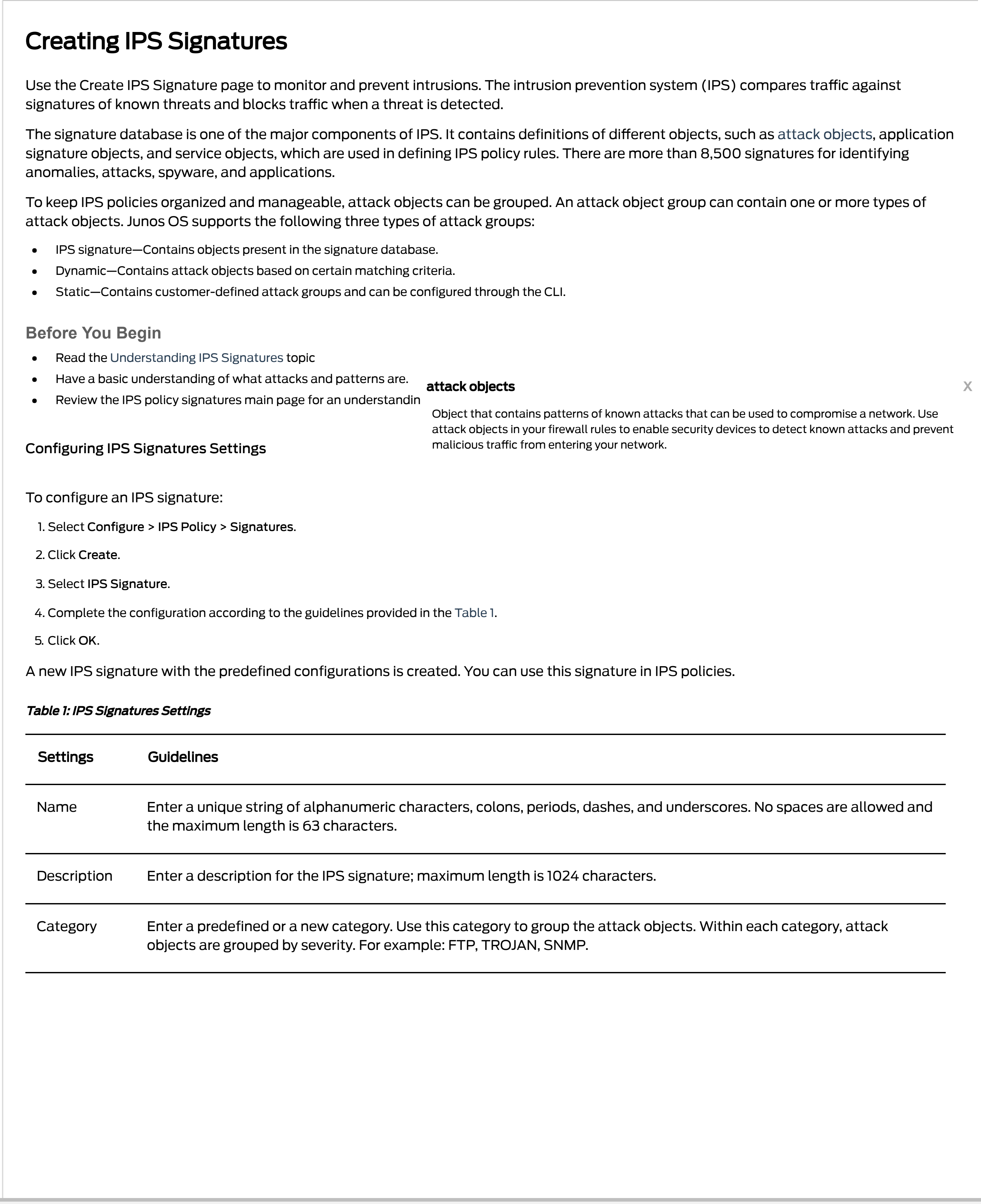
EXHIBIT 20

TechLibrary > Junos Space Security Director ▾ > Security Director Application Guide



Creating IPS Signatures

Use the Create IPS Signature page to monitor and prevent intrusions. The intrusion prevention system (IPS) compares traffic against signatures of known threats and blocks traffic when a threat is detected.

The signature database is one of the major components of IPS. It contains definitions of different objects, such as attack objects, application signature objects, and service objects, which are used in defining IPS policy rules. There are more than 8,500 signatures for identifying anomalies, attacks, spyware, and applications.

To keep IPS policies organized and manageable, attack objects can be grouped. An attack object group can contain one or more types of attack objects. Junos OS supports the following three types of attack groups:

- IPS signature—Contains objects present in the signature database.
- Dynamic—Contains attack objects based on certain matching criteria.
- Static—Contains customer-defined attack groups and can be configured through the CLI.

Before You Begin

- Read the Understanding IPS Signatures topic
- Have a basic understanding of what attacks and patterns are.
- Review the IPS policy signatures main page for an understandin

attack objects X

Object that contains patterns of known attacks that can be used to compromise a network. Use attack objects in your firewall rules to enable security devices to detect known attacks and prevent malicious traffic from entering your network.

Configuring IPS Signatures Settings

To configure an IPS signature:

1. Select **Configure** > **IPS Policy** > **Signatures**.
2. Click **Create**.
3. Select **IPS Signature**.
4. Complete the configuration according to the guidelines provided in the Table 1.
5. Click OK.

A new IPS signature with the predefined configurations is created. You can use this signature in IPS policies.

Table 1: IPS Signatures Settings

Settings	**Guidelines**
Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 63 characters.
Description	Enter a description for the IPS signature; maximum length is 1024 characters.
Category	Enter a predefined or a new category. Use this category to group the attack objects. Within each category, attack objects are grouped by severity. For example: FTP, TROJAN, SNMP.

Settings	Guidelines
Action	Select an action you want IPS signature to take when the monitored traffic matches the attack objects specified in the rules: • None—No action is taken. Use this action to only generate logs for some traffic. • Close Client & Server—Closes the connection and sends an RST packet to both the client and the server. • Close Client—Closes the connection and sends an RST packet to the client but not to the server. • Close Server—Closes the connection and sends an RST packet to the server but not to the client. • Ignore—Stops scanning traffic for the rest of the connection if an attack match is found. IPS disables the rulebase for the specific connection. • Drop—Drops all packets associated with the connection, preventing traffic for the connection from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing. • Drop Packet—Drops a matching packet before it can reach its destination but does not close the connection. Use this action to drop packets for attacks in traffic that is prone to spoofing, such as UDP traffic. Dropping a connection for such traffic could result in a denial of service that prevents you from receiving traffic from a legitimate source-IP address.
Keywords	Enter unique identifiers that can be used to search and sort log records. Keywords should related to the attack and the attack object. For example, **Amanda Amindexd Remote Overflow**.
Severity	Select a severity level for the attack that the signature will report: • Critical—Contains attack objects matching exploits that attempt to evade detection, cause a network device to crash, or gain system-level privileges. • Info—Contains attack objects matching normal, harmless traffic containing URLs, DNS lookup failures, SNMP public community strings, and peer-to-peer (P2P) parameters. You can use informational attack objects to obtain information about your network. • Major—Contains attack objects matching exploits that attempt to disrupt a service, gain user-level access to a network device, or activate a Trojan horse previously loaded on a device. • Minor—Contains attack objects matching exploits that detect reconnaissance efforts attempting to access vital information through directory traversal or information leaks. • Warning—Contains attack objects matching exploits that attempt to obtain noncritical information or scan a network with a scanning tool. The most dangerous level is critical, which attempts to crash your server or gain control of your network. Informational is the least dangerous level and is used by network administrators to discover holes in their security systems.
Signature Details	
Binding	Select an option to detect the service or protocol that the attack uses to enter your network: • IP—Allows IPS to match the signature for a specified IP protocol type. • ICMP—Allows IPS to match the signature for a specified ICMP ID. • TCP—Allows IPS to match the signature for specified TCP port(s). • UDP—Allows IPS to match the signature for specified UDP port(s). • RPC—Allows IPS to match the signature for a specified remote procedure call (RPC) program number. The RPC protocol is used by distributed processing applications to handle interaction between processes remotely. • Service—Allows IPS to match the signature for a specified service. • IPv6 or ICMPv6—Specifies the header match information for the signature attack. You can specify that IPS search a packet for a pattern match for IPv6 and ICMPv6 header information.
Protocol	Enter the name of the network protocol. For example: IGMP, IP-IP.
Next Header	Enter the type of IP protocol for the header that immediately follows the IPv6 header. For example, if the device performs IPsec on exchanged packets, the Next Header value is probably 50 (ESP extension header) or 51 (AH extension header).
Port Range(s)	Enter the port ranges for TCP and UDP protocol types.
Program	Enter the program ID for the RPC protocol.

Settings	Guidelines
Service	Specify the service that the attack uses to enter your network. You can select the specific service used to perpetrate the attack as the service binding. For example, suppose you select the DISCARD service. Discard protocol is an Application Layer protocol where TCP/9, UDP/9 describes the process for discarding TCP or UDP data sent to port 9.
Time Scope	Select the scope within which the count of an attack occurs: • Source IP—Detect attacks from the source address for the specified number of times, regardless of the destination address. • Dest IP—Detect attacks sent to the destination address for the specified number of times, regardless of the source address. • Peer—Detect attacks between source and destination IP addresses of the sessions for the specified number of times.
Time Count	Specify the number of times that the attack object must detect an attack within the specified scope before the device considers the attack object to match the attack. The range is from 0 through 4,294,967,295.
Match Assurance	Specify this filter to track attack objects based on the frequency that the attack produces a false positive on your network. Select an option: • High—Provides information on the frequently tracked false positive occurrences. • Medium—Provides information on the occasionally tracked false positive occurrences. • Low—Provides information on the rarely tracked false positive occurrences.
Performance Impact	Specify this filter to filter out slow-performing attack objects. You can use this filter to only select the appropriate attacks based on performance impacts. Select an option: • High—Add a high performance impact attack object that is vulnerable to an attack. The performance impact of signatures is high7 to high9, where the application identification is slow. • Medium—Add a medium performance impact attack object that is vulnerable to an attack. The performance impact of signatures is medium4 to medium6, where the application identification is normal. • Low—Add a low performance impact attack object that is vulnerable to an attack. The performance impact of signatures is low1 to low3, where the application identification is faster. • Unknown—Set all attack objects to unknown by default. As you fine-tune IPS to your network traffic, you can change this setting to help you track performance impact. The performance impact of signatures is 0 = unknown, where the application identification is also unknown.
Expression	Enter a Boolean expression of attack members used to identify the way attack members should be matched. For example: m01 AND m02, where m01, m02 are the attack members.
Scope	Specify if the attack is matched within a session or across transactions in a session: • session—Allows multiple matches for the object within the same session. • transaction—Matches the object across multiple transactions that occur within the same session.
Reset	Enable this option to generate a new log each time an attack is detected within the same session. If this option is not selected, then the attack is logged only once per session.
Ordered	Enable this option to create a compound attack object that must match each member signature or protocol anomaly in the order you specify. If you do not specify an order, the compound attack object still must match all members, but the pattern or protocol anomalies can appear in the attack in any order. A compound attack object detects attacks that use multiple methods to exploit a vulnerability.

Settings	Guidelines
Add Signature	
Context	Select an option to define the location of the signature. If you know the service and the specific service context, specify that service and then specify the appropriate service contexts. If you know the service, but are unsure of the specific service context, specify one of the general contexts. For example: line—Specify this context to detect a pattern match within a specific line within your network traffic.
Direction	Specify the connection direction of the attack: • Client to Server—Detects the attack only in client-to-server traffic. • Server to Client—Detects the attack only in server-to-client traffic. • Any—Detects the attack in either direction. Using a single direction (instead of Any) improves performance, reduces false positives, and increases detection accuracy.
Pattern	Enter a signature pattern of the attack you want to detect. A signature is a pattern that always exists within an attack; if the attack is present, so is the signature. To create the attack pattern, you must first analyze the attack to detect a pattern (such as a segment of code, a URL, or a value in a packet header), and then create a syntactical expression that represents that pattern. For example: Use \[<character-set>\] for case-insensitive matches.
Regex	Enter a regular expression to define rules to match malicious or unwanted behavior over the network. For example: For the syntax \[hello\], the expected pattern is hello, which is case sensitive. The example matches can be: hElLo, HEllO, and heLLO.
Negated	Select this option to exclude the specified pattern from being matched. Negating a pattern means that the attack is considered matched if the pattern defined in the attack does not match the specified pattern.
Add Anomaly	
Anomaly	Select an option to detect abnormal or ambiguous messages within a connection according to the set of rules for the particular protocol being used. Protocol anomaly detection works by finding deviations from protocol standards, most often defined by RFCs and common RFC extensions.
Direction	Specify the connection direction of the attack: • Client to Server—Detects the attack only in client-to-server traffic. • Server to Client—Detects the attack only in server-to-client traffic. • Any—Detects the attack in either direction. Using a single direction (instead of Any) improves performance, reduces false positives, and increases detection accuracy.
Supported Detectors	Click the **Supported Detectors** link to display a table that shows the device platforms and the version number of the IPS protocol detector currently running on the device. For example: • Platform - SRX550

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**