



# Cisco Cyber Threat Defense Solution 1.1

## How-To Guide: NetFlow Security Event Logging

### Guide

---

## Introduction

### What is the Cisco Cyber Threat Defense Solution?

The network security threat landscape is ever evolving, but always at the cutting edge are custom-written, stealthy threats that evade traditional security perimeter defenses. The Cisco® Cyber Threat Defense Solution provides greater visibility into these threats by identifying suspicious network traffic patterns within the network interior. These suspicious patterns are then supplemented with contextual information necessary to discern the level of threat associated with the activity.

The Cisco Cyber Threat Defense Solution, jointly developed and offered with Lancope®, leverages Cisco networking technology including NetFlow®, Network Based Application Recognition (NBAR), and the Identity Services Engine to provide visibility and context to allow the identification of suspicious traffic patterns within the network interior. The level of visibility and context provided can allow security analysts to detect targets, potential damage, and threatening behavior such as:

- Network reconnaissance
- Interior network malware proliferation
- Command and control traffic
- Data exfiltration

### About This Document

This document describes deployment, implementation, and usage best practices in incorporating the Cisco ASA as an effective source of visibility and context as part of the Cisco Cyber Threat Defense Solution. This document assumes that the reader has a working familiarity with the Cyber Threat Defense Solution and has at least read the **Introduction to the Cisco Cyber Threat Defense Solution How-To Documents** available at <http://www.cisco.com/go/threatdefense>.

### About NSEL

The Cisco ASA implementation of NetFlow is known as NetFlow Security Event Logging (NSEL). First introduced in ASA software version 8.2(1), NSEL allows specific, high-volume, traffic-related events to be exported from the security appliance in a more efficient and scalable manner than that provided by standard syslog logging.

NSEL is built on top of the NetFlow v9 protocol; however, the fields within the NetFlow v9 record are used differently than in standard NetFlow reporting.

The primary difference between standard NetFlow and NSEL is that NSEL is a stateful flow tracking mechanism that exports only those records that indicate significant events in an IP flow. NSEL events are used to export data about flow status, and are triggered by the event that caused the state change, rather than by activity timers as in standard NetFlow. The ASA currently reports on three event types:

- Flow Create
- Flow Tear Down
- Flow Denied

A few other differences between NSEL and standard NetFlow version 9 implementations should also be noted:

- NSEL is bidirectional. A connection through a Cisco IOS device generates two flows, one for each direction, whereas NSEL sends a single flow per connection.
- NSEL will report a total byte count for the bi-directional flow, rather than a byte count for each direction.
- NSEL does not report a packet count.
- NSEL has predefined templates for the three event types. These templates are usually exported before any NSEL data records.
- NSEL flow-export actions are not supported in interface-based policies; they can only be applied in a global service policy.

NSEL offers unique advantages and can provide greater insight and visibility into the traffic passing through the network edge if the NSEL records and data are processed and handled accordingly. As a component of the Cisco Cyber Threat Defense Solution, the Lancop StealthWatch System understands and leverages the unique fields to provide visibility and context to assist the security analyst in detecting network threats.

## Configuring NSEL

NSEL is configured on the ASA appliance using the Modular Policy Framework (MPF). The simplest way to enable NSEL for all flows is to configure it as part of the global policy as described in the following procedures.

### Procedure 1 Configure the NSEL collector.

#### Step 1. Configure the NSEL collector.

This step defines the NetFlow collector to which the NetFlow records will be sent by the ASA.

```
ASA(config)# flow-export destination interface-name collector-ip-address port
```

Where *interface-name* refers to the interface on the ASA appliance where the collector (at *collector-ip-address* and *port*) can be reached. For example:

```
ASA(config)# flow-export destination inside 192.168.200.25 2055
```

### Procedure 2 Configure NSEL in the global policy.

#### Step 1. Enter the global\_policy configuration.

```
ASA(config)# policy-map global_policy
```

#### Step 2. Enter class-default configuration.

```
ASA(config-pmap)# class class-default
```

#### Step 3. Define the flow-export action for all traffic.

```
ASA(config-pmap-c)# flow-export event-type all destination collector-ip-address
```

Where the *collector-ip-address* is the same IP address given to the collector created earlier.

### Procedure 3 (Optional) Tune the template timeout interval.

#### Step 1. Modify the interval in which the template records are sent.

```
ASA(config)# flow-export template timeout-rate 2
```

**Best practice:** Use an interval rate of 2 minutes, as shown here.

#### Procedure 4 (Optional) Disable redundant syslog messages.

Since the purpose of NSEL was to create a higher-performance method of logging flow-based events, enabling NSEL will create several redundant syslog messages. In high-performance deployments, it is beneficial to disable these redundant messages.

**Step 1.** Disable redundant syslog messages.

```
ASA(config)# logging flow-export-syslogs disable
```

**Step 2.** Show the status of redundant syslog messages.

```
ASA# show logging flow-export-syslogs
```

#### Procedure 5 Verify.

**Step 1.** Verify the configuration using **show** commands.

**Step 2.** Check the runtime counters to see NSEL statistical and error data.

```
ASA# show flow-export counters
destination: management 192.168.200.25 2055
Statistics:
  packets sent                2896
Errors:
  block allocation failure    0
  invalid interface           0
  template send failure       0
  no route to collector       0
```

If the configuration is correct, the output of the command should show:

- The destination to be the IP address of the StealthWatch FlowCollector
- Packets sent to be greater than zero (assuming that flows are traversing the device)
- Zero errors

**Step 3.** Verify that the ASA is in the exporter tree of the StealthWatch FlowCollector in the SMC.

**Step 4.** Open the Flow Table (Right-click the ASA and select Flows → Flow Table)

Final Configuration

```
!
flow-export destination management <ip-address> 2055
!
policy-map global_policy
  class class-default
    flow-export event-type all destination <ip-address>
!
flow-export template timeout-rate 2
logging flow-export syslogs disable
!
```

### Additional Information:

NSEL configuration: [http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/monitor\\_nsel.html](http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/monitor_nsel.html).

NSEL Implementation Note: <http://www.cisco.com/en/US/docs/security/asa/asa84/system/netflow/netflow.html>.

## Using NSEL Data

As previously mentioned, NSEL is different than traditional NetFlow: NSEL is a mechanism of logging flow-based events using the NetFlow protocol instead of Syslog. When using NSEL data, it is important to keep this distinction in mind in order to get the most value out of the data. This section will discuss how to use NSEL data as an extremely effective component of the Cyber Threat Defense solution.

### Flow Action

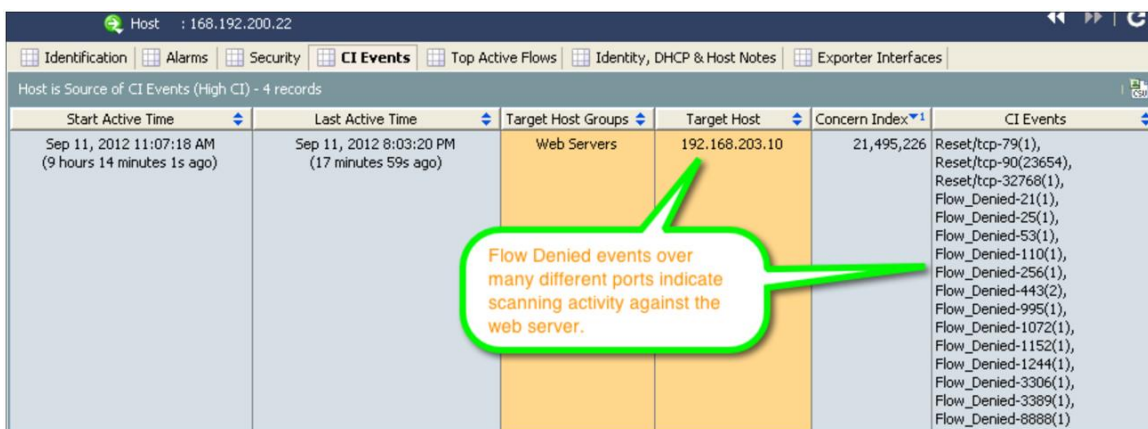
Recall that NSEL is a stateful flow tracking mechanism, that NSEL records are generated by the ASA for significant flow events (flow created, flow denied and flow tear down), and that this information is transported as a field inside the NSEL record. StealthWatch will interpret these fields and defines them as a Flow Action, as seen in the figure below. If a flow is permitted through the firewall (indicated by flow created and tear down events), the Flow Action field will show Permitted; if the flow is blocked by the firewall ACL, the Flow Action field will show Denied.

Flow Action	Client Host	Translated Host	Client Host Groups	Server Host	Server Host Groups
Permitted	192.168.203.10	168.192.203.10	Web Servers	168.192.200.22	United States
Permitted	192.168.203.10	168.192.203.10	Web Servers	168.192.200.22	United States
Permitted	168.192.200.22	168.192.203.10	United States	192.168.203.10	Web Servers
Denied	168.192.200.22	168.192.203.10	United States	192.168.203.10	Web Servers
Denied	168.192.200.22	168.192.203.10	United States	192.168.203.10	Web Servers

The Flow Denied action can provide a useful inspection point to run queries and to identify suspicious activity, such as scanning.

Flow Action	Client Host	Client Host Groups	Server Host	Server Host Groups	Service Summary
Denied	168.192.200.22	United States	192.168.203.10	Web Servers	Undefined TCP (90/tcp)
Denied	168.192.200.22	United States	192.168.203.10	Web Servers	Undefined TCP (900/tcp)
Denied	168.192.200.22	United States	192.168.203.10	Web Servers	Undefined TCP (648/tcp)
Denied	168.192.200.22	United States	192.168.203.10	Web Servers	Undefined TCP (720/tcp)
Denied	168.192.200.22	United States	192.168.203.10	Web Servers	Undefined TCP (100/tcp)
Denied	168.192.200.22	United States	192.168.203.10	Web Servers	Undefined TCP (1022/tcp)
Denied	168.192.200.22	United States	192.168.203.10	Web Servers	Undefined TCP (19/tcp)
Denied	168.192.200.22	United States	192.168.203.10	Web Servers	Undefined TCP (32/tcp)
Denied	168.192.200.22	United States	192.168.203.10	Web Servers	Undefined TCP (512/tcp)

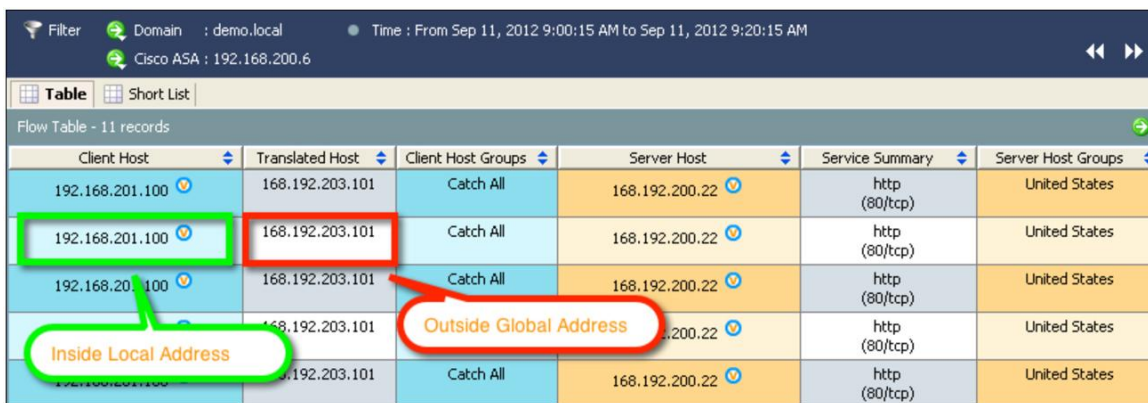
The context provided by the Flow Action fields is taken into account by the behavioral algorithms inside StealthWatch. Concern Index (CI) points are assigned to an IP address for each Flow Denied event it generates and Target Index (TI) points are accumulated for IP addresses that are the targets of Flow Denied events. StealthWatch's ability to use NSEL information to conduct sophisticated behavioral analysis on the flow data can enhance the ability of the solution to identify malicious users and threats, as illustrated in the below figure.



Start Active Time	Last Active Time	Target Host Groups	Target Host	Concern Index*1	CI Events
Sep 11, 2012 11:07:18 AM (9 hours 14 minutes 1s ago)	Sep 11, 2012 8:03:20 PM (17 minutes 59s ago)	Web Servers	192.168.203.10	21,495,226	Reset/tcp-79(1), Reset/tcp-90(23654), Reset/tcp-32768(1), Flow_Denied-21(1), Flow_Denied-25(1), Flow_Denied-53(1), Flow_Denied-110(1), Flow_Denied-256(1), Flow_Denied-443(2), Flow_Denied-995(1), Flow_Denied-1072(1), Flow_Denied-1152(1), Flow_Denied-1244(1), Flow_Denied-3306(1), Flow_Denied-3389(1), Flow_Denied-8888(1)

### Stitching Flows Across NAT

One of the historical challenges in forensics investigations has been to reconstruct flow data as it traversed a network device that performs Network Address Translation (NAT), particularly in an environment using dynamic translations. Using NSEL data from the ASA in combination with StealthWatch, it is possible to easily go from a global (translated) IP address to the local IP address, as seen in the below figure. If a Cisco Identity Services Engine (ISE) is deployed, it is additionally possible to attribute that local IP address to a username and device.



Client Host	Translated Host	Client Host Groups	Server Host	Service Summary	Server Host Groups
192.168.201.100	168.192.203.101	Catch All	168.192.200.22	http (80/tcp)	United States
192.168.201.100	168.192.203.101	Catch All	168.192.200.22	http (80/tcp)	United States
192.168.201.100	168.192.203.101	Catch All	168.192.200.22	http (80/tcp)	United States
192.168.201.100	168.192.203.101	Catch All	168.192.200.22	http (80/tcp)	United States
192.168.201.100	168.192.203.101	Catch All	168.192.200.22	http (80/tcp)	United States

The following procedure describes an example investigative workflow using the following scenario: A security investigator has received notification from a third party that a global IP address belonging to their organization has been participating in a Distributed Denial of Service attack, and the investigator must now identify the infected host.

#### Procedure 1 Find the local IP address.

**Step 1.** Open the Flow Table for the Cisco ASA (Right-click the ASA icon → Flows → Flow Table).

**Step 2.** Set the filter condition for the reported time period and target IP address (Server Host).

**Step 3.** Locate the global IP address in the Translated Host column.



**Step 4.** Identify the local IP address in the Client Host column.

Client Host	Translated Host	Client Host Groups	Server Host	Service Summary	Server Host Groups
192.168.201.100	168.192.203.101	Catch All	168.192.200.22	http (80/tcp)	United States
192.168.201.100	168.192.203.101	Catch All	168.192.200.22	http (80/tcp)	United States
192.168.201.100	168.192.203.101	Catch All	168.192.200.22	http (80/tcp)	United States
192.168.201.100	168.192.203.101	Catch All	168.192.200.22	http (80/tcp)	United States
192.168.201.100	168.192.203.101	Catch All	168.192.200.22	http (80/tcp)	United States

## Procedure 2 Determine malicious activity.

**Step 1.** From the Flow Table, right-click the Client Host IP address of the suspected attacker and open the Host Snapshot.

**Step 2.** Adjust the date and time filter to be for the appropriate day.

**Step 3.** Look for any Alarms and CI Events associated with this host.

Start Active Time	Last Active Time	Target Host Groups	Target Host	Concer...	CI Events
Sep 11, 2012 3:40:07 AM (7 hours 10 minutes 32s ago)	Sep 11, 2012 3:44:41 AM (7 hours 5 minutes 58s ago)	United States	65.197.197.0/24	15,066	Addr_Scan/tcp-80(66)
Sep 10, 2012 10:22:36 PM (12 hours 28 minutes 3s ago)	Sep 11, 2012 8:46:20 AM (2 hours 4 minutes 19s ago)	Catch All	192.168.200.10	6	ICMP_Port_Unreach(3)

**Step 4.** Investigate other suspicious flows related to this host from the Flow Table.

## Procedure 3 Locate the user and infected machine.

**Step 1.** From the Host Snapshot, select the Identity, DHCP & Host Notes tab.

**Step 2.** In the Identity and Device Table, observe the identifying information (username, device details, access interface, etc.)

Start Active Time	End Active Time	User Name	MAC Address	Device Type	Domain Name	Network A...	Network Ac...
Sep 11, 2012 8:46:18 AM (49 minutes 50s ago)	Current	CHARLES-COMPA Alice	00:50:56:90:00:38 (VMware, Inc.)	Microsoft-Worksta tion	demo.local	192.168.200.2	GigabitEthernet0 /2

## Interpreting NSEL Data

The stateful record format of NSEL data differs from standard or traditional NetFlow and as such requires slightly different handling than traditional NetFlow. These differences are handled by StealthWatch behind the scenes, but it is worthwhile to be familiar with the differences to maximize the benefit of using NSEL data.

---

The biggest difference between traditional NetFlow and NSEL is that NSEL uses stateful records, including an indication of which host initiated a flow, thus making it easy to distinguish clients and servers. However, the byte count reported by NSEL is a total for data moving in both directions, making it difficult to separate how much data was uploaded or downloaded. Another significant difference is that NSEL currently does not report packet counts, making it difficult to detect Denial of Service attacks using NSEL data alone.

NSEL export from the ASA is currently driven by significant events in the flow, and while this is useful for the context gained, it does however present challenges when viewing flow data for active flows. Because byte counts are only delivered on Flow Tear Down events, a long-lived active flow may appear inside StealthWatch with no byte counts associated until the flow is closed.

**Best Practice:** In order to maximize benefit from ASA data, it is recommended to have another device exporting traditional NetFlow to StealthWatch for the same flow data, in order to fill in the missing timeout, packet and byte count data. This will ensure complete flow visibility while maintaining the unique context advantages delivered through NSEL.

## Conclusion

NetFlow export from the ASA, known as NSEL, takes a logging-based approach to NetFlow rather than the reporting-based approach used by traditional NetFlow implementations, and as a result has some differences in behavior. These differences, if properly understood, can add visibility and context, and thereby greatly enhance the value of a Cyber Threat Defense Solution deployment. The context provided by the permit/deny actions reported in NSEL data, combined with the behavioral analysis inside StealthWatch can greatly assist the security operator in identifying suspicious activity inside the network. For more information on how to use the Cyber Threat Defense Solution to detect advanced threats, refer to the other guides in the Cyber Threat Defense How-to series available at <http://www.cisco.com/go/threatdefense>.



Americas Headquarters  
Cisco Systems, Inc.  
San Jose, CA

Asia Pacific Headquarters  
Cisco Systems (USA) Pte. Ltd.  
Singapore

Europe Headquarters  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)