Configuring Netflow on a Cisco ASA Firewall

Cisco ASA firewalls export flow information a little differently than other devices. Here is how to configure an ASA to send flows to a TotalView server.

ASA Configuration

The following configuration should be added via the privileged config prompt:

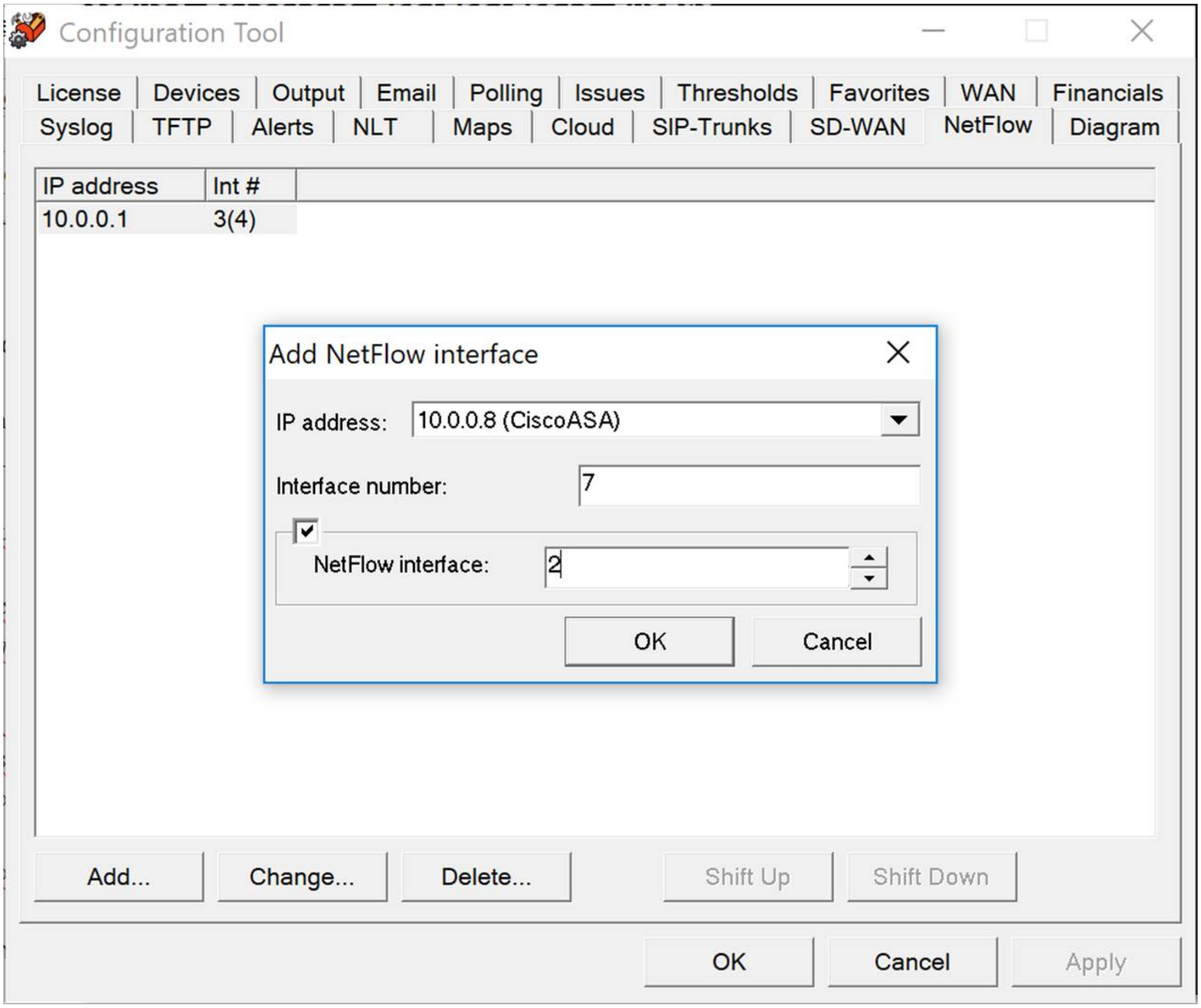
```
flow-export destination inside 10.10.0.10 2055       ← Send flow records to the TotalView server port 2055
flow-export template timeout-rate 10                  ← Send template records every 10 minutes
!
access-list flow_export_acl extended permit ip any any     ← Include all traffic in the ACL
!
class-map flow_export_class                           ← Set up a class-map to define the type of traffic to match
match access-list flow_export_acl                     ← Match the “all traffic” ACL
!
policy-map flow_export_policy                         ← Create a policy
class flow_export_class                               ← Use the previously defined class
  flow-export event-type all destination 10.10.0.10 ← Export all events to the TotalView server
!
service-policy flow_export_policy global              ← Apply the policy globally
```

Note: Don’t forget to save the configuration after making these changes.

TotalView Configuration

TotalView must be monitoring the device via SNMP to be able to monitor a device’s Netflow.

Run the Config Tool and click on the “Netflow” tab. Click “Add” to add a Netflow device and interface. You should see the following dialog box:



IP address	Int #
10.0.0.1	3(4)

IP address: 10.0.0.8 (CiscoASA)

Interface number: 7

☑ NetFlow interface: 2

Select the monitored device with the IP address drop down.
Enter the interface number that corresponds with the flows that you want to see associated.
For Cisco ASA, check the box and enter the Netflow interface that associates with the VLAN that the interface associates with. This can be seen in the config file like such:

```
interface Ethernet0/5
switchport access vlan 2
```

It can also be determined by using the "show switch vlan" command:

```
CiscoASA# show switch vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -----------------
------------
1    inside                           up        Et0/1, Et0/2,
Et0/3, Et0/4
                                                Et0/6, Et0/7
2    outside                          up        Et0/0, Et0/5
3    -                                down
4    -                                down
```

```
5    -                                down
6    -                                down
7    -                                down
8    -                                down
9    -                                down
10   -                                down
```

Once the interface is configured, click “OK” or “Apply” to make the configuration change and have the service restarted.

Note: It may take 10-15 minutes for flows to show up depending on how often the flow template records are sent.