

How to configure Netflow on a Cisco ASA:

ASA NetFlow export is dependent on the version of ASA software running. ASA version 8.2 software supports NetFlow export across all ASA models, but some models may function on a lower software level. The following fields must be included in the ASA configuration to export flow data to the Orion NetFlow Traffic Analyzer module.

Notes:

- This sample configuration has been verified on an ASA 5505 running ASA software version 8.2(1)12.
- Configured firewall rules should be tested when ASA configuration changes are made.
- Some ASA systems will not export without the **flow-export enable** command also included.
- There is a bug in ASA versions prior to 8.2.1.12 that causes flow information to be reported from incorrect interfaces.
- In all ASA exporters, flow information is exported without regard to flow direction. As a result, duplicate flows appear to come from both endpoints of a conversation, and it can be difficult to determine which endpoint is receiving and which endpoint is transmitting in a selected conversation.

The following commands must be included in your global service policy for ASA NetFlow export to function.

1. (config)# **flow-export destination** <interface name> <Orion server IP address> **2055**

Notes:

- Replace <interface name> with the interface name that will be used to send exports to Orion NTA. This interface must be on the same side of the ASA as the Orion server.
 - Replace *Orion server IP address* with the IP address of your Orion NTA server.
2. (config)# **flow-export template timeout-rate** <#_minutes>
Note: This command sets the interval, in minutes, at which template information is sent to your NTA server. The default is 1 minutes, and this will probably work in most cases.
 3. (config)# **flow-export delay flow-create** <#_seconds>
Note: This command sets the flow-create delay to allow short-lived, identical flows to be exported as a single flow if they occur during the specified delay period. Setting this delay to 60 seconds should work for most environments.
 4. (config)# **logging flow-export syslogs disable**
Note: This setting is optional, but it is recommended, as it eliminates the impact of flow-exported syslogs that may cause performance issues. This setting is not supported by all ASA software versions
 5. (config)# **access-list netflow-export extended permit ip any any**
Note: This command defines an access list called netflow-export to specify the traffic of interest. The provided syntax includes all traffic.
 6. (config)# **class-map netflow-export-class**
Note: This command enters class map configuration mode and defines a class called netflow-export-class.
 7. (config-cmap)# **match access-list netflow-export**
Note: This command maps the netflow-export access list to the defined netflow-export-class class.
 8. (config)# **policy-map netflow-policy**
Note: This command enters policy map configuration mode and defines a policy called netflow-policy.
 9. (config-pmap)# **class netflow-export-class**
Note: This command maps the netflow-export-class class to the defined netflow-policy policy.



10. (config-pmap-c)# **flow-export event-type all destination** <Orion server IP address>

Notes:

- This command defines both the NSEL event types (all) to be exported and the export target (your Orion NTA server).
- Replace *Orion server IP address* with the IP address of your Orion NTA server.

Steps **8-10** create a new policy map for NetFlow, but you can also add the created class map (netflow-export-class) to an existing or current policy. If this is a new policy, you will need to apply the policy map to your ASA either at an interface policy level or at the global level. If you are applying the netflow-policy policy at the global level, use the following command:

11. (config)# **service-policy netflow-policy global**

Note: This command maps the netflow-policy policy to the existing global policy.

This article applies to:

Orion NetFlow Traffic Analyzer 3.5 SP2 and higher