

Creating Custom Attack Objects (NSM Procedure)

This section includes the following:

- Configuring General Properties for Attack Objects on page 1
- Creating a Signature Attack Object on page 3

Configuring General Properties for Attack Objects

To create a custom attack object:

1. In the Object Manager, click **Attack Objects > IDP Objects** to display the IDP Objects dialog box.
2. Click the **Custom Attacks** tab.
3. Click the + icon to display the Custom Attack dialog box.
4. Configure general attack object settings using Table 1 on the General tab.

Table 1: Custom Attack Dialog Box: General Tab Settings

Setting	Description
Name	Specifies the name to be displayed in the UI. TIP: You might want to include the protocol the attack uses as part of the attack name.
Description	Specifies details about the attack. Entering a description is optional when creating a new attack object, but it can help you remember important information about the attack. View the attack descriptions for predefined attacks for examples.
Severity	Specifies a severity rating: Info, Warning, Minor, Major, or Critical. Critical attacks are the most dangerous—typically these attacks attempt to crash your server or gain control of your network. Informational attacks are the least dangerous and typically are used by network administrators to discover holes in their own security system.
Category	Specifies a predefined category or defines a new category.
Keywords	Specifies keywords—unique identifiers that can be used to search and sort log records.
Recommended	Specifies that this attack object is part of your highest risk set of attack objects. Later, when you add this attack object to dynamic groups, you can specify whether only recommended attack objects will be included.
Attack Versions	Skip this for now.
Detection Performance	Select High , Medium , Low , or Not Defined .

5. On the Extended tab, using Table 2. Configure additional attack details.

Table 2: Custom Attack Dialog Box: Extended Tab Settings

Setting	Description
Primary URL Secondary URL Tertiary URL	Enter up to three URLs (primary, secondary, tertiary) for external references you used when researching the attack.
CVE	Common Vulnerabilities and Exposures (CVE) is a standardized list of vulnerabilities and other information security exposures. The CVE number is an alphanumeric code, such as CVE-2209
Bugtraq	A moderated mailing list that discusses and announces computer security vulnerabilities. The BugTraq ID number is a three-digit code, such as 831 or 120.
Impact	Enter details about the impact of a successful attack, including information on system crashes and access granted to the attacker.
Description	Enter a description of the custom attacks.
Tech Info	Enter details on the vulnerability, the commands used to execute the attack, which files are attacked, registry edits, and other low-level information.
Patches	List any patches available from the product vendor, as well as information on how to prevent the attack.

6. Return to the General tab.
7. Under Attack Versions, click the + icon to display the New Attack wizard.
8. On the Target Platform and Type page, select a device platform (IDP 4.0, for example) and attack type.

Table 3 summarizes attack types and provides references to the next steps required to implement the technical configuration of the attack objects for each type.

Table 3: Attack Object Types

Type	Description
Signature	<p>Uses a stateful attack signature (a pattern that always exists within a specific section of the attack) to detect known attacks.</p> <p>Stateful signature attack objects also include the protocol or service used to perpetrate the attack and the context in which the attack occurs.</p> <p>If you know the exact attack signature, the protocol, and the attack context used for a known attack, select this option.</p>

Table 3: Attack Object Types (continued)

Type	Description
Protocol Anomaly	<p>Detects unknown or sophisticated attacks that violate protocol specifications (RFCs and common RFC extensions).</p> <p>You cannot create new protocol anomalies, but you can configure a new attack object that controls how the security device handles a predefined protocol anomaly when detected.</p> <p>If you do not know that exact attack signature, but you do know the protocol anomaly that detects the attack, select this option.</p>
Compound Attack	<p>Detects attacks that use multiple methods to exploit a vulnerability. This object combines multiple signatures and/or protocol anomalies into a single attack object, forcing traffic to match all combined signatures and/or anomalies within the compound attack object before traffic is identified as an attack.</p> <p>By combining and even specifying the order in which signatures or anomalies must match, you can be very specific about the events that need to take place before IDP identifies traffic as an attack.</p> <p>If you need to detect an attack that uses several benign activities to attack your network, or if you want to enforce a specific sequence of events to occur before the attack is considered malicious, select this option</p>

9. Click **Ok**.

Creating a Signature Attack Object

To configure a signature attack object:

1. Configure general attack object properties. For information, see “Configuring General Properties for Attack Objects” on page 1.

On the Target Platform and Type page, select **Signature** and click **Next**.

2. On the Custom Attack–General Properties page, configure the settings described in Table 4.

Table 4: Custom Attack – General Properties

Property	Description
False Positives	Select the frequency that the attack object produces a false positive on your network: Unknown, Rarely, Occasionally, Frequently .

Table 4: Custom Attack – General Properties (continued)

Property	Description
Service Binding	<p>Any–If you are unsure of the correct service, select Any to match the signature in all services. Because some attacks use multiple services to attack your network, you might want to select the Any service binding to detect the attack regardless of which service the attack selects for a connection.</p> <p>NOTE: You must select a service binding other than Any if you want to select a context for the attack.</p> <hr/> <p>IP–If you are not sure of the correct service, but know the IP protocol type, select IP protocol type for the service binding.</p> <p>Specify the protocol type number.</p> <p>If you select this option, you should also specify an attack pattern and IP header values later in the wizard. However, if you use a context binding of first packet, you must leave the attack pattern empty.</p> <hr/> <p>TCP, UDP, or ICMP–Attacks that do not use a specific service might use a specific protocol to attack your network. Some TCP and UDP attacks use standard ports to enter your network and establish a connection.</p> <p>For TCP and UDP protocol types, specify the port ranges.</p> <hr/> <p>RPC–The remote procedure call (RPC) protocol is used by distributed processing applications to handle interaction between processes remotely. When a client makes a remote procedure call to an RPC server, the server replies with a remote program; each remote program uses a different program number.</p> <p>To detect attacks that use RPC, configure the service binding as RPC and specify the RPC program ID.</p> <hr/> <p>Service–Most attacks use a specific service to attack your network.</p> <p>If you select Service, the wizard displays a second selection box where you specify the service used for the attack.</p> <p>If you select this option, you are restricted to general attack contexts (packet, first packet, stream, stream 256, or line context).</p>
Time Binding	<p>Enable–Time attributes control how the attack object identifies attacks that repeat for a certain number of times.</p> <hr/> <p>Scope–Select the scope within which the count occurs:</p> <ul style="list-style-type: none"> ■ Source– Detects attacks from the source IP address for the specified number of times, regardless of the destination IP address. ■ Destination–Detects attacks to the destination IP address for the specified number of times, regardless of the source IP address. ■ Peer–Detects attacks between source and destination IP addresses of the sessions for the specified number of times. <hr/> <p>Count/Min–Enter the number of times per minute that the attack object must detect an attack within the specified scope before the device considers the attack object to match the attack.</p>

Click **Next**.

3. On the Custom Attack – Attack Patterns page, configure the settings described in Table 5.

Table 5: Custom Attack – Attack Patterns

Setting	Description	
Pattern	\0 <octal_number >	For a direct binary match.
	\X <hexadecimal-number > \X	For a direct binary match.
	\[<character-set > \]	For case insensitive matches.
	.	To match any symbol.
	*	To match 0 or more symbols.
	+	To match 1 or more symbols.
	?	To match 0 or 1 symbols.
	()	Grouping of expressions.
		Alternation. Typically used with ().
	[<start > - <end >]	Character range.
	[^ <start > - <end >]	Negation of character range.
Negate	Select this option to negate the attack pattern.	

Table 5: Custom Attack – Attack Patterns (continued)

Setting	Description
Context	<p>Select the context used by the attack to enter your network.</p> <p>If you know the service and the specific service context, select that service and then select the appropriate service contexts.</p> <p>If you know the service, but are unsure of the specific service context, select Other and then select one of the following general contexts:</p> <ul style="list-style-type: none">■ Packet–Detects the pattern at the packet level. When you select this option, you should also specify the Service Binding (in the General tab) and define the service header options (in the Header Match tab). Although not required, specifying these additional parameters helps to improve the accuracy of the attack object.■ First Packet–Inspects only the first packet of a stream. When the flow direction for the Attack Object is set to any, IDP checks the first packet of both the server-to-client (STC) and client-to-server (CTS) flows. If you know that the attack signature appears in the first packet of a session, choosing first packet instead of packet reduces the amount of traffic the security device needs to monitor, which improves performance.■ Stream Select–Reassembles packets and extracts the data to search for a pattern match. However, IDP does not recognize packet boundaries for stream contexts, so data for multiple packets is combined. Select this option only when no other context option contains the attack.■ Stream 256–Reassembles packets and searches for a pattern match within the first 256 bytes of a traffic stream. When the flow direction is set to any, DI checks the first 256 bytes of both the STC and CTS flows. If you know that the attack signature will appear in the first 256 bytes of a session, choosing stream 256 instead of stream reduces the amount of traffic that the security device must monitor and cache, improving performance.■ Line–Detects a pattern match within a specific line within your network traffic.
Direction	<p>Select the direction in which to detect the attack:</p> <ul style="list-style-type: none">■ 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.
Flow	<p>Select the flow in which to detect the attack:</p> <ul style="list-style-type: none">■ Control–Detects the attack in the initial connection that is established persistently to issue commands, requests, and so on.■ Auxiliary–Detects the attack in the response connection established intermittently to transfer requested data.■ Both–Detects the attack in the initial and response connections. <p>TIP: Using a single flow (instead of Both) improves performance and increases detection accuracy.</p>

Click **Next**.

4. On the Custom Attack – IP Settings and Header Matches page, specify signature settings as described in Table 6.



NOTE: The IP tab specifies the contents of the IP header in a malicious packet. You cannot specify IP header contents if you selected a line, stream, stream 256, or a service context in the Attack Patterns tab.



TIP: If you are unsure of the IP flags and IP fields for the malicious packet, leave all fields blank. If not values are set, IDP attempts to match the signature for all IP header contents.

Table 6: Custom Attack: IP Settings and Header Matches

Setting	Description
Type of Service	Enter the service type. Common service types are: <ul style="list-style-type: none">■ 0000 Default■ 0001 Minimize Cost■ 0002 Maximize Reliability■ 0003 Maximize Throughput■ 0004 Minimize Delay■ 0005 Maximize Security
Total Length	Enter the number of bytes in the packet, including all header fields and the data payload.
ID	Enter the unique value used by the destination system to reassemble a fragmented packet.
Time-to-live	Enter the time-to-live (TTL) value of the packet. This value represents the number of routers the packet can pass through. Each router that processes the packet decrements the TTL by 1; when the TTL reaches 0, the packet is discarded.
Protocol	Enter the protocol used in the attack.
Source	Specify the IP address of the attacking device.
Destination	Specify the IP address of the attack target.
RB	Reserved bit. Specifies that IDP looks for a pattern match whether or not the IP flag is set (none), only if the flag is set (set), or only if the flag is not set (unset).
MF	More fragments. Specifies that IDP looks for a pattern match whether or not the IP flag is set (none), only if the flag is set (set), or only if the flag is not set (unset).
DF	Don't fragment. Specifies that IDP looks for a pattern match whether or not the IP flag is set (none), only if the flag is set (set), or only if the flag is not set (unset).

5. If you selected TCP for Service Binding and packet or first-data-packet as the Context, click the **Protocols** tab, select TCP packet header fields, and configure TCP Header Match settings as described in Table 7.

Table 7: TCP Header Match Settings

Setting	Description
Source Port	The port number on the attacking device.
Destination Port	The port number of the attack target.
Sequence Number	The sequence number of the packet. This number identifies the location of the data in relation to the entire data sequence.
ACK Number	The ACK number of the packet. This number identifies the next sequence number; the ACK flag must be set to activate this field.
Header Length	The number of bytes in the TCP header.
Window Size	The number of bytes in the TCP window size.
Data Length	The number of bytes in the data payload. For SYN, ACK, and FIN packets, this field should be empty.
Urgent Pointer	The data in the packet is urgent; the URG flag must be set to activate this field.
URG Bit	When set, the urgent flag indicates that the packet data is urgent.
ACK Bit	When set, the acknowledgment flag acknowledges receipt of a packet.
PSH Bit	When set, the push flag indicates that the receiver should push all data in the current sequence to the destination application (identified by the port number) without waiting for the remaining packets in the sequence.
RST Bit	When set, the reset flag resets the TCP connection, discarding all packets in an existing sequence.
FIN Bit	When set, the final flag indicates that the packet transfer is complete and the connection can be closed.
R1 Bit, R2 Bit	Reserved bit. Unused.

- If you selected UDP for Service Binding and packet or first-data-packet as the Context, click the **Protocols** tab, select UDP packet header fields, and configure UDP Header Match settings as described in Table 8.

Table 8: UDP Header Match Settings

Setting	Description
Source Port	Enter the port number on the attacking device.
Destination Port	Enter the port number of the attack target.
Data Length	Enter the number of bytes in the data payload.

7. If you selected ICMP for Service Binding and packet or first-data-packet as the Context, click the **Protocols** tab, select ICMP packet header fields, and configure ICMP Header Match settings as described in Table 9.

Table 9: ICMP Header Match Settings

Setting	Description
ICMP Type	Enter the primary code that identifies the function of the request/reply.
ICMP Code	Enter the secondary code that identifies the function of the request/reply within a given type.
Sequence Number	Enter the sequence number of the packet. This number identifies the location of the request/reply in relation to the entire sequence.
ICMP ID	Enter the identification number which is a unique value used by the destination system to associate requests and replies.

8. Click **Finish**.

- Related Topics**
- Attack Objects in Intrusion Detection and Prevention Security Policies Overview
 - Working with Attack Groups (NSM Procedure)
 - Viewing Predefined Attack Objects (NSM Procedure)
 - Updating the IDP Detector Engine (NSM Procedure)

Published: 2009-08-20