CCNP Security IPS 642-627 Quick Reference

Gary Halleen

Cisco Press

Chapter 3
Cisco Intrusion Detection and Prevention Signatures

Configuring Signatures and Alerts

Signatures are the foundation of an intrusion prevention system (IPS). This chapter shows you how to tune and configure signatures to control how the sensor behaves. There are default signatures, tuned signatures (default signatures that you have modified), and your own custom signatures. Most built-in signatures generate an alert when fired.

Event actions can be defined either per signature, or as part of an event action override policy. When possible, it is simpler to manage using the policy.

Frequent configuration tasks include enabling or disabling signatures and defining the actions that should occur upon firing.

To access the signatures for configuration, choose **Configuration, Signature Definitions, Signature Configuration**.

Here are the possible actions that you can configure in response to a signature firing:

- **Deny Attacker Inline** terminates the current packet and future packets from the attacker address for a specified period of time. If the attack uses TCP traffic, it also sends a TCP Reset packet to the host under attack. This is the most severe of the deny actions.
- **Deny Attacker Service Pair Inline** terminates the current packet and future packets from the attacker address victim port pair for a specified period of time. For example, if the attack uses TCP port 80, future traffic from that attacker to any protected host on port 80 is blocked, but traffic on other ports is allowed.

 Please see page 62 for more details.

- **Deny Attacker Victim Pair Inline** terminates the current packet and future packets from the attacker address and victim address pair for a specified period of time. Future traffic on port from the attacking IP address to the victim IP address is blocked.
- **Deny Connection Inline** terminates the current packet and future packets in the TCP flow.
- **Deny Packet Inline** drops the packet.
- **Log Attacker Packets** starts IP logging on packets that contain the attacker address. A pcap format file is captured on the sensor.
- **Log Pair Packets** starts IP logging on packets that contain the attacker and victim IP address pair.
- **Log Victim Packets** starts IP logging on packets that contain the victim address.
- **Produce Alert** generates an alert.
- **Produce Verbose Alert** generates an alert that contains a pcap of the packet that caused the signature to fire.
- **Request Block Connection** sends a request to a blocking device to block the connection. Blocking devices can be ASA firewalls, switches, routers, or access points.
- **Request Block Host** sends a request to a blocking device to block the attacker host.
- **Request SNMP Trap** generates an SNMP trap if the trap destination is already configured.
- **Reset TCP Connection** sends one or more TCP Reset packets.
- **Modify Packet Inline** modifies illegal portions of a packet. This event action is only available to the Normalizer engine.

Notice that many of the response actions to a signature firing involve denying attackers access to your protected network. To manage denied attackers, choose **Monitoring, Denied Attackers**.

 Please see page 62 for more details.

Signature Engines

An IPS sensor relies on signature engines to efficiently monitor your network using the many signatures that make up the operation of the sensor. Each signature engine is responsible for running a group for the signatures. As new signature engines are released, engines may be added or removed. The list of signatures and engine here is current as of Engine 4.

Many signature engines support entire categories of signatures. Signature engines include tunable parameters. Some parameters are specific to an engine, and others are more common.

Common Parameters

Some common signature parameters include Signature ID, Alert Severity, and Signature Fidelity Rating.

The Summary mode common parameter controls the number of alarms generated:

- Fire Once.
- Fire All is an alarm for all activity that matches signature characteristics.
- Summarize consolidates alarms.
- Global summarize consolidates alarms for all address combinations.

Summary threshold and global summary threshold values enable you to configure automatic summarization based on the number of alerts detected. This can prevent you from being overwhelmed by a large number of events produced by the sensor.

ATOMIC

ATOMIC support signatures are triggered by the content of a single packet. They do not store any state information across packets.

 Please see page 62 for more details.

ATOMIC signature engines are

- ATOMIC ARP
- ATOMIC IP
- ATOMIC IP ADVANCED
- ATOMIC IPv6

FIXED

The FIXED signature engines support regular expressions for pattern matching. Also, alarm functionality is provided for Internet Control Message Protocol (ICMP), User Datagram Protocol (UDP), and Transmission Control Protocol (TCP). State information is maintained because pattern matches are made across a stream of packets. FIXED differs from STRING signatures in that FIXED signatures watch all TCP/UDP ports, whereas STRING watch only defined ports.

The FIXED engines are

- STRING ICMP
- STRING TCP
- STRING UDP

FLOOD

The FLOOD signature engines are designed to detect attacks in which the attacker floods traffic to a single host or an entire network.

FLOOD signature engines are

- FLOOD NET
- FLOOD HOST

 Please see page 62 for more details.

SERVICE

SERVICE engines analyze traffic at and above Layer 5 of the OSI model. They provide protocol decoding for numerous protocols.

SERVICE signature engines are

- SERVICE DNS
- SERVICE FTP
- SERVICE FTP V2
- SERVICE GENERIC
- SERVICE GENERIC ADVANCED
- SERVICE H225
- SERVICE HTTP
- SERVICE HTTP V2
- SERVICE IDENT
- SERVICE MSRPC
- SERVICE MSSQL
- SERVICE NTP
- SERVICE P2P
- SERVICE RPC
- SERVICE SMB
- SERVICE SMB ADVANCED

 Please see page 62 for more details.

- SERVICE SMTP V1
- SERVICE SNMP
- SERVICE SSH
- SERVICE TNS

STRING

The STRING signature engines support regular expressions for pattern matching. Also, alarm functionality is provided for ICMP, UDP, and TCP. State information is maintained because pattern matches are made across a stream of packets.

The STRING engines are

- STRING ICMP
- STRING ICMP XL
- STRING TCP
- STRING TCP XL
- STRING UDP
- STRING UDP XL
- MULTI STRING

 Please see page 62 for more details.

SWEEP

The SWEEP signature engines detect attacks that involve the attacker making connections to multiple hosts/ports.

The SWEEP engines are

- SWEEP
- SWEEP OTHER TCP (supports signatures that fire when a mix of TCP packets have different flags set)

TROJAN

TROJAN engines are designed to detect Trojan program attacks against your network:

- TROJAN BO2K examines UDP and TCP traffic for Back Orifice.
- TROJAN TFN2K examines UDP, TCP, or ICMP traffic for irregular traffic patterns and corrupted headers.
- TROJAN UDP examines UDP traffic for Trojan attacks.

TRAFFIC

The TRAFFIC signature engines analyze nonstandard protocols, such as TFN2K, LOKI, and DDOS. The engines are

- TRAFFIC ICMP examines protocols such as LOKI.
- TRAFFIC ANOMALY examines UDP, TCP, and other traffic for worms.

 Please see page 62 for more details.

AIC

The AIC engines provide Layer 4 to Layer 7 inspection for HTTP and FTP. The engines are

- AIC FTP
- AIC HTTP

To use these engines, you must enable Application Policy enforcement. To do this, choose **Configuration, Signature Definitions,** *signature policy name***, Active Signatures, Advanced**. Place a check mark on **Enable HTTP** or **Enable FTP**, as desired.

STATE

The STATE engine enables the sensor to inspect the various states of Cisco login, an LPR format string, or Simple Mail Transfer Protocol (SMTP).

META

The META signature engine provides event correlation. This engine takes signature events as its input instead of packets. An example is many signatures firing within a certain time limit to indicate the Nimda attack.

NORMALIZER

The NORMALIZER engine detects and correlates ambiguities or illegal packets of data flows through the sensor. Proper packet sequencing and reassembly are options for this engine. The NORMALIZER engine is only available for inline traffic.

 Please see page 62 for more details.

Customizing Signatures

You can tune the built-in signatures or create your own. You might tune signatures for one of the following reasons:

- To reduce background noise. The sensor can cause a lot of alarms on a busy and complex network.
- To reduce false positives.
- To reduce false negatives.
- To more closely sync to the devices being protected. This means that the sensor is more aware of your network's needs.
- To increase performance.

Noise Reduction

Consider the following noise reduction principles:

- You do not have to display noisy events. If a signature is generating too much noise, and you do not want to see it, you can filter it, or you can disable the Produce Alert event action.
- When disabling events, be sure to list what attacks can no longer be detected.
- Rethink your strategy periodically based on new attacks.
- Try to modify the signature for some hosts.

False-Positive Reduction

You have two main strategies for dealing with false-positive alerts. You can selectively disable alerts, and you can match signatures more closely to the environment.

 Please see page 62 for more details.

You should also consider tuning alert triggering by changing the thresholds used within a signature. You can increase the limits if you find that they are exceeded too often. You can also tune a signature's content. You might change the range of allowed parameters, or modify string matching.

Follow these guidelines to reduce false positives:

- Unskilled operators benefit the most.
- When disabling events, be sure to list what attacks can no longer be detected.
- Rethink your strategy periodically based on new attacks.
- Try to modify the signature for some hosts.

False-Negative Reduction

You can reduce false negatives by doing the following:

- Increase the time span that a sensor uses to detect scans and sweeps.
- Lower the limit if the number of correlated events that must happen is too high.
- Try to modify the settings on a per-host basis.

To combat evasion, use all available anti-evasion measures. You should detect conditions that normally should not occur, such as fragmentation overlaps, fragmentation database timeouts, TCP stream or sequence overlaps, out-of-memory errors, or unexpected dropping of packets at the sensor.

Follow these guidelines to reduce false negatives:

- Tune signature thresholds.
- Tune signature content.
- Employ maximum anti-evasion measures.

 Please see page 62 for more details.

Syncing to Protected Devices

Specific tuning recommendations are based on the systems being monitored. For Windows systems, follow these guidelines:

- For IP reassembly, use the reassembly mode of NT.
- Enable all IIS signatures if you are running an IIS server.
- Enable general Windows/NetBIOS signatures.
- Consider the more specific Windows/NetBIOS signatures.
- De-obfuscation inside the HTTP protocol is turned on for all HTTP signatures by default. It uses the ISS dialect.

For Solaris systems, follow these guidelines:

- The IP reassembly mode should be set to Solaris.
- Enable UNIX Remote Procedure Class (RPC) signatures.
- Enable UNIX remote services (r-services) signatures.
- Enable general RPC/Network File System signatures depending on the server's role.

If you are monitoring Linux systems, follow these guidelines:

- Set the IP reassembly mode to Linux.
- Enable the UNIX RPC signatures.
- Enable UNIX r-services signatures.
- Enable general RPC/NFS signatures, depending on the server's role.

 Please see page 62 for more details.

Focusing IPS Sensors to Policy

To take a more policy-based approach, detect unauthorized protocols, detect unauthorized applications, detect unauthorized actions, and enable almost all signatures.

Performance Optimization Guidelines

You should consider the following:

- Filter traffic before capture. Place the sensor behind a firewall; selective capture.
- Reduce detection capabilities. Disable unneeded signatures, simplify signatures; unidirectional capture.
- Load balance to multiple sensors.

 Please see page 62 for more details.

CCNP Security IPS 642-627 Quick Reference

Gary Halleen

Technical Reviewer: Jorge Vargas

Published by:

Cisco Press

800 East 96th Street

Indianapolis, IN 46240 USA

Digital Edition April 2011

ISBN-10: 0-13-256641-9

ISBN-13: 978-0-13-256641-4

Warning and Disclaimer

This book is designed to provide information about CCNP Security. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc., shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this Quick Reference.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this Quick Reference should not be regarded as affecting the validity of any trademark or service mark.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Corporate and Government Sales

Cisco Press offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales.

For more information, please contact: U.S. Corporate and Government Sales 1-800-382-3419

corpsales@pearsontechgroup.com

For sales outside the U.S., please contact: International Sales international@pearsoned.com

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**