

## Viewing NSM Predefined Reports

You can use the predefined reports to validate the effectiveness of your security policies.

Table 1 describes NSM DI/IDP predefined reports. These reports are related to attacks.

**Table 1: NSM DI/IDP Predefined Reports**

Report	Description
Top 100 Attacks (last 24 hours)	Those attacks that are detected most frequently within the last 24 hours.
Top 100 Attacks Prevented (last 24 hours)	Those attacks that are prevented most frequently within the last 24 hours.
Top 20 Attackers (All Attacks - last 24 hours)	IP addresses that have most frequently been the source of an attack during the last 24 hours.
Top 20 Attackers Prevented (All Attacks - last 24 hours)	IP addresses that have most frequently been prevented from attacking the network during the last 24 hours.
Top 20 Targets (last 24 hours)	IP addresses that have most frequently been the target of an attack during the last 24 hours.
Top 20 Targets Prevented (last 24 hours)	IP addresses that have most frequently prevented attacks during the last 24 hours.
All Attacks by Severity (last 24 hours)	Number of attacks by severity level (set in attack objects).
All Attacks Prevented by Severity (last 24 hours)	Number of attacks prevented by severity level (set in attack objects).
All Attacks Over Time (last 7 days)	All attacks detected during the last 7 days.
All Attacks Prevented Over Time (last 7 days)	All attacks prevented during the last 7 days.
All Attacks Over Time (last 30 days)	All attacks detected during the last 30 days.
All Attacks Prevented Over Time (last 30 days)	All attacks prevented during the last 30 days.
Critical Attacks (last 24 hours)	All attacks categorized as “critical” detected during the past 24 hours.
Critical Attacks Prevented (last 24 hours)	All attacks categorized as “critical” prevented during the past 24 hours.
Critical through Medium Attacks (last 24 hours)	All attacks categorized as either “critical” or “medium” detected during the past 24 hours.
Critical through Medium Attacks Prevented (last 24 hours)	All attacks categorized as either “critical” or “medium” prevented during the past 24 hours.
Top 50 Scan Sources (last 7 days)	IP addresses that have most frequently performed a scan of a managed device.
Top 50 Scan Targets (last 7 days)	IP addresses that have most frequently been the target of a scan over the last 7 days.

**Table 1: NSM DI/IDP Predefined Reports (continued)**

Report	Description
Profiler - New Hosts (last 7 days)	New hosts listed in the Profiler over the last 7 days.
Profiler - New Ports (last 7 days)	New ports listed in the Profiler over the last 7 days.
Profiler - New Protocols (last 7 days)	New protocols listed in the Profiler over the last 7 days.
Top IDP Rules	The total number of log entries generated by specific rules in your IDP policies. You can use the Top Rules report to identify those rules that are generating the most log events. This enables you to better optimize your rulebases by identifying those rules that are most and least effective. You can then modify or remove those rules from your security policies.

Table 2 describes Profiler predefined reports. These reports are related to activity by hosts in your network.

**Table 2: NSM Profiler Predefined Reports**

Report	Description
Top 10 Peers by Count	Ten source and destination IP addresses that appeared most frequently in the Profiler logs.
Top 10 Peers with maximum hits	Ten source and destination IP addresses that had the highest number of hits in the Profiler logs.

Table 3 describes the predefined application volume tracking reports. The reports are related to application use in your network.

**Table 3: NSM: Application Volume Tracking Reports**

Report	Description
Top 10 Applications by Volume	Applications with the highest volume in bytes in the past 24 hours.
Top 10 Application Categories by Volume	Application categories with the highest volume in bytes in the past 24 hours.
Top 5 Applications by Volume over Time (last 1 hour)	Applications with the highest volume in bytes in the past 1 hour.
Top 5 Application Categories by Volume (last 1 hour)	Application categories with the highest volume in bytes in the past 1 hour.
Top 5 Source by Volume over Time (last 1 hour)	Source IP addresses with the highest volume in bytes in the past 1 hour.
Top 5 Destination by Volume over Time (last 1 hour)	Destination IP addresses with the highest volume in bytes in the past 1 hour.

**Related Topics** ■ Creating NSM Custom Reports

- NSM Logs and Reports Overview

---

Published: 2009-08-20