



APPENDIX **B**

Signature Engines

This appendix describes the IPS signature engines. It contains the following sections:

- [About Signature Engines, page B-1](#)
- [Master Engine, page B-3](#)
- [AIC Engine, page B-8](#)
- [Atomic Engine, page B-10](#)
- [Flood Engine, page B-11](#)
- [Meta Engine, page B-12](#)
- [Multi String Engine, page B-13](#)
- [Normalizer Engine, page B-15](#)
- [Service Engines, page B-16](#)
- [State Engine, page B-31](#)
- [String Engines, page B-32](#)
- [Sweep Engine, page B-34](#)
- [Traffic ICMP Engine, page B-36](#)
- [Trojan Engines, page B-37](#)

About Signature Engines

A signature engine is a component of the Cisco IPS that is designed to support many signatures in a certain category. An engine is composed of a parser and an inspector. Each engine has a set of parameters that have allowable ranges or sets of values.



Note

The 5.1 engines support a standardized Regex.

IPS 5.1 contains the following signature engines:

- AIC—Provides thorough analysis of web traffic.

It provides granular control over HTTP sessions to prevent abuse of the HTTP protocol. It allows administrative control over applications, such as instant messaging and gotomypc, that try to tunnel over specified ports. You can also use AIC to inspect FTP traffic and control the commands being issued.

There are two AIC engines: AIC FTP and AIC HTTP.

For more information on configuring the AIC engine signatures, see [Configuring Application Policy, page 5-27](#).

- Atomic—The Atomic engines are now combined into two engines with multi-level selections. You can combine Layer-3 and Layer-4 attributes within one signature, for example IP + TCP. The Atomic engine uses the standardized Regex support.

- Atomic IP —Inspects IP protocol packets and associated Layer-4 transport protocols.

This engine lets you specify values to match for fields in the IP and Layer-4 headers, and lets you use Regex to inspect Layer-4 payloads.



Note All IP packets are inspected by the Atomic IP engine. This engine replaces the 4.x Atomic ICMP, Atomic IP Options, Atomic L3 IP, Atomic TCP, and Atomic UDP engines.

- Atomic ARP—Inspects Layer-2 ARP protocol. The Atomic ARP engine is different because most engines are based on Layer-3-IP.

- Flood—Detects ICMP and UDP floods directed at hosts and networks.

There are two Flood engines: Flood HOST and Flood NET.

- Meta—Defines events that occur in a related manner within a sliding time interval. This engine processes events rather than packets.
- Multi String—Inspects Layer 4 transport protocols and payloads by matching several strings for one signature.

This engine inspects stream-based TCP and single UDP and ICMP packets.



Note The Multi String engine is new for IPS 5.1.

- Normalizer—Configures how the IP and TCP normalizer functions and provides configuration for signature events related to the IP and TCP normalizer. Allows you to enforce RFC compliance.
- Service—Deals with specific protocols. Service engine has the following protocol types:

- DNS—Inspects DNS (TCP and UDP) traffic.
- FTP—Inspects FTP traffic.
- GENERIC—Decodes custom service and payload.
- H225— Inspects VoIP traffic.

Helps the network administrator make sure the SETUP message coming in to the VoIP network is valid and within the bounds that the policies describe. Is also helps make sure the addresses and Q.931 string fields such as url-ids, email-ids, and display information adhere to specific lengths and do not contain possible attack patterns.

- HTTP—Inspects HTTP traffic.

The WEBPORTS variable defines inspection port for HTTP traffic.

- IDENT—Inspects IDENT (client and server) traffic.
- MSRPC—Inspects MSRPC traffic.
- MSSQL—Inspects Microsoft SQL traffic.

- NTP—Inspects NTP traffic.
- RPC—Inspects RPC traffic.
- SMB—Inspects SMB traffic.
- SNMP—Inspects SNMP traffic.
- SSH—Inspects SSH traffic.
- State—Stateful searches of strings in protocols such as SMTP.
The state engine now has a hidden configuration file that is used to define the state transitions so new state definitions can be delivered in a signature update.
- String—Searches on Regex strings based on ICMP, TCP, or UDP protocol.
There are three String engines: String ICMP, String TCP, and String UDP.
- Sweep—Analyzes sweeps from a single host (ICMP and TCP), from destination ports (TCP and UDP), and multiple ports with RPC requests between two nodes.
- Traffic ICMP—Analyzes nonstandard protocols, such as TFN2K, LOKI, and DDOS. There are only two signatures with configurable parameters.
- Trojan—Analyzes traffic from nonstandard protocols, such as BO2K andTFN2K.
There are three Trojan engines: Bo2k, Tfn2k, and UDP. There are no user-configurable parameters in these engines.

Master Engine

The Master engine provides structures and methods to the other engines and handles input from configuration and alert output. This section describes the Master engine, and contains the following topics:

- [General Parameters, page B-4](#)
- [Alert Frequency, page B-5](#)
- [Event Actions, page B-6](#)

General Parameters

The following parameters are part of the Master engine and apply to all signatures.

Table B-1 lists the general master engine parameters.

Table B-1 Master Engine General Parameters

Parameter	Description	Value
alert-severity	Severity of the alert: <ul style="list-style-type: none"> • Dangerous alert • Medium-level alert • Low-level alert • Informational alert 	high medium low informational
engine	Specifies the engine the signature belongs to.	—
event-counter	Grouping for event count settings.	—
event-count	Number of times an event must occur before an alert is generated.	1 to 65535
event-count-key	The storage type on which to count events for this signature: <ul style="list-style-type: none"> • Attacker address • Attacker and victim addresses • Attacker address and victim port • Victim address • Attacker and victim addresses and ports 	Axxx AxBx Axxb xxBx AaBb
specify-alert-interval	Enables alert interval.	yes no
alert-interval	Time in seconds before the event count is reset.	2 to 1000
promisc-delta	Delta value used to determine seriousness of the alert.	0 to 30
sig-fidelity-rating	Rating of the fidelity of this signature.	0 to 100
sig-description	Grouping for your description of the signature.	—
sig-name	Name of the signature.	<i>sig-name</i>
sig-string-info	Additional information about this signature that will be included in the alert message.	<i>sig-string-info</i>
sig-comment	Comments about this signature.	<i>sig-comment</i>
alert-traits	Traits you want to document about this signature.	0 to 65335
release	The release in which the signature was most recently updated.	<i>release</i>
status	Whether the signature is enabled or disabled, active or retired.	enabled retired



Caution

We do not recommend that you change the promisc-delta setting for a signature.

Promiscuous delta lowers the RR of certain alerts in promiscuous mode. Because the sensor does not know the attributes of the target system and in promiscuous mode cannot deny packets, it is useful to lower the prioritization of promiscuous alerts (based on the lower risk rating) so the administrator can focus on investigating higher risk rating alerts.

In inline mode, the sensor can deny the offending packets and they never reach the target host, so it does not matter if the target was vulnerable. The attack was not allowed on the network and so we do not subtract from the risk rating value.

Signatures that are not service, OS, or application-specific have 0 for the promiscuously delta. If the signature is specific to an OS, service, or application, it has a promiscuous delta of 5, 10, or 15 calculated from 5 points for each category.

Alert Frequency

The purpose of the alert frequency parameter is to reduce the volume of the alerts written to the Event Store to counter IDS DoS tools, such as stick. There are four modes: Fire All, Fire Once, Summarize, and Global Summarize. The summary mode is changed dynamically to adapt to the current alert volume. For example, you can configure the signature to Fire All, but after a certain threshold is reached, it starts summarizing.

Table B-2 lists the alert frequency parameters.

Table B-2 Master Engine Alert Frequency Parameters

Parameter	Description	Value
alert-frequency	Summary options for grouping alerts.	—
summary-mode	Mode used for summarization.	—
fire-all	Fires an alert on all events.	—
fire-once	Fires an alert only once.	—
global-summarize	Summarizes an alert so that it only fires once regardless of how many attackers or victims.	—
summarize	Summarizes alerts.	—
specify-summary-threshold	(Optional) Enables summary threshold.	yes no
summary-threshold	Threshold number of alerts to send signature into summary mode.	0 to 65535
specify-global-summary-threshold	Enable global summary threshold.	yes no
global-summary-threshold	Threshold number of events to take alerts into global summary.	1 to 65535
summary-interval	Time in seconds used in each summary alert.	1 to 1000
summary-key	The storage type on which to summarize this signature: <ul style="list-style-type: none"> Attacker address Attacker and victim addresses Attacker address and victim port Victim address Attacker and victim addresses and ports 	Axxx AxBx Axxb xxBx AaBb

Event Actions

Most of the following event actions belong to each signature engine unless they are not appropriate for that particular engine.

Table B-3 describes the event actions.

Table B-3 **Event Actions**

Event Action Name	Description
Deny Attacker Inline	(Inline mode only) Does not transmit this packet and future packets originating from the attacker address for a specified period of time. ¹ Note This is the most severe of the deny actions. It denies current and future packets from a single attacker address. To clear all denied attacker entries, choose Monitoring > Denied Attackers > Clear List , which permits the addresses back on the network. For the procedure, see Monitoring the Denied Attackers List, page 11-2 .
Deny Attacker Service Pair Inline	(Inline mode only) Does not transmit this packet and future packets on the attacker address victim port pair for a specified period of time.
Deny Attacker Victim Pair Inline	(Inline mode only) Does not transmit this packet and future packets on the attacker/victim address pair for a specified period of time. Note For deny actions, to set the specified period of time and maximum number of denied attackers, choose Configuration > Event Action Rules > General Settings . For the procedure, see Configuring the General Settings, page 7-26 .
Deny Connection Inline	(Inline mode only) Does not transmit this packet and future packets on the TCP flow.
Deny Packet Inline	(Inline mode only) Does not transmit this packet. Note You cannot delete the event action override for Deny Packet Inline because it is protected. If you do not want to use that override, disable it
Log Attacker Packets	Starts IP logging packets containing the attacker address. Note This action causes an alert to be written to the Event Store, even if Produce Alert is not selected.
Log Pair Packets	Starts IP logging packets containing the attacker-victim address pair. Note This action causes an alert to be written to the Event Store, even if Produce Alert is not selected.
Log Victim Packets	Starts IP logging packets containing the victim address.
Modify Packet Inline	Modifies packet data to remove ambiguity about what the end point might do with the packet. Note Modify Packet Inline is not an option for Add Event Action Filter or Add Event Action Override.

Table B-3 Event Actions (continued)

Event Action Name	Description
Produce Alert	Writes the event to the Event Store as an alert. Note The Produce Alert action is not automatic when you enable alerts for a signature. To have an alert create in the Event Store, you must select Produce Alert. If you add a second action, you must include Produce Alert if you want an alert sent to the Event Store. Also, every time you configure the event actions, a new list is created and it replaces the old list. Make sure you include all the event actions you need for each signature.
Produce Verbose Alert	Includes an encoded dump of the offending packet in the alert. Note This action causes an alert to be written to the Event Store, even if Produce Alert is not selected.
Request Block Connection	Sends a request to ARC to block this connection. Note You must have blocking devices configured to implement this action. For more information, see Chapter 8, “Configuring Attack Response Controller for Blocking and Rate Limiting.”
Request Block Host	Sends a request to ARC to block this attacker host. Note You must have blocking devices configured to implement this action. For more information, see Chapter 8, “Configuring Attack Response Controller for Blocking and Rate Limiting.” Note For block actions, to set the duration of the block, choose Configuration > Event Action Rules > General Settings . For the procedure, see Configuring the General Settings, page 7-26 .
Request Rate Limit	Sends a rate limit request to ARC to perform rate limiting. You must have rate limiting devices configured to implement this action. For more information, see Chapter 8, “Configuring Attack Response Controller for Blocking and Rate Limiting.” Note Request Rate Limit applies to a select set of signatures. For the list of signatures for which you can request a rate limit, see Understanding Rate Limiting, page 8-3 .
Request SNMP Trap	Sends a request to NotificationApp to perform SNMP notification. Note This action causes an alert to be written to the Event Store, even if Produce Alert is not selected. You must have SNMP configured on the sensor to implement this action. For more information, see Chapter 9, “Configuring SNMP.”
Reset TCP Connection	Sends TCP resets to hijack and terminate the TCP flow. Note Reset TCP Connection only works on TCP signatures that analyze a single connection. It does not work for sweeps or floods.

1. The sensor maintains a list of attackers being denied by the system. To remove an entry from the denied attacker list, you can view the list of attackers and clear the entire list, or you can wait for the timer to expire. The timer is a sliding timer for each entry. Therefore, if attacker A is being denied, but issues another attack, the timer for attacker A is reset and attacker A remains in the denied attacker list until the timer expires. If the denied attacker list is at capacity and cannot add a new entry, the packet will still be denied.

AIC Engine

The AIC engine inspects HTTP web traffic and enforces FTP commands. This section describes the AIC engine and its parameters, and contains the following topics:

- [Overview, page B-8](#)
- [AIC Engine Parameters, page B-8](#)

Overview

The AIC engine defines signatures for deep inspection of web traffic. It also defines signatures that authorize and enforce FTP commands.

There are two AIC engines: AIC HTTP and AIC FTP.

The AIC engine has the following features:

- Web traffic:
 - RFC compliance enforcement
 - HTTP request method authorization and enforcement
 - Response message validation
 - MIME type enforcement
 - Transfer encoding type validation
 - Content control based on message content and type of data being transferred
 - URI length enforcement
 - Message size enforcement according to policy configured and the header
 - Tunneling, P2P and instant messaging enforcement.

This enforcement is done using regular expressions. There are predefined signature but you can expand the list.

- FTP traffic:
 - FTP command authorization and enforcement

AIC Engine Parameters

AIC provides thorough analysis of web traffic. It provides granular control over HTTP sessions to prevent abuse of the HTTP protocol. It allows administrative control over applications, such as instant messaging and gotomypc, that try to tunnel over specified ports. Inspection and policy checks for P2P and instant messaging are possible if these applications are running over HTTP.

AIC also provides a way to inspect FTP traffic and control the commands being issued.

You can enable or disable the predefined signatures or you can create policies through custom signatures. The AIC engine runs when HTTP traffic is received on AIC web ports. If traffic is web traffic, but not received on the AIC web ports, the Service HTTP engine is executed. AIC inspection can be on any port if it is configured as an AIC web port and the traffic to be inspected is HTTP traffic.

**Caution**

The AIC web ports are regular HTTP web ports. You can turn on AIC web ports to distinguish which ports should watch for regular HTTP traffic and which ports should watch for AIC enforcement. You might use AIC web ports, for example, if you have a proxy on port 82 and you need to monitor it. We recommend that you do not configure separate ports for AIC enforcement.

For the procedures for configuring AIC engine signatures, see [Configuring Application Policy, page 5-27](#). For an example of a custom AIC signature, see [Example Recognized Define Content Type \(MIME\) Signature, page 5-35](#).

Table B-4 lists the parameters that are specific to the AIC HTTP engine.

Table B-4 AIC HTTP Engine Parameters

Parameter	Description
signature-type	Specifies the type of AIC signature.
content-types	AIC signature that deals with MIME types: <ul style="list-style-type: none"> define-content-type associates actions such as denying a specific MIME type (image/gif), defining a message-size violation, and determining that the MIME-type mentioned in the header and body do not match. define-recognized-content-types lists content types recognized by the sensor.
define-web-traffic-policy	Specifies the action to take when noncompliant HTTP traffic is seen. The alarm-on-non-http-traffic [true false] command enables the signature. This signature is disabled by default.
max-outstanding-requests-overrun	Maximum allowed HTTP requests per connection (1 to 16).
msg-body-pattern	Uses Regex to define signatures that look for specific patterns in the message body.
request-methods	AIC signature that allows actions to be associated with HTTP request methods: <ul style="list-style-type: none"> define-request-method, such as get, put, and so forth. recognized-request-methods lists methods recognized by the sensor.
transfer-encodings	AIC signature that deals with transfer encodings: <ul style="list-style-type: none"> define-transfer-encoding associates an action with each method, such as compress, chunked, and so forth. recognized-transfer-encodings lists methods recognized by the sensor. chunked-transfer-encoding-error specifies actions to be taken when a chunked encoding error is seen.

Table B-5 lists the parameters that are specific to the AIC FTP engine.

Table B-5 AIC FTP Engine Parameters

Parameter	Description
signature-type	Specifies the type of AIC signature.
ftp-commands	Associates an action with an FTP command: <ul style="list-style-type: none"> ftp-command—Lets you choose the FTP command you want to inspect.
unrecognized-ftp-command	Inspects unrecognized FTP commands.

Atomic Engine

The Atomic engine contains signatures for simple, single packet conditions that cause alerts to be fired. This section describes the Atomic engine, and contains the following topics:

- [Atomic ARP Engine, page B-10](#)
- [Atomic IP Engine, page B-11](#)

Atomic ARP Engine

The Atomic ARP engine defines basic Layer-2 ARP signatures and provides more advanced detection of the ARP spoof tools dsniff and ettercap.

Table B-6 lists the parameters that are specific to the Atomic ARP engine.

Table B-6 Atomic ARP Engine Parameters

Parameter	Description
specify-mac-flip	Fires an alert when the MAC address changes more than this many times for this IP address.
specify-type-of-arp-sig	Specifies the type of ARP signatures you want to fire on: <ul style="list-style-type: none"> Source Broadcast (default)—Fires an alarm for this signature when it sees an ARP source address of 255.255.255.255. Destination Broadcast—Fires an alarm for this signature when it sees an ARP destination address of 255.255.255.255. Same Source and Destination—Fires an alarm for this signature when it sees an ARP destination address with the same source and destination MAC address Source Multicast—Fires an alarm for this signature when it sees an ARP source MAC address of 01:00:5e:(00-7f).
specify-request-inbalance	Fires an alert when there are this many more requests than replies on the IP address.
specify-arp-operation	The ARP operation code for this signature.

Atomic IP Engine

The Atomic IP engine defines signatures that inspect IP protocol headers and associated Layer-4 transport protocols (TCP, UDP, and ICMP) and payloads.


Note

The Atomic engines do not store persistent data across packets. Instead they can fire an alert from the analysis of a single packet.

Table B-7 lists the parameters that are specific to the Atomic IP engine.

Table B-7 Atomic IP Engine Parameters

Parameter	Description
fragment-status	Specifies whether or not fragments are wanted.
specify-ip-payload-length	Specifies IP datagram payload length.
specify-ip-header-length	Specifies IP datagram header length.
specify-ip-addr-options	Specifies IP addresses.
specify-ip-id	Specifies IP identifier.
specify-ip-total-length	Specifies IP datagram total length.
specify-ip-option-inspection	Specifies IP options inspection.
specify-l4-protocol	Specifies Layer 4 protocol.
specify-ip-tos	Specifies type of server.
specify-ip-ttl	Specifies time to live.
specify-ip-version	Specifies IP protocol version.

Flood Engine

The Flood engine defines signatures that watch for any host or network sending multiple packets to a single host or network. For example, you can create a signature that fires when 150 or more packets per second (of the specific type) are found going to the victim host.

There are two types of Flood engines: Flood Host and Flood Net.

Table B-8 lists the parameters specific to the Flood Host engine.

Table B-8 Flood Host Engine Parameters

Parameter	Description	Value
protocol	Which kind of traffic to inspect.	ICMP UDP
rate	Threshold number of packets per second.	0 to 65535 ¹
icmp-type	Specifies the value for the ICMP header type.	0 to 65535

Table B-8 Flood Host Engine Parameters (continued)

Parameter	Description	Value
dst-ports	Specifies the destination ports when you choose UDP protocol.	0 to 65535 ² a-b[,c-d]
src-ports	Specifies the source ports when you choose UDP protocol.	0 to 65535 ³ a-b[,c-d]

1. An alert fires when the rate is greater than the packets per second.
2. The second number in the range must be greater than or equal to the first number.
3. The second number in the range must be greater than or equal to the first number.

Table B-9 lists the parameters specific to the Flood Net engine.

Table B-9 Flood Net Engine Parameters

Parameter	Description	Value
gap	Gap of time allowed (in seconds) for a flood signature.	0 to 65535
peaks	Number of allowed peaks of flood traffic.	0 to 65535
protocol	Which kind of traffic to inspect.	ICMP TCP UDP
rate	Threshold number of packets per second.	0 to 65535 ¹
sampling-interval	Interval used for sampling traffic.	1 to 3600
icmp-type	Specifies the value for the ICMP header type.	0 to 65535

1. An alert fires when the rate is greater than the packets per second.

Meta Engine

The Meta engine defines events that occur in a related manner within a sliding time interval. This engine processes events rather than packets. As signature events are generated, the Meta engine inspects them to determine if they match any or several Meta definitions. The Meta engine generates a signature event after all requirements for the event are met.

All signature events are handed off to the Meta engine by SEAP. SEAP hands off the event after processing the minimum hits option. Summarization and event action are processed after the Meta engine has processed the component events. For more information about SEAP, see [Signature Event Action Processor, page 7-4](#).



Caution

A large number of Meta signatures could adversely affect overall sensor performance.

Table B-10 lists the parameters specific to the Meta engine.

Table B-10 Meta Engine Parameters

Parameter	Description	Value
meta-reset-interval	Time in seconds to reset the META signature.	0 to 3600
component-list	List of Meta components: <ul style="list-style-type: none"> • edit—Edits an existing entry • insert—Inserts a new entry into the list: <ul style="list-style-type: none"> – begin—Places the entry at the beginning of the active list – end—Places the entry at the end of the active list – inactive—Places the entry into the inactive list – before—Places the entry before the specified entry – after—Places the entry after the specified entry • move—Moves an entry in the list 	<i>name</i>
meta-key	Storage type for the Meta signature: <ul style="list-style-type: none"> • Attacker address • Attacker and victim addresses • Attacker and victim addresses and ports • Victim address 	AaBb AxBx Axxx xxBx
unique-victim-ports	Number of unique victims ports required per Meta signature.	1 to 256
component-list-in-order	Whether to fire the component list in order.	true false

For an example of a custom Meta engine signature, see [Example MEG Signature, page 5-43](#).

Multi String Engine

The Multi String engine lets you define signatures that inspect Layer 4 transport protocol (ICMP, TCP, and UDP) payloads using multiple string matches for one signature. You can specify a series of regular expression patterns that must be matched to fire the signature. For example, you can define a signature that looks for regex 1 followed by regex 2 on a UDP service. For UDP and TCP you can specify port numbers and direction. You can specify a single source port, a single destination port, or both ports. The string matching takes place in both directions.

Use the Multi String engine when you need to specify more than one regex pattern. Otherwise, you can use the String ICMP, String TCP, or String UDP engine to specify a single regex pattern for one of those protocols.

Table B-11 lists the parameters specific to the Multi String Engine.

Table B-11 Multi String Engine Parameters

Parameter	Description	Value
inspect-length	Length of stream or packet that must contain all offending strings for the signature to fire.	0 to 4294967295
protocol	Layer 4 protocol selection.	icmp tcp udp
regex-component	List of regex components: <ul style="list-style-type: none"> • regex-string—The string to search for. • spacing-type—Type of spacing required from the match before or from the beginning of the stream/packet if it is the first entry in the list. 	list (1 to 16 items) exact minimum
port-selection	Type of TCP or UDP port to inspect: <ul style="list-style-type: none"> • both-ports—Specifies both source and destination port. • dest-ports—Specifies a range of destination ports. • source-ports—Specifies a range of source ports.¹ 	0 to 65535 ²
exact-spacing	Exact number of bytes that must be between this regex string and the one before, or from the beginning of the stream/packet if it is the first entry in the list.	0 to 4294967296
min-spacing	Minimum number of bytes that must be between this regex string and the one before, or from the beginning of the stream/packet if it is the first entry in the list.	0 to 4294967296
swap-attacker-victim	True if address (and ports) source and destination are swapped in the alert message. False for no swap (default).	true false

1. Port matching is performed bidirectionally for both the client-to-server and server-to-client traffic flow directions. For example, if the source-ports value is 80, in a client-to-server traffic flow direction, inspection occurs if the client port is 80. In a server-to-client traffic flow direction, inspection occurs if the server port is port 80.
2. A valid value is a comma-separated list of integer ranges a-b[,c-d] within 0 to 65535. The second number in the range must be greater than or equal to the first number.



Caution

The Multi String engine can have a significant impact on memory usage.

Normalizer Engine

The Normalizer engine deals with IP fragmentation and TCP normalization. This section describes the Normalizer engine, and contains the following topics:

- [Overview, page B-15](#)
- [Normalizer Engine Parameters, page B-16](#)

Overview

The Normalizer engine deals with IP fragment reassembly and TCP stream reassembly. With the Normalizer engine you can set limits on system resource usage, for example, the maximum number of fragments the sensor tries to track at the same time.

**Note**

You cannot add custom signatures to the Normalizer engine. You can tune the existing ones.

- IP Fragmentation Normalization

Intentional or unintentional fragmentation of IP datagrams can hide exploits making them difficult or impossible to detect. Fragmentation can also be used to circumvent access control policies like those found on firewalls and routers. And different operating systems use different methods to queue and dispatch fragmented datagrams. If the sensor has to check for all possible ways that the end host will reassemble the datagrams, the sensor becomes vulnerable to denial of service attacks. Reassembling all fragmented datagrams inline and only forwarding completed datagrams, refragmenting the datagram if necessary, prevents this. The IP Fragmentation Normalization unit performs this function.

- TCP Normalization

Through intentional or natural TCP session segmentation, some classes of attacks can be hidden. To make sure policy enforcement can occur with no false positives and false negatives, the state of the two TCP endpoints must be tracked and only the data that is actually processed by the real host endpoints should be passed on. Overlaps in a TCP stream can occur, but are extremely rare except for TCP segment retransmits. Overwrites in the TCP session should not occur. If overwrites do occur, someone is intentionally trying to elude the security policy or the TCP stack implementation is broken. Maintaining full information about the state of both endpoints is not possible unless the sensor acts as a TCP proxy. Instead of the sensor acting as a TCP proxy, the segments will be ordered properly and the normalizer will look for any abnormal packets associated with evasion and attacks.

Sensors in promiscuous mode report alerts on violations. Sensors in inline mode perform the action specified in the event-action parameter, such as produce-alert, deny-packet-inline, and modify-packet-inline.

For the procedures for configuring signatures in the Normalizer engine, see [Configuring IP Fragment Reassembly, page 5-35](#), and [Configuring TCP Stream Reassembly, page 5-38](#).

Normalizer Engine Parameters

Table B-12 lists the parameters that are specific to the Normalizer engine.

Table B-12 Normalizer Engine Parameters

Parameter	Description
edit-default-sigs-only	Editable signatures.
specify-fragment-reassembly-timeout	(Optional) Enables fragment reassembly timeout.
specify-hijack-max-old-ack	(Optional) Enables hijack-max-old-ack.
specify-max-dgram-size	(Optional) Enables maximum datagram size.
specify-max-fragments	(Optional) Enables maximum fragments.
specify-max-fragments-per-dgram	(Optional) Enables maximum fragments per datagram.
specify-max-last-fragments	(Optional) Enables maximum last fragments.
specify-max-partial-dgrams	(Optional) Enables maximum partial datagrams.
specify-max-small-frags	(Optional) Enables maximum small fragments.
specify-min-fragment-size	(Optional) Enables minimum fragment size.
specify-service-ports	(Optional) Enables service ports.
specify-syn-flood-max-embryonic	(Optional) Enables SYN flood maximum embryonic.
specify-tcp-closed-timeout	(Optional) Enables TCP closed timeout.
specify-tcp-embryonic-timeout	(Optional) Enables TCP embryonic timeout.
specify-tcp-idle-timeout	(Optional) Enables TCP idle timeout.
specify-tcp-max-mss	(Optional) Enables TCP maximum mss.
specify-tcp-max-queue	(Optional) Enables TCP maximum queue.
specify-tcp-min-mss	(Optional) Enables TCP minimum mss.
specify-tcp-option-number	(Optional) Enables TCP option number.

Service Engines

The Service engines analyze L5+ traffic between two hosts. These are one-to-one signatures that track persistent data. The engines analyze the L5+ payload in a manner similar to the live service.

The Service engines have common characteristics but each engine has specific knowledge of the service that it is inspecting. The Service engines supplement the capabilities of the generic string engine specializing in algorithms where using the string engine is inadequate or undesirable.

This section contains the following topics:

- [Service DNS Engine, page B-17](#)
- [Service FTP Engine, page B-18](#)
- [Service Generic Engine, page B-19](#)
- [Service H225 Engine, page B-20](#)
- [Service HTTP Engine, page B-22](#)

- [Service IDENT Engine, page B-24](#)
- [Service MSRPC Engine, page B-25](#)
- [Service MSSQL Engine, page B-26](#)
- [Service NTP Engine, page B-26](#)
- [Service RPC Engine, page B-27](#)
- [Service SMB Engine, page B-28](#)
- [Service SNMP Engine, page B-29](#)
- [Service SSH Engine, page B-30](#)

Service DNS Engine

The Service DNS engine specializes in advanced DNS decode, which includes anti-evasive techniques, such as following multiple jumps. It has many parameters such as lengths, opcodes, strings, and so forth. The Service DNS engine is a biprotocol inspector operating on both TCP and UDP port 53. It uses the stream for TCP and the quad for UDP.

Table B-13 lists the parameters specific to the Service DNS engine.

Table B-13 Service DNS Engine Parameters

Parameter	Description	Value
protocol	Protocol of interest for this inspector.	TCP UDP
specify-query-chaos-string	(Optional) Enables the DNS Query Class Chaos String.	<i>query-chaos-string</i>
specify-query-class	(Optional) Enables the query class: <ul style="list-style-type: none"> • query-class—DNS Query Class 2 Byte Value 	0 to 65535
specify-query-invalid-domain-name	(Optional) Enables query invalid domain name: <ul style="list-style-type: none"> • query-invalid-domain-name—DNS Query Length greater than 255 	true false
specify-query-jump-count-exceeded	(Optional) Enables query jump count exceeded: <ul style="list-style-type: none"> • query-jump-count-exceeded—DNS compression counter 	true false
specify-query-opcode	(Optional) Enables query opcode: <ul style="list-style-type: none"> • query-opcode—DNS Query Opcode 1 byte Value 	0 to 65535
specify-query-record-data-invalid	(Optional) Enables query record data invalid: <ul style="list-style-type: none"> • query-record-data-invalid—DNS Record Data incomplete 	true false

Table B-13 Service DNS Engine Parameters (continued)

Parameter	Description	Value
specify-query-record-data-len	(Optional) Enables the query record data length: <ul style="list-style-type: none"> query-record-data-len—DNS Response Record Data Length 	0 to 65535
specify-query-src-port-53	(Optional) Enables the query source port 53: <ul style="list-style-type: none"> query-src-port-53—DNS packet source port 53 	true false
specify-query-stream-len	(Optional) Enables the query stream length: <ul style="list-style-type: none"> query-stream-len—DNS Packet Length 	0 to 65535
specify-query-type	(Optional) Enables the query type: <ul style="list-style-type: none"> query-type—DNS Query Type 2 Byte Value 	0 to 65535
specify-query-value	(Optional) Enables the query value: <ul style="list-style-type: none"> query-value—Query 0 Response 1 	true false

Service FTP Engine

The Service FTP engine specializes in FTP port command decode, trapping invalid **port** commands and the PASV port spoof. It fills in the gaps when the String engine is not appropriate for detection. The parameters are Boolean and map to the various error trap conditions in the **port** command decode. The Service FTP engine runs on TCP ports 20 and 21. Port 20 is for data and the Service FTP engine does not do any inspection on this. It inspects the control transactions on port 21.

[Table B-14](#) lists the parameters that are specific to the Service FTP engine.

Table B-14 Service FTP Engine Parameters

Parameter	Description	Value
direction	Direction of traffic: <ul style="list-style-type: none"> Traffic from service port destined to client port Traffic from client port destined to service port 	from-service to-service
ftp-inspection-type	Type of inspection to perform: <ul style="list-style-type: none"> Looks for an invalid address in the FTP port command Looks for an invalid port in the FTP port command Looks for the PASV port spoof 	bad-port-cmd-address bad-port-cmd-port pasv

Table B-14 Service FTP Engine Parameters (continued)

Parameter	Description	Value
service-ports	A comma-separated list of ports or port ranges where the target service resides.	0 to 65535 ¹ a-b[,c-d]
swap-attacker-victim	True if address (and ports) source and destination are swapped in the alert message. False for no swap (default).	true false

1. The second number in the range must be greater than or equal to the first number.

Service Generic Engine

The Service Generic engine allows programmatic signatures to be issued in a config-file-only signature update. It has a simple machine and assembly language that is defined in the configuration file. It runs the machine code (distilled from the assembly language) through its virtual machine, which processes the instructions and pulls the important pieces of information out of the packet and runs them through the comparisons and operations specified in the machine code.

It is intended as a rapid signature response engine to supplement the String and State engines.



Note

You cannot use the Service Generic engine to create custom signatures.



Caution

Only advanced users should tune Service Generic engine signatures.

Table B-15 lists the parameters specific to the Service Generic engine.

Table B-15 Service Generic Engine Parameters

Parameter	Description	Value
specify-dst-port	(Optional) Enables the destination port: <ul style="list-style-type: none"> dst-port—Destination port of interest for this signature 	0 to 65535
specify-ip-protocol	(Optional) Enables IP protocol: <ul style="list-style-type: none"> ip-protocol—The IP protocol this inspector should examine 	0 to 255

Table B-15 Service Generic Engine Parameters (continued)

Parameter	Description	Value
specify-payload-source	(Optional) Enables payload source inspection: <ul style="list-style-type: none"> • payload-source—Payload source inspection for the following types: <ul style="list-style-type: none"> – Inspects ICMP data – Inspects Layer 2 headers – Inspects Layer 3 headers – Inspects Layer 4 headers – Inspects TCP data – Inspects UDP data 	icmp-data l2-header l3-header l4-header tcp-data udp-data
specify-src-port	(Optional) Enables the source port: <ul style="list-style-type: none"> • src-port—Source port of interest for this signature 	0 to 65535

Service H225 Engine

This section describes the Service H225 engine, and contains the following topics:

- [Overview, page B-20](#)
- [Service H255 Engine Parameters, page B-21](#)

Overview

The Service H225 engine analyzes H225.0 protocol, which consists of many subprotocols and is part of the H.323 suite. H.323 is a collection of protocols and other standards that together enable conferencing over packet-based networks.

H.225.0 call signaling and status messages are part of the H.323 call setup. Various H.323 entities in a network, such as the gatekeeper and endpoint terminals, run implementations of the H.225.0 protocol stack. The Service H225 engine analyzes H225.0 protocol for attacks on multiple H.323 gatekeepers, VoIP gateways, and endpoint terminals. It provides deep packet inspection for call signaling messages that are exchanged over TCP PDUs. The Service H225 engine analyzes the H.225.0 protocol for invalid H.255.0 messages, and misuse and overflow attacks on various protocol fields in these messages.

H.225.0 call signaling messages are based on Q.931 protocol. The calling endpoint sends a Q.931 setup message to the endpoint that it wants to call, the address of which it procures from the admissions procedure or some lookup means. The called endpoint either accepts the connection by transmitting a Q.931 connect message or rejects the connection. When the H.225.0 connection is established, either the caller or the called endpoint provides an H.245 address, which is used to establish the control protocol (H.245) channel.

Especially important is the SETUP call signaling message because this is the first message exchanged between H.323 entities as part of the call setup. The SETUP message uses many of the commonly found fields in the call signaling messages, and implementations that are exposed to probable attacks will mostly also fail the security checks for the SETUP messages. Therefore, it is highly important to check the H.225.0 SETUP message for validity and enforce checks on the perimeter of the network.

The Service H225 engine has built-in signatures for TPKT validation, Q.931 protocol validation, and ASN.1PER validations for the H225 SETUP message. ASN.1 is a notation for describing data structures. PER uses a different style of encoding. It specializes the encoding based on the data type to generate much more compact representations.

You can tune the Q.931 and TPKT length signatures and you can add and apply granular signatures on specific H.225 protocol fields and apply multiple pattern search signatures of a single field in Q.931 or H.225 protocol.

The Service H225 engine supports the following features:

- TPKT validation and length check
- Q.931 information element validation
- Regular expression signatures on text fields in Q.931 information elements
- Length checking on Q.931 information elements
- SETUP message validation
- ASN.1 PER encode error checks
- Configuration signatures for fields like ULR-ID, E-mail-ID, h323-id, and so forth for both regular expression and length.

There is a fixed number of TPKT and ASN.1 signatures. You cannot create custom signatures for these types. For TPKT signatures, you should only change the value-range for length signatures. You should not change any parameters for ASN.1. For Q.931 signatures, you can add new regular expression signatures for text fields. For SETUP signatures, you can add signatures for length and regular expression checks on various SETUP message fields.

Service H255 Engine Parameters

Table B-16 lists parameters specific to the Service H225 engine.

Table B-16 Service H.225 Engine Parameters

Parameter	Description	Value
message-type	Type of H225 message to which the signature applies: <ul style="list-style-type: none"> • SETUP • ASN.1-PER • Q.931 • TPKT 	asn.1-per q.931 setup tpkt
policy-type	Type of H225 policy to which the signature applies: <ul style="list-style-type: none"> • Inspects field length. • Inspects presence. If certain fields are present in the message, an alert is sent. • Inspects regular expressions. • Inspects field validations. • Inspects values. <p>Regex and presence are not valid for TPKT signatures.</p>	length presence regex validate value

Table B-16 Service H.225 Engine Parameters (continued)

Parameter	Description	Value
specify-field-name	(Optional) Enables field name for use. Only valid for SETUP and Q.931 message types. Gives a dotted representation of the field name that this signature applies to. <ul style="list-style-type: none"> field-name—Field name to inspect. 	1 to 512
specify-invalid-packet-index	(Optional) Enables invalid packet index for use for specific errors in ASN, TPKT, and other errors that have fixed mapping. <ul style="list-style-type: none"> invalid-packet-index—Inspection for invalid packet index. 	0 to 255
specify-regex-string	The regular expression to look for when the policy type is regex. This is never set for TPKT signatures: <ul style="list-style-type: none"> A regular expression to search for in a single TCP packet (Optional) Enables min match length for use. The minimum length of the Regex match required to constitute a match. This is never set for TPKT signatures. 	regex-string specify-min-match-length
specify-value-range	Valid for the length or value policy types (0x00 to 6535). Not valid for other policy types. <ul style="list-style-type: none"> value-range—Range of values. 	0 to 65535 ¹ a-b

1. The second number in the range must be greater than or equal to the first number.

Service HTTP Engine

This section describes the Service HTTP engine, and contains the following topics:

- [Overview, page B-22](#)
- [Service HTTP Engine Parameters, page B-23](#)

Overview

The Service HTTP engine is a service-specific string-based pattern-matching inspection engine. The HTTP protocol is one of the most commonly used in today’s networks. In addition, it requires the most amount of preprocessing time and has the most number of signatures requiring inspection making it critical to the system’s overall performance.

The Service HTTP engine uses a Regex library that can combine multiple patterns into a single pattern-matching table allowing a single search through the data. This engine searches traffic directed to web services only to web services, or HTTP requests. You cannot inspect return traffic with this engine. You can specify separate web ports of interest in each signature in this engine.

HTTP deobfuscation is the process of decoding an HTTP message by normalizing encoded characters to ASCII equivalent characters. It is also known as ASCII normalization.

Before an HTTP packet can be inspected, the data must be deobfuscated or normalized to the same representation that the target system sees when it processes the data. It is ideal to have a customized decoding technique for each host target type, which involves knowing what operating system and web server version is running on the target. The Service HTTP engine has default deobfuscation behavior for the Microsoft IIS web server.

Service HTTP Engine Parameters

For an example Service HTTP custom signature, see [Example Service HTTP Signature, page 6-33](#).

[Table B-17](#) lists the parameters specific the Service HTTP engine.

Table B-17 Service HTTP Engine Parameters

Parameter	Description	Value
de-obfuscate	Applies anti-evasive deobfuscation before searching.	true false
max-field-sizes	Maximum field sizes grouping.	—
specify-max-arg-field-length	(Optional) Enables maximum argument field length: <ul style="list-style-type: none"> max-arg-field-length—Maximum length of the arguments field. 	0 to 65535
specify-max-header-field-length	(Optional) Enables maximum header field length: <ul style="list-style-type: none"> max-header-field-length—Maximum length of the header field. 	0 to 65535
specify-max-request-length	(Optional) Enables maximum request field length: <ul style="list-style-type: none"> max-request-length—Maximum length of the request field. 	0 to 65535
specify-max-uri-field-length	(Optional) Enables the maximum URI field length: <ul style="list-style-type: none"> max-uri-field-length—Maximum length of the URI field. 	0 to 65535
regex	Regular expression grouping.	—
specify-arg-name-regex	(Optional) Enables searching the Arguments field for a specific regular expression: <ul style="list-style-type: none"> arg-name-regex—Regular expression to search for in the HTTP Arguments field (after the ? and in the Entity body as defined by Content-Length). 	—
specify-header-regex	(Optional) Enables searching the Header field for a specific regular expression: <ul style="list-style-type: none"> header-regex—Regular Expression to search in the HTTP Header field. The Header is defined after the first CRLF and continues until CRLFCRLF. 	—

Service MSRPC Engine

This section describes the Service MSRPC engine, and contains the following topics:

- [Overview, page B-25](#)
- [Service MSRPC Engine Parameters, page B-25](#)

Overview

The Service MSRPC engine processes MSRPC packets. MSRPC allows for cooperative processing between multiple computers and their application software in a networked environment. It is a transaction-based protocol, implying that there is a sequence of communications that establish the channel and pass processing requests and replies.

MSRPC is an ISO layer 5-6 protocol and is layered on top of other transport protocols such as UDP, TCP, and SMB. The MSRPC engine contains facilities to allow for fragmentation and reassembly of the MSRPC PDUs.

This communication channel is the source of recent Windows NT, Windows 2000, and Window XP security vulnerabilities.

The Service MSRPC engine only decodes the DCE and RPC protocol for the most common transaction types.

Service MSRPC Engine Parameters

[Table B-19](#) lists the parameters specific to the Service MSRPC engine.

Table B-19 *Service MSRPC Engine Parameters*

Parameter	Description	Value
protocol	Protocol of interest for this inspector.	tcp udp
specify-operation	(Optional) Enables using MSRPC operation: <ul style="list-style-type: none"> • operation—MSRPC operation requested. Required for SMB_COM_TRANSACTION commands. Exact match. 	0 to 65535
specify-regex-string	(Optional) Enables using a regular expression string: <ul style="list-style-type: none"> • specify-exact-match-offset—Enables the exact match offset: <ul style="list-style-type: none"> – exact-match-offset—The exact stream offset the regular expression string must report for a match to be valid. • specify-min-match-length—Enables the minimum match length: <ul style="list-style-type: none"> – min-match-length—Minimum number of bytes the regular expression string must match. 	0 to 65535
specify-uuid	(Optional) Enables UUID: <ul style="list-style-type: none"> • uuid—MSRPC UUID field. 	000001a0000 00000c00000 0000000046

Service MSSQL Engine

The Service MSSQL engine inspects the protocol used by Microsoft's SQL server (MSSQL).

There is one MSSQL signature. It fires an alert when it detects an attempt to log in to an MSSQL server with the default sa account.

You can add custom signatures based on MSSQL protocol values, such as login username and whether a password was used.

Table B-20 lists the parameters specific to the Service MSSQL engine.

Table B-20 Service MSSQL Engine Parameters

Parameter	Description	Value
password-present	Whether or not a password was used in an MS SQL login.	true false
specify-sql-username	(Optional) Enables using an SQL username: <ul style="list-style-type: none"> sql-username—Username (exact match) of user logging in to MS SQL service. 	sa

Service NTP Engine

The Service NTP engine inspects NTP protocol. There is one NTP signature, the NTPd readvar overflow signature, which fires an alert if a readvar command is seen with NTP data that is too large for the NTP service to capture.

You can tune this signature and create custom signatures based on NTP protocol values, such as mode and size of control packets.

Table B-21 lists the parameters specific to the Service NTP engine.

Table B-21 Service NTP Engine Parameters

Parameter	Description	Value
inspection-type	Type of inspection to perform.	
inspect-ntp-packets	Inspects NTP packets: <ul style="list-style-type: none"> control-opcode—Opcode number of an NTP control packet according to RFC1305, Appendix B. max-control-data-size—Maximum allowed amount of data sent in a control packet. mode —Mode of operation of the NTP packet per RFC 1305. 	0 to 65535
is-invalid-data-packet	Looks for invalid NTP data packets. Checks the structure of the NTP data packet to make sure it is the correct size.	true false
is-non-ntp-traffic	Checks for nonNTP packets on an NTP port.	true false

Service RPC Engine

The Service RPC engine specializes in RPC protocol and has full decode as an anti-evasive strategy. It can handle fragmented messages (one message in several packets) and batch messages (several messages in a single packet).

The RPC portmapper operates on port 111. Regular RPC messages can be on any port greater than 550. RPC sweeps are like TCP port sweeps, except that they only count unique ports when a valid RPC message is sent. RPC also runs on UDP.

Table B-22 lists the parameters specific to the Service RPC engine.

Table B-22 Service RPC Engine Parameters

Parameter	Description	Value
direction	Direction of traffic: <ul style="list-style-type: none"> Traffic from service port destined to client port. Traffic from client port destined to service port. 	from-service to-service
protocol	Protocol of interest.	tcp udp
service-ports	A comma-separated list of ports or port ranges where the target service resides.	0 to 65535 ¹ a-b[,c-d]
specify-is-spoof-src	(Optional) Enables the spoof source address: <ul style="list-style-type: none"> is-spoof-src—Fires an alert when the source address is 127.0.0.1. 	true false
specify-port-map-program	(Optional) Enables the portmapper program: <ul style="list-style-type: none"> port-map-program—The program number sent to the portmapper for this signature. 	0 to 999999999
specify-rpc-max-length	(Optional) Enables RPC maximum length: <ul style="list-style-type: none"> rpc-max-length—Maximum allowed length of the entire RPC message. Lengths longer than what you specify fire an alert. 	0 to 65535
specify-rpc-procedure	(Optional) Enables RPC procedure: <ul style="list-style-type: none"> rpc-procedure—RPC procedure number for this signature. 	0 to 1000000
specify-rpc-program	(Optional) Enables RPC program: <ul style="list-style-type: none"> rpc-program—RPC program number for this signature. 	0 to 1000000

1. The second number in the range must be greater than or equal to the first number.

Service SMB Engine

The Service SMB engine inspects SMB packets. You can tune SMB signatures and create custom SMB signatures based on SMB control transaction exchanges and SMB NT_Create_AndX exchanges.

Table B-23 lists the parameters specific to the Service SMB engine.

Table B-23 Service SMB Engine Parameters


Parameter	Description	Value
service-ports	A comma-separated list of ports or port ranges where the target service resides.	0 to 65535 a-b[,c-d] ¹
specify-allocation-hint	(Optional) Enables MSRPC allocation hint: <ul style="list-style-type: none"> allocation-hint—MSRPC Allocation Hint, which is used in SMB_COM_TRANSACTION command parsing.² 	0 to 42949677295
specify-byte-count	(Optional) Enables byte count: <ul style="list-style-type: none"> byte-count—Byte count from SMB_COM_TRANSACTION structure.³ 	0 to 65535
specify-command	(Optional) Enables SMB commands: <ul style="list-style-type: none"> command—SMB command value.⁴ 	0 to 255
specify-direction	(Optional) Enables traffic direction: <ul style="list-style-type: none"> direction—Lets you specify the direction of traffic: <ul style="list-style-type: none"> Traffic from service port destined to client port. Traffic from client port destined to service port. 	from service to service
specify-file-id	(Optional) Enables using a transaction file ID: <ul style="list-style-type: none"> file-id—Transaction File ID.⁵  <p>Note This parameter may limit a signature to a specific exploit instance and its use should be carefully considered.</p>	0 to 65535
specify-function	(Optional) Enables named pipe function: <ul style="list-style-type: none"> function—Named Pipe function.⁶ 	0 to 65535
specify-hit-count	(Optional) Enables hit counting: <ul style="list-style-type: none"> hit-count—The threshold number of occurrences in scan-interval to fire alerts.⁷ 	0 to 65535
specify-operation	(Optional) Enables MSRPC operation: <ul style="list-style-type: none"> operation—MSRPC operation requested. Required for SMB_COM_TRANSACTION commands. An exact match is required. 	0 to 65535

Table B-23 Service SMB Engine Parameters (continued)

Parameter	Description	Value
specify-resource	(Optional) Enables resource: <ul style="list-style-type: none"> resource—Specifies that pipe or the SMB filename is used to qualify the alert. In ASCII format. An exact match is required. 	<i>resource</i>
specify-scan-interval	(Optional) Enables scan interval: <ul style="list-style-type: none"> scan-interval—The interval in seconds used to calculate alert rates.⁸ 	0 to 131071
specify-set-count	(Optional) Enables counting setup words: <ul style="list-style-type: none"> set-count—Number of Setup words.⁹ 	0 to 255
specify-type	(Optional) Enables searching for the Type field of an MSRPC packet: <ul style="list-style-type: none"> type —Type Field of MSRPC packet. 0 = Request; 2 = Response; 11 = Bind; 12 = Bind Ack 	0 to 255
specify-word-count	(Optional) Enables word counting for command parameters: <ul style="list-style-type: none"> word-count—Word count for the SMB_COM_TRANSACTION command parameters.¹⁰ 	0 to 255
swap-attacker-victim	True if address (and ports) source and destination are swapped in the alert message. False for no swap (default).	true false

1. The second number in the range must be greater than or equal to the first number.
2. An exact match is optional.
3. An exact match is optional.
4. An exact match is required. Currently supporting the 37 (0x25) SMB_COM_TRANSACTION command \x26amp and the 162 (0xA2) SMB_COM_NT_CREATE_ANDX command.
5. An exact match is optional.
6. An exact match is required. Required for SMB_COM_TRANSACTION commands.
7. Valid for signatures 3302 and 6255 only.
8. Valid for signatures 3302 and 6255 only.
9. An exact match is required. Usually two are required for SMB_COM_TRANSACTION commands.
10. An exact match is required. Only 16 word transactions are decoded.

Service SNMP Engine

The Service SNMP engine inspects all SNMP packets destined for port 161. You can tune SNMP signatures and create custom SNMP signatures based on specific community names and object identifiers.

Instead of using string comparison or regular expression operations to match the community name and object identifier, all comparisons are made using the integers to speed up the protocol decode and reduce storage requirements.

Table B-24 lists the parameters specific to the Service SNMP engine.

Table B-24 Service SNMP Engine Parameters

Parameter	Description	Value
inspection-type	Type of inspection to perform.	—
brute-force-inspection	Inspects for brute force attempts: <ul style="list-style-type: none"> brute-force-count—The number of unique SNMP community names that constitute a brute force attempt. 	0 to 65535
invalid-packet-inspection	Inspects for SNMP protocol violations.	—
non-snmp-traffic-inspection	Inspects for non-SNMP traffic destined for UDP port 161.	—
snmp-inspection	Inspects SNMP traffic: <ul style="list-style-type: none"> specify-community-name [yes no]: <ul style="list-style-type: none"> community-name—Searches for the SNMP community name, that is, the SNMP password. specify-object-id [yes no]: <ul style="list-style-type: none"> object-id—Searches for the SNMP object identifier. 	<i>community-name</i> <i>object-id</i>

Service SSH Engine

The Service SSH engine specializes in port 22 SSH traffic. Because all but the setup of an SSH session is encrypted, the engine only looks at the fields in the setup. There are two default signatures for SSH. You can tune these signatures, but you cannot create custom signatures.

Table B-25 lists the parameters specific to the Service SSH engine.

Table B-25 Service SSH Engine Parameters

Parameter	Description	Value
length-type	Inspects for one of the following SSH length types: <ul style="list-style-type: none"> key-length—Length of the SSH key to inspect for: <ul style="list-style-type: none"> length—Keys larger than this fire the RSAREF overflow. user-length—User length SSH inspection: <ul style="list-style-type: none"> length—Keys larger than this fire the RSAREF overflow. 	0 to 65535
service-ports	A comma-separated list of ports or port ranges where the target service resides.	0 to 65535 ¹ a-b[,c-d]
specify-packet-depth	(Optional) Enables packet depth: <ul style="list-style-type: none"> packet-depth—Number of packets to watch before determining the session key was missed. 	0 to 65535

1. The second number in the range must be greater than or equal to the first number.

State Engine

The State engine provides state-based regular expression-based pattern inspection of TCP streams. A state engine is a device that stores the state of something and at a given time can operate on input to transition from one state to another and/or cause an action or output to take place. State machines are used to describe a specific event that causes an output or alarm.

There are three state machines in the State engine: SMTP, Cisco Login, and LPR Format String.

Table B-26 lists the parameters specific to the State engine.

Table B-26 State Engine Parameters

Parameter	Description	Value
state-machine	State machine grouping.	—
cisco-login	Specifies the state machine for Cisco login: <ul style="list-style-type: none"> state-name—Name of the state required before the signature fires an alert: <ul style="list-style-type: none"> Cisco device state Control-C state Password prompt state Start state 	cisco-device control-c pass-prompt start
lpr-format-string	Specifies the state machine to inspect for the LPR format string vulnerability: <ul style="list-style-type: none"> state-name—Name of the state required before the signature fires an alert: <ul style="list-style-type: none"> Abort state to end LPR Format String inspection Format character state State state 	abort format-char start
smtp	Specifies the state machine for the SMTP protocol: <ul style="list-style-type: none"> state-name—Name of the state required before the signature fires an alert: <ul style="list-style-type: none"> Abort state to end LPR Format String inspection Mail body state Mail header state SMTP commands state Start state 	abort mail-body mail-header smtp-commands start
direction	Direction of the traffic: <ul style="list-style-type: none"> Traffic from service port destined to client port. Traffic from client port destined to service port. 	from-service to-service

Table B-26 State Engine Parameters (continued)

Parameter	Description	Value
service-ports	A comma-separated list of ports or port ranges where the target service resides.	0 to 65535 a-b[,c-d] ¹
specify-exact-match-offset	(Optional) Enables exact match offset: <ul style="list-style-type: none"> exact-match-offset—The exact stream offset the regular expression string must report for a match to be valid. 	0 to 65535
specify-min-match-length	(Optional) Enables minimum match length: <ul style="list-style-type: none"> min-match-length—Minimum number of bytes the regular expression string must match. 	0 to 65535
swap-attacker-victim	True if address (and ports) source and destination are swapped in the alert message. False for no swap (default).	true false

1. The second number in the range must be greater than or equal to the first number.

String Engines

This section describes the String engine, and contains the following topics:

- [Overview, page B-32](#)
- [String ICMP Engine Parameters, page B-33](#)
- [String TCP Engine Parameters, page B-33](#)
- [String UDP Engine Parameters, page B-34](#)

Overview

The String engine is a generic-based pattern-matching inspection engine for ICMP, TCP, and UDP protocols. The String engine uses a regular expression engine that can combine multiple patterns into a single pattern-matching table allowing for a single search through the data.

There are three String engines: String ICMP, String TCP, and String UDP.

String ICMP Engine Parameters

For an example custom String engine signature, see [Example String TCP Signature, page 6-28](#).

[Table B-27](#) lists the parameters specific to the String ICMP engine.

Table B-27 String ICMP Engine Parameters

Parameter	Description	Value
direction	Direction of the traffic: <ul style="list-style-type: none"> Traffic from service port destined to client port. Traffic from client port destined to service port. 	from-service to-service
icmp-type	ICMP header TYPE value.	0 to 18 ¹ a-b[,c-d]
specify-exact-match-offset	(Optional) Enables exact match offset: <ul style="list-style-type: none"> exact-match-offset—The exact stream offset the regular expression string must report for a match to be valid. 	0 to 65535
specify-min-match-length	(Optional) Enables minimum match length: <ul style="list-style-type: none"> min-match-length—Minimum number of bytes the regular expression string must match. 	0 to 65535
swap-attacker-victim	True if address (and ports) source and destination are swapped in the alert message. False for no swap (default).	true false

1. The second number in the range must be greater than or equal to the first number.

String TCP Engine Parameters

For an example custom String engine signature, see [Example String TCP Signature, page 6-28](#).

[Table B-28](#) lists the parameters specific to the String TCP engine.

Table B-28 String TCP Engine

Parameter	Description	Value
direction	Direction of the traffic: <ul style="list-style-type: none"> Traffic from service port destined to client port. Traffic from client port destined to service port. 	from-service to-service
service-ports	A comma-separated list of ports or port ranges where the target service resides.	0 to 65535 ¹ a-b[,c-d]
specify-exact-match-offset	(Optional) Enables exact match offset: <ul style="list-style-type: none"> exact-match-offset—The exact stream offset the regular expression string must report for a match to be valid. 	0 to 65535

Table B-28 String TCP Engine (continued)

Parameter	Description	Value
specify-min-match-length	(Optional) Enables minimum match length: <ul style="list-style-type: none"> min-match-length—Minimum number of bytes the regular expression string must match. 	0 to 65535
strip-telnet-options	Strips the Telnet option characters from the data before the pattern is searched. ²	true false
swap-attacker-victim	True if address (and ports) source and destination are swapped in the alert message. False for no swap (default).	true false

1. The second number in the range must be greater than or equal to the first number.
2. This parameter is primarily used as an IPS anti-evasion tool.

String UDP Engine Parameters

For an example custom String engine signature, see [Example String TCP Signature, page 6-28](#).

[Table B-29](#) lists the parameters specific to the String UDP engine.

Table B-29 String UDP Engine

Parameter	Description	Value
direction	Direction of the traffic: <ul style="list-style-type: none"> Traffic from service port destined to client port. Traffic from client port destined to service port. 	from-service to-service
service-ports	A comma-separated list of ports or port ranges where the target service resides.	0 to 65535 ¹ a-b[,c-d]
specify-exact-match-offset	(Optional) Enables exact match offset: <ul style="list-style-type: none"> exact-match-offset—The exact stream offset the regular expression string must report for a match to be valid. 	0 to 65535
specify-min-match-length	(Optional) Enables minimum match length: <ul style="list-style-type: none"> min-match-length—Minimum number of bytes the regular expression string must match. 	0 to 65535
swap-attacker-victim	True if address (and ports) source and destination are swapped in the alert message. False for no swap (default).	true false

1. The second number in the range must be greater than or equal to the first number.

Sweep Engine

The Sweep engine analyzes traffic between two hosts or from one host to many hosts. You can tune the existing signatures or create custom signatures. The Sweep engine has protocol-specific parameters for ICMP, UDP, and TCP.

The alert conditions of the Sweep engine ultimately depend on the count of the unique parameter. The unique parameter is the threshold number of distinct hosts or ports depending on the type of sweep. The unique parameter triggers the alert when more than the unique number of ports or hosts is seen on the address set within the time period. The processing of unique port and host tracking is called counting.

You can configure source and destination address filters, which means the sweep signature will exclude these addresses from the sweep-counting algorithm.

**Caution**

Event action filters based on source and destination IP addresses do not function for the Sweep engine, because they do not filter as regular signatures. To filter source and destination IP addresses in sweep alerts, use the source and destination IP address filter parameters in the Sweep engine signatures.

A unique parameter must be specified for all signatures in the Sweep engine. A limit of 2 through 40 (inclusive) is enforced on the sweeps. 2 is the absolute minimum for a sweep, otherwise, it is not a sweep (of one host or port). 40 is a practical maximum that must be enforced so that the sweep does not consume excess memory. More realistic values for unique range between 5 and 15.

TCP sweeps must have a TCP flag and mask specified to determine which sweep inspector slot in which to count the distinct connections.

The ICMP sweeps must have an ICMP type specified to discriminate among the various types of ICMP packets.

Table B-30 lists the parameters specific to the Sweep engine.

Table B-30 Sweep Engine Parameters

Parameter	Description	Value
dst-addr-filter	Destination IP address to exclude from the sweep counting algorithm.	<A.B.C.D>- <A.B.C.D> [,<A.B.C.D>- <A.B.C.D>]
src-addr-filter	Source IP address to exclude from the sweep counting algorithm.	<A.B.C.D>- <A.B.C.D> [,<A.B.C.D>- <A.B.C.D>]
protocol	Protocol of interest for this inspector.	icmp udp tcp
specify-icmp-type	(Optional) Enables the ICMP header type: <ul style="list-style-type: none"> icmp-type—ICMP header TYPE value. 	0 to 255
specify-port-range	(Optional) Enables using a port range for inspection: <ul style="list-style-type: none"> port-range—UDP port range used in inspection. 	0 to 65535 a-b[,c-d]
fragment-status	Specifies whether fragments are wanted or not: <ul style="list-style-type: none"> Any fragment status. Do not inspect fragments. Inspect fragments. 	any no-fragments want-fragments
inverted-sweep	Uses source port instead of destination port for unique counting.	true false

Table B-30 Sweep Engine Parameters (continued)

Parameter	Description	Value
mask	Mask used in TCP flags comparison: <ul style="list-style-type: none"> • URG bit • ACK bit • PSH bit • RST bit • SYN bit • FIN bit 	urg ack psh rst syn fin
storage-key	Type of address key used to store persistent data: <ul style="list-style-type: none"> • Attacker address • Attacker and victim addresses • Attacker address and victim port 	Axxx AxBx Axxb
suppress-reverse	Does not fire when a sweep has fired in the reverse direction on this address set.	true false
swap-attacker-victim	True if address (and ports) source and destination are swapped in the alert message. False for no swap (default).	true false
tcp-flags	TCP flags to match when masked by mask: <ul style="list-style-type: none"> • URG bit • ACK bit • PSH bit • RST bit • SYN bit • FIN bit 	urg ack psh rst syn fin
unique	Threshold number of unique port connections between the two hosts.	0 to 65535

Traffic ICMP Engine

The Traffic ICMP engine analyzes nonstandard protocols, such as TFN2K, LOKI, and DDOS. There are only two signatures (based on the LOKI protocol) with user-configurable parameters.

Tribe Flood Net 2000 (TFN2K) is the newer version of the TFN. It is a Distributed Denial Of Service (DDoS) agent that is used to control coordinated attacks by infected computers (zombies) to target a single computer (or domain) with bogus traffic floods from hundreds or thousands of unknown attacking hosts. TFN2K sends randomized packet header information, but it has two discriminators that can be used to define signatures. One is whether the L3 checksum is incorrect and the other is whether the character 64 'A' is found at the end of the payload. TFN2K can run on any port and can communicate with ICMP, TCP, UDP, or a combination of these protocols.

LOKI is a type of back door Trojan. When the computer is infected, the malicious code creates an “Icmp Tunnel” that can be used to send small payload in ICMP replies (which may go straight through a firewall if it is not configured to block ICMP.) The LOKI signatures look for an imbalance of ICMP echo requests to replies and simple ICMP code and payload discriminators.

The DDoS category (excluding TFN2K) targets ICMP-based DDoS agents. The main tools used here are TFN (Tribe Flood Net) and Stacheldraht. They are similar in operation to TFN2K, but rely on ICMP only and have fixed commands: integers and strings.

Table B-31 lists the parameters specific to the Traffic ICMP engine.

Table B-31 TRAFFIC.ICMP Engine Parameters

Parameter	Description	Value
parameter-tunable-sig	Whether this signature has configurable parameters.	yes no
inspection-type	Type of inspection to perform: <ul style="list-style-type: none"> Inspects for original LOKI traffic. Inspects for modified LOKI traffic. 	is-loki is-mod-loki
reply-ratio	Inbalance of replies to requests. The alert fires when there are this many more replies than requests.	0 to 65535
want-request	Requires an ECHO REQUEST be seen before firing the alert.	true false

Trojan Engines

The Trojan engines analyze nonstandard protocols, such as BO2K and TFN2K. There are three Trojan engines: Trojan BO2K, Trojan TFN2K, and Trojan UDP.

BackOrifice (BO) was the original Windows back door Trojan that ran over UDP only. It was soon superseded by BackOrifice 2000 (BO2K). BO2K supported UDP and TCP both with basic XOR encryption. They have plain BO headers that have certain cross-packet characteristics.

BO2K also has a stealthy TCP module that was designed to encrypt the BO header and make the cross-packet patterns nearly unrecognizable.

The UDP modes of BO and BO2K are handled by the Trojan UDP engine. The TCP modes are handled by the Trojan BO2K engine.

There are no specific parameters to the Trojan engines, except for swap-attacker-victim in the Trojan UDP engine.

