

Configuring Cisco ASAs for NSEL Export



It is recommended that only users with experience in configuring Cisco devices follow these steps.



Cisco ASA devices are primarily designed for network security and not traffic routing, and as a result NSEL does not provide complete export capability. Read more at [Choosing Export Protocol](#).

This section offers a brief guide for configuring NSEL export on a Cisco ASA device. NSEL stands for Net Flow Secure Event Logging - a traffic export mechanism that is built on NetFlow v9 technology. For more detailed information, go to [Cisco website](#).

Supported Devices

Devices	Versions	Notes
Cisco ASA	8.4(5)+	Excluding 8.5(1), 8.6(1), 8.7(1), 9.0(1), and 9.1(1)

Configuration Example

First define the interface for NSEL export.

```
ASA(config)# interface fa 0/0
ASA(config)# nameif inside
```

Define the NetFlow global parameters. Define a NetFlow collector **IP address** that can be used in the policy-map (in this example collector IP address is 1.1.1.1). The port is arbitrary and based on the collector implementation.

```
ASA(config)# flow-export destination inside 1.1.1.1 2055
```

OPTIONAL: Configure a delay for flow-create NSEL events in seconds. Increasing flow-create delay will cause fewer NSEL events to be exported to NetVizura NetFlow collector. E.g. setting delay to 120 will cause only one NSEL event to be exported, for flows shorter than 2 minutes.

```
ASA(config)# flow-export delay flow-create 120
```

OPTIONAL: Configure the template timeout-rate. These are minutes between sending a template record to NetVizura NetFlow collector. NetVizura requires templates in order to process flow exports. E.g. if you set timeout-rate to 30 it may take up to 30 minutes before you see any data in the charts. After that NetVizura will continue processing flows without any delay.

```
ASA(config)# flow-export template timeout-rate 5
```

Configure flow-update events to provide periodic byte counters for flow traffic. This represents an interval between two NSEL update events in minutes. **NetVizura requires this value to be less than 5**. Smaller value of refresh interval will produce bigger load on NetVizura NetFlow collector, but it will provide more accurate traffic statistics.

```
ASA(config)# flow-export active refresh-interval 1
```

Next create an ACL to flag interesting traffic and apply it to a class-map

```
ASA(config)# access-list flow_export_acl extended permit ip any any
ASA(config)# class-map flow_export_class
ASA(config-cmap)# match access-list flow_export_acl
ASA(config-cmap)# exit
```

Configure a unique NetFlow policy map and apply it globally. "event-type" option defines what you want NSEL to export (all, flow-create, flow-update, flow-deny, flow-teardown).

```
ASA(config)# policy-map flow_export_policy
ASA(config-pmap)# class flow_export_class
ASA(config-pmap-c)# flow-export event-type all destination 1.1.1.1
ASA(config-pmap-c)# service-policy flow_export_policy global
ASA(config-pmap-c)# end
```



If you create a new policy map and apply it globally according to the previous step, the remaining inspection policies are deactivated. Alternatively, to insert a NetFlow class in the existing policy, enter the class `flow_export_class` command after the `policy-map global_policy` command.

For more information about creating or modifying the Modular Policy Framework, see the [firewall configuration guide](#).