SolarWinds Technical Reference
Understanding Cisco ASA NetFlow

This Technical Reference focuses in Cisco’s implementation of NetFlow for ASA devices.

| Cisco Adaptive Security Appliance (ASA) NetFlow Overview | 3 |
| Understanding the Implementation Requirements | 4 |
| Troubleshooting ASA NetFlow | 6 |
Cisco Adaptive Security Appliance (ASA) NetFlow Overview

NetFlow configuration of and operations for ASA devices is very different from typical NetFlow. ASA devices began supporting NetFlow as of ASA software version 8.1(2), but there were several issues with that release. The 8.2(2), and later, releases provide a much more robust NetFlow implementation. An Internet search for “ASA NetFlow” yields a mountain of information, and if you are not familiar with NetFlow v9 or ASAs it can be information overload. This paper is aimed at providing guidance and insight for the implementation, interpretation, and troubleshooting of NetFlow on ASA appliances. The goal of this paper is to highlight and explain the important information about ASA NetFlow, allowing you to implement ASA NetFlow with confidence.

The following table explores some of the main differences between ASA NetFlow and most other NetFlow Implementations.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Typical NetFlow</th>
<th>ASA NetFlow</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version support</td>
<td>V5 and v9</td>
<td>V9 with fixed templates</td>
</tr>
<tr>
<td>Flow export trigger</td>
<td>TCP RST or FIN flags detected, flow timers, cache full</td>
<td>Network Security Event Logging (NSEL) detects a state change in a flow</td>
</tr>
<tr>
<td>Implementation</td>
<td>Independent CLI commands or SNMP set commands</td>
<td>Independent CLI for templates commands, modular policy framework for flow definitions</td>
</tr>
<tr>
<td>NetFlow show commands</td>
<td>Expose detailed interface and exporter statistics</td>
<td>Limited – See ASA Command Reference</td>
</tr>
<tr>
<td>Directionality</td>
<td>Interface ingress and egress</td>
<td>All flows are shown without a direction marker (Also referred to as bidirectional)</td>
</tr>
</tbody>
</table>

Here is a brief description of the terms specific to NetFlow v9 and the ASA implementation.

The ASA device is the NetFlow exporter. The Orion NetFlow Traffic Analyzer is the NetFlow collector. A flow template is exported by the NetFlow exporter and sent to the NetFlow collector. Templates are used as parsers by the collector to define fields in the flow data exports. Templates carry no actual flow data; they only tell the collector how to interpret flow data. NetFlow v9 uses flow templates to define flow data similar to how SNMP uses MIBS to define SNMP data. Flow data packets carry only flow information. Templates and flow data are never mixed within a single packet. Both flow data packets and flow template packets must be received by the NetFlow collector in order to display ASA NetFlow information on the NetFlow Traffic Analyzer web console. Both template packets and flow data packets can contain up to 30 separate records. These records are sometimes referred to as Protocol Data Units (PDUs).

Network Security Event Logging (NSEL) is the method ASAs use to trigger flow exports. Three event types are defined by NSEL:

- Flow creation
- Flow denial
- Flow teardown
Understanding the Implementation Requirements

Syntax Conventions - The below commands follow these conventions:

- Braces ({})) indicate a required choice.
- Square brackets ([]) indicate optional elements.
- **Boldface** indicates commands that should be entered exactly as shown.
- *Italics* indicate arguments for which you must supply values.

*Note:* When implementing ASA NetFlow this paper should be used only in conjunction with the step-by-step instruction provided in the SolarWinds KB [Configuring Cisco ASA devices for use with Orion NTA](#).

For an ASA device to export NetFlow data, the ASA must be configured with specific commands. Some of these commands are independent CLI commands, meaning that the commands are not dependent on other commands in terms of order or precedence.

Before an ASA can be added to NTA it must first be managed by Orion. This will require the normal steps to adding a node in Orion and the Orion server must be a known host to the ASA SNMP server. The following command must be placed on the ASA config before adding the ASA in Orion.

```
(config)# snmp-server host {InterfaceName} {OrionServerIPAddress} community {Read-onlyCommunityString}
```

The independent CLI commands are used to configure the export of flow templates only. These commands are:

```
(config)# flow-export destination {InterfaceName} {OrionServerIPAddress} 2055

(config)# flow-export template timeout-rate (#Minutes)

(config)# flow-export delay flow-create (#Seconds)
```

The first command is mandatory and starts the export of flow templates to the collector. To export to multiple collectors, repeat this command with once for each collector, using a unique collector’s IP address each time. The second and third commands are used to alter template timers from their default values.

The next set of commands implements the flow exports using Cisco’s *Modular Policy Framework*. Modular Policy Framework is used to implement several security and QoS features and it consists of the following three entities:

- Traffic identification using a class map
- Actions to be taken as described by a policy map
- Application of the policy to an interface using a service policy
Because of the inherent hierarchy in this configuration, the commands are not independent. You cannot create a policy map without an existing class map and the service policy is dependent on both class and policy maps being in place. Depending on the software version there are six to seven individual commands that implement the three mappings. These are:

```bash
(config)# access-list netflow-export extended permit ip any any
(config)# class-map netflow-export-class
(config-cmap)# match access-list netflow-export
(config)# policy-map {existing global policy map name}
(config-pmap)# class netflow-export-class
(config-pmap-c)# flow-export event-type all destination {OrionServerIPAddress}
```

This command can be used to export flows to one or more NetFlow collectors. To export to multiple collectors either repeat this command with a unique collector IP address each time, or issue the command once leaving a space between each collector's unique IP address at the end of the command.

For example

```bash
(config-pmap-c)# flow-export event-type all destination 10.110.21.5
(config-pmap-c)# flow-export event-type all destination 10.110.21.65
```

Or

```bash
(config-pmap-c)# flow-export event-type all destination 10.110.21.5 10.110.21.65
```

Support for multiple collectors may vary by ASA version.

Version 8.1 exporters require the `flow-export enable` command. This command was deprecated in version 8.2. This command is independent of other commands and is entered at the (config) prompt.
The last step in Modular Policy Framework is normally to map the policy to an interface. With ASA NetFlow this is achieved differently. The existing global policy is already mapped to the service policy. So by referring to the existing global policy the connection is made. Service policy commands to map the NetFlow policy to a particular interface directly are not supported in ASAs. The NetFlow policy map is linked to the global policy and the global policy’s service policy and applied to all interfaces automatically.

It can be difficult to remember the format for these commands and where hyphens should be used. The rule for hyphen use is that if there are two or more words that specify a single entity or a single action, they are hyphenated. For example, a class map is a single entity; therefore it is specified as class-map in CLI. Netflow-export-class refers to the class defined in the (config)# class-map netflow-export-class command and so is also a single entity. Flow-export specifies a single action as does flow-create and are hyphenated as well.

## Troubleshooting ASA NetFlow

### General NetFlow Troubleshooting

1. On the NTA Summary view of the Web Console, the NetFlow Collector Service resource status icon should be up (green). If it is not go to Administrative Tools > Services and start the service.

2. The NetFlow Sources resource should list the device sending NetFlow. If it does, click the plus icon and drill down to the interfaces. If it does not list the device, ensure the device is being managed by Orion and check NetFlow Settings to see if the device is a listed NetFlow Source. If it is not a listed source and not managed by Orion, add the device to Orion, and then add it to NetFlow Sources. If the interface shows up after drilling down, check the time on the last received NetFlow column. If the time listed is current then click on the interface name to see the data. If the time is old or says “never” proceed to the next step.

3. Start a packet capture program on the Orion server’s LAN interface. Capture packets for a couple of minutes and then sort by source IP and look for the NetFlow exporter’s IP address (source IP) with cflow protocol packets. If there are no cflow packets coming from the exporter check the exporter using the show flow export counters commands. The flow counters should be non-zero and should increment when this command is reissued. Make sure the IP source address of the exporter in the capture is the same IP address that Orion is using to manage the ASA.
ASA Specific Troubleshooting

- Check the packet capture for template packets and data packets. Both are classified as cflow protocol. ASA devices export thirteen templates. You can normally identify template packets by the record count of thirteen. Depending on the traffic load on the exporter, data packets may have various record counts. To confirm the packet type, expand the flowset section of the packet.
• If you only see template packets and no data packets, ASA exporter may be misconfigured. Check the ASA Modular Policy Framework configuration for errors, typos, or missing commands. If the exporter configuration is correct, check the network path from the ASA for possible firewalls or other devices interfering with the export delivery.

• If you are seeing data packets only and no template packets there are two probable causes. The packet capture may have been too short resulting in a valid template not being captured. This can be seen by expanding the data packets and finding a no template error. If this is the case check the exporter for the (config)#flow-export template timeout-rate 1 command. The default timeout is 30 minutes which may cause the templates to be dropped from the collector's memory. Template packets are only 1K so increasing the timeout to 1 minute has no adverse effect on the network. Running a capture for more than 1 minute will then ensure that templates are collect as well as data.