

Configuring Run-Time Parameters (NSM Procedure)

Run-time parameters include options for tuning IDP detection methods. In general, you modify these settings only if you encounter false positives or performance issues. These options control the security module operations.

To configure run-time parameters:

1. In NSM Device Manager, double-click the IDP device for which you want to configure run-time parameters. The device configuration editor appears
2. Click **Sensor Settings**.
3. Click the **Run-time Parameters** tab.
4. Configure run-time settings using Table 1.
5. Click **Apply**.
6. Click **OK**.

Table 1: IDP Device Configuration: Run-Time Parameters

| Setting | Description |
|--------------------|--|
| Backdoor Detection | <p>Minimum interval between consecutive small packets (microseconds) / Maximum interval between consecutive small packets (microseconds)—Controls the minimum and maximum intervals (in microseconds) between the arrival of two consecutive small packets in suspected interactive traffic. If the IDP device sees small packets arrive in less than the minimum or more than the maximum number of microseconds, it does not consider the traffic to be interactive.</p> <p>The defaults are 20,000 and 2,00,00,000. This means that consecutive small packets must arrive within 20,000 to 2,00,00,000 microseconds to be considered interactive.</p> <p>Byte threshold for packet sizes in a backdoor connection—Controls the maximum number of bytes a TCP packet must contain before the IDP device uses the packet for backdoor detection heuristics. The default is 20 bytes.</p> <p>Minimum number of data carrying TCP packets—Controls the minimum number of data-carrying TCP packets in suspected interactive traffic. The default is 20 packets.</p> <p>Minimum percentage of back-to-back small packets—Controls the minimum percentage of consecutive small packets in suspected interactive traffic. If the IDP device sees less than this percentage, it does not report a backdoor event. The default is 20 %.</p> <p>Ratio of small packets to the total packets (percentage)—Controls the minimum percentage of small packets that the IDP device uses for backdoor detection heuristics. If the IDP device sees less than this minimum, it does not report a backdoor event. The default is 20 %.</p> |

Table 1: IDP Device Configuration: Run-Time Parameters (continued)

| Setting | Description |
|-----------------|--|
| Flow Management | <p>Timeout (seconds) for non-UDP/TCP/ICMP flows—Each connection through the security module typically has two non-UDP/TCP/ICMP flows, one in each direction. If IDP does not see flow activity for the specified timeout, it removes the idle flow from the flow table. The default is 30 seconds.</p> |
| | <p>Timeout (seconds) for UDP flows—Each connection through the security module typically has two UDP flows, one in each direction. If IDP does not see flow activity for the specified timeout, it removes the idle flow from the flow table. The default is 30 seconds.</p> |
| | <p>Timeout (seconds) for TCP flows—Each connection through the security module typically has two TCP flows, one in each direction. If IDP does not see flow activity for the specified timeout, it removes the idle flow from the flow table. The default is 30 seconds.</p> |
| | <p>Timeout (seconds) for ICMP flows—Each connection through the security module typically has two ICMP flows, one in each direction. If IDP does not see flow activity for the specified timeout, it removes the idle flow from the flow table. The default is 30 seconds.</p> |
| | <p>Maximum TCP Sessions—Controls the maximum number of TCP sessions that IDP maintains. If IDP reaches the maximum, it drops all new sessions and writes a SESSION_LIMIT_EXCEEDED log. Defaults vary according to model.</p> |
| | <p>Maximum UDP Sessions—Controls the maximum number of UDP sessions that IDP maintains. If IDP reaches the maximum, it drops all new sessions and writes a SESSION_LIMIT_EXCEEDED log. Defaults vary according to model.</p> |
| | <p>Maximum ICMP Sessions—Control s the maximum number of ICMP sessions that IDP maintains. If IDP reaches the maximum, it drops all new sessions and writes a SESSION_LIMIT_EXCEEDED log. Defaults vary according to model.</p> |
| | <p>Maximum IP (non-UDP/TCP/ICMP) sessions—Controls the maximum number of IP sessions that IDP maintains. If IDP reaches the maximum, it drops all new sessions and writes a SESSION_LIMIT_EXCEEDED log. Defaults vary according to model.</p> |
| | <p>Reset flow table with policy load/unload— Enables IDP to reset the flow table each time you load or unload a security policy. If you do not enable this option, IDP maintains the flow table until all flows referencing that security policy go away. This setting is enabled by default. We recommend that you keep this setting enabled to preserve memory.</p> |
| | <p>Log flow related errors—Enables logging for flow-related errors. This setting is not enabled by default.</p> |
| IP Actions | <p>Reset block table with policy load/unload—Allows the IDP device to reset the block table. The block table maintains the state of active IP actions each time a security policy loads or unloads. This setting is enabled by default.</p> |

Table 1: IDP Device Configuration: Run-Time Parameters (continued)

| Setting | Description |
|---------------------|--|
| Intrusion Detection | <p>Buffer Overflow emulator—Turns on buffer overflow emulation.</p> <hr/> <p>Attack matches per packet when Signature Hierarchy (0 to disable) take effect—Sets the threshold for activating Signature Hierarchy calculations.</p> <p>Common attack can be composed of several known vulnerabilities. Each vulnerability has an attack object, and each would generate a separate log entry if the signature hierarchy feature were disabled.</p> <p>For example, for a policy with critical, high, medium, low, and info attacks and logging enabled, a single detection of HTTP:IIS:COMMAND-EXEC attack generates the following logs:</p> <ul style="list-style-type: none"> ■ HTTP:IIS:COMMAND-EXEC [wininnt/system32/cmd.exe] (medium) ■ HTTP:WIN-CMD:WIN-CMD-EXE [cmd.exe] (medium) ■ HTTP:REQERR:REQ-MALFORMED-URL [anomaly for %xx] (medium) ■ HTTP:DIR:TRAVERSE-DIRECTORY (anomaly for ../) (medium) ■ HTTP:REQERR:REQ-LONG-UTF8CODE (anomaly for oe) (medium) ■ TCP:AUDIT:BAD-SYN-NONSYN (info) ■ HTTP:AUDIT:URL (info) ■ TCP:AUDIT:BAD-SYN-NONSYN (info) <p>If the number of attacks in a packet exceeds the set value, then IDP examines its signature hierarchy to see if some attacks are actually part of a larger attack. If so, then only the parent attack is displayed in the logs. In this example, if the value was set to 9 or lower, then only a log for HTTP:IIS:COMMAND-EXEC would be generated.</p> <p>An attack in the signature hierarchy may have multiple parents or multiple children. If a child attack is part of two discovered parents, IDP takes action based on the parent with the highest severity.</p> <p>Specify 0 to disable.</p> |

Table 1: IDP Device Configuration: Run-Time Parameters (continued)

| Setting | Description |
|---|---|
| Run-time Parameters | RPC program timeout (seconds) –IDP performs a stateful inspection of all RPC messages on port 111, then builds a table of program-to-port mapping for each RPC server that it finds on the network. This setting indicates how long an entry in the table is maintained. The default is 300 seconds. |
| | RPC transaction timeout (Seconds) –All RPC messages (port 111) are based on a request/response protocol. When the IDP receives a request, it adds the request to a request table. If IDP does not receive an RPC reply in the specified timeout, the RPC entry times out. The default is 5 seconds. |
| | Exempt management server flows –Exempts NSM connections from IDP processing. This setting is enabled by default. |
| | Fragment timeout (seconds) –Controls when IDP drops an incomplete fragment chain because one or more fragments did not arrive. If IDP does not receive missing fragments in the specified timeout, it generates a log (FRAGMENT_TIME_EXCEEDED). The default is 5 seconds. |
| | Minimum fragment size (bytes) –IDP drops all IP fragments less than the specified size (bytes). The default is 0 bytes (no fragments are dropped). |
| | Maximum fragments per IP datagram –An IP datagram can be broken into many fragments which, when assembled, should not exceed 64 K. Because IP fragment processing is CPU and memory intensive, this setting controls the size of the IP fragment chain. If the number of fragments in a chain exceeds this number, IDP drops the entire fragment chain. The default is 65,535 bytes. |
| | Maximum concurrent fragments in queue –IDP can perform pseudo reassembly of IP fragment chains. This setting controls the maximum number of reassembled fragment chains. Once this limit is reached, IDP drops all new IP fragment chains and generates a log (TOO_MANY_FRAGMENTS). If your network produces a large number of IP fragments, such as those produced by Network File System (NFS), increase the number of fragments per chain to eliminate unnecessary logs. The default is 16 fragments. |
| | Log fragment related errors –Logs fragment related errors. This setting is not enabled by default. |
| | Enable GRE decapsulation support –Enables IDP to decode generic routing encapsulation (GRE) tunnels where IP-in-GRE or PPP-in-GRE encapsulation is used. This allows IDP to inspect the packet in its original form. GRE decapsulation is not enabled by default. |
| | Enable GTP decapsulation support –Enables GPRS Tunneling Protocol (GTP) decapsulation. IDP supports decapsulation of UDP GTPv0 and GTPv1 only. GTP decapsulation is not enabled by default. |
| Enable SSL decryption support –Enables SSL inspection. SSL decryption is not enabled by default. | |

Table 1: IDP Device Configuration: Run-Time Parameters (continued)

| Setting | Description |
|-----------------|---|
| SYN Protector | <p>Timeout for half-open SYN protected flows—A half-open SYN flow occurs during the TCP three-way handshake, after the client has sent a SYN/ACK packet to the server. The half-open connection is now in the SYN_RECV state, and is placed into a connection queue while it waits for an ACK or RST packet. The connection remains in the queue until the connection-establishment timeout expires and the half-open connection is deleted. This setting controls the connection establishment timer, which determines the number of seconds that the security module maintains a half-open SYN protected flow. The default is 5 seconds.</p> <hr/> <p>Lower SYN's-per-second threshold below which SYN Protector will be deactivated / Upper SYN's-per-second threshold above which SYN Protector will be activated—The SYN Protector rulebase is activated when the number of SYN packets per second is greater than the sum of the lower SYN's-per-second threshold and the upper SYN's-per-second threshold.</p> <p>The SYN Protector rulebase is deactivated when the number of SYN packets per second is less than the lower SYN's-per-second threshold.</p> <p>The defaults are 1000 and 20. The SYN Protector is activated when SYN's-per-second reach 1020 and deactivated when SYN's-per-second fall below 1000.</p> |
| TCP Reassembler | <p>Ignore packets in TCP flows where a SYN hasn't been seen (recommended)—The absence of SYN flags in TCP flows is suspect, yet still a very common occurrence. IDP can ignore packets within TCP flows that do not yet contain a SYN flag. This is enabled by default.</p> <hr/> <p>Close flows as soon as a FIN is seen—Enables when a TCP connection closes, IDP sees a FIN packet from each side of the connection followed by an ACK packet from each side of the connection. However, TCP does not guarantee delivery of the final ACK.</p> <p>Enables IDP to quickly close a TCP connection after receiving a FIN packet. When enabled, IDP maintains a connection waiting for a final ACK for 5 seconds, then closes the connection. This is enabled by default and recommended.</p> <hr/> <p>Timeout for connected, idle TCP flows (seconds)—Controls the number of seconds that IDP maintains connected (but idle) TCP flows. The default is 3600 seconds.</p> <hr/> <p>Timeout for closed TCP flows (seconds)—Controls when IDP sees a RST packet or FIN/FIN + ACK packets on a TCP connection, it closes the connection flows. IDP drops any further packets for the closed flow, but does not delete existing, closed flows from the flow table. Controls the number of seconds that closed TCP flows are maintained in the flow table. The default is 5 seconds.</p> <hr/> <p>Timeout for CLOSE-WAIT/LAST-ACK TCP flows (seconds)—Controls when a TCP connection closes, IDP sees a FIN packet from each side of the connection followed by an ACK packet from each side of the connection. However, TCP does not guarantee delivery of the final ACK.</p> <p>Controls the number of seconds a connection is maintained while waiting for the final ACK.</p> <p>To improve IDP performance during heavy loads, decrease the timeout—this reduces the size of the flow table by closing connections sooner. The default is 120 seconds.</p> |

Table 1: IDP Device Configuration: Run-Time Parameters (continued)

| Setting | Description |
|--------------------|--|
| Traffic Signatures | <p>Byte threshold for suspicious flows—Specifies a threshold for what IDP considers a small packet. A scan typically uses small packets to access its targets. You can exclude suspicious flows that contain large packets to prevent false positives when detecting scans.</p> <p>If IDP sees more than this maximum, it does not consider the connection to be a scan. The default is 20 bytes.</p> <hr/> <p>Reporting frequency when scan is in progress —Controls how often IDP generates "in progress" logs for a stealthy scan.</p> <p>Attackers can perform blatant scans very quickly, mapping your network in just a few seconds, but these scans typically trigger IDSes and leave evidence behind. Stealthy scans are performed over much longer time periods, lasting hours, days, or even weeks, making them more difficult to detect. The default is 30 seconds.</p> <hr/> <p>The number of IP tracked for session rate —Controls the number of IP addresses tracked by the session rate counter. If IDP sees more addresses than the maximum, it does not track the additional IP addresses. The default is 32,767 IP addresses.</p> |

- Related Topics**
- Updating the IDP Detector Engine (NSM Procedure)
 - Configuring SYN Protector Rulebase Rules (NSM Procedure)
 - Configuring Router Parameters (NSM Procedure)

Published: 2009-08-20