



# Cisco Cyber Threat Defense for the Data Center Solution: Cisco Validated Design

Last Updated: March 3, 2014



## About the Authors



Matt Robertson

Matt is a Technical Marketing Engineer at Lancope focused on behavior-based detection and analysis of security events. Previously, Matt was a Technical Marketing Engineer in the Security Technology Group at Cisco Systems, where he regularly worked with Cisco's largest customers all over the world developing solutions for advanced threat detection and defense.



Chris O'Brien

Chris is a technical marketing manager with Cisco's Computing Systems Product Group. He is currently focused on developing infrastructure best practices and solutions that are designed, tested, and documented to facilitate and improve customer deployments. Previously, he was an application developer and has worked in the IT industry for more than 20 years.

# CONTENTS

Introduction	4
Document Map	5
Products and Releases	5
Solution Overview	6
Architecture	6
Introduction to NetFlow	8
Design Considerations	11
Determining Flows-per-Second Volume	11
Deploying the Lancope StealthWatch System	12
Cisco NetFlow Generation Appliance	12
Cisco ASA 5500 Series Adaptive Security Appliances	14
Cisco Nexus 7004	16
Cisco Nexus 1000V VSM	17
Cisco Identity Services Engine	20
Design Considerations for the Lancope StealthWatch System	26
Design Considerations for StealthWatch FlowCollector	26
Design Considerations for StealthWatch Management Console	28
Concluding Remarks	28
References	29
About the Cisco Validated Design Program	30

# Cisco Cyber Threat Defense for the Data Center Solution: Cisco Validated Design

---

## Introduction

The threat landscape has evolved: government organizations and large enterprises are being inundated with targeted, custom attacks sometimes referred to as advanced persistent threats (APTs). A common thread among these custom, targeted attacks is that the motivated attackers are able to successfully bypass the perimeter security controls of an enterprise network to establish an operational footprint inside the network. Although the motivation for targeted attacks often varies, a common focus is espionage of critically sensitive data or stealing specific types of information for financial gain. Because this information often resides in the data center, it becomes crucial to implement a program to detect these threats.

The Cisco Cyber Threat Defense Solution for the Data Center provides a proactive capability for detecting threats already operating in an internal network or data center. This solution uses telemetry from network devices to provide deep and pervasive visibility across the data center, allowing the security operator to understand the “who, what, when, where, and how” of network traffic to identify suspicious and anomalous activities. The level of visibility and context provided by the Cisco Cyber Threat Defense Solution for the Data Center can greatly reduce the window of vulnerability and put control back into the hands of the security operator.

The Cisco Cyber Threat Defense for the Data Center Solution can provide the information and visibility to support the security operator in a wide spectrum of security tasks that include (but are not limited to) the following:

- Detecting botnet command and control channels
- Detecting network reconnaissance activity in the data center
- Detecting and monitoring the spread of malware throughout the data center network
- Detecting the occurrence of a data loss event
- Identifying a denial-of-service (DoS) attack

The Cisco Cyber Threat Defense for the Data Center Solution leverages Cisco networking technology such as NetFlow, as well as identity, device profiling, and user policy services from the Cisco Identity Services Engine (ISE).



---

**Corporate Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

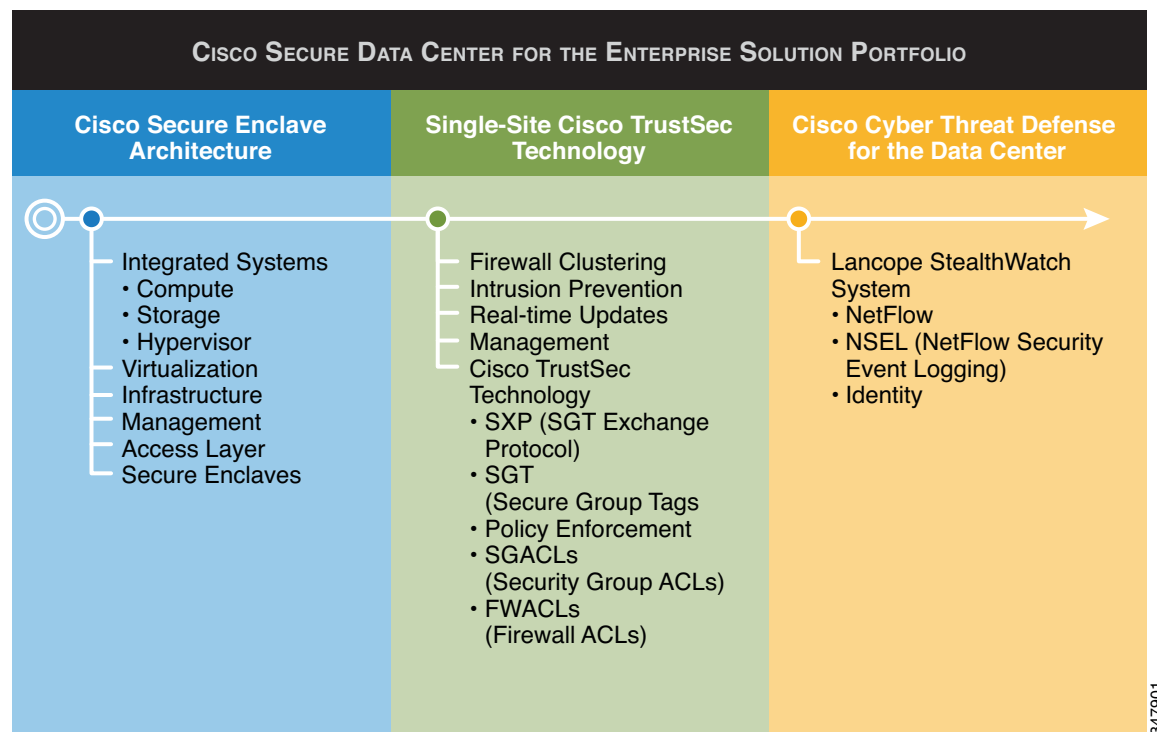
Copyright © 2014 Cisco Systems, Inc. All rights reserved

Cisco has partnered with Lancope to jointly develop and offer the Cisco Cyber Threat Defense Solutions. Available from Cisco, the Lancope StealthWatch System serves as the NetFlow analyzer and management system in the Cisco Cyber Threat Defense Solution for the Data Center.

## Document Map

Figure 1 shows the relationship and focus areas for the Secure Enclaves, Secure Data Center for Enterprise, and the Cyber Threat Defense for the Data Center solutions. For additional content outside the scope of this document, see the following URL: <http://www.cisco.com/go/designzone>.

**Figure 1** *Cyber Threat Defense Solution 1.1. Architecture*



This guide describes the design and provides design guidance for the Cisco Cyber Threat Defense for the Data Center Solution.

## Products and Releases

The Cisco Cyber Threat Defense for the Data Center solution uses the components listed in Table 1.

**Table 1** *Cisco Cyber Threat Defense for the Data Center Solution Components*

Component	Hardware	Release
Cisco Adaptive Security Appliance	ASA 5585-SSP60	Cisco ASA Software Release 9.1(4)
Cisco NetFlow Generation Appliance	3140	Cisco NGA Software Release 1.0(2)

**Table 1** *Cisco Cyber Threat Defense for the Data Center Solution Components (continued)*

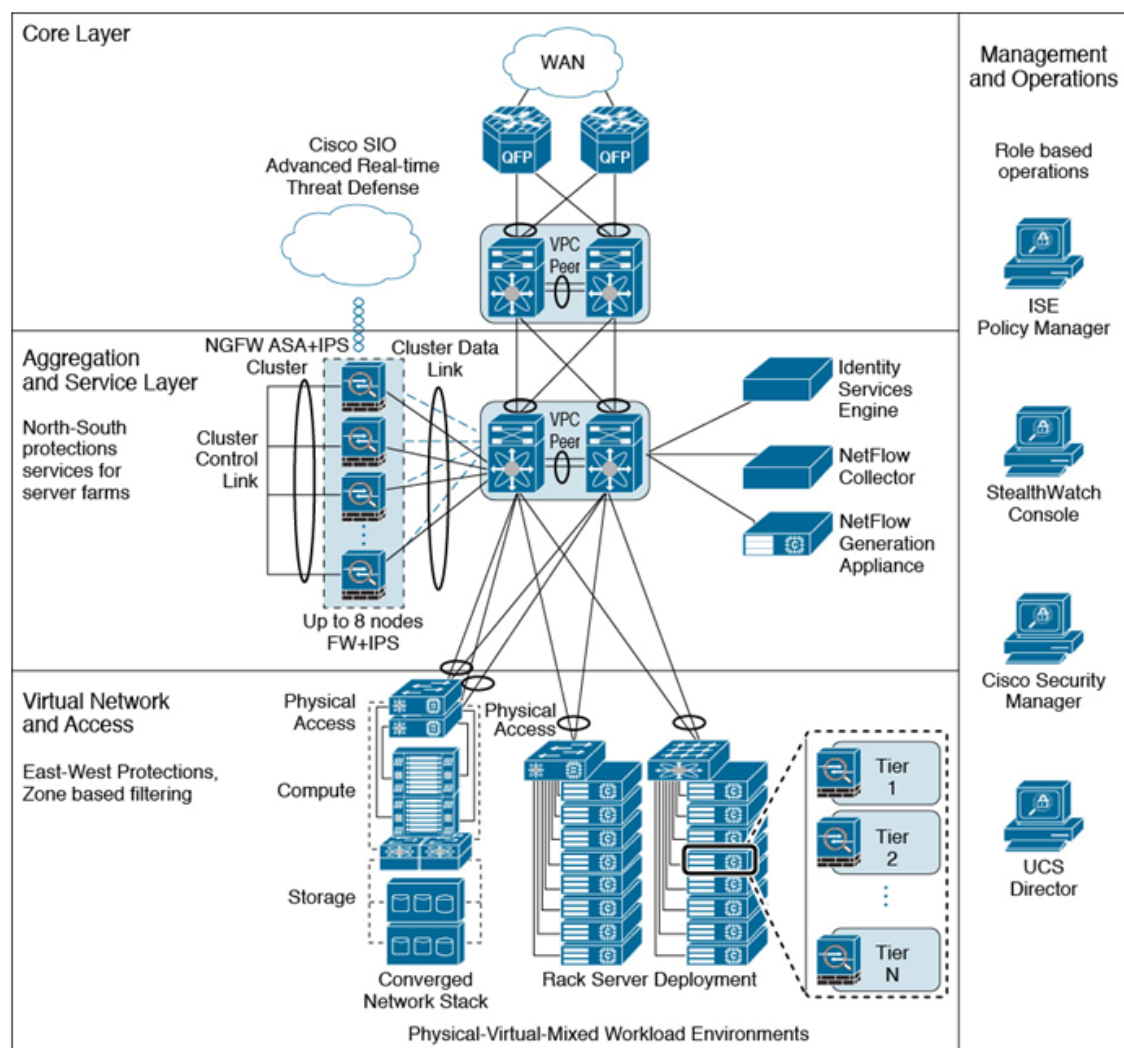
Cisco Nexus 7000	7004	NX-OS Version 6.1(2)
Cisco Nexus 1000V Virtual Services Module (VSM)	Virtual machine	4.2(1)SV2(2.1a)
Cisco Identity Services Engine	Virtual machine	Cisco ISE Software Version 1.2
Lancope StealthWatch Management Console	Virtual machine	StealthWatch 6.4
Lancope StealthWatch FlowCollector	Virtual machine	StealthWatch 6.4

## Solution Overview

### Architecture

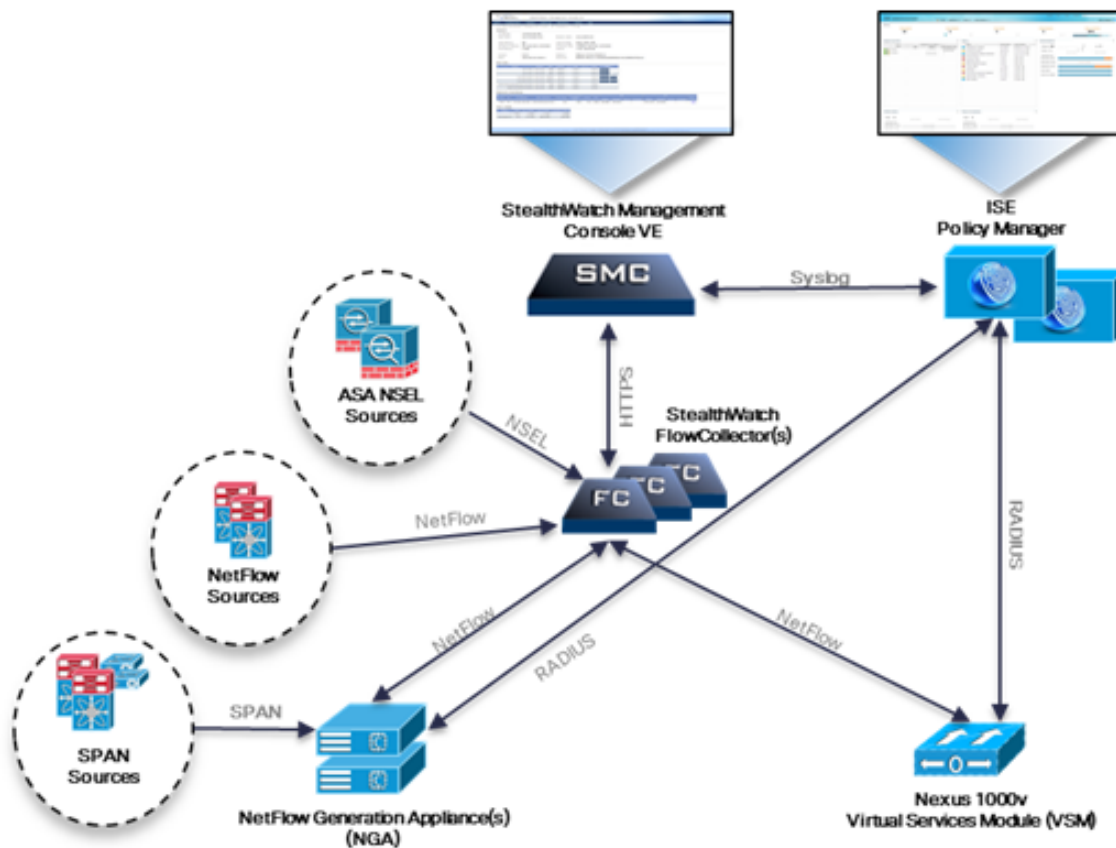
The Cisco Cyber Threat Defense for the Data Center Solution provides comprehensive visibility into all network traffic through the use of Cisco NetFlow technology. Cisco NetFlow technology is supported across Cisco data center switches and devices to enable telemetry to be implemented at all layers of the network. [Figure 2](#) illustrates the high-level system topology of the Cisco Cyber Threat Defense for the Data Center Solution.

**Figure 2 Cisco Cyber Threat Defense for the Data Center Solution Topology**



Coupling this enhanced visibility with identity and context information from the Cisco TrustSec solution enables security operators to better understand the data center network traffic. [Figure 3](#) illustrates the topology of the Lancope StealthWatch System, TrustSec with ISE, and NetFlow Generation Appliance (NGA) devices.

**Figure 3**



Visibility into data center network traffic is provided through NetFlow export from Cisco Nexus switches, NGA, and the Cisco Adaptive Security Appliance (ASA) using NetFlow Security Event Logging (NSEL). Identity services, including user name, device profile, and security group information, are provided through the Cisco TrustSec Solution, using ISE. The Lancope StealthWatch FlowCollector provides NetFlow collection services and performs analysis to detect suspicious activity. The StealthWatch Management Console provides centralized management for all StealthWatch appliances and provides real-time data correlation, visualization, and consolidated reporting of combined NetFlow and identity analysis.

The minimum system requirement to gain flow data and behavior visibility is to deploy one or more NetFlow generators with a single StealthWatch FlowCollector managed by a StealthWatch Management Console. The minimum requirement to gain identity services is to deploy the Cisco ISE and one or more authenticating access devices in a valid Cisco TrustSec Monitoring Mode deployment.

# Introduction to NetFlow

A *flow* is identified as a unidirectional stream of packets between a given source and destination. NetFlow is a Cisco application that measures the IP network traffic attributes of a traffic flow as it traverses the Cisco device. NetFlow was initially created to measure network traffic characteristics such as bandwidth, application performance, and utilization; and has historically been used for billing and accounting, network capacity planning, and availability monitoring. NetFlow is a reporting technology:



as traffic traverses a device, the device gathers information about the traffic flow and reports on the information after the flow has occurred. NetFlow reporting has tremendous security applications as well, including the ability to provide non-repudiation, anomaly detection, and investigative capabilities.

The Cisco Cyber Threat Defense for the Data Center Solution uses NetFlow Version 9. NetFlow Version 9 completely separates the collection and export process and allows the customization of the NetFlow collection. Using this approach, the Cisco Cyber Threat Defense for the Data Center Solution captures NetFlow data across the infrastructure to maximize the security monitoring potential by collecting packet fields such as TCP flags, Time To Live (TTL) values, and protocol.

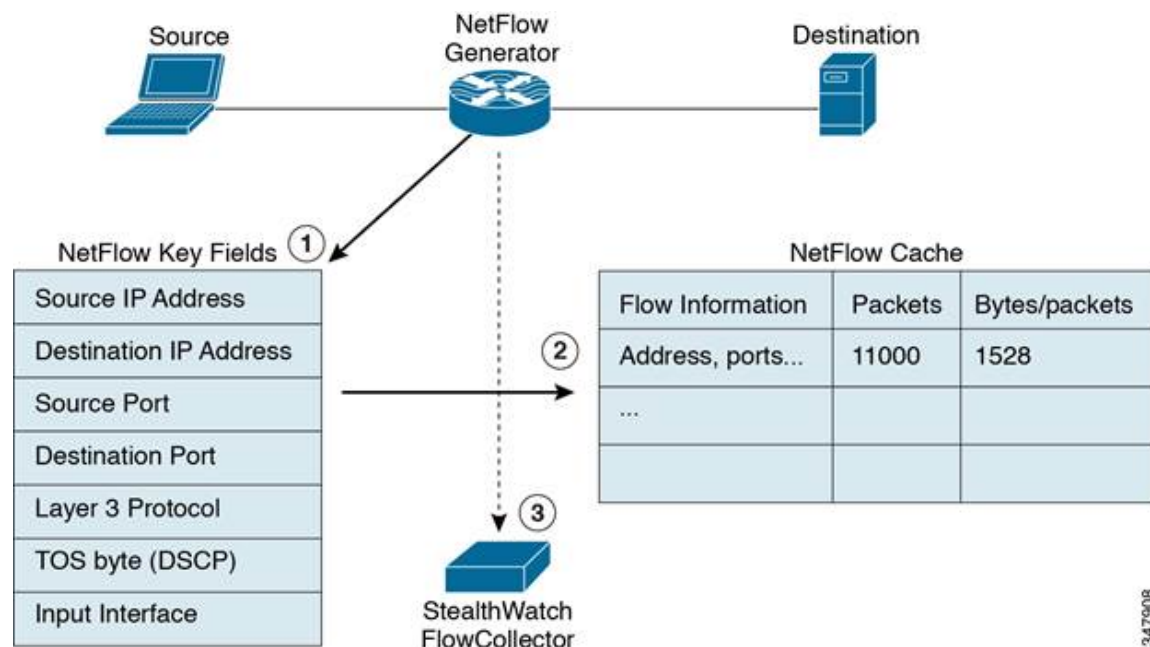


**Tip**

**Best practice:** Use the Cisco Flexible NetFlow feature wherever possible.

Some of the components in the Cisco Cyber Threat Defense for the Data Center Solution support both NetFlow v5 and v9 as well as the ability to create a customizable flow record. Support differs across platforms. Cisco recommends following the flow record configuration in this guide to achieve maximum results. Figure 4 illustrates NetFlow operation on a Cisco device.

**Figure 4** NetFlow Operation on a Cisco Device



1. As a flow traverses a Cisco device (NetFlow Generator), the NetFlow key fields are extracted.
2. The key fields are used to identify the flow in the NetFlow cache, which is the database of flows maintained on the device. In addition to the Key Fields, the Cisco device collects additional configured collection fields, such as TCP flags, byte counters, and start and end times, and stores this information in the NetFlow cache entry for this flow.
3. When the flow terminates or a timeout event occurs, a NetFlow Protocol Data Unit (PDU), known as a flow record, is generated and sent to a FlowCollector.

The Cisco Cyber Threat Defense for the Data Center Solution implementation should use NetFlow in a complete (non-sampled) manner. Sampled NetFlow leaves blind spots, because only a certain percentage of network flows have associated NetFlow records, making it difficult to detect the single traffic anomalies that indicate malicious activity.

Some data center network devices support NetFlow via software, rather than hardware support, such as the Cisco Nexus 1000V. Give some consideration to a software device's current utilization when deploying software-supported NetFlow services, because NetFlow enablement can affect device performance. An alternative to using NetFlow natively on the Nexus 1000V is to use a Lancope StealthWatch FlowSensor VE to generate NetFlow records from the virtual access layer.

Cisco devices with hardware-supported NetFlow suffer minimal performance degradation when NetFlow services are enabled. The most significant performance limitation in these devices is the size of the NetFlow cache supported by the hardware.

[Table 1](#) shows whether Cisco Cyber Threat Defense for the Data Center Solution components support NetFlow in hardware or software.

**Table 2      NetFlow Support—Hardware, Software, or SPAN**

Component	Hardware Support	Software Support
Cisco NetFlow Generation Appliance	Yes	
Cisco Nexus 1000V Series		Yes
Cisco Adaptive Security Appliance (ASA)		Yes <sup>1</sup>
Cisco Nexus 7000	SPAN <sup>2</sup>	

1. The ASA NetFlow implementation, known as NetFlow Security Event Logging (NSEL), is different than most software-supported NetFlow implementations. See the ASA section in this guide for more information.
2. In this design, NetFlow is not enabled natively on the Nexus 7000 switches for design consideration reasons. See the Nexus 7004 section in this guide for more information.

# Design Considerations

## Determining Flows-per-Second Volume

One necessary design task is to determine and measure the flows-per-second (fps) volume that will be generated by the network infrastructure in the data center. The number (volume) of fps indicates how many records the StealthWatch FlowCollectors will need to be able to receive and analyze; this number must be taken into consideration when selecting the StealthWatch FlowCollector model (described in a subsequent section).

Determining the fps number before the deployment of the Cisco Cyber Threat Defense for the Data Center Solution requires careful thought. Many factors can affect the volume of flows generated by the network devices, so predicting the exact number can be difficult. In general, a NetFlow generator generates between 1000 and 5000 fps per 1 Gbps of traffic passing through it; however, this is a general guideline and should be used only as a starting point.

Note that traffic throughput (Gbps) has no direct bearing on the fps number; the only measure that has a direct impact is the number (and rate) of flows passing through the device. For instance, a single high-volume (1 Gbps) flow could be passing through a port, resulting in an fps number of less than one; in contrast, there could be many small-volume flows passing through a port, resulting in low total throughput but a high fps number (4000 flows with a total throughput of 100 Mbps, for example). The fps number on a single device is largely influenced by the following measures:

- Number of unique flows passing through the device
- New connections per second
- Lifetime of flows (short-lived vs. long-lived)

To assist in predicting the FPS volume, use the Lancope FPS Estimator, available at the following URL: <http://www.lancope.com/fps-estimator>.

Although generally not a significant concern, consider the impact that NetFlow records will have on network traffic. NetFlow generally adds very little traffic to the network, because a NetFlow record represents the reporting for an entire traffic flow. However, certain traffic sets can generate more NetFlow records than other sets. Following are some of the factors that can influence the network overhead introduced by NetFlow:

- Flows per second.
- NetFlow record size. The Data Center Cyber Threat Defense Solution recommends NetFlow v9, which results in an average of 34 NetFlow records per 1500-byte packet.
- Flow timers (active and inactive timeouts for a flow). The Data Center Cyber Threat Defense Solution recommends an active timer of 60 seconds and an inactive timer of 15 seconds.

To predict the impact of enabling NetFlow, use the Lancope NetFlow Bandwidth Calculator, available at the following URL:

<http://www.lancope.com/resource-center/netflow-bandwidth-calculator-stealthwatch-calculator/>.



**Tip**

**Best practice:** If minimizing NetFlow overhead is a concern, NetFlow collection should be done as close to the NetFlow generator as possible.



**Tip**

**Best practice:** In an asymmetric routing situation, all devices in the asymmetric route should send NetFlow records to the same FlowCollector.

# Deploying the Lancopé StealthWatch System

The deployment and configuration of the Lancopé StealthWatch System as a component of the Cyber Threat Defense Solution for the Data Center followed the guidelines established in the Cisco Cyber Threat Defense Solution Cisco Validated Design Guide available at the following URL: [http://www.cisco.com/en/US/solutions/collateral/ns1015/ns1238/cyber\\_threat\\_defense\\_design\\_guide.pdf](http://www.cisco.com/en/US/solutions/collateral/ns1015/ns1238/cyber_threat_defense_design_guide.pdf). As a result, this guide does not provide details for the deployment and configuration of the Lancopé StealthWatch System. Readers are encouraged to consult the Cisco Cyber Threat Defense Solution CVD for guidelines regarding the design and deployment of the Lancopé StealthWatch System.

## Cisco NetFlow Generation Appliance

### Design

In large data centers, generating NetFlow at high rates can be challenging. The Cisco NetFlow Generation Appliance (NGA), a purpose-built, high-performance solution for flow visibility in multi-gigabit data centers, can restore flow visibility in these environments in a scalable and affordable manner.

The Cisco NGA has four 10G monitoring interfaces and up to four independent flow caches and flow monitors. This means that the Cisco NGA can receive up to 40 gigabits of data and support various combinations of data ports, record templates, and export parameters. This is important to consider when placing the NGA inside the data center.

The NGA can be placed to receive data from the physical access, aggregation, and core layers. The objective is to ensure complete visibility of all traffic within the data center, as well as traffic that is leaving the data center. Traffic within the virtual environment (VM-to-VM traffic) can be monitored using the Nexus 1000V, while traffic entering and leaving the data center can be monitored using edge devices such as the ASA and Nexus 7000. Strategically placing the NGA in the aggregation and core layers ensures effective monitoring of traffic within the data center, as well as providing additional statistics for traffic leaving the data center. The Cisco NGA is very scalable and can support up to 64 million active flows.



**Tip**

**Best Practice:** NGA monitoring interfaces should be sourced from choke points to ensure complete visibility into traffic inside the data center.

### Implementation

When configuring NetFlow on the NGA, keep in mind the following supported items:

- Up to ten filters—These define which flows are to be sent to certain collectors. This allows you to use your collector's analysis applications and load balance NetFlow data across collectors.
- Up to four managed devices—As discussed earlier, managed device settings allow you to collect interface information from your traffic sources.
- Up to six collectors—Enabling NetFlow export to up to six NetFlow collectors allows you to load-balance NetFlow data export and to monitor specific applications in your data center.
- Up to four monitors—Up to four independent flow monitors (flow caches) may be active simultaneously. Each monitor supports up to three records. Of those three records, only one IPv4, one IPv6, and one Layer 2 record type are supported.

After the Cisco NGA is deployed, the configuration of the NetFlow export is an eight-step process. For information on the deployment of the Cisco NGA as a component of the Cisco Cyber Threat Defense Solution of the Data Centre, see the How-To guide “Gain Visibility in the Data Center with the Cisco NetFlow Generation Appliance.” The How-To guide can also be used as a NetFlow configuration guide, because the following configuration steps used as a component of the Cisco Cyber Threat Defense Solution for the Data Center followed the steps contained in that guide.

### Procedure

- Step 1** Click **Setup-> Quick Setup**.
- Step 2** Define a unique name to identify this configuration; for example, *Cyber\_Example*.
- Step 3** Check the box for each data port that is configured to receive data. For information about configuring SPAN sessions on the Nexus 7000, see the section about the Nexus 7000 configuration.
- Step 4** Enter the IP address of the StealthWatch FlowCollector in the Collector Address box.
- Step 5** Enter the port on which the StealthWatch FlowCollector will be collecting NetFlow information; by default, this is UDP 2055.
- Step 6** Select **version 9** and define the Flow Record to include the fields shown in [Figure 5](#).

**Figure 5 Quick Setup**

Quick Setup

\* Name

\* Data Port 1 ☒ 2 ☐ 3 ☐ 4 ☐

\* Collector Address (IPv4)

\* Collector Port (UDP)

\* NetFlow Version ☐ v5 ☒ v9

<p>Match Fields</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> CoS</li> <li><input type="checkbox"/> Ethertype</li> <li><input checked="" type="checkbox"/> Input SNMP Interface</li> <li><input checked="" type="checkbox"/> IP Protocol</li> <li><input checked="" type="checkbox"/> IPv4 Destination Address</li> <li><input checked="" type="checkbox"/> IPv4 Source Address</li> <li><input checked="" type="checkbox"/> IPv4 TOS</li> <li><input checked="" type="checkbox"/> Layer 4 Destination Port</li> <li><input checked="" type="checkbox"/> Layer 4 Source Port</li> <li><input type="checkbox"/> MAC Destination Address</li> <li><input type="checkbox"/> MAC Source Address</li> <li><input type="checkbox"/> MPLS Label</li> <li><input type="checkbox"/> Output SNMP Interface</li> <li><input type="checkbox"/> VLAN ID</li> </ul>	<p>Collect Fields</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Application ID</li> <li><input checked="" type="checkbox"/> Byte Count</li> <li><input checked="" type="checkbox"/> First Timestamp</li> <li><input checked="" type="checkbox"/> IPv4 ICMP Code</li> <li><input checked="" type="checkbox"/> IPv4 ICMP Type</li> <li><input checked="" type="checkbox"/> Last Timestamp</li> <li><input checked="" type="checkbox"/> Max TTL/Hop Limit</li> <li><input checked="" type="checkbox"/> Min TTL/Hop Limit</li> <li><input type="checkbox"/> Network Encapsulation</li> <li><input checked="" type="checkbox"/> Packet Count</li> <li><input checked="" type="checkbox"/> TCP Header Flags</li> </ul>
---	---

**Optional**



### Note

The MAC fields are optional, based on whether Managed Device settings are configured or not. If Managed Device settings are configured, the MAC fields should be selected; if Managed Device settings are not configured, the MAC fields should not be selected.

**Step 7** Click **Submit**. The following components are created:

- A collector named *Cyber\_Example\_collector*
  - An exporter named *Cyber\_Example\_exporter*
  - A monitor named *Cyber\_Example\_monitor*
  - A record named *Cyber\_Example\_record*
- 

## Cisco ASA 5500 Series Adaptive Security Appliances

### About NetFlow Security Event Logging

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

In addition, note the following differences between NSEL and standard NetFlow version 9 implementations:

- 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 reports 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 be applied only in a global service policy.



**Tip**

**Best practice:** To maximize benefit from ASA data, Cisco recommends having another device exporting traditional NetFlow to StealthWatch for the same flow data, to fill in the missing timeout, packet, and byte count data. This ensures complete flow visibility while maintaining the unique context advantages delivered through NSEL.

---

## 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

#### 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
```

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

- a. Enter the `global_policy` configuration.

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

- b. Enter `class-default` configuration.

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

- c. 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.

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

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.

#### Step 4 Disable redundant syslog messages.

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

- a. Disable redundant syslog messages.

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

- b. Show the status of redundant syslog messages.

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

## 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
!

```

## Cisco Nexus 7004

The Cisco Nexus 7004 supports NetFlow in hardware with the F2 and Enhanced F2 Series modules. Without these modules, NetFlow is supported in software, which consumes CPU resources. Because the Nexus 7004 supports Switched Port Analyzer (SPAN), the solution uses SPAN to send the raw traffic to the NGA for NetFlow generation in hardware. The SPAN method using NGA is the best recommendation for NetFlow in a data center environment because it minimizes design considerations around NetFlow cache size. This maintains the performance of the Nexus 7004 without losing NetFlow information.

The Nexus 7004 mirrors raw traffic information to the NGA using a SPAN port. The NGA then generates the NetFlow record and sends it to the Lancope StealthWatch FlowCollector.

SPAN provides an efficient, high-performance traffic monitoring service by duplicating network traffic to one or more monitor interfaces as it traverses the switch. In this design, the Nexus 7004 runs local SPAN, which mirrors traffic from one or more interfaces and/or VLANs on the switch to one or more other interfaces on the same switch.

With local SPAN, the system copies traffic from a SPAN source to a SPAN destination. Both the SPAN source and the SPAN destination are local to the switch where you configure the SPAN session. Therefore, the monitoring device, whether a network analyzer, an RMON probe, and so on, must be directly attached to the switch.

In local SPAN, the SPAN source is one or both of the following:

- One or more physical interfaces—These interfaces can be any type of Ethernet interface of any configuration (Layer 2 access port, trunk port, or routed interface)
- One or more VLANs—These VLANs can be pure Layer 2 switched VLANs or VLANs with a Switched Virtual Interface (SVI, that is, a VLAN interface) defined. SPAN of primary and/or secondary PVLANS is also supported.

## Configuration

Switched Port Analyzer (SPAN) on the Cisco Nexus 7000 series device monitor the traffic between Ethernet ports. The following procedure captures the validated SPAN configuration.

### Procedure

---

**Step 1** Configure the destination port for the Nexus 7000 SPAN monitor session.

Configure the destination interface.

```

N7k(config)# interface port-channel 8
N7k(config-if)# switchport monitor

```

**Step 2** Configure the monitor session on the Nexus 7000.

**a.** Configure the SPAN monitor session.

```

N7k(config-if)# monitor session 1

```



- b. Configure the source interface for the SPAN monitor session.  

```
N7k(config-if)# source interface port-channel20 rx
```
- c. Configure the destination interface for the SPAN monitor session.  

```
N7k(config-if)# destination interface port-channel8
```
- d. Enable the monitor session, by default the session is disabled.  

```
N7k(config-if)# no shut
```

## Final Configuration

```
!
interface port-channel8
  description <<*** NGA SPAN PORTS ***>>
  switchport mode trunk
  switchport monitor
!
monitor session 1
  description SPAN ASA Data Traffic from Po20
  source interface port-channel20 rx
  destination interface port-channel8
  no shut
```

## Cisco Nexus 1000V VSM

The Cisco Nexus 1000V VSM supports NetFlow in software. In this design, it does not act as an aggregation device as the Nexus 7004 does, and it does not need to generate as much NetFlow information as would the Nexus 7004. The Nexus 1000V VSM connects directly to the Lancop StealthWatch Flow Collector for NetFlow collection. Be aware of the performance impact NetFlow will have on the Nexus 1000V when determining what types of flows to generate and send to the Flow Collector.

## Design Considerations

NetFlow on the Nexus 1000v has the following configuration guidelines and limitations:

- If a source interface is not configured, the NetFlow exporter will remain disabled.
- In Cisco Nexus 1000V, the Mgmt0 interface is configured by default as the source interface for an exporter. You can change the source interface if needed.
- Cisco Nexus 1000V includes the following predefined flow records that can be used instead of configuring a new one.
  - *netflow-original*—Cisco Nexus 1000V predefined traditional IPv4 input NetFlow with origin ASs (routing related fields are ignored)
  - *netflow ipv4 original-input*—Cisco Nexus 1000V predefined traditional IPv4 input NetFlow
  - *netflow ipv4 original-output*—Cisco Nexus 1000V predefined traditional IPv4 output NetFlow
  - *netflow ipv4 protocol-port*—Cisco Nexus 1000V predefined protocol and ports aggregation scheme

- Up to 256 NetFlow interfaces are allowed per distributed virtual switch (DVS).
- Up to 32 NetFlow interfaces are allowed per host.
- A maximum of one flow monitor per interface per direction is allowed.
- Up to 8 flow monitors are allowed per virtual Ethernet module (VEM).
- Up to 2 flow exporters are permitted per monitor.
- Up to 32 NetFlow policies are allowed per DVS.
- Up to 8 NetFlow policies are allowed per host.

## Configuring NetFlow Export

### Procedure

#### Step 1 Enable the NetFlow feature.

The NetFlow feature is enabled with a simple command:

```
N1Kv(config)#feature netflow
```

#### Step 2 Configure the Flow Exporter.

The flow exporter configuration defines where flow records will be sent (the FlowCollector), including destination IP address and port.

##### a. Define the exporter.

```
N1Kv(config)#flow exporter nf-export-1
```

##### b. (Optional) Add a description.

```
N1Kv(config-flow-exporter)#description <<*** SEA Lancope Flow Collector ***>>
```

##### c. Define the source.

```
N1Kv(config-flow-exporter)#source mgmt0
```

##### d. Define the destination IP address.

```
N1Kv(config-flow-exporter)#destination ip-address-of-FlowCollector use-vrf management
```

##### e. Define the transport protocol.

```
N1Kv(config-flow-exporter)#transport udp 2055
```

##### f. Define the version to use.

```
N1Kv(config-flow-exporter)#version 9
```

##### g. Set the resend timers.

```
N1Kv(config-flow-exporter-version-9)#option exporter-stats timeout 300
N1Kv(config-flow-exporter-version-9)#option interface-table timeout 300
```

#### Step 3 Create the Flow Monitor.

The flow monitor represents the device's memory-resident NetFlow database, and links together a flow record and flow exporter configuration.

##### a. Define the flow monitor.

```
N1Kv(config)#flow monitor sea-enclaves
```

- b. (Optional) Add a description.

```
N1Kv(config-flow-monitor)#description <<*** SEA Lancope Flow Monitor ***>>
```

- c. Configure the flow record.

```
N1Kv(config-flow-monitor)#record netflow-original
```

- d. Configure the exporter.

```
N1Kv(config-flow-monitor)#exporter nf-export-1
```

- e. Define the active timeout.

The active timeout refers to how often NetFlow records are generated for flows that are still active. Cisco recommends using a value of 60 seconds.

```
N1Kv(config-flow-monitor)#timeout active 60
```

- f. Define the inactive timeout.

The inactive timeout refers to the time period in which flows that are inactive (not transmitting data) but still resident in the cache are timed-out of the cache. Cisco recommends using a value of 15 seconds.

```
N1Kv(config-flow-monitor)#timeout inactive 15
```

#### Step 4 Apply the Flow Monitor to an interface or port profile

The flow monitor should be applied to all interfaces or port profiles that need to be monitored.

- a. Enter interface configuration mode.

```
N1Kv(config)#port-profile type vethernet enc1-3001
```

- b. Apply the Flow Monitor on ingress traffic.

```
N1Kv(config-if)#ip flow monitor sea-enclaves input
```

#### Step 5 Verify.

Check the configuration using **show** commands.

```
N1Kv#show flow [exporter|monitor|interface]
```

## Final Configuration

```
!
feature netflow
!
flow exporter nf-export-1
  description <<*** SEA Lancope Flow Collector ***>>
  destination 172.26.164.240 use-vrf management
  transport udp 2055
  source mgmt0
  version 9
  option exporter-stats timeout 300
  option interface-table timeout 300
!
flow monitor sea-enclaves
  record netflow-original
  exporter nf-export-1
```

```

timeout active 60
timeout inactive 15
!
!
!
port-profile type vethernet enc1-3001
ip flow monitor sea-enclaves input
!

```

For additional information, see the following URL:

[http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus1000/sw/4\\_0/system\\_management/configuration/guide/n1000v\\_sys\\_manage/system\\_9flow.html#wp1240270](http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus1000/sw/4_0/system_management/configuration/guide/n1000v_sys_manage/system_9flow.html#wp1240270).

## Cisco Identity Services Engine

The Cisco Cyber Threat Defense for the Data Center Solution is designed to operate cohesively with the Cisco TrustSec Solution, meaning that both solutions can be deployed simultaneously, and together offer administrators enhanced visibility and control over their network.

Cisco Identity Services Engine (ISE), an integral part of the Cisco TrustSec solution, provides visibility and control into who and what are connected to the network. Integration between the Lancope StealthWatch Management Console (SMC) and the Cisco ISE allows the administrator to quickly associate a user and device identity with a flow or set of flows from within the SMC console.

Figure 6 illustrates this enhanced capability where the username, device type, and all other session information is available alongside all associated flows with an IP address.

**Figure 6** *StealthWatch Management Console*

The screenshot shows the StealthWatch Management Console interface. On the left, the 'Identity Services' option is highlighted in the navigation tree. The main window displays the 'Identity and Device Table' with 737 records. The table has the following columns: End Active Time, User Name, Host, Host Groups, MAC Address, and Device Type. The data rows show sessions for users 'student45', 'student44', 'student42', and 'student43'.

End Active Time	User Name	Host	Host Groups	MAC Address	Device Type
Current	student45	student45.cyber.local (172.30.1.145)	Students, Atlanta	00:24:00:15:79:13 (Dell Inc.)	Windows7-Workstation
Current	student44	student44.cyber.local (172.30.1.144)	Students, Atlanta	00:19:b9:30:24:44 (Dell Inc.)	Windows7-Workstation
Current	student42	student42.cyber.local (172.30.1.142)	Students, Atlanta	5c:26:0e:14:d9:0f (Dell Inc.)	Windows7-Workstation
Current	student43	student43.cyber.local (172.30.1.143)	Students, Atlanta	d4:be:d9:1c:e6:0c (Dell Inc.)	Windows7-Workstation

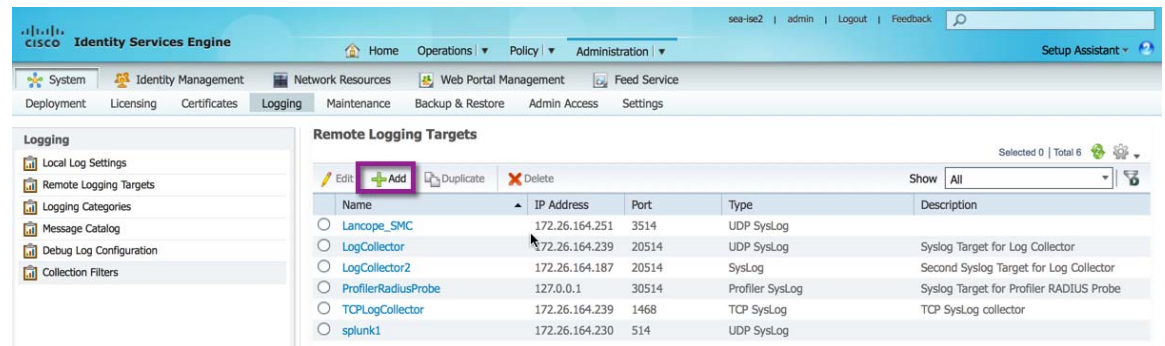
## Configuration

The Lancope StealthWatch Management Console (SMC) version 6.4 accepts and parses syslog messages from any ISE node to collect identity information. The Lancope SMC must be configured as a remote logging target on the ISE monitoring node with the RADIUS Accounting, Profiler, and Administrative and Operational Audit Logging categories set to log to the SMC target. The following steps describe how to configure the SMC and ISE integration.

## Procedure

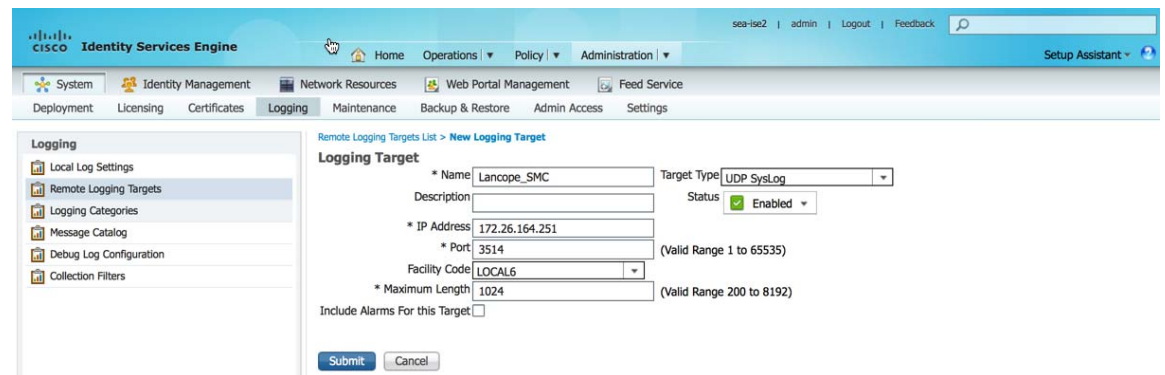
- Step 1** Configure ISE to send syslog to the SMC.
- Log in to the Cisco ISE dashboard.
  - Go to **Administration > Logging**.
  - Click **Remote Logging Targets > Add**. (See [Figure 7](#).)

**Figure 7** Remote Logging Targets



- Enter a name and optional description for the logging target, the IP address of the SMC, and the UDP port number to use as the destination of the syslog messages. (See [Figure 8](#).)

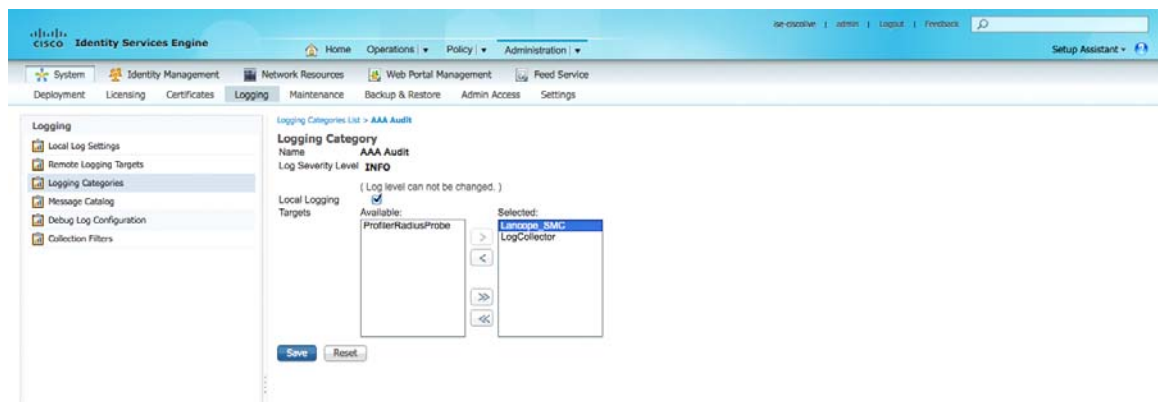
**Figure 8** Logging Target



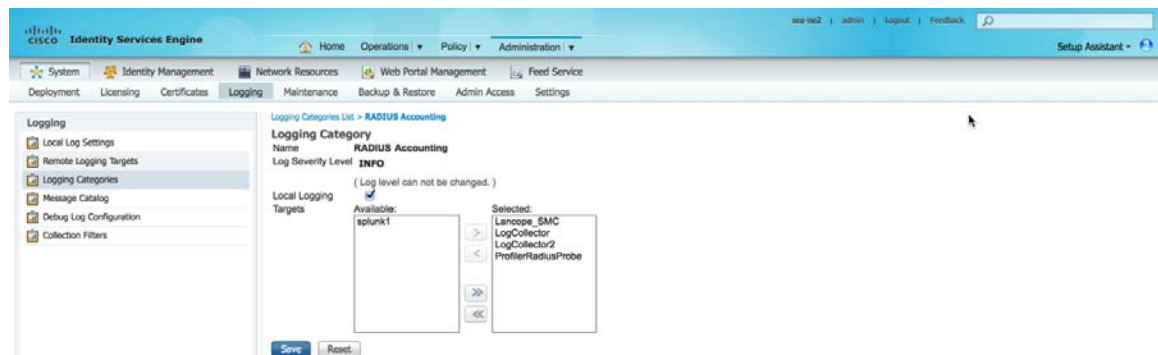
### Note

The SMC defaults to listening on port 3514. Cisco recommends using this port. If you choose to configure ISE with a different destination port, you will need to change the configuration of the SMC as well. Do not use port 514 or port 8514, because those are reserved for other services on the SMC.

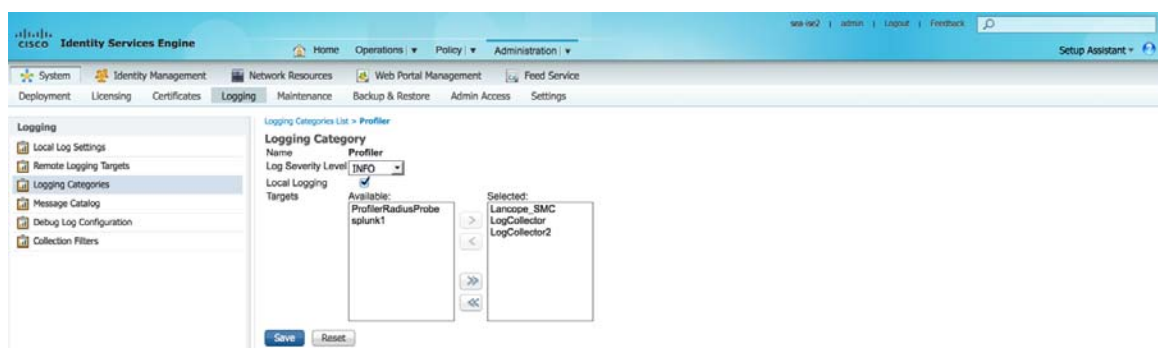
- Click **Submit**.
- Click **Logging Categories** and then **Accounting > AAA Audit**. Select the name of the SMC syslog target from the previous step, then click the top right arrow to move the target from the **Available** box to the **Selected** box and click **Save**. (See [Figure 9](#).)

**Figure 9** *Logging Category (1)*

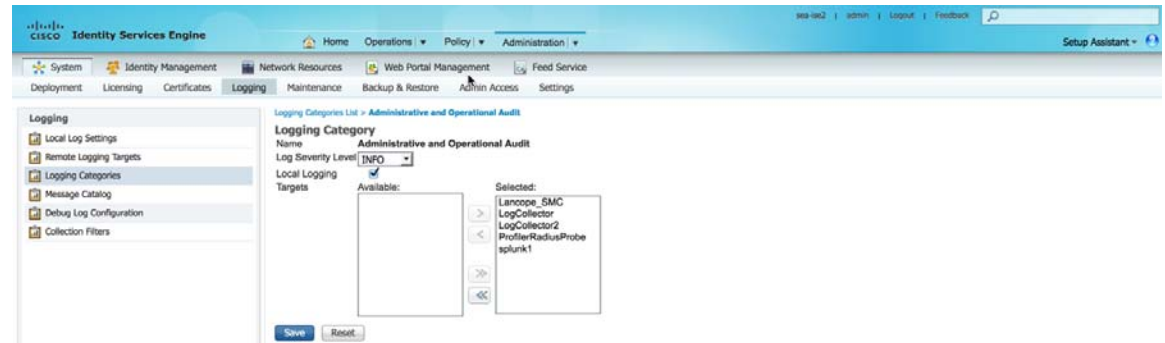
- g. Click **Logging Categories** and then **Accounting > RADIUS Accounting**. Select the name of the SMC syslog target from the previous step, then click the top right arrow to move the target from the **Available** box to the **Selected** box and click **Save**. (See [Figure 10](#).)

**Figure 10** *Logging Category (2)*

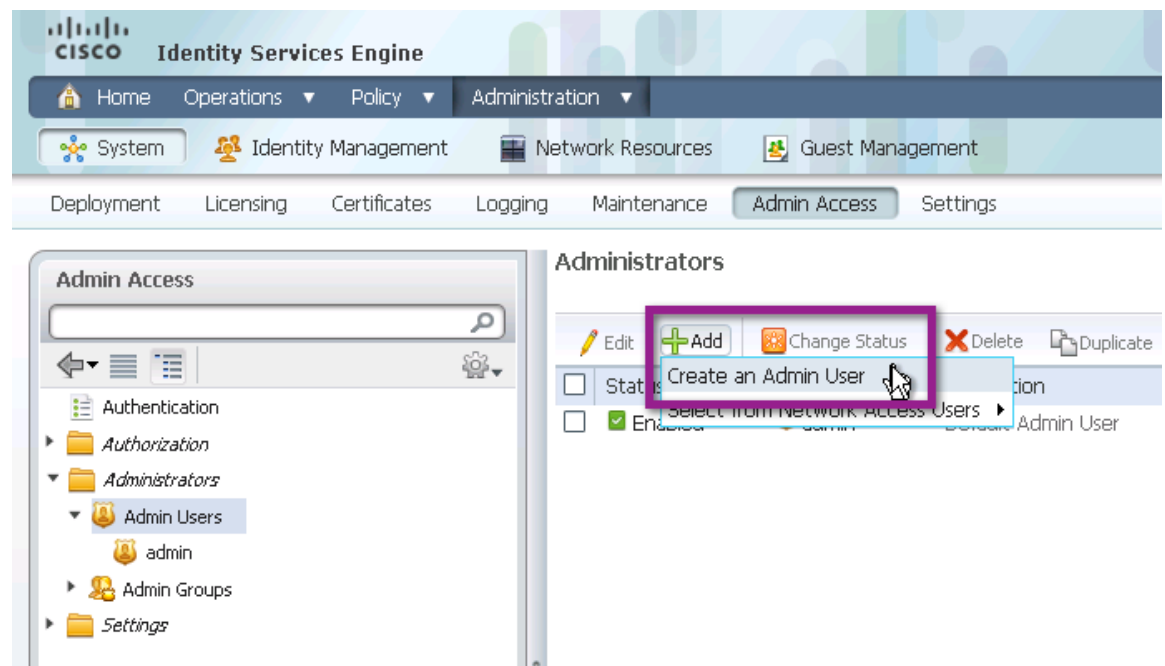
- h. Click **Logging Categories** again and then **Profiler**. Select the SMC syslog target and move it from **Available** to **Selected**. (See [Figure 11](#).)

**Figure 11** *Logging Category (3)*

- i. Finally, click **Logging Categories** and then **Administrative and Operational Audit**, and move the SMC syslog target from **Available** to **Selected** for this category as well. (See [Figure 12](#).)

**Figure 12**      **Logging Category (4)**

- Step 2** Create an admin user on the ISE for monitoring access.
- Log in to the ISE dashboard.
  - Go to **Administration > System > Admin Access > Administrators**.
  - Select **Admin Users**. Click **Add** and select **Create an Admin User**. (See [Figure 13](#).)

**Figure 13**      **Administrators**

- Fill out the Admin User, Password, User Information, Account Options, and Admin Groups sections using the information in [Table 3](#).

**Table 3**      **ISE Fields**

Configuration Item	Settings
Admin User	Give the Admin user a name that is easy to distinguish. Ensure that the account status is set to <b>Enabled</b> .
Password	Create a password for the user.

**Table 3 ISE Fields**

User Information	Optional: Add information to describe the user.
Account Options	Optional: Add a meaningful description; for example: <i>Account used by the StealthWatch Management Console to access ISE Session information for the Cisco Cyber Threat Defense Solution</i>
Admin Groups	Put the user in the pre-defined <b>Helpdesk Admin</b> group.

e. Click **Submit**.

**Step 3** Configure the Certificate Authority certificates.

The SMC must be configured to trust the certificate authority that issued the Cisco ISE's Identity Certificate. If best practices were followed in the deployment of the StealthWatch System, this procedure is already complete. If not, the Certificate Authority's certificate needs to be obtained and installed on the SMC.

- a. Log into the SMC (administration) web interface.
- b. From the home page, click **Configuration Certificate Authority Certificates**.
- c. Click **Choose File** and then browse the local disk to locate the CA certificate.
- d. Give the certificate a name to identify it in the SMC configuration.
- e. Click **Add Certificate**.

**Step 4** Register the Cisco ISE with the Lancope SMC.

At this point in the deployment, it has been verified that there are active authentication sessions in the Cisco ISE, and that they can be retrieved by an external entity using a configured username and password.

- a. Log in to the SMC client software.
- b. Highlight the domain, then click **Configuration > Add Cisco ISE ...**
- c. Enter a name for the ISE deployment. Configure the collection port to which ISE will be sending syslog messages (this cannot be UDP 514). Enter the ISE username and credentials that were previously configured and click **Add**. (See [Figure 14](#).)



**Figure 14 Add Cisco ISE**

Enter the name and configuration details for your Cisco ISE cluster below and click Add to configure each node in the cluster.

To collect data from these devices, you must enable RADIUS Accounting, Profiler, and Administrative and Operational Audit logging categories on all of the ISE devices in the cluster. For more information, click [here](#).

Name:

Collection Port:

User Name:

Password:

Cisco ISE Deployment Nodes

- d. In the Dialog box, enter the configuration details for the primary ISE MnT node. Click **OK**. (See [Figure 15](#).)

**Figure 15 Add Cisco ISE Deployment Node**

Enter the name and configuration details for your Cisco ISE cluster below and click Add to configure each node in the cluster.

To collect data from these devices, you must enable RADIUS Accounting, Profiler, and Administrative and Operational Audit logging categories on all of the ISE devices in the cluster. For more information, click [here](#).

Name:

IP Address:

- e. (Optional) Click **Add** to add additional ISE Nodes to the deployment.
- f. Click **OK**.

# Design Considerations for the Lancop StealthWatch System

The Lancop StealthWatch System, available from Cisco, is the leading solution for flow-based security monitoring available on the market today, and serves as the NetFlow analyzer and management system in the Cisco Cyber Threat Defense for the Data Center Solution. [Table 4](#) briefly introduces and describes each component used in this solution.

**Table 4** *Lancop StealthWatch System Components*

Component	Description
StealthWatch Management Console	Manages, coordinates, and configures all StealthWatch appliances to correlate security and network intelligence across the enterprise. Retrieves authenticated session information from the Cisco ISE to correlate flow and identity.
StealthWatch FlowCollector	Serves as a central collector for flow data generated by NetFlow-enabled devices. The StealthWatch FlowCollector monitors, categorizes, and analyzes network traffic to create comprehensive security intelligence at both the network and host level.

## Design Considerations for StealthWatch FlowCollector

The StealthWatch FlowCollector serves as a central collection and analysis point for NetFlow data generated by all NetFlow generators in the Cisco Cyber Threat Defense for the Data Center Solution. The choice of what number(s) and model(s) of StealthWatch FlowCollectors are needed in the solution deployment depends on the following factors:

- Decisions made in the previous sections influencing the volume of flows per second that will be reaching the StealthWatch FlowCollector
- The StealthWatch FlowCollector deployment strategy
- The physical capacity of each StealthWatch FlowCollector

StealthWatch FlowCollectors can be deployed in a distributed or centralized manner. In a distributed deployment, FlowCollectors are deployed at multiple sites and are usually placed close to the source producing the highest number of NetFlow records. This deployment has the advantage of limiting the overhead introduced by NetFlow. In a centralized deployment, all StealthWatch FlowCollectors are placed in a single data center (possibly behind a load balancer), providing the benefit of a single collection location and possibly a single IP address globally for NetFlow collection. This deployment offers advantages in environments where NetFlow generators are far apart.

In general, a single FlowCollector should be used for as much related traffic as possible. The benefits of centralized collection diminish when the traffic is not similar.

When a particular FlowCollector receives flow data, it de-duplicates any duplicate flow records it receives, meaning that a single database entry is created for that flow. This de-duplication process ensures that the FlowCollector stores the flow data in the most efficient way while preserving details about each flow exporter and eliminating the reporting of inflated traffic volumes.

In an ideal implementation, every router that exports data related to a particular flow sends that data to the same FlowCollector. However, each unique host pair (or conversation) consumes additional resources on the FlowCollector. If the number of simultaneous connections gets too high, flow records

are purged from memory. Take care during deployment planning to ensure that each FlowCollector has sufficient resources to keep state on all active conversations without purging records until after the conversations have been idle for some time.

**Tip**

All NetFlow records belonging to a flow should be sent to the same StealthWatch FlowCollector.

Each StealthWatch FlowCollector can support a minimum guaranteed flow volume, as illustrated in [Table 5](#). However, also consider the following factors in the selection of a StealthWatch FlowCollector for the Cisco Cyber Threat Defense for the Data Center Solution:

- Exporter count—The number of NetFlow generation devices that each StealthWatch FlowCollector can accept.
- Data rate—The rate of fps that the StealthWatch FlowCollector is receiving.
- Host count—The number of hosts (both inside and outside the network) for which the StealthWatch FlowCollector can maintain state. Cisco recommends that the number of inside hosts not exceed 60 percent of the host count value.
- Flow storage—The amount of granular flow data required for a particular location on the network.

**Note**

A system that approaches both the maximum number of exporters and the maximum data rate for a particular chassis may suffer from performance problems. For example, an estimated 10–20 percent reduction in the maximum data rate may occur at the maximum number of exporters.

**Table 5** *StealthWatch FlowCollector Appliance Specifications*

Model	Flows per Second	Exporters	Hosts	Storage
StealthWatch FlowCollector 1000	Up to 30,000	Up to 500	Up to 250,000	1.0 TB
StealthWatch FlowCollector 2000	Up to 60,000	Up to 1000	Up to 500,000	2.0 TB
StealthWatch FlowCollector 4000	Up to 120,000	Up to 2000	Up to 1,000,000	4.0 TB

[Table 6](#) lists the support for a StealthWatch FlowCollector VE based on the amount of reserved memory and the number of CPUs for the VM.

**Table 6** *StealthWatch FlowCollector VE Specifications*

Flows per second	Exporters	Hosts	Reserved Memory	Reserved CPUs
Up to 4500	Up to 250	Up to 125,000	4GB	2
Up to 15,000	Up to 500	Up to 250,000	8 GB	3
Up to 22,500	Up to 1000	Up to 500,000	16 GB	4
Up to 30,000	Up to 1000	Up to 500,000	32 GB	5

## Design Considerations for StealthWatch Management Console

The StealthWatch Management Console (SMC) manages the entire StealthWatch System installation and is licensed by the number of FlowCollectors that are connected to it and the total volume of flows monitored across the entire system.

Table 7 shows the SMC models and the number of StealthWatch FlowCollectors they can support.

**Table 7 SMC Appliance Specifications**

SMC Model	Maximum FlowCollectors	Size	Storage	Memory
SMC 1000	5	1 RU	1.0 TB	8 GB
SMC 2000	25	2 RU	2.0 TB	16 GB

Table 8 lists the number of FlowCollectors and concurrent users (based on reserved memory and CPUs) that the SMC VE can support.

**Table 8 SMC VE Specifications**

FlowCollectors	Concurrent Users	Reserved Memory	Reserved CPUs
1	2	4 GB	2
3	5	8 GB	3
5	10	16 GB	4



### Note

If a high number of host groups and monitored interfaces is expected in the deployment, a higher-performance SMC should be considered, because the amount of data being sent to the SMC can increase in these deployments.

## Concluding Remarks

This guide describes the design topology and provides design guidance for the Cisco Cyber Threat Defense for the Data Center Solution. This solution aids in advanced threat detection in the data center and accelerating response to the threats. Consult other guides in the Cisco Cyber Threat Defense Guide Series on how to best leverage this solution for Cyber Threat Defense outside the data center. Consult the Secure Enclaves Architecture Design Guide for more information for data center architecture designs.

# References

- Cisco Cyber Threat Defense Solution—<http://www.cisco.com/go/threatdefense>
- Secure Data Center for the Enterprise Solution—<http://www.cisco.com/go/securedatacenter>
- Lancope NetFlow Bandwidth Calculator—  
<http://www.lancope.com/resource-center/netflow-bandwidth-calculator-stealthwatch-calculator/>
- Cisco Cyber Threat Defense Solution 1.1 Cisco Validated Design—  
[http://www.cisco.com/en/US/solutions/collateral/ns1015/ns1238/cyber\\_threat\\_defense\\_design\\_guide.pdf](http://www.cisco.com/en/US/solutions/collateral/ns1015/ns1238/cyber_threat_defense_design_guide.pdf)
- Gaining Visibility and Context Through NetFlow Security Event Logging—  
[http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/threat-defense/guide\\_c07-728135.pdf](http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/threat-defense/guide_c07-728135.pdf)
- Gaining Visibility in the Data Center with the Cisco NetFlow Generation Appliance—  
[http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/threat-defense/guide\\_c07-728136.pdf](http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/threat-defense/guide_c07-728136.pdf)
- Cisco TrustSec Solution 2.0 Design and Implementation Guide—  
[http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec\\_2.0/trustsec\\_2.0\\_dig.pdf](http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_2.0/trustsec_2.0_dig.pdf)

## About the Cisco Validated Design Program

The CVD program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information, visit <http://www.cisco.com/go/designzone>.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, “DESIGNS”) IN THIS MANUAL ARE PRESENTED “AS IS,” WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California. Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco’s trademarks can be found at <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. (1005R) Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.