax for content pattern elements. These specify how the Fortinet rules parser searches for matches based on a content pattern of text, binary data, or both. Using content pattern options, you can control the following:
 - offset and depth values to restrict matches to certain locations in packets
 - URI pattern matches
 - case sensitivity
 - wildcard pattern matches
 - source and destination address comparison
- [Table 8 on page 31](#) describes the syntax for the IP elements. These specify how the Fortinet rules parser searches for matches for IP header and payload attributes.
- [Table 9 on page 32](#) describes the syntax for the TCP elements. These specify how the Fortinet rules parser searches for matches for TCP flag, sequence, and session information.
- [Table 10 on page 33](#) describes the syntax for the ICMP elements. These specify how the Fortinet rules parser searches for matches for ICMP field information.

Table 5: Protocol, source and destination elements (rule header)

Keyword	Description
-p <protocol_str>	This is a mandatory entry. Match the specified protocol or protocols, separated by commas, for example: -p tcp,udp,icmp,ip.
-s <source-ip_range /netmask>	Match packets based on the source IP address or address range. <ul style="list-style-type: none"> The IP address can be a single address or an address range. For example, 192.168.1.1 matches a single IP address, 192.168.1.0 matches IP addresses on the 192.168.1.0 subnetwork, and 192.168.1.1-192.168.1.10 matches addresses within this range. The netmask can be in the format /255.xxx.xxx.xxx or in CIDR format /yy, where yy is the number of 1s (ones) on the network side of the netmask, for example 192.168.1.1/32. Use ! to invert the match. For example, -s !192.22.33.0/24 matches all packets with source addresses that are not on the 192.22.33.0 subnetwork. The default is to match any source IP address if the -s option is not used.
-d <dest-ip_range/ netmask>	Match packets based on the destination IP address or range. <ul style="list-style-type: none"> The IP address can be a single address or an address range. For example, 192.168.1.1 matches a single IP address, 192.168.1.0 matches IP addresses on the 192.168.1.0 subnetwork, and 192.168.1.1-192.168.1.10 matches addresses within this range. The netmask can be in the format /255.xxx.xxx.xxx or in the CIDR format /yy, where yy is the number of 1s (ones) on the network side of the netmask, for example 192.168.1.1/32. Use ! to invert the match. For example, -s !192.22.0.0/24 matches all packets with destination addresses that are not on the 192.22.33.0 subnetwork. The default is to match any destination IP address if the -d option is not used.
--sport <start- port_integer:end -port_integer>	Match TCP or UDP packets based on the source port or port range. The port number can be a single port or a port range. For example, 22 matches port 22 and 22:80 matches ports 22 to 80. For a port range, if the first port number is omitted, port 0 is assumed; for example, --sport :80 matches ports 0 to 80. If the last port number is omitted, port 65535 is assumed; for example, --sport 22: matches ports 22 to 65535. Use ! to invert the match. For example, --sport !22 matches all ports except port 22 and --sport !22:80 matches all ports outside the range 22 to 80. The default is to match all ports if the -sport option is not used.
--dport <start- port_integer:end -port_integer>	Match TCP or UDP packets based on the destination port or port range. The port number can be a single port or a port range. For example, 22 matches port 22 and 22:80 matches ports 22 to 80. For a port range, if the first port number is omitted, port 0 is assumed; for example, --dport :80 matches ports 0 to 80. If the last port number is omitted, port 65535 is assumed; for example, --dport 22: matches ports 22 to 65535. Use ! to invert the match. For example, --dport !22 matches all ports except port 22 and --dport !22:80 matches all ports outside the range 22 to 80. The default is to match all ports if the -dport option is not used.
--bi-dir	Match traffic between the address and port pairs in either direction. Use this option to analyze both sides of a session, such as a telnet or POP3 session.

Table 6: Log action elements (rule header)

Keyword	Description
-j LOG	Add a message to the IDS log for this rule. This element must appear immediately after the protocol, source, and destination definitions and before the log prefix string, for example: <pre>-p udp --dport 10080:10081 -j LOG "INPUT packets"</pre> See "IDS log messages" in the <i>FortiGate Log Configuration and Reference Guide</i> .
--log-prefix "prefix_str"	Add a prefix to NIDS alert email messages and to the IDS log messages for this rule.
--rev <rev_integer>	Identify the rule revision number in alerts for this rule. Revisions, along with rule IDs, allow signatures and descriptions to be refined and replaced with updated information.
--reference <system_str><id_str>	Include a reference to a rule ID in an external attack identification system, for example, Bugtraq at www.securityfocus.com/bid/ , in alerts for this rule.

Table 7: Content elements (rule options)

Keyword	Description
<code>--content "content_str"</code>	<p>Search for an exact match pattern in the packet payload. The content string can contain mixed binary data (enclosed in pipe () characters and represented as bytecode) and text, for example:</p> <pre>--content " 90C8 C0FF FFFF /bin/sh"</pre> <p>Do not use the characters <code>:</code>, <code>;</code>, <code>\</code>, <code>"</code> in a content string. Use <code>!</code> to match packets that do not contain the content string. For example, <code>content !"GET"</code> matches packets that do not contain the word GET.</p> <p>Use with <code>--nc</code> to remove case sensitivity and <code>--regex</code> if you are including wildcard patterns.</p>
<code>--offset <offset_integer></code>	Specify the number of bytes to offset the starting search position for the content pattern match from the beginning of the packet payload. For example, type <code>3</code> to search for a content pattern starting at byte 4.
<code>--depth <depth_integer></code>	Specify the maximum search depth for a pattern match attempt. This option limits the pattern match function to the possible search region for a given content string. For example, type <code>20</code> to limit the search to 20 bytes.
<code>--uri "URI_str"</code>	<p>Search for a content pattern in the universal resource indicator (URI) portion of a packet. This option allows searches to be matched against only the URI portion of a request, avoiding false alerts from server data files.</p> <p>Use with <code>--nc</code> to remove case sensitivity and <code>--regex</code> if you are including wildcard patterns.</p> <p>Use <code>!</code> to invert the match so that the Fortinet rules parser searches for any URI string except the one that you typed.</p>
<code>--nc</code>	Match the preceding content string and/or URI string without sensitivity to uppercase and lowercase characters.
<code>--regex</code>	Match a wildcard pattern in a content string and/or URI string. If you include the <code>--regex</code> , the Fortinet rules parser interprets an asterisk (*) in the content string or URI string as "any character, any number of times" and a question mark (?) as "any single character".
<code>--sameip</code>	Match if the source IP address is the same as the destination IP address. The message prefix in a rule that uses this option could be <code>"SRC IP = DST IP"</code> .

Table 8: IP elements (rule options)

Keyword	Description
<code>--fragment <bitvalue_str></code>	<p>Match the fragment and reserved bits in the IP header:</p> <ul style="list-style-type: none"> • M: more fragments bit • R: reserved bit • D: don't fragment bit <p>In the bitvalue string, list one or more bits (do not use comma separators). For example, <code>--fragment MR</code> matches the more fragments and reserved bits. Use <code>!</code> to match if the specified bits are not set. For example, <code>--fragment !R</code> matches if the reserved bit is not set.</p>
<code>-ttl <ttl_integer></code>	Match the value of the IP header time-to-live (TTL) field. This option is for detecting traceroute attempts.
<code>-tos <tos_integer></code>	Match the value of the IP header type of service (TOS) field.
<code>-id <id_integer></code>	Match the value of the IP header fragment ID field. Some hacking tools set this field; for example, the value 31337 is popular with some hackers.
<code>-ip-option <ipoption_str></code>	<p>Match the IP option fields:</p> <ul style="list-style-type: none"> • <code>rr</code>: record route • <code>eol</code>: end of list • <code>nop</code>: no op • <code>ts</code>: time stamp • <code>sec</code>: IP security • <code>lsrr</code>: loose source routing • <code>ssrr</code>: strict source routing • <code>satid</code>: stream identifier <p>For example, <code>-ip-option lsrr</code> matches packets with the IP option field set to <code>lsrr</code>. Loose and strict source routing are not often used in Internet applications, so these options are frequently monitored for NIDS attacks. Specify only one option per rule.</p>
<code>-dsize [<>]<size_integer></code> <code>[<<>size_integer]</code>	<p>Match the IP packet payload size against a value or range of values (in bytes). Use the greater than (<code>></code>) and less than (<code><</code>) characters to indicate ranges and limits. For example, if a service has a buffer of a certain size, set this option to watch for attempted buffer overflows. This option tests for a buffer overflow much faster than a payload content check.</p> <p>The <code>></code> and <code><</code> operators are optional. For example, <code>dsize >400<>500</code> returns all packets with 400 to 500 bytes in their payload sections.</p> <p>The match is always false on a stream rebuilt packet.</p>

Table 9: TCP elements (rule options)

Keyword	Description
<pre>--tcp-flags <flag_str>[,<mask_str>]</pre>	<p>Match the TCP flag settings in a packet:</p> <ul style="list-style-type: none"> • F: FIN • S: SYN • R: RST • P: PSH • A: ACK • U: URG) • 2: reserved bit 2 • 1: reserved bit 1 • 0: no TCP flags set <p>You can use the following logical operators:</p> <ul style="list-style-type: none"> • + matches all specified flags plus any others. • * matches any of the specified flags. • ! matches if the specified flags are not set. <p>For example:</p> <ul style="list-style-type: none"> • <code>--tcp-flags SA</code> matches if the SYN and ACK flags are set. • <code>--tcp-flags A+</code> matches if the ACK flag and any others are set. • <code>--tcp-flags !SA</code> matches if the S and A flags are not set. <p>You can specify an option mask to write rules to detect session initiation packets, such as an explicit congestion notification (ECN) packet (a SYN packet with the previously reserved bits 1 and 2 set). For example, the Fortinet rules parser could check for a flags value of <code>S,12</code> if you want to find SYN packets regardless of the values of the reserved bits.</p>
<pre>--tcp-seq <sequence_integer></pre>	Match the TCP static sequence field value.
<pre>--tcp-ack <ack_integer></pre>	Match the TCP header acknowledge field value. Used to detect NMAP TCP pings, which set this field to zero and send a packet with the TCP ACK flag set to determine if a network host is active.
<pre>--rpc <appl_integer> [,<proc_integer> *] [,<version_integer> *]</pre>	Inspect remote procedure call (RPC) requests and matches the application, procedure, and program version. Wildcards are valid for both the procedure and version numbers and are indicated with a *, for example, <code>rpc 100000,*,3</code> .

Table 10: ICMP elements (rule options)

Keyword	Description
<code>--icmp-type <type_integer></code>	Match the ICMP type field value. RFC 792 specifies numeric values, some of which are obsolete. You can set the value out of range to detect invalid ICMP type values that are sometimes used in DoS and flooding attacks.
<code>--icmp-code <code_integer></code>	Match the ICMP code field value, similar to the ICMP type field value. You can set the value out of range to detect suspicious traffic.
<code>--icmp-id <id_integer></code>	Match the ICMP ID in an ICMP ECHO packet. Some covert channel programs use static ICMP fields when they communicate.
<code>--icmp-seq <seq_integer></code>	Match the ICMP sequence field value in an ICMP ECHO packet. Some covert channel programs use static ICMP fields when they communicate.

Managing user-defined signatures

After creating or editing a list of user-defined signatures, you can upload them to the FortiGate unit. The list of user-defined signatures functions as a signature group on the NIDS. As with any signature group, it can be enabled and disabled.

You can also download the user-defined signature list. After editing or adding more signatures to the signature list, you can upload it again to the FortiGate unit.

Uploading a user-defined signature list

To upload the user-defined signature list from the management computer to the FortiGate unit:


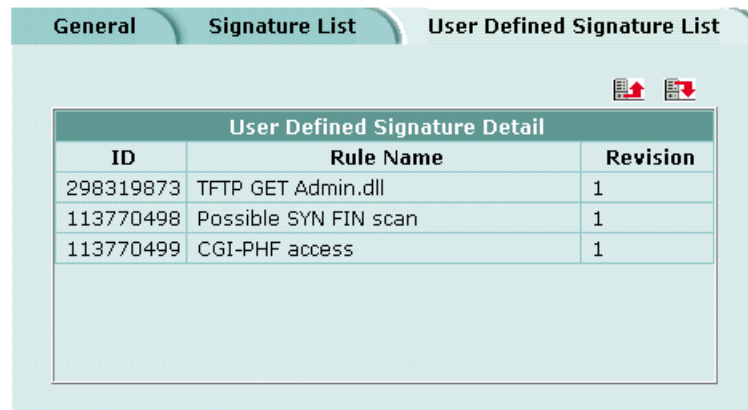
- 1 Go to **NIDS > Detection > User Defined Signature List**.
- 2 Select Upload .
- 3 Type the path and filename of the text file for the user-defined signature list or select Browse and locate the file.
- 4 Select OK to upload the text file for the user-defined signature list.
- 5 Select Return to display the uploaded user-defined signature list.

Figure 4: Example user-defined signature list




User Defined Signature Detail		
ID	Rule Name	Revision
298319873	TFTP GET Admin.dll	1
113770498	Possible SYN FIN scan	1
113770499	CGI-PHF access	1

Using the CLI:

```
execute restore nidsuserdefsig <name_str> <tftp_ip>
```

Downloading a user-defined signature list

To download the user-defined signature list:

- 1 Go to **NIDS > Detection > User Defined Signature List**.
- 2 Select Download .

The FortiGate unit downloads the user-defined signature list to a text file on the management computer. You can specify a location to which to download the text file as well as a name for the text file.
- 3 After editing the signature list, you can upload it again using the procedure [“Managing user-defined signatures” on page 33](#).

Using the CLI:

```
execute backup nidsuserdefsig <name_str> <tftp_ip>
```

Preventing attacks

The NIDS Prevention module contains signatures that are designed to protect your network against attacks. The signatures detect anomalies in the data packets and protocol definitions for ICMP, IP, TCP and UDP. When anomalies are found, the system takes action to prevent damage. In some cases packets are dropped; in other cases network access is blocked.

In addition to being able to enable and disable all signatures, you can modify the threshold value for some signatures. When the threshold is exceeded, the NIDS Prevention module will take action to block the attack. Some signatures are enabled by default.

When the NIDS Prevention module blocks an attack, it generates an attack message which can be logged or emailed.

The NIDS Prevention module operates similarly to the NIDS Detection module. However, the modules use unique signatures and generate unique messages.

The signatures contained in the NIDS Prevention module are updated when the FortiGate unit receives a new software load. New signatures cannot be downloaded from Fortinet or created by users.

This chapter describes:

- [General configuration steps](#)
- [Enabling NIDS attack prevention](#)
- [Enabling attack prevention signatures](#)
- [Configuring signature threshold values](#)
- [Configuring synflood signature values](#)
- [Example: NIDS configuration](#)

General configuration steps

As a minimum, you must enable the NIDS Prevention module. You can then decide which signatures to enable or disable. You can also change the threshold values for some signatures.

To configure the FortiGate unit to prevent network-based attacks:

- 1 Enable the NIDS Prevention module.
The module is disabled by default. See [“Enabling NIDS attack prevention” on page 36](#).
- 2 Enable the NIDS protection signatures that you require to protect your network against specific types of attack.
Some signatures are enabled by default; others must be selected. See [“Enabling attack prevention signatures” on page 37](#).
- 3 Optionally, configure the signature threshold values.
When a threshold value is exceeded, the NIDS Protection module will block the attack being made against your network. See [“Configuring signature threshold values” on page 38](#).
- 4 Optionally, configure the synflood signature values.
In addition to a threshold, the synflood signature has other values that you can configure. See [“Configuring synflood signature values” on page 40](#).



Note: After the FortiGate unit reboots, the NIDS Prevention module and synflood prevention are always disabled.

Enabling NIDS attack prevention

The NIDS Prevention module is disabled by default. You must enable it when you configure a new FortiGate unit, or when you reboot a FortiGate unit.

To enable NIDS attack prevention:

- 1 Go to **NIDS > Prevention**.
- 2 Select Enable in the top left corner.

Using the CLI:

```
set nids prevention status enable
```

Enabling attack prevention signatures

The NIDS Prevention module contains signatures that are designed to protect your network against attacks. Some signatures are enabled by default; others must be enabled.

In addition to enabling and disabling signatures, you can modify them. For some signatures, you can change the threshold value. See [“Configuring signature threshold values” on page 38](#). For SYN flood attack prevention, you can change the threshold value, the queue size and time out value. See [“Configuring synflood signature values” on page 40](#).

To enable attack prevention signatures:




- 1 Go to **NIDS > Prevention**.
- 2 Check the box in the Enable column beside each signature that you want to enable.
- 3 Select Check All  to enable all signatures in the attack prevention signature list.
- 4 Select Uncheck All  to disable all signatures in the attack prevention signature list.
- 5 Select Reset to Default Values  to enable only the default attack prevention signatures and return to the default threshold values.

Figure 5: Example NIDS attack prevention signature list entries



Signature Abbreviation	Summary	Protocol	Enable	Modify
synflood	syn flood attack	TCP	<input type="checkbox"/>	
portscan	port scan attack	TCP	<input checked="" type="checkbox"/>	
synfrag	syn fragment attack	TCP	<input checked="" type="checkbox"/>	
synfin	syn with fin attack	TCP	<input checked="" type="checkbox"/>	
noflag	tcp with no flag attack	TCP	<input checked="" type="checkbox"/>	
finnoack	fin without ack attack	TCP	<input checked="" type="checkbox"/>	
srcsession	source session limit	TCP	<input type="checkbox"/>	
winnuke	winnuke attack	TCP	<input checked="" type="checkbox"/>	
land	top land attack	TCP	<input checked="" type="checkbox"/>	
ftpovfl	ftp buffer overflow attack	TCP	<input checked="" type="checkbox"/>	
smtpovfl	smtp buffer overflow attack	TCP	<input checked="" type="checkbox"/>	
pop3ovfl	pop3 buffer overflow attack	TCP	<input checked="" type="checkbox"/>	
url	invalid url attack	TCP	<input checked="" type="checkbox"/>	
udpflood	udp flood attack	UDP	<input type="checkbox"/>	
udpland	udp land attack	UDP	<input checked="" type="checkbox"/>	
udpsrcsession	udp source session limit	UDP	<input type="checkbox"/>	
icmpflood	icmp flood attack	ICMP	<input checked="" type="checkbox"/>	
icmpfrag	icmp fragment attack	ICMP	<input type="checkbox"/>	
icmpdeath	ping of death attack	ICMP	<input checked="" type="checkbox"/>	
icmplarge	large icmp packet attack	ICMP	<input checked="" type="checkbox"/>	
icmpsweep	icmp sweep attack	ICMP	<input checked="" type="checkbox"/>	
icmsrcsession	icmp source session limit	ICMP	<input type="checkbox"/>	
icmpland	icmp land attack	ICMP	<input checked="" type="checkbox"/>	
iprr	ip record routing	IP	<input type="checkbox"/>	
ipssrr	ip strict source record routing	IP	<input type="checkbox"/>	



Note: Attack messages can be recorded in the attack log and emailed to system administrators. See [“NIDS messaging” on page 45](#).

Using the CLI:

```
set nids prevention <protocol_str> <attack_str> status
{enable | disable}

set nids prevention reset
```

Configuring signature threshold values

You can change the default threshold values for the attack prevention signatures listed in [Table 11](#). The threshold depends on the type of attack. For flooding attacks, the threshold is the maximum number of packets received per second. For overflow attacks, the threshold is the buffer size for the command. For large ICMP attacks, the threshold is the ICMP packet size limit to pass through.

For example, setting the icmpflood signature threshold to 500 will allow 500 echo requests from a source address, to which the system sends echo replies. If the number of requests is 501 or higher, the FortiGate unit will block the attacker to eliminate disruption of system operations.

If you enter a threshold value of 0 or a number out of the allowable range, the FortiGate unit uses the default value.

Table 11: Attack prevention signatures with threshold values

Signature abbreviation	Signature name	Threshold value units	Default threshold value	Minimum threshold value	Maximum threshold value
synflood	TCP Synflood	Maximum number of SYN segments received per second	200	30	3000
portscan	TCP Port Scan	Maximum number of SYN segments received per second	128	10	256
srcsession	TCP Source Session	Total number of TCP sessions initiated from the same source	2048	128	10240
ftpovfl	FTP Overflow	Maximum buffer size for an FTP command (bytes)	256	128	1024
smtpovfl	SMTP Overflow	Maximum buffer size for an SMTP command (bytes)	512	128	1024
pop3ovfl	TCP POP3 Overflow	Maximum buffer size for a POP3 command (bytes)	512	128	1024

Table 11: Attack prevention signatures with threshold values (Continued)

Signature abbreviation	Signature name	Threshold value units	Default threshold value	Minimum threshold value	Maximum threshold value
udpflood	UDP Flood	Maximum number of UDP packets received from the same source or sent to the same destination per second	2048	512	102400
udpsrcsession	UDP Over Limit Session	Total number of UDP sessions initiated from the same source	1024	512	102400
icmpflood	ICMP Flood	Maximum number of UDP packets received from the same source or sent to the same destination per second	256	128	102400
icmpsrcsession	ICMP Over Limit Session	Total number of ICMP sessions initiated from the same source	128	64	2048
icmpsweep	ICMP Sweep	Maximum number of ICMP packets received from the same source per second	32	16	2048
icmplarge	ICMP Large	Maximum ICMP packet size (bytes)	32000	1024	64000

To set Prevention signature threshold values:



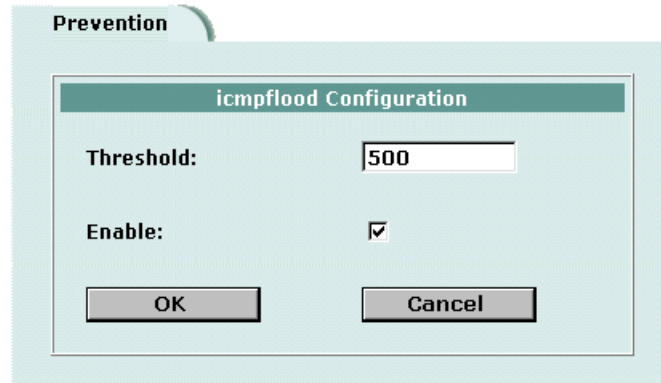
- 1 Go to **NIDS > Prevention**.
- 2 Select Modify  beside the signature for which you want to set the Threshold value. Signatures that do not have threshold values do not have Modify  icons.
- 3 Type the Threshold value.
- 4 Select the Enable check box.
- 5 Select OK.

Figure 6: Example signature configuration

**Using the CLI:**

```
set nids prevention <protocol_str> <attack_str> status {enable
| disable}

set nids prevention <protocol_str> <attack_str> threshold
<value_integer>
```


Configuring synflood signature values

With SYN flood, the attacker sends TCP connection requests to the target with invalid source addresses. The target responds to the requests, but because the source addresses are invalid, never receives a reply. As a result, the connection table on the target fills up and further connections are refused.

To prevent SYN flood attacks, the FortiGate unit monitors the number of packets it receives with SYN flags requesting new connections. When the number of packets from a single source exceeds the threshold value, the FortiGate unit begins functioning as a proxy; it responds to the connection requests in place of the target. If the FortiGate unit does not receive a response from the source within the time out limit, then it knows that it is dealing with an attacker and blocks the connection.

Value	Description	Minimum value	Maximum value	Default value
Threshold	Number of SYN requests sent to a destination host or server per second. If the SYN requests are being sent to all ports on the destination, as opposed to just one port, the threshold quadruples (4 x).	30	3000	200
Queue Size	Maximum number of proxied connections that the FortiGate unit handles. The FortiGate unit discards additional proxy requests.	10	10240	1024
Timeout	Number of seconds for the SYN cookie to keep a proxied connection alive. This value limits the size of the proxy connection table.	3	60	15

To configure synflood signature values:

- 1 Go to **NIDS > Prevention**.
- 2 Select Modify  for the synflood signature.
- 3 Type the Threshold value.
- 4 Type the Queue Size.
- 5 Type the Timeout value.
- 6 Select the Enable check box.
Alternatively, select the synflood Enable check box in the Prevention signature list.
- 7 Select OK.

Using the CLI:

```
set nids prevention tcp synflood status enable
set nids prevention tcp synflood threshold <threshold_integer>
set nids prevention tcp synflood timeout <timeout_integer>
set nids prevention tcp synflood queue_size <queue-size_integer>
```

Example: NIDS configuration


Preventing TCP and UDP attacks

Company A has just experienced a TCP SYN flood attack and has been notified about similar TCP and UDP attacks occurring against other companies. The administrator wants to prevent these types of attacks from disrupting network operations.

General configuration steps

- 1 Enable the NIDS for the external interface.
- 2 Configure checksum verification for TCP and UDP.
- 3 Enable the NIDS Prevention module.
 - Enable and configure the TCP and UDP signatures for which you want the NIDS Prevention module to prevent attacks.
 - Change the default values for the synflood signature and accept the default threshold values for the remaining signatures.
- 4 Configure the NIDS to monitor the traffic received by the monitored interface and accepted by firewall policies.
- 5 Configure the NIDS to record a detailed message about each attack.

Web-based manager configuration steps

- 1 Go to **NIDS > Detection > General**.
 - Monitored Interface: external
 - Checksum Verifications: TCP, UDP
 - Select Apply.
- 1 Go to **NIDS > Prevention**.
 - Select Enable Prevention in the top left corner.
- 2 Select Modify  for the synflood signature.
 - Threshold: 50 (SYN/second)
 - Queue Size: 500 (proxied connections)
 - Timeout: 30 (seconds)
 - Select Enable
 - Select OK.
- 3 Select the Enable check box for the synfin signature.
- 4 Repeat step 3 for each of the following signatures: noflag, finnoack, udpflood
- 5 Go to **Log&Report > Log Setting**.
 - Select Config Policy for the log locations you have set.
 - Select Attack Log.
 - Select Attack Prevention.
 - Select OK.

CLI configuration steps

- 1 Enable the NIDS for the external interface.

```
set nids detection interface external status enable
```
- 2 Enable checksum verification for TCP and UDP.

```
set nids detection checksum tcp,udp
```
- 3 Enable the NIDS Prevention module.

```
set nids prevention status enable
```
- 4 Configure the synflood signature.

```
set nids prevention tcp synflood status enable
set nids prevention tcp synflood threshold 50
set nids prevention tcp synflood queue_size 500
set nids prevention tcp synflood timeout 30
```
- 5 Enable the following signatures: noflag, finnoack, udpflood.

```
set nids prevention tcp noflag status enable
set nids prevention tcp finnoack status enable
set nids prevention udp udpflood status enable
```
- 6 Log the attack messages to the attack log.

```
set log policy destination {syslog | webtrends | local | memory  
| console} ids status enable category prevention
```


NIDS messaging

Whenever the NIDS detects or prevents an attack, it generates an attack message. You can configure the system to add the message to the attack log and to send an alert email to up to three destinations. System administrators can use this information to respond to the threat in a timely fashion.



Note: In some cases, the NIDS will generate multiple NIDS response messages for the same event. For example, if the detection signature and the prevention signature are both enabled for port scan, and a port scan attack occurs, two messages will be generated. You can distinguish between the messages by their unique ID numbers.

This section includes the following topics:

- [Managing the attack log](#)
- [Managing alert emails](#)

Managing the attack log

You can configure the NIDS to log an attack message whenever it detects or prevent an attack.

This section includes the following topics:

- [Logging attack messages to the attack log](#)
- [Viewing attack messages](#)
- [Attack message example](#)

Logging attack messages to the attack log

To log attack messages to the attack log:

- 1 Go to **Log&Report > Log Setting**.
- 2 Select Config Policy for the log locations you have set.

Possible log locations:

- a computer running a syslog server,
- a computer running a WebTrends firewall reporting server,
- the FortiGate hard disk (if the unit has a hard disk),
- the FortiGate memory (if the unit does not have a hard disk).

- 3 Select Attack Log.
- 4 Select Attack Detection and Attack Prevention.

- 5 Select OK.



Note: For information about log message content and formats, and about log locations, see the *Logging Configuration and Reference Guide*.


Using the CLI:

```
set log policy destination {syslog | webtrends | local | memory  
| console} ids status {enable | disable} category <detection |  
prevention | none>
```

Viewing attack messages

Use this procedure to view attack messages that have been logged to memory or to the hard drive.

To view attack messages:

- 1 Go to **Log&Report > Logging**.
- 2 Select **Attack Log**.
 - If the attack messages have been logged to memory, a list of messages displays.
 - If the attack messages have been logged to the hard drive, a list of log files displays.
- 3 Scroll through the list, or use the navigational tools to search for individual messages or log files. To view the messages contained in a log file, select View .



Note: For information about log message content and formats, and about log locations, see the *Logging Configuration and Reference Guide*.

Using the CLI:

```
get log elog
```

Attack message example

Each attack message includes the date and time of the attack, the log ID, the attack type (IDS), the attack sub-type (detection or prevention), the source and destination IP addresses of the attack, the interface where the attack occurred, the service, and the message sent in alert emails. The message consists of the attack name and a URL. The URL links to a FortiResponse Attack Analysis web page that provides detailed information about the attack.

An example attack message contains the following information:

```
2003-07-24 10:44:18 log_id=0400000000 type=ids  
subtype=detection pri=alert attack_id=17956868  
src=192.168.1.254 dst=192.168.1.10 icmp_type=0x05 cmp_code=0x01  
interface=port1 status=detected proto=001 service=icmp  
msg="icmp: redirect host[Reference: http://www.fortinet.com/  
ids/ID17956868]"
```

Managing alert emails

Attack messages that have been logged to the attack log can be used to generate alert emails.

This section includes the following topics:

- [Configuring the FortiGate unit to send alert emails](#)
- [Enabling the FortiGate unit to send alert emails for intrusions](#)
- [Customizing alert email messages](#)
- [Alert email example](#)
- [Using alert emails to view detailed attack information](#)

Configuring the FortiGate unit to send alert emails

This procedure involves configuring the email settings on the FortiGate unit. The settings include the SMTP server name and user address, plus the email addresses for up to three system administrators.

To configure the FortiGate unit to send alert emails:

- 1** Go to **System > Network > DNS**.
- 2** If they have not already been added, add the primary and secondary DNS server addresses provided to you by your ISP.
Because the FortiGate unit uses the SMTP server name to connect to the mail server, it must be able to look up this name on your DNS server.
- 3** Select Apply.
- 4** Go to **Log&Report > Alert Mail > Configuration**.
- 5** Enable Authentication if a password is required to use the SMTP server.
- 6** In the SMTP Server field, enter the name of the SMTP server to which the FortiGate unit should send email.
The SMTP server can be located on any network connected to the FortiGate unit.
- 7** In the SMTP User field, enter a valid email address in the format user@domain.com. This address appears in the From header of the alert email.
- 8** Add the Password if the SMTP server requires it.
- 9** Enter up to three destination email addresses in the Email To fields.
These are the actual email addresses that the FortiGate unit sends alert emails to.
- 10** Select Apply to save the alert email settings.

Using the CLI:

```
set alertemail configuration auth {enable | disable} server  
<smtp-server_str> user <smtp-user_str> passwd <password_str>  
mailto {<email1_str> [<email2_str> [<email3_str>]] | none}
```

Enabling the FortiGate unit to send alert emails for intrusions

By completing this procedure, you enable the FortiGate unit to send an alert email when the NIDS detects or prevents an intrusion.

To enable alert email:

- 1 Go to **Log&Report > Alert Mail > Categories**.
- 2 Select Enable alert email for intrusions.

Whenever the NIDS detects or prevents an intrusion, the FortiGate unit will send an alert email to notify the system administrator.

- 3 Select Apply.


Using the CLI:

```
set alertemail setting option <intrusions | none>
```

Customizing alert email messages

You can customize the email message that is sent when the NIDS detects or prevents an intrusion.

To customize alert email messages:

- 1 Go to **System > Config > Replacement Messages**.
- 2 Select Modify  for:

Service	Name	Description
alert mail	intrusion message	Alert email for NIDS events

Default message: `The following intrusion was observed`

You can change the message as required. Messages can be in plain text or can include HTML coding.

- 3 Select OK to save your changes.

Alert email example

The alert email is based on the attack message. As a minimum, the alert email contains an attack name and a URL. The URL links to a FortiResponse Attack Analysis web page that provides detailed information about the attack.

An example alert email contains the following information:

```
The following intrusion was observed: web-misc: webdav search
request[Reference: http://www.fortinet.com/ids/ID103350288]
Interface-port1: TCP 192.168.5.37:46790 -> 192.168.5.39:80.
```

Using alert emails to view detailed attack information

Each alert email contains a URL that links to a FortiResponse Attack Analysis web page. The web page includes a description of the attack, the potential impact of the attack, the vulnerabilities that the attack attempts to exploit, and links to additional information.

To view the Attack Analysis web page for an attack:

- 1 Copy the Attack Analysis web page URL from an alert email.

For example:

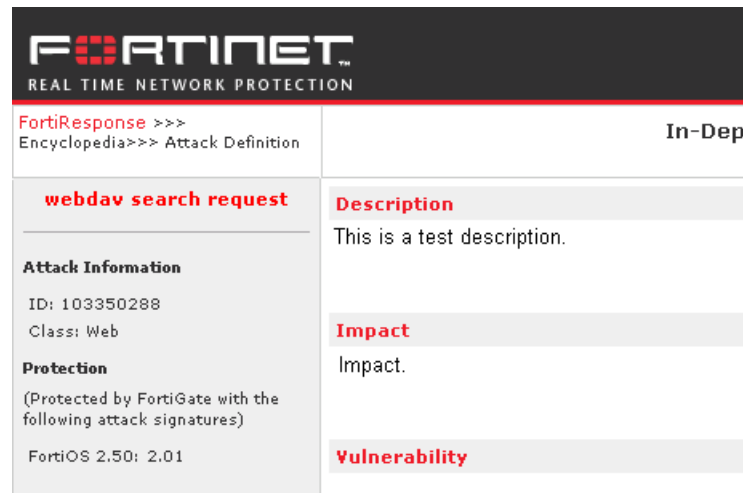
The following intrusion was observed: web-misc: webdav search request[Reference: <http://www.fortinet.com/ids/ID103350288>] Interface-port1: TCP 192.168.5.37:46790 -> 192.168.5.39:80.

- 2 Paste the Attack Analysis web page URL into a web browser:

For example:

<http://www.fortinet.com/ids/ID103350288>

Figure 7: Example FortiResponse Attack Analysis web page



The screenshot shows the FortiResponse interface. At the top is the Fortinet logo with the tagline 'REAL TIME NETWORK PROTECTION'. Below the logo, the breadcrumb path is 'FortiResponse >>> Encyclopedia>>> Attack Definition' and 'In-Dep' is visible on the right. The main content area is titled 'webdav search request' and is divided into two columns. The left column contains 'Attack Information' (ID: 103350288, Class: Web) and 'Protection' (Protected by FortiGate with the following attack signatures: FortiOS 2.50: 2.01). The right column contains 'Description' (This is a test description.), 'Impact' (Impact.), and 'Vulnerability'.



Note: You can also use the NIDS Detection module to view detailed information about attacks. For details, see [“Using signatures to view detailed attack information”](#) on page 21.

Reducing the number of NIDS attack log and email messages

Intrusion attempts may generate an excessive number of attack messages. To help you distinguish real warnings from false alarms, the FortiGate unit provides methods to reduce the number of unnecessary messages. Based on the frequency that messages are generated, the FortiGate unit will automatically delete duplicates. If you determine that you are still receiving an excessive number of unnecessary messages, you can manually disable message generation for signature groups.

Automatic message reduction

The content of the attack log and alert email messages that the NIDS produces includes the ID number and name of the attack that generated the message. The attack ID number and name in the message are identical to the ID number and rule name that appear in the NIDS Detection module on the Signature Group Members list.

The FortiGate unit uses an alert email queue in which each new message is compared with the previous messages. If the new message is not a duplicate, the FortiGate unit sends it immediately and puts a copy in the queue. If the new message is a duplicate, the FortiGate unit deletes it and increases an internal counter for the number of message copies in the queue.

The FortiGate unit holds duplicate alert email messages for 60 seconds. If a duplicate message has been in the queue for more than 60 seconds, the FortiGate unit deletes the message and increases the copy number. If the copy number is greater than 1, the FortiGate unit sends a summary email that includes “Repeated x times” in the subject header, the statement “The following email has been repeated x times in the last y seconds”, and the original message.

Manual message reduction

If you want to reduce the number of messages that the NIDS generates, you can review the content of attack log messages and alert email. If a large number of the messages are nuisance alerts (for example, web attacks when you are not running a web server), you can disable the signature group for that attack type. Use the ID number in the attack log or alert email to locate the attack in the signature group list. See [“Managing attack detection signatures” on page 19](#).

Glossary

Connection: A link between machines, applications, processes, and so on that can be logical, physical, or both.

DMZ, Demilitarized Zone: Used to host Internet services without allowing unauthorized access to an internal (private) network. Typically, the DMZ contains servers accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (email) servers and DNS servers.

DMZ interface: The FortiGate interface that is connected to a DMZ network.

DNS, Domain Name Service: A service that converts symbolic node names to IP addresses.

Ethernet: A local-area network (LAN) architecture that uses a bus or star topology and supports data transfer rates of 10 Mbps. Ethernet is one of the most widely implemented LAN standards. A newer version of Ethernet, called 100 Base-T (or Fast Ethernet), supports data transfer rates of 100 Mbps. And the newest version, Gigabit Ethernet, supports data rates of 1 gigabit (1,000 megabits) per second.

External interface: The FortiGate interface that is connected to the Internet.

FTP, File transfer Protocol: An application and TCP/IP protocol used to upload or download files.

Gateway: A combination of hardware and software that links different networks. Gateways between TCP/IP networks, for example, can link different subnetworks.

HTTP, Hyper Text Transfer Protocol: The protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

HTTPS: The SSL protocol for transmitting private documents over the Internet using a Web browser.

Internal interface: The FortiGate interface that is connected to an internal (private) network.

Internet: A collection of networks connected together that span the entire globe using the NFSNET as their backbone. As a generic term, it refers to any collection of interdependent networks.

ICMP, Internet Control Message Protocol: Part of the Internet Protocol (IP) that allows for the generation of error messages, test packets, and information messages relating to IP. This is the protocol used by the ping function when sending ICMP Echo Requests to a network host.

IKE, Internet Key Exchange: A method of automatically exchanging authentication and encryption keys between two secure servers.

IMAP, Internet Message Access Protocol: An Internet email protocol that allows access to your email from any IMAP compatible browser. With IMAP, your mail resides on the server.

IP, Internet Protocol: The component of TCP/IP that handles routing.

IP Address: An identifier for a computer or device on a TCP/IP network. An IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255.

L2TP, Layer Two (2) Tunneling Protocol: An extension to the PPTP protocol that enables ISPs to operate Virtual Private Networks (VPNs). L2TP merges PPTP from Microsoft and L2F from Cisco Systems. To create an L2TP VPN, your ISP's routers must support L2TP.

IPSec, Internet Protocol Security: A set of protocols that support secure exchange of packets at the IP layer. IPSec is most often used to support VPNs.

LAN, Local Area Network: A computer network that spans a relatively small area. Most LANs connect workstations and personal computers. Each computer on a LAN is able to access data and devices anywhere on the LAN. This means that many users can share data as well as physical resources such as printers.

MAC address, Media Access Control address: A hardware address that uniquely identifies each node of a network.

MIB, Management Information Base: A database of objects that can be monitored by an SNMP network manager.

Modem: A device that converts digital signals into analog signals and back again for transmission over telephone lines.

MTU, Maximum Transmission Unit: The largest physical packet size, measured in bytes, that a network can transmit. Any packets larger than the MTU are divided into smaller packets before being sent. Ideally, you want the MTU your network produces to be the same as the smallest MTU of all the networks between your machine and a message's final destination. If your messages are larger than one of the intervening MTUs, they get broken up (fragmented), which slows down transmission speeds.

Netmask: Also called subnet mask. A set of rules for omitting parts of a complete IP address to reach a target destination without using a broadcast message. It can indicate a subnetwork portion of a larger network in TCP/IP. Sometimes referred to as an Address Mask.

NTP, Network Time Protocol: Used to synchronize the time of a computer to an NTP server. NTP provides accuracies to within tens of milliseconds across the Internet relative to Coordinated Universal Time (UTC).

Packet: A piece of a message transmitted over a packet-switching network. One of the key features of a packet is that it contains the destination address in addition to the data. In IP networks, packets are often called datagrams.

Ping, Packet Internet Grouper: A utility used to determine whether a specific IP address is accessible. It works by sending a packet to the specified address and waiting for a reply.

POP3, Post Office Protocol: A protocol used to transfer e-mail from a mail server to a mail client across the Internet. Most e-mail clients use POP.

PPP, Point-to-Point Protocol: A TCP/IP protocol that provides host-to-network and router-to-router connections.

PPTP, Point-to-Point Tunneling Protocol: A Windows-based technology for creating VPNs. PPTP is supported by Windows 98, 2000, and XP. To create a PPTP VPN, your ISP's routers must support PPTP.

Port: In TCP/IP and UDP networks, a port is an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.

Protocol: An agreed-upon format for transmitting data between two devices. The protocol determines the type of error checking to be used, the data compression method (if any), how the sending device indicates that it has finished sending a message, and how the receiving device indicates that it has received a message.

RADIUS, Remote Authentication Dial-In User Service: An authentication and accounting system used by many Internet Service Providers (ISPs). When users dial into an ISP they enter a user name and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system.

Router: A device that connects LANs into an internal network and routes traffic between them.

Routing: The process of determining a path to use to send data to its destination.

Routing table: A list of valid paths through which data can be transmitted.

Server: An application that answers requests from other devices (clients). Used as a generic term for any device that provides services to the rest of the network such as printing, high capacity storage, and network access.

SMTP, Simple Mail Transfer Protocol: In TCP/IP networks, this is an application for providing mail delivery services.

SNMP, Simple Network Management Protocol: A set of protocols for managing networks. SNMP works by sending messages to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

SSH, Secure shell: A secure Telnet replacement that you can use to log into another computer over a network and run commands. SSH provides strong secure authentication and secure communications over insecure channels.

Subnet: A portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. For example, all devices with IP addresses that start with 100.100.100. would be part of the same subnet. Dividing a network into subnets is useful for both security and performance reasons. IP networks are divided using a subnet mask.

Subnet Address: The part of the IP address that identifies the subnetwork.

TCP, Transmission Control Protocol: One of the main protocols in TCP/IP networks. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

UDP, User Datagram Protocol: A connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP, UDP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It is used primarily for broadcasting messages over a network.

VPN, Virtual Private Network: A network that links private networks over the Internet. VPNs use encryption and other security mechanisms to ensure that only authorized users can access the network and that data cannot be intercepted.

Virus: A computer program that attaches itself to other programs, spreading itself through computers or networks by this mechanism usually with harmful intent.

Worm: A program or algorithm that replicates itself over a computer network, usually through email, and performs malicious actions, such as using up the computer's resources and possibly shutting the system down.

Index

A

- alert email
 - configuring 47
 - content of messages 49
 - customizing 48
 - enabling 47
 - reducing messages 49
- attack definitions
 - updating 21
- attack detection
 - checksum verification 19
 - disabling the NIDS 18
 - enabling and disabling signatures 20
 - general configuration steps 18
 - introduction 5
 - overview 13
 - selecting signature groups 19
 - signature examples 15
 - signature groups 13
 - updating attack definitions 21
 - viewing the signature list 20
- attack log
 - content of messages 49
 - enabling 45
 - reducing messages 49
- attack prevention
 - configuring signature threshold values 38
 - configuring synflood signature values 40
 - enabling NIDS attack prevention 36
 - enabling prevention signatures 37
 - general configuration steps 36
 - introduction 6
 - overview 35
- attack types
 - Denial of Service (DoS) 6
 - evasion 7
 - exploits 7
 - NIDS evasion 7
 - reconnaissance 7

C

- checksum verification
 - configuring 19
- customer service 11

D

- Denial of Service (DoS) attacks 6
- disabling NIDS 18

E

- evasion attacks 7
- exploit attacks 7

F

- Fortinet customer service 11

G

- general configuration 18

H

- HTTPS 51

I

- ICMP 51
 - configuring checksum verification 19
- IKE 51
- IMAP 51
- Internet key exchange 51
- IP
 - configuring checksum verification 19
- IPSec 51

L

- L2TP 51

M

- MAC address 52

messages

- configuring alert email 47
- customizing alert email 48
- enabling alert email 47
- introduction 6
- logging NIDS response messages 45
- overview 45
- reducing alert email 20, 49
- reducing log messages 20, 49

MTU size

- definition 52

N

NIDS

- general configuration 18
- NIDS Detection module 5, 13
- NIDS evasion attacks 7
- NIDS features 6
- NIDS Prevention module 6, 35
- NIDS Response module 6
- NIDS software modules 5
- NTP 52

P

- POP3 52
- PPTP 52

R

RADIUS

- definition 52
- reconnaissance attacks 7
- routing 52
- routing table 52

S

service

- service name 16, 17

signature groups 13

signature threshold values 38

SMTP 47

- definition 52

SNMP

- definition 52

SSH 53

SSL 51

subnet

- definition 53

subnet address

- definition 53

synflood signature values 40

T

TCP

- configuring checksum verification 19

technical support 11

U

UDP

- configuring checksum verification 19

user-defined signatures

- complete signature syntax 26
- conventions 26
- creating 24
- detailed signature syntax 27
- downloading a user-defined signature list 34
- general configuration steps 25
- managing 33
- notes 25
- overview 23
- syntax 25
- uploading a user-defined signature list 33

W

What's new in this release 8