

# SonicOS 5.8: NetFlow Reporting

---

## Document Scope

Rapid growth of IP networks has created interest in new business applications and services. These new services have resulted in increases in demand for network bandwidth, performance, and predictable quality of service as well as VoIP, multimedia and security oriented network services. Simultaneously, the need has emerged for measurement technology to support this growth by efficiently providing the information required to record network and application resource utilization. NetFlow provides solutions for each of these challenges.

This SonicOS 5.8.0 feature module guide provides an overview of NetFlow benefits and includes technical overview of features, details about the NetFlow cache, export formats and NetFlow operation. This document also provides configuration and troubleshoot procedures and examples.

This document contains the following sections:

- “NetFlow Reporting Overview” section on page 1
- “Administrator Prerequisites” section on page 4
- “Configuring NetFlow Reporting Task List” section on page 5
- “User Configuration Tasks” section on page 12
- “Appendix” section on page 19

## NetFlow Reporting Overview

This section provides an introduction to the NetFlow Reporting feature. After reading the NetFlow Reporting Overview section, you will be able to start configuring your SonicWALL security appliance network interface to enable NetFlow services. This section contains the following subsections:

- “NetFlow Benefits” section on page 2
- “What Is A Flow?” section on page 2
- “NetFlow Export Version Formats” section on page 3
- “NetFlow Export Packet Header Format” section on page 3
- “Supported Interfaces, Encapsulations and Protocols” section on page 3
- “NetFlow Collectors” section on page 4
- “Supported Platforms” section on page 4
- “Supported Standards” section on page 4

## NetFlow Benefits

NetFlow traditionally enables several key customer applications including:

- **Network Monitoring**—NetFlow data enables extensive near real time network monitoring capabilities. Flow-based analysis techniques may be utilized to visualize traffic patterns associated with individual routers and switches as well as on a network-wide basis (providing aggregate traffic or application based views) to provide proactive problem detection, efficient troubleshooting, and rapid problem resolution.
- **Application Monitoring and Profiling**—NetFlow data enables network managers to gain a detailed, time-based, view of application usage over the network. This information is used to plan, understand new services, and allocate network and application resources (e.g. Web server sizing and VoIP deployment) to responsively meet customer demands.
- **User Monitoring and Profiling**—NetFlow data enables network engineers to gain detailed understanding of customer/user utilization of network and application resources. This information may then be utilized to efficiently plan and allocate access, backbone and application resources as well as to detect and resolve potential security and policy violations.
- **Network Planning**—NetFlow can be used to capture data over a long period of time producing the opportunity to track and anticipate network growth and plan upgrades to increase the number of routing devices, ports, or higher- bandwidth interfaces. NetFlow services data optimizes network planning including peering, backbone upgrade planning, and routing policy planning. NetFlow helps to minimize the total cost of network operations while maximizing network performance, capacity, and reliability. NetFlow detects unwanted WAN traffic, validates bandwidth and Quality of Service (QOS) and allows the analysis of new network applications. NetFlow will give you valuable information to reduce the cost of operating your network.
- **Security Analysis**—NetFlow identifies and classifies DDOS attacks, viruses and worms in real-time. Changes in network behavior indicate anomalies that are clearly demonstrated in NetFlow data. The data is also a valuable forensic tool to understand and replay the history of security incidents.

NetFlow has two key components: (1) the NetFlow cache or data source which stores IP Flow information and (2) the NetFlow export or transport mechanism that sends NetFlow data to a network management collector for data reporting.

## What Is A Flow?

A flow is identified as a unidirectional stream of packets between a given source and destination—both defined by a network-layer IP address and transport-layer source and destination port numbers. Specifically, a flow is identified as the combination of the following seven key fields:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Layer 3 protocol type
- Input logical interface (ifIndex)

These seven key fields define a unique flow. If a flow has one different field than another flow, then it is considered a new flow. A flow contains other accounting fields (such as the AS number in the NetFlow export Version 5 flow format) that depend on the version record format that you configure for export. Flows are processed in a NetFlow cache.

## NetFlow Export Version Formats

The NetFlow Export datagram consists of a header and a sequence of flow records. The header contains information such as sequence number, record count and systime. The flow record contains flow information, for example IP addresses, ports, and routing information. For more information, see [“Appendix” section on page 19](#)

The Version 5 format is an enhancement that adds Border Gateway Protocol (BGP) autonomous system information and flow sequence numbers. The distinguishing feature of the NetFlow Version 9 format is that it is template based. Templates provide an extensible design to the record format, a feature that should allow future enhancements to NetFlow services without requiring concurrent changes to the basic flow-record format.

Using templates with NetFlow Version 9 provides several key benefits:

- Almost any information can be exported from a router or switch including layer 2 through 7 information, routing information, IPv6, IPv4, multicast and MPLS information. This new information will allow new applications for flow data and new views of network behavior.
- Third-party business partners who produce applications that provide collector or display services for NetFlow will not be required to recompile their applications each time a new NetFlow export field is added. Instead, they may be able to use an external data file that documents the known template formats.
- New features can be added to NetFlow more quickly, without breaking current implementations.
- NetFlow is "future-proofed" against new or developing protocols, because the Version 9 format can be adapted to provide support for them and other non-Flow based data measurements.

## NetFlow Export Packet Header Format

In these versions, the datagram consists of a header and one or more flow records. The first field of the header contains the version number of the export datagram. Typically, a receiving application that accepts any of the format versions allocates a buffer large enough for the largest possible datagram from any of the format versions and then uses the header to determine how to interpret the datagram. The second field in the header contains the number of records in the datagram (indicating the number of expired flows represented by this datagram) and is used to index through the records. Datagram headers for NetFlow Export versions 5 and 9 also include a "sequence number" field used by NetFlow data consuming applications to check for lost datagrams.

## Supported Interfaces, Encapsulations and Protocols

NetFlow supports IPv4 (and IPv4-encapsulated) routed traffic over a wide range of interface types and encapsulations. This includes Frame Relay, Asynchronous Transfer Mode, Inter-Switch Link, 802.1q, Multi-link Point to Point Protocol, General Routing Encapsulation, Layer 2 Tunneling Protocol, Multi-protocol Label Switching VPNs, and IP Sec Tunnels.

NetFlow is supported per interface.

NetFlow support for multicast exists on all SonicWALL platforms.

NetFlow supports IPv6 environments in the release of SonicOS 5.8 and up.

## NetFlow Collectors

SonicWALL NetFlow collector provides fast, scalable, and economical data collection from multiple NetFlow Export-enabled devices. The collector consumes flow datagrams from multiple NetFlow Export-enabled devices and performs data volume reduction through selective filtering and aggregation, performs bi-directional flow analysis and flow de-duplication.

## Supported Platforms

This feature is supported only on the SonicOS 5.8 release. The SonicOS 5.8 release supports the following platforms:

- TZ series
- NSA series

## Supported Standards

SonicOS 5.8 NetFlow Reporting is supported on the following NetFlow Export Formats:

- NetFlow Version 5
- NetFlow Version 9
- IPFIX (NetFlow Version 10)
- IPFIX with extensions

## Administrator Prerequisites

### NetFlow Activation and Deployment Information

SonicWALL recommends careful planning of NetFlow deployment with NetFlow services activated on strategically located edge/aggregation routers which capture the data required for planning, monitoring and accounting applications. Key deployment considerations include the following:

- Understanding your application-driven data collection requirements: accounting applications may only require originating and terminating router flow information whereas monitoring applications may require a more comprehensive (data intensive) end-to-end view
- Understanding the impact of network topology and routing policy on flow collection strategy: for example, avoid collecting duplicate flows by activating NetFlow on key aggregation routers where traffic originates or terminates and not on backbone routers or intermediate routers which would provide duplicate views of the same flow information
- NetFlow can be implemented in the SonicOS management interface to understand the number of flow in the network and the impact on the router. NetFlow export can then be setup at a later date to complete the NetFlow deployment.

NetFlow is in general an ingress measurement technology which should be deployed on appropriate interfaces on edge/aggregation or WAN access routers to gain a comprehensive view of originating and terminating traffic to meet customer needs for accounting, monitoring or network planning data. The key mechanism for enhancing NetFlow data volume manageability is careful planning of NetFlow deployment. NetFlow can be deployed incrementally (i.e. interface by interface) and strategically (i.e. on well chosen routers) —instead of widespread deployment of NetFlow on every router in the network.

# Configuring NetFlow Reporting Task List

The **Log > Flow Reporting** screen allows you to view statistics based on Flow Reporting and Internal Reporting. From this screen, you can also configure settings for internal and external flow reporting and external flow reporting.

The screenshot shows the 'Flow Reporting' interface. At the top, there's a 'Log /' breadcrumb and a title 'Flow Reporting'. Below the title are several buttons: 'Accept' (with a green checkmark), 'Cancel', 'Clear', 'Default', 'Generate ALL Templates', 'Generate Static Flows', a dropdown menu set to 'flow', and a 'Download' button. The main content area is divided into two panels. The left panel, titled 'Flow Reporting Statistics', lists: NetFlow/IPFIX Packets Sent: 0, Data Flows Enqueued: 16115155, Data Flows Dequeued: 16115124, Data Flows Dropped: 0, Data Flows Skipped Reporting: 0, General Flows Enqueued: 8497, General Flows Dequeued: 8497, General Flows Dropped: 0, Netflow/IPFIX Templates sent: 0, and General Static Flows Reported: 0. The right panel, titled 'App Flow Reporting Statistics', lists: Data Flows Enqueued: 7097792, Data Flows Dequeued: 7097789, Data Flows Dropped: 0, Data Flows Skipped Reporting: 0, General Flows Enqueued: 8497, General Flows Dequeued: 8497, General Flows Dropped: 0, General Static Flows Dequeued: 299998, App Flow Collector Errors: 0, and Total Flows in DB: 382113.

## Flow Reporting Statistics

The Flow Reporting Statistics apply to all external flows. This section shows reports of the flows that are sent to the server, not collected, dropped, stored in and removed from the memory, reported and non reported to the server. This section also includes the number of NetFlow/IPFIX templates sent and general static flows reported.

<b>NetFlow/IPFIX Packets Sent</b>	Total number of IPFIX/NetFlow packets sent to the external collector.
<b>Data Flows Enqueued</b>	Total number of connection related flows that is collected so far.
<b>Data Flows Dequeued</b>	Total number of connection related flows that have been reported either to internal collectors or external collectors.
<b>Data Flows Dropped</b>	Total number of collected connection related flows that failed to get reported.
<b>Data Flows Skipped Reporting</b>	Total number of connection related flows that skipped reporting. This can happen when running in periodic mode where collected flows are more than configured value for reporting.
<b>General Flows Enqueued</b>	Total number of all non-connection related flows that have been collected.
<b>General Flows Dequeued</b>	Total number of all non-connection related flows that have been reported either to external collectors or internal collectors.
<b>General Flows Dropped</b>	Total number of all non-connection related flows dropped due to too many requests.

<b>NetFlow/IPFIX Templates Sent</b>	Total number of templates that has been reported to the external collector.
<b>General Static Flows Reported</b>	Total number of static non-connection related flows that have been reported. This includes lists of applications/viruses/spyware/intrusions/table-map/column-map/location map.

## App Flow Reporting Statistics

The App Flow Reporting Statistics apply to all internal flows. Similar to the Flow Reporting Statistics, this section shows reports of the flows that are sent to the server, not collected, dropped, stored in and removed from the memory, reported and non reported to the server. This section also includes the number of static flows removed from the queue, internal errors, and the total number of flows within the internal database.

<b>Data Flows Enqueued</b>	Total number of connection related flows that have been queued to internal collector.
<b>Data Flows Dequeued</b>	Total number of connection related flows that have been successfully inserted into the database.
<b>Data Flows Dropped</b>	Total number of collected connection related flows that failed to get inserted into the database due to high connection rate.
<b>Data Flows Skipped Reporting</b>	Total number of connection related flows that skipped reporting.
<b>General Flows Enqueued</b>	Total number of all non-connection related flows in DB queue.
<b>General Flows Dequeued</b>	Total number of all non-connection related flows in DB queue.
<b>General Flows Dropped</b>	Total number of all non-connection related flows failed to get inserted due to high rate.
<b>General Static Flows Dequeued</b>	Total number of non-connection related static flows that have been successfully inserted into the DB.
<b>App Flow Collector Errors</b>	Total number of internal database errors.
<b>Total Flows in DB</b>	Total number of connection related flows in DB.

## Settings

The Settings section has configurable options for internal flow reporting, external flow reporting, and the IPFIX collector. You can also configure the settings for what is reported to an external controller.

Settings	
Enable Flow Reporting and Visualization	<input checked="" type="checkbox"/>
Report to EXTERNAL flow collector	<input checked="" type="checkbox"/>
Enable INTERFACE based reporting (advanced)	<input type="checkbox"/>
Enable firewall/app rules based reporting (advanced)	<input type="checkbox"/>
External flow reporting type	IPFIX with extensions
External collector's IP address	10.203.21.63
Use IDLE unit as an external collector	<input type="checkbox"/>
Source IP to use for collector on a VPN tunnel	0.0.0.0
External collector's UDP port number	2055
Send templates at regular intervals	<input type="checkbox"/>
Send static flows at regular intervals	<input type="checkbox"/>
Send static flows for following tables	Applications, Viruses, Spyware, Intrusions, Location Map, Services, Rating Map
Send dynamic flows for following tables	Connections, Users, URLs, URL ratings, VPNs, Devices, SPAMs, Locations, VOIPs
Include following additional reports via IPFIX	Interface Stats, Core utilization, Memory utilization

- **Enable Flow Reporting and Visualization**—This is a global checkbox that enables or disables the complete flow reporting feature. Selecting this checkbox enables flow reporting and visualization, which you can view on the Dashboard screen. When this is disabled, both internal and external flow reporting are also disabled.
- **Report to App Flow Collector**—Selecting this checkbox enables the specified flows to be reported to a flow collector within the SonicWALL appliance. Note that this option is enabled by default and used for visualization. If disabled, the Flow Monitor and Real Time Monitor on the Dashboard will not display any flows. You may leave this option disabled if you choose to rely only on external reporting, rather than SonicWALL visualization.

- **Report to EXTERNAL flow collector**—Selecting this checkbox enables the specified flows to be reported to an external flow collector. Some options include another SonicWALL appliance configured as a collector, a SonicWALL Linux collector, or a third party collector. Note that not all collectors will work with all modes of flow reporting.
- **Enable INTERFACE Based Reporting**—Selecting this checkbox enables flow reporting based on the initiator or responder interface. This provides a way to control what flows are reported externally or internally. If enabled, the flows are verified against the per interface flow reporting configuration, located in the Network>Interface screen. If an interface has its flow reporting disabled, then flows associated with that interface are skipped.

The screenshot shows the 'Advanced Settings' section of a configuration window. The 'Enable flow reporting' checkbox is checked and highlighted in yellow. Other visible settings include 'Link Speed' set to 'Auto Negotiate', 'Use Default MAC Address' selected, and 'Override Default MAC Address' set to '00:17:C5:69:F3:54'.

- **Enable Firewall-Rules Based Reporting**—Selecting this checkbox enables flow reporting based on already existing firewall rules. This is similar to interface-based reporting; the only difference is instead of checking per interface settings, the per firewall rule is selected. Every firewall rule has a checkbox to enable flow reporting. If a flow matching a firewall rule is to be reported, this enabled checkbox will force to verify if firewall rules have flow reporting enabled or not. This is an additional way to control which flows need to be reported. Note that this option is applicable to both internal and external flow reporting.

The screenshot shows the 'Settings' section of a configuration window. The 'Enable flow reporting' checkbox is checked and highlighted in yellow. Other visible settings include 'Action' set to 'Allow', 'From Zone' and 'To Zone' set to '-Select a zone-', 'Service' set to '-Select a service-', 'Source' and 'Destination' set to '-Select a network-', 'Users Allowed' set to 'All', and 'Schedule' set to 'Always on'.

- **External Flow Reporting Type**—If the “Report to EXTERNAL Flow Collector” option is selected, you must specify the flow reporting type from the provided list in the dropdown menu: NetFlow version-5, NetFlow version-9, IPFIX, or IPFIX with extensions. If the reporting type is set to Netflow versions 5, 9, or IPFIX, then any third-party collector can be used to show flows reported from the device. It uses standard data types as defined in IETF. If the reporting type is set to IPFIX with extensions, then the collectors that are SonicWALL flow aware can only be used.

The following are recommended options for collectors:

- A second SonicWALL appliance, acting as an external collector
- An external Linux collector running the SonicWALL provided package



- A third-party collector that is SonicWALL flow aware, such as Plixer Scrutinizer

For Netflow versions and IPFIX reporting types, only connection related flows are reported per the standard. For IPFIX with extensions, connection related flows are reported with SonicWALL specific data type, as well as various other tables to correlate flows with Users, Applications, Viruses, VPN, and so on.

- **External Collector's IP Address**—Specify the external collector's IP address. This IP address must be reachable from the SonicWALL firewall in order for the collector to generate flow reports.
- **Source IP to Use for Collector on a VPN Tunnel**—If the external collector must be reached by a VPN tunnel, specify the source IP for the correct VPN policy. **Note:** *Select Source IP from the local network specified in the VPN policy. If specified, Netflow/IPFIX flow packets will always take the VPN path.*
- **External Collector's UDP Port Number**—Specify the UDP port number that Netflow/IPFIX packets are being sent over. The default port is 2055.

— **Send Templates at Regular Intervals**—Selecting this checkbox will enable the appliance to send Template flows at regular intervals. Netflow version-9 and IPFIX use templates that must be known to an external collector before sending data. Per IETF, a reporting device must be capable of sending templates at a regular interval to keep the collector in sync with the device. If the collector is not needed, you may disable it here. **Note: This option is available with Netflow version-9, IPFIX, and IPFIX with extensions only.**

— **Send Static Flows for Following Tables**—Select the static mapping tables to be generated to a flow from the dropdown list. Values include: Applications, Viruses, Spyware, Intrusions, Location Maps, Services, Rating Maps, Table Maps, and Column Maps.

Selecting the Send Static Flows at Regular Intervals checkbox enables the sending of these specified static flows.

When running in IPFIX with extensions mode, SonicWALL reports multiple types of data to an external device in order to correlate User, VPN, Application, Virus, etc. In this mode, data is both static and dynamic. Static tables are needed once since they rarely change. Depending on the capability of the external collector, not all static tables are needed. You can select the tables needed in this section. **Note: This option is available with IPFIX with extensions only.**

— **Send Dynamic Flows for Following Tables**—Select the dynamic mapping tables to be generated to a flow from the dropdown list. Values include: Connections, Users, URLs, URL Ratings, VPNs, Devices, SPAMs, Locations, and VoIPs.

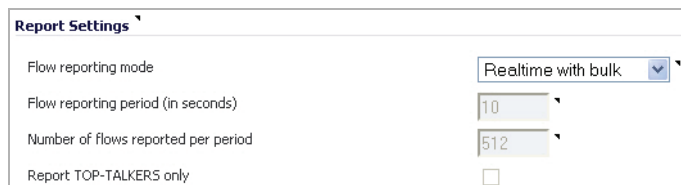
When running in IPFIX with extensions mode, SonicWALL reports multiple types of data to an external device in order to correlate User, VPN, Application, Virus, etc. In this mode, data is both static and dynamic. Static tables are needed once since they rarely change. Depending on the capability of the external collector, not all static tables are needed. You can select the tables needed in this section. **Note: This option is available with IPFIX with extensions only.**

— **Include Following Additional Reports via IPFIX**—Select additional IPFIX reports to be generated to a flow. Select values from the dropdown list. Values include: Logs, Interface Stats, Core Utilization, and Memory Utilization.

When running in IPFIX with extensions mode, SonicWALL is capable of reporting more data that is not related to connection and flows. These tables are grouped under this section (Additional Reports). Depending on the capability of the external collector, not all additional tables are needed. In this section, users can select tables that are needed. **Note: This option is available with IPFIX with extensions only.**

## Report Settings

This section allows you to configure flow reporting settings, such as realtime, real time with bulk, or periodic reporting. Note that modifying this section does not have an effect on internal reporting settings.



The screenshot shows a configuration window titled "Report Settings". It contains four settings:

- Flow reporting mode:** A dropdown menu currently set to "Realtime with bulk".
- Flow reporting period (in seconds):** A text input field containing the value "10".
- Number of flows reported per period:** A text input field containing the value "512".
- Report TOP-TALKERS only:** An unchecked checkbox.

- **Flow Reporting Mode**—Select from the dropdown list to have your SonicWALL appliance generate Netflow or IPFIX packets in one of the following values:
  - **Realtime**—One flow record is sent per packet
  - **Realtime with bulk**—More than one flow record is sent per packet
  - **Periodic**—A report is sent at a regular interval

Typically, the SonicWALL flow reporting subsystem receives flows and other table data asynchronously from other parts of the firewall. This section specifies how and when that data needs to be reported.
- **Flow Reporting Period (in seconds)**—When **Periodic** is selected, specify the number of seconds to wait before reporting the collected flows. In this mode, SonicWALL collects all flows from the firewall and waits until the time is elapses. Once the time elapses, the flows are reported externally to the collector.
- **Number of Flows Reported per Period**—When **Periodic** is selected, specify the number of flows to be reported within each period. If the SonicWALL appliance collects more flows than what is specified in this field, the first *n* will be collected and reported. For example, if 10 is the specified number of flows reported, but the SonicWALL collects 20, the first 10 will be reported.
- **Report TOP-TALKERS only**—When **Periodic** is selected, select this checkbox to enable the SonicWALL to report flows with the maximum amount of traffic. Among the collected flows, the SonicWALL selects those based on traffic, then sends them in descending order.

## Event Settings

The Event Settings section allows you to configure the conditions under which a flow is reported. Note that this section only applies to Connection related flows.

Setting	Value
Report flows on connection OPEN	<input checked="" type="checkbox"/>
Report flows on threat detection	<input checked="" type="checkbox"/>
Report flows on application detection	<input checked="" type="checkbox"/>
Report flows on user detection	<input checked="" type="checkbox"/>
Report flows on VPN tunnel detection	<input checked="" type="checkbox"/>
Report flows on kilo BYTES exchanged	<input type="checkbox"/>
Kilobytes exchanged	100
Report ONCE	<input type="checkbox"/>
Report flows on connection CLOSE	<input checked="" type="checkbox"/>
Report DROPPED flows	<input checked="" type="checkbox"/>
Skip reporting of STACK flows (connections)	<input checked="" type="checkbox"/>
Include following URL types	Gifs, Pngs, Js, Xmls, Jsons, Css, Htmls, Aspx, Cms

- **Report Flows on Connection OPEN**—Enable this to report flows when the Connection is open. This is typically when a connection is established.
- **Report Flows on Threat Detection**—Enable this to report flows specific to threats. Upon detections of virus, intrusion, or spyware, the flow is reported again.
- **Report Flows on Application Detection**—Enable this to report flows specific to applications. Upon performing a deep packet inspection, the SonicWALL appliance is able to detect if a flow is part of a certain application. Once identified, the flow is reported again.
- **Report Flows on User Detection**—Enable this to report flows specific to users. The SonicWALL appliance associates flows to a user-based detection based on its login credentials. Once identified, the flow is reported again.
- **Report Flows on VPN Tunnel Detection**—Enable this to report flows sent through the VPN tunnel. Once flows sent over the VPN tunnel are identified, the flow is reported again.
- **Report Flows on Kilo BYTES exchanged**—Enable this to report flows based on a specific number of traffic, in kilobytes, is exchanged. This option is ideal for flows that are active for a long time and need to be monitored.
  - **Kilobytes exchanged**—When the above option is enabled, specify the number of kilobytes exchanged to be reported.
  - **Report Once**—When the **Report Flows on Kilo BYTES exchanged** option is enabled, enabling this option will send the report only once. Leave it unselected if you want reports sent periodically.
- **Report Flows on Connection CLOSED**—Enable this to report flows when the Connection is closed.
- **Report DROPPED Flows**—Enable this to report dropped flows. This applies to flows that are dropped due to firewall rules.
- **Skip Reporting of STACK Flows (connections)**—Enable this to skip the reporting of STACK flows for connections. Note that all flows as a result of traffic initiated or terminated by the firewall itself are considered stack traffic.
- **Include following URL types**—Select the type of URLs to be generated into a flow. Select values from the dropdown list. Values include: Gifs, Jpegs, Pngs, Js, Xmls, Jsons, Css, Htmls, Aspx, and Cms. **Note: This option is applies to both App Flow (internal) and external reporting when used with IPFIX with extensions.**

# User Configuration Tasks

Depending on the type of flows you are collecting, you will need to determine which type of reporting will work best with your setup and configuration. This section includes configuration examples for each supported NetFlow solution, as well as configuring a second appliance to act as a collector.

- “NetFlow version 5 Configuration Procedures” section on page 12
- “NetFlow version 9 Configuration Procedures” section on page 13
- “IPFIX (NetFlow version 10) Configuration Procedures” section on page 14
- “IPFIX with Extensions Configuration Procedures” section on page 15

## NetFlow version 5 Configuration Procedures

To configure typical Netflow version 5 flow reporting, follow the steps listed below.

- Step 1** Select the checkbox to **Enable flow reporting**. Note that if this is disabled, both internal and external flow reporting are also disabled.
- Step 2** Select the **Report to EXTERNAL flow collector** checkbox to enable flows to be reported to an external flow collector. Note that you may enable this option if you prefer to receive external flows, rather than the SonicWALL visualization. Remember, not all collectors will work with all modes of flow reporting.
- Step 3** **Enable INTERFACE based reporting** by selecting the checkbox. Once enabled, the flows reported are based on the initiator or responder interface. Note that this step is *optional*.
- Step 4** **Enable Firewall-Rules Based Reporting** by selecting the checkbox. Once enabled, the flows reported are based on already existing firewall rules. Note that this step is *optional*, but is required if flow reporting is done on selected interfaces.
- Step 5** Select **Netflow version-5** as the **External Flow Reporting Type** from the dropdown list if the **Report to EXTERNAL flow collector** option is selected. Next, specify the **External Collector's IP address** in the provided field.
- Step 6** For the **Source IP to Use for Collector on a VPN Tunnel**, specify the source IP if the external collector must be reached by a VPN tunnel. Note that this step is *optional*.
- Step 7** Specify the **External Collector's UDP port number** in the provided field. The default port is 2055.

The screenshot shows a 'Settings' window with the following configuration:

- Enable Flow Reporting and Visualization:** ☒
- Report to EXTERNAL flow collector:** ☒
- Enable INTERFACE based reporting (advanced):** ☒
- Enable firewall/app rules based reporting (advanced):** ☐
- External flow reporting type:** Netflow version-5 (dropdown)
- External collector's IP address:** 10.203.21.63
- Use IDLE unit as an external collector:** ☐
- Source IP to use for collector on a VPN tunnel:** 0.0.0.0
- External collector's UDP port number:** 2055
- Send templates at regular intervals:** ☒
- Send static flows at regular intervals:** ☐
- Send static flows for following tables:** Applications, Viruses, Spyware, Intrusions, Location Map, Services, Rating Map (dropdown)
- Send dynamic flows for following tables:** Connections, Users, URLs, URL ratings, VPNs, Devices, SPAMs, Locations, VOIPs (dropdown)
- Include following additional reports via IPFIX:** Interface Stats, Core utilization, Memory utilization (dropdown)

**Note**

The highlighted fields are the required fields for successful Netflow version 5 configuration. All other configurable fields are optional, as noted in the above steps.

## NetFlow version 9 Configuration Procedures

To configure Netflow version 9 flow reporting, follow the steps listed below.

- Step 1** Select the checkbox to **Enable flow reporting**. Note that if this is disabled, both internal and external flow reporting are also disabled.
- Step 2** Select the **Report to EXTERNAL flow collector** checkbox to enable flows to be reported to an external flow collector. Note that you may enable this option if you prefer to receive external flows, rather than the SonicWALL visualization. Remember, not all collectors will work with all modes of flow reporting.
- Step 3** **Enable INTERFACE based reporting** by selecting the checkbox. Once enabled, the flows reported are based on the initiator or responder interface. Note that this step is *optional*.
- Step 4** **Enable Firewall-Rules Based Reporting** by selecting the checkbox. Once enabled, the flows reported are based on already existing firewall rules. Note that this step is *optional*, but is required if flow reporting is done on selected interfaces.
- Step 5** Select **Netflow version-9** as the **External Flow Reporting Type** from the dropdown list if the **Report to EXTERNAL flow collector** option is selected. Next, specify the **External Collector's IP address** in the provided field.
- Step 6** For the **Source IP to Use for Collector on a VPN Tunnel**, specify the source IP if the external collector must be reached by a VPN tunnel. Note that this step is *optional*.
- Step 7** Specify the **External Collector's UDP port number** in the provided field. The default port is 2055.
- Step 8** Enable the option to **Send templates at regular intervals** by selecting the checkbox. Note that Netflow version-9 uses templates that must be known to an external collector before sending data. After enabling this option, you can **Generate ALL Templates** by clicking the button in the topmost toolbar.

**Note**

The highlighted fields are the required fields for successful Netflow version 9 configuration. All other configurable fields are optional, as noted in the above steps.

## IPFIX (NetFlow version 10) Configuration Procedures

To configure IPFIX, or NetFlow version 10, flow reporting, follow the steps listed below.

- Step 1** Select the checkbox to **Enable flow reporting**. Note that if this is disabled, both internal and external flow reporting are also disabled.
- Step 2** Select the **Report to EXTERNAL flow collector** checkbox to enable flows to be reported to an external flow collector. Note that you may enable this option if you prefer to receive external flows, rather than the SonicWALL visualization. Remember, not all collectors will work with all modes of flow reporting.
- Step 3** **Enable INTERFACE based reporting** by selecting the checkbox. Once enabled, the flows reported are based on the initiator or responder interface. Note that this step is *optional*.
- Step 4** **Enable Firewall-Rules Based Reporting** by selecting the checkbox. Once enabled, the flows reported are based on already existing firewall rules. Note that this step is *optional*, but is required if flow reporting is done on selected interfaces.
- Step 5** Select **IPFIX** as the **External Flow Reporting Type** from the dropdown list if the **Report to EXTERNAL flow collector** option is selected. Next, specify the **External Collector's IP address** in the provided field.
- Step 6** For the **Source IP to Use for Collector on a VPN Tunnel**, specify the source IP if the external collector must be reached by a VPN tunnel. Note that this step is *optional*.
- Step 7** Specify the **External Collector's UDP port number** in the provided field. The default port is 2055.
- Step 8** Enable the option to **Send templates at regular intervals** by selecting the checkbox. Note that Netflow version-9 uses templates that must be known to an external collector before sending data. After enabling this option, you can **Generate ALL Templates** by clicking the button in the topmost toolbar.



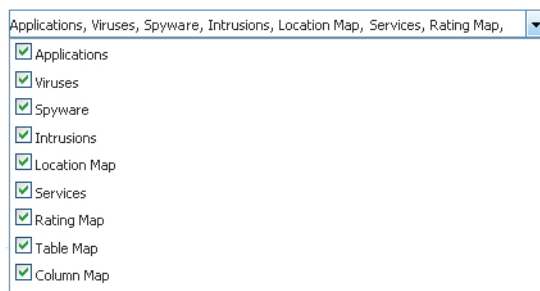
### Note

The highlighted fields are the required fields for successful IPFIX configuration. All other configurable fields are optional, as noted in the above steps.

## IPFIX with Extensions Configuration Procedures

To configure IPFIX with extensions flow reporting, follow the steps listed below.

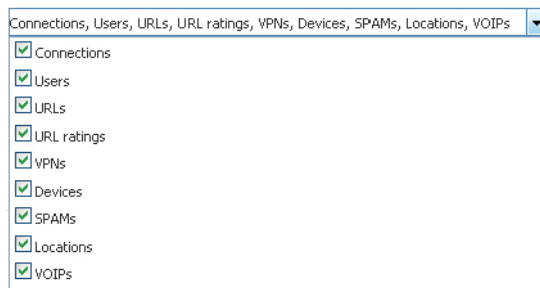
- Step 1** Select the checkbox to **Enable flow reporting**. Note that if this is disabled, both internal and external flow reporting are also disabled.
- Step 2** Select the **Report to EXTERNAL flow collector** checkbox to enable flows to be reported to an external flow collector. Note that you may enable this option if you prefer to receive external flows, rather than the SonicWALL visualization. Remember, not all collectors will work with all modes of flow reporting.
- Step 3** **Enable INTERFACE based reporting** by selecting the checkbox. Once enabled, the flows reported are based on the initiator or responder interface.
- Step 4** **Enable Firewall-Rules Based Reporting** by selecting the checkbox. Once enabled, the flows reported are based on already existing firewall rules.
- Step 5** Select **IPFIX with extensions** as the **External Flow Reporting Type** from the dropdown list if the **Report to EXTERNAL flow collector** option is selected. Next, specify the **External Collector's IP address** in the provided field.
- Step 6** For the **Source IP to Use for Collector on a VPN Tunnel**, specify the source IP if the external collector must be reached by a VPN tunnel.
- Step 7** Specify the **External Collector's UDP port number** in the provided field. The default port is 2055.
- Step 8** Enable the option to **Send templates at regular intervals** by selecting the checkbox. Note that Netflow version-9 uses templates that must be known to an external collector before sending data. After enabling this option, you can **Generate ALL Templates** by clicking the button in the topmost toolbar.
- Step 9** Enable the option to **Send static flows at regular intervals** by selecting the checkbox. After enabling this option, you can **Generate Static Flows** by clicking the button in the topmost toolbar.
- Step 10** Select the tables you wish to receive static flows for from the dropdown list.



Applications, Viruses, Spyware, Intrusions, Location Map, Services, Rating Map, ▼

- ☒ Applications
- ☒ Viruses
- ☒ Spyware
- ☒ Intrusions
- ☒ Location Map
- ☒ Services
- ☒ Rating Map
- ☒ Table Map
- ☒ Column Map

- Step 11** Select the tables you wish to receive dynamic flows for from the dropdown list.



Connections, Users, URLs, URL ratings, VPNs, Devices, SPAMs, Locations, VOIPs ▼

- ☒ Connections
- ☒ Users
- ☒ URLs
- ☒ URL ratings
- ☒ VPNs
- ☒ Devices
- ☒ SPAMs
- ☒ Locations
- ☒ VOIPs

**Step 12** Select any additional reports to be generated to a flow from the dropdown list.

Interface Stats, Core utilization, Memory utilization

☐ Logs  
☒ Interface Stats  
☒ Core utilization  
☒ Memory utilization

Settings

Enable Flow Reporting and Visualization	<input checked="" type="checkbox"/>
Report to EXTERNAL flow collector	<input checked="" type="checkbox"/>
Enable INTERFACE based reporting (advanced)	<input checked="" type="checkbox"/>
Enable firewall/app rules based reporting (advanced)	<input type="checkbox"/>
External flow reporting type	IPFIX with extensions
External collector's IP address	10.203.21.63
Use IDLE unit as an external collector	<input type="checkbox"/>
Source IP to use for collector on a VPN tunnel	0.0.0.0
External collector's UDP port number	2055
Send templates at regular intervals	<input checked="" type="checkbox"/>
Send static flows at regular intervals	<input type="checkbox"/>
Send static flows for following tables	Applications, Viruses, Spyware, Intrusions, Location Map, Services, Rating Map,
Send dynamic flows for following tables	Connections, Users, URLs, URL ratings, VPNs, Devices, SPAMs, Locations, VOIPs
Include following additional reports via IPFIX	Interface Stats, Core utilization, Memory utilization



## Configuring Report Settings

After configuring the Settings section to what best suits your App Flow, External, or IPFIX collector configuration, continue through this section to specify Flow Reporting Settings. Refer to the [“Report Settings” section on page 10](#) for more information about each setting.

- Step 1** Select the **Flow reporting mode** from the dropdown list. Note that **Realtime with bulk** is the default setting.

For **Realtime** or **Realtime with bulk**, continue to [“Configuring Event Settings” section on page 17](#).

For **Periodic**, continue to Step 2.

- Step 2** Specify the **Flow reporting period**. This is the number of seconds the appliance will wait before reporting the collected amount of flows. The default value is 10 seconds.
- Step 3** Next, specify the **Number of flows reported per period**.
- Step 4** Select the **Report TOP-TALKERS only** checkbox to enable the SonicWALL appliance to report flows with the maximum amount of traffic.

## Configuring Event Settings

After configuring the Report Settings, continue through this section to configure the conditions under which a flow is reported. Selecting a checkbox will enable the configuration. Refer to the [“Event Settings” section on page 11](#) for more information about each setting.

## Verifying Netflow with Extensions Configurations

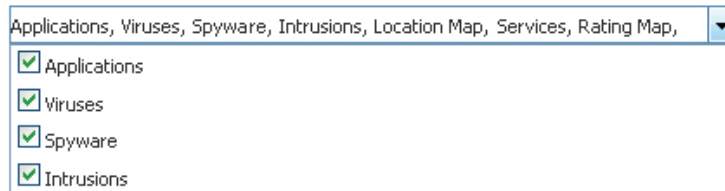
One external flow reporting option that works with Netflow with Extensions is the third-party collector called Plixer Scrutinizer. This collector displays a range of reporting and analysis that is both Netflow and SonicWALL flow aware.



**Note** You will need an account with Plixer Scrutinizer.

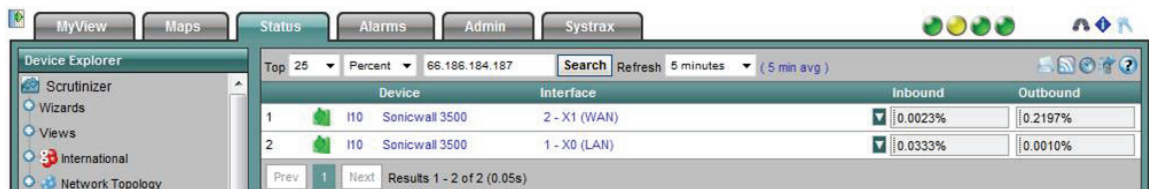
To verify your Netflow with Extensions reporting configurations, perform the following steps.

- Step 1** Navigate to the SonicWALL **Log > Flow Reporting** screen. Enable the **Report to EXTERNAL flow collector** option on the Settings section.
- Step 2** Specify the **External collector's IP address** and respective **UDP Port Number**.
- Step 3** Enable the option to **Send templates at regular intervals**.
- Step 4** Enable the option to **Send static flows at regular intervals**.
- Step 5** Select the tables you wish to receive static flows for from the provided dropdown list. Then, click **Accept**.



**Note** Currently, Scrutinizer supports Applications and Threats only. Future versions of Plixer will support the following Static Flows: Location Map, Services, Rating Map, Table Map, and Column Map.

- Step 6** Next, navigate to the **Network > Interfaces** screen.
- Step 7** Confirm that Flow Reporting is enabled per interface by clicking the **Configure** icon of the interface you are requesting data from.
- Step 8** On the Advanced tab, select the checkbox to **Enable flow reporting**. Then, click **OK**.
- Step 9** Login to Plixer Scrutinizer. The data displays within minutes.



# Appendix

The following appendix describes the various NetFlow tables. Also, this section describes in detail the IPFIX with extensions tables that are exported when the SonicWALL is configured to report flows.

This appendix includes the following sections:

- “Static Tables” section on page 19
- “Dynamic Tables” section on page 19
- “Templates” section on page 20
  - “NetFlow version 5” section on page 21
  - “NetFlow version 9” section on page 22
  - “IPFIX (NetFlow version 10)” section on page 22
  - “IPFIX with Extensions” section on page 23

## Static Tables

Static Tables are tables with data that does not change over time. However, this data is required to correlate with other tables. Static tables are usually reported at a specified interval, but may also be configured to send just once. The following is a list of Static IPFIX tables that may be exported:

- **Table Layout Map**—This table reports SonicWALL’s list of tables to be exported, including Table ID and Table Names.
- **Column Map**—This table represents SonicWALL’s list of columns to be reported with Name, Type Size, and IPFIX Standard Equivalents for each column of every table.
- **Rating Map**—This table represents SonicWALL’s list of Rating IDs and the Name of the Rating Type.
- **Location Map**—This table represents SonicWALL’s location map describing the list of countries and regions with their IDs.
- **Applications Map**—This table reports all applications the SonicWALL appliance identifies, including various Attributes, Signature IDs, App IDs, Category Names, and Category IDs.
- **Intrusions Map**—This table reports all intrusions detected by the SonicWALL appliance.
- **Viruses Map**—This table reports all viruses detected by the SonicWALL appliance.
- **Spyware Map**—This table reports all spyware detected by the SonicWALL appliance.
- **Services Map**—This table represents SonicWALL’s list of Services with Port Numbers, Protocol Type, Range of Port Numbers, and Names.

## Dynamic Tables

Unlike Static tables, the data of Dynamic tables change over time and are sent repeatedly, based on the activity of the SonicWALL appliance. The columns of these tables grow over time, with the exception of a few tables containing statistics or utilization reports. The following is a list of Dynamic IPFIX tables that may be exported:

- **Flow Table**—This table reports SonicWALL connections. The same flow tables can be reported multiple times by configuring triggers.
- **Location**—This table reports the Locations and Domain Names of an IP address.
- **Users**—This table reports users logging in to the SonicWALL appliance via LDAP/RADIUS, Local, or SSO.

- **URLs**—This table reports URLs accessed through the SonicWALL appliance.
- **Log**—This table reports all unfiltered logs generated by the SonicWALL appliance.
- **Interface Statistics**—This table reports statistics for all interfaces including VLANs. The statistics include Interface ID, Interface Name, Interface IP, Interface MAC, Interface Status, Interface Speed, Interface Mode, Interface Counters, and Interface Rolling Average Rate.
- **Core Utilization**—This table reports all Core utilization by percentage.
- **Memory Utilization**—This table reports all Memory utilization (Free, Used, Used by DB) of the SonicWALL appliance.
- **VoIP**—This table reports all VoIP/H323 calls through the SonicWALL appliance.
- **SPAM**—This table reports all email exchanges through the SPAM service.
- **Connected Devices**—This table reports the list of all devices connected through the SonicWALL appliance, including the MAC addresses, IP addresses, Interface, and NETBIOS name of connected devices.
- **VPN Tunnels**—This table reports all VPN tunnels established through the SonicWALL appliance.
- **URL Rating**—This table reports Rating IDs for all URLs accessed through the SonicWALL appliance.

## Templates

The following section shows examples of the type of Netflow template tables that are exported. You can perform a Diagnostic Report of your own Netflow Configuration by navigating to the **System > Diagnostics** screen, and click the **Download Report** button in the “Tech Support Report” section.

System /

**Diagnostics**

**Tech Support Report**

☐ VPN Keys
 ☐ ARP Cache
 ☐ DHCP Bindings
 ☐ IKE Info

☒ Enable Periodic Secure Backup of Diagnostic Reports to MySonicwall
 

Time Interval (minutes)

## NetFlow version 5

The NetFlow version 5 datagram consists of a header and one or more flow records, using UDP to send export datagrams. The first field of the header contains the version number of the export datagram. The second field in the header contains the number of records in the datagram, which can be used to search through the records. Because NetFlow version 5 is a fixed datagram, no templates are available, and will follow the format of the tables listed below.

### NetFlow version 5 Header Format

Bytes	Contents	Description
0-1	version	NetFlow export format version number
2-3	count	Number of flows exported in this packet (1-30)
4-7	SysUptime	Current time in milliseconds since the export device booted
8-11	unix_secs	Current count of seconds since 0000 UTC 1970
12-15	unix_nsecs	Residual nanoseconds since 0000 UTC 1970
16-19	flow_sequence	Sequence counter of total flows seen
20	engine_type	Type of flow-switching engine
20	engine_id	Slot number of the flow-switching engine
22-23	sampling_interval	First two bits hold the sampling mode; remaining 14 bits hold value of sampling interval

### NetFlow version 5 Flow Record Format

Bytes	Contents	Description
0-3	srcaddr	Source IP address
4-7	dstaddr	Destination IP address
8-11	nexthop	IP address of the next hop router
12-13	input	SNMP index of input interface
14-15	output	SNMP index of output interface
16-19	dPkts	Packets in the flow
20-23	dOctets	Total number of Layer 3 bytes in the packets of the flow
24-27	First	SysUptime at start of flow
28-31	Last	SysUptime at the time the last packet of the flow was received
32-33	srcport	TCP/UDP source port number or equivalent
34-35	dstport	TCP/UDP destination port number or equivalent
36	pad1	Unused (zero) bytes
37	tcp_flags	Cumulative OR of TCP flags
38	prot	IP protocol type (for example, TCP=6; UDP=17)
39	tos	IP type of service (ToS)
40-41	src_as	Autonomous system number of the source, either origin or peer
42-43	dst_as	Autonomous system number of the destination, either origin or peer
44	src_mask	Source address prefix mask bits

Bytes	Contents	Description
45	dst_mask	Destination address prefix mask bits
46-47	pad2	Unused (zero) bytes

## NetFlow version 9

An example of a NetFlow version 9 template is displayed below.

```
Netflow-v9 Template ID = 256, Name = Flow, Number of Elements = 12, Total Length = 41
Field = 1, Field bytes = 4
Field = 2, Field bytes = 4
Field = 4, Field bytes = 1
Field = 8, Field bytes = 4
Field = 7, Field bytes = 2
Field = 10, Field bytes = 4
Field = 11, Field bytes = 2
Field = 12, Field bytes = 4
Field = 14, Field bytes = 4
Field = 15, Field bytes = 4
Field = 21, Field bytes = 4
Field = 22, Field bytes = 4
```

The following table details the NetFlow version 9 Template FlowSet Field Descriptions.

Field Name	Description
Template ID	The SonicWALL appliance generates templates with a unique ID based on FlowSet templates matching the type of NetFlow data being exported.
Name	The name of the NetFlow template.
Number of Elements	The amount of fields listed in the NetFlow template.
Total Length	The total length in bytes of all reported fields in the NetFlow template.
Field Type	The field type is a numeric value that represents the type of field. Note that values of the field type may be vendor specific.
Field bytes	The length of the specific Field Type, in bytes.

## IPFIX (NetFlow version 10)

An example of an IPFIX (NetFlow version 10) template.

```
IPFix Template ID = 256, Name = Flow, Number of Elements = 12, Total Length = 41
Field = 1, Field bytes = 4
Field = 2, Field bytes = 4
Field = 4, Field bytes = 1
Field = 8, Field bytes = 4
Field = 7, Field bytes = 2
Field = 10, Field bytes = 4
Field = 11, Field bytes = 2
Field = 12, Field bytes = 4
Field = 14, Field bytes = 4
Field = 15, Field bytes = 4
Field = 21, Field bytes = 4
Field = 22, Field bytes = 4
```

The following table details the IPFIX Template FlowSet Field Descriptions.

Field Name	Description
Template ID	The SonicWALL appliance generates templates with a unique ID based on FlowSet templates matching the type of NetFlow data being exported.
Name	The name of the NetFlow template.
Number of Elements	The amount of fields listed in the NetFlow template.
Total Length	The total length in bytes of all reported fields in the NetFlow template.

Field Name	Description
Field Type	The field type is a numeric value that represents the type of field. Note that values of the field type may be vendor specific.
Field bytes	The length of the specific Field Type, in bytes.

## IPFIX with Extensions

IPFIX with extensions exports templates that are a combination of NetFlow fields from the aforementioned versions and SonicWALL IDs. These flows contain several extensions, such as Enterprise-defined field types and Enterprise IDs. Note that the SonicWALL Specific Enterprise ID (EntID) is defined as 8741.

The following Name Template is a standard for the IPFIX with extensions templates. The values specified are static and correlate to the Table Name of all the NetFlow exportable templates.

```

STATIC TABLES
-----
Table MAP table
Table(Template) Id=256, Table Name=Flow IPFIX
Table(Template) Id=257, Table Name=Flow IPFIX extn
Table(Template) Id=258, Table Name=Table Map
Table(Template) Id=259, Table Name=Column Map
Table(Template) Id=260, Table Name=User
Table(Template) Id=261, Table Name=Application
Table(Template) Id=262, Table Name=URL
Table(Template) Id=263, Table Name=Rating
Table(Template) Id=264, Table Name=IPS
Table(Template) Id=265, Table Name=GAV
Table(Template) Id=266, Table Name=Anti Spyware
Table(Template) Id=267, Table Name=Location Map
Table(Template) Id=268, Table Name=Location
Table(Template) Id=269, Table Name=Log
Table(Template) Id=270, Table Name=if-stat
Table(Template) Id=271, Table Name=core-stat
Table(Template) Id=272, Table Name=Voip
Table(Template) Id=273, Table Name=Services
Table(Template) Id=274, Table Name=Spam
Table(Template) Id=275, Table Name=memory
Table(Template) Id=276, Table Name=devices
Table(Template) Id=277, Table Name=vpn tunnels
Table(Template) Id=278, Table Name=URL rating

```

The following template is an example of an IPFIX with extensions template.

```

IPfix Template ID = 257, Name = Flow IPFIX extn, Number of Elements = 39, Total Length = 148
EField = 1, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=time stamp
EField = 2, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow identifier
EField = 3, Field bytes = 6, EntId = 8741, type = mac address-48bits, name=initiator gw MAC
EField = 4, Field bytes = 6, EntId = 8741, type = mac address-48bits, name=responder gw MAC
EField = 5, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=initiator IP Addr
EField = 6, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=responder IP Addr
EField = 7, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=initiator Gw-IP Addr
EField = 8, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=responder Gw-IP Addr
EField = 9, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=initiator iface
EField = 10, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=responder iface
EField = 167, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init vpn spi out
EField = 168, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp vpn spi out
EField = 11, Field bytes = 2, EntId = 8741, type = unsigned int-16bits, name=initiator port
EField = 12, Field bytes = 2, EntId = 8741, type = unsigned int-16bits, name=responder port
EField = 13, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init to resp pkts
EField = 14, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init to resp octets
EField = 15, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp to init pkts
EField = 16, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp to init octets
EField = 169, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init to resp delta pkts
EField = 170, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init to resp delta octets
EField = 171, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp to init delta pkts
EField = 172, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp to init delta octets
EField = 17, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow start time
EField = 18, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow end time
EField = 19, Field bytes = 2, EntId = 8741, type = unsigned int-16bits, name=internal flags
EField = 20, Field bytes = 1, EntId = 8741, type = unsigned char-8bits, name=protocol type
EField = 173, Field bytes = 1, EntId = 8741, type = unsigned char-8bits, name=flow block reason
EField = 22, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to application id
EField = 23, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to user id
EField = 25, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to ips id
EField = 26, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to virus id
EField = 27, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to spyware id
EField = 113, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow init pkt rate
EField = 114, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow resp pkt rate
EField = 111, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow init octets rate
EField = 112, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow resp octets rate
EField = 115, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow resp pkt size
EField = 116, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow resp pkt size
EField = 191, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=snwl option

IPfix Template ID = 258, Name = table-map, Number of Elements = 2, Total Length = 36
EField = 28, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=template identifier
EField = 29, Field bytes = 32, EntId = 8741, type = string-null terminated, name=table name

IPfix Template ID = 259, Name = column-map, Number of Elements = 4, Total Length = 44
EField = 30, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=column identifier
EField = 31, Field bytes = 32, EntId = 8741, type = string-null terminated, name=column name
EField = 32, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=column type
EField = 33, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=column standard IPFIX ID

```

## Solution Document Version History

Version Number	Date	Notes
1	8/31/2004	This document was created by A. Mendoza.
2	9/22/2010	Added Log > Flow Reporting reference tables.
3	11/10/2010	Incorporated Manish's draft instructions on NetFlow configuration settings.
4	11/22/2010	Incorporated Manish's changes regarding 'Collector' section and configuration examples.
5	12/03/2010	Added Appendix section.
6	1/07/2011	Updated UI screenshots.

Part Number: 232-001989-00 Rev. B