Cisco Cyber Threat Defense Solution 1.0: Design and Implementation Guide

Current Document Version: 1.0

April 9, 2012

Table of Contents

Introduction

The threat landscape has evolved; government organizations and large enterprises are being inundated with targeted, custom attacks referred to by the media as advanced persistent threats (APTs). These APTs are often in the form of motivated and possibly well-financed attackers who are able to bypass the perimeter defenses of an organization to gain an operational footprint on the network. Given the ability of these threats to bypass perimeter defences, many government organizations and large enterprises, in order to protect their operational objectives, are turning to tools that can help to identify and study these advanced threats that are operating on their networks.

The Cisco® Cyber Threat Defense Solution 1.0 provides a proactive capability in detecting threats already operating on an internal network. The solution uses network intelligence to provide deep and pervasive visibility across an entire network, allowing the security operator to understand the "who, what, when, where, why, and how" of network traffic and discover anomalies. This approach gives the operator much more visibility into the nature of suspicious flows in the access and distribution layers, where traditional network security platforms are usually not present. The level of visibility and context provided by the Cisco Cyber Threat Defense Solution 1.0 can greatly reduce the window of vulnerability and put control back into the hands of the security operator.

Deploying the Cisco Cyber Threat Defense Solution 1.0 across the entire network can provide the information and necessary visibility to support the security operator in a wide spectrum of security tasks that include (but are not limited to):

1. Detecting the occurrence of a data loss event

2. Detecting network reconnaissance activity on the internal network

3. Detecting and monitoring the spread of malware throughout the internal network

4. Detecting botnet command and control channels on the internal network

The Cisco Cyber Threat Defense Solution 1.0 leverages Cisco networking technology, including NetFlow, Network-Based Application Recognition (NBAR), as well as identity, device profiling, posture, and user policy services from the Cisco Identity Services Engine (ISE).

Cisco has partnered with Lancope to jointly develop and offer the Cisco Cyber Threat Defense Solution 1.0. Available from Cisco, the Lancope® StealthWatch® System 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 Solution 1.0.

This guide describes the deployment and implementation detail of the Cisco Cyber Threat Defense Solution 1.0. The objective of this guide is to highlight any design and deployment considerations and then walk the reader through the implementation of an operational deployment of the solution.

Products and Releases

The Cisco Cyber Threat Defense Solution 1.0 is a tested system that has been demonstrated to achieve all stated objectives using the components in the following table.

Cisco Cyber Threat Defense Solution 1.0 Components

Component	Hardware	Release	Image Type and License
Cisco Catalyst® 3560-X or 3750-X Series	Version ID: 02 Revision 0x03 10 GE Service Module	Cisco IOS® Software Release 15.0(1)SE	Universal and IP Services
Cisco Catalyst 4500E Series	Supervisor 7E	Cisco IOS-XE Software Release 3.02.01.SG	Universal and IP Base
	Supervisor 7L-E	Cisco IOS-XE Software Release 3.02.00.XO	Universal and IP Base
Cisco Catalyst 6500 Series	Supervisor 2T	Cisco IOS Software Release 12.2(50)SY	Advanced Enterprise Services
Cisco ISR G2	Any	Cisco IOS Software Release 15.1(2)T3	Universal and IP Base
Cisco Adaptive Security Appliance	Any	Cisco ASA Software Release 8.4.3	Any
Cisco Identity Services Engine	Any	Cisco Identity Services Engine 1.1	Any
Lancope StealthWatch Management Console	Any	StealthWatch 6.2	Any

Component	Hardware	Release	Image Type and License
Lancope StealthWatch FlowCollector	Any	StealthWatch 6.2	Any
Lancope StealthWatch FlowSensor	Any	StealthWatch 6.2	Any
Lancope StealthWatch FlowReplicator	Any	StealthWatch 5.6.1	Any

Note: Currently only the WS-X6908-10G-2T/2TXL, WS-X6816-10T-2T/2TXL, WS-X6716-10G with DFC4/DFC4XL, and WS-X6716-10T with DFC4/DFC4XL line cards can perform NetFlow record export in a Supervisor Engine 2T-based system. All future Cisco Catalyst 6500 Series modules will support this ability.

Note: On Catalyst 3560-X/3750-X Series Switches, NetFlow services are only supported on the Service Module's two 10 Gigabit Ethernet ports. As of the current release, these ports support only 10 Gigabit Ethernet cabling or Fibre-Channel SFPs.

Best Practice: It may not be possible to build an entire network consisting solely of the listed Cisco network devices. In these situations, in order to implement the pervasive visibility required by the solution, it may be necessary to use the Lancope SteathWatch FlowSensor to gain visibility into the network.

Solution Overview

Architecture

The Cisco Cyber Threat Defense Solution 1.0 provides comprehensive visibility into all network traffic through the use of Cisco NetFlow technology. Cisco NetFlow technology is supported across Cisco enterprise switches and routers to enable complete non-performance impacting telemetry to be implemented at all layers of the network. Coupling this enhanced visibility with identity and context information from the Cisco TrustSec® solution enables security operators to better understand a network's traffic. The figure below illustrates the high-level system architecture of the Cisco Cyber Threat Defense Solution 1.0.

Cisco Cyber Threat Defense Solution 1.0 Architecture
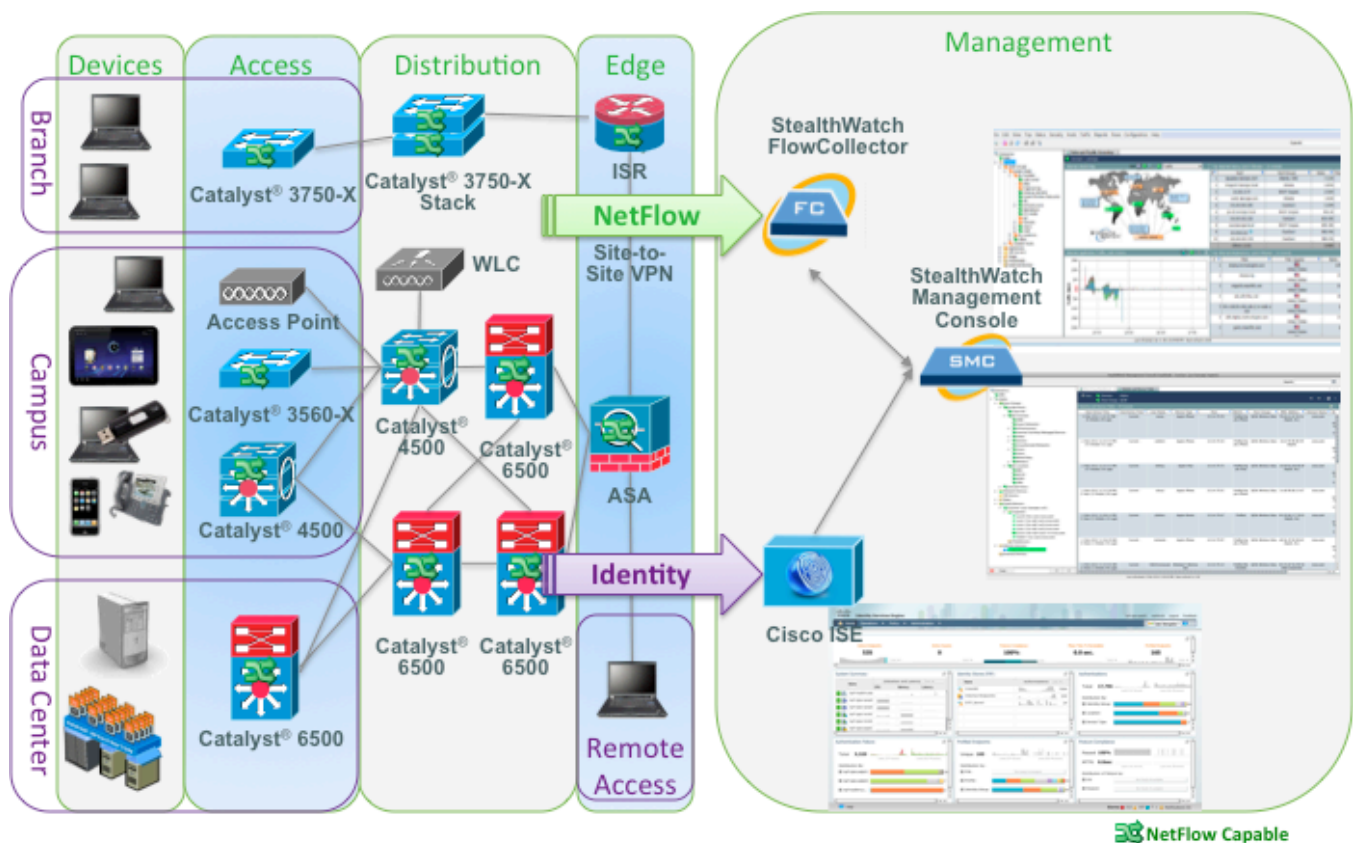
Visibility into network traffic is provided through NetFlow export from Cisco routers and switches while identity services, including the user name and profile information is provided through the

Cisco TrustSec Solution. 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.

Cisco Cyber Threat Defense Solution 1.0 components include network devices to authenticate users and generate NetFlow data, components from the Lancope StealthWatch System, and components from Cisco TrustSec. The minimum system requirement to gain flow 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 Identity Services Engine and one or more authenticating access devices in a valid Cisco TrustSec Monitoring Mode deployment.

Introduction to NetFlow

NetFlow is a Cisco application that measures IP network traffic attributes of a traffic flow (a flow is identified as a unidirectional stream of packets between a given source and destination) as it traverses the Cisco device. NetFlow was initially created to measure network traffic characteristics such as bandwidth, application performance, and utilization. NetFlow 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 will gather information about the traffic flow and report 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.

NetFlow has gone through many versions since it was first introduced, as can be seen in the following table. Fixed export format versions (1,5,7,8) are not flexible or adaptable, and each new version contains new export fields that are incompatible with the previous version. NetFlow Version 9 completely separates the collection and export process and allows the customization of the NetFlow collection.

NetFlow Versions

Version	Status
1	Original; similar to v5 but without sequence numbers or BGP info
2	Never released
3	Never released

Version	Status
4	Never released
5	Fixed format; most common version in production
6	Never released
7	Similar to v5 but does not include AS interface, TCP flag and ToS information; specific to Catalyst 6500 and 7600
8	Choice of 11 aggregation schemes; never gained wide use in the enterprise
9	Flexible, extensible export format to enable support of additional fields and technologies
IPFIX	Similar to v9 but standardized and with variable length fields

The Cisco Cyber Threat Defense Solution 1.0 takes advantage of the customization capability of Flexible NetFlow Feature in Cisco IOS allowing for customizable NetFlow v9 Records. Using this approach the Cisco Cyber Threat Defense Solution 1.0 has defined NetFlow Records for each solution device to maximize the security monitoring potential of each device by collecting packet fields such as TCP flags, Time To Live (TTL) values, protocol, and application name using NBAR. Many of these fields are not available in previous versions of the NetFlow protocol; and without them present, the advantages offered by some of the finely tuned detection algorithms present in the Cisco Cyber Threat Defense Solution 1.0 would be lost.

Best Practice: Use the Cisco IOS Flexible NetFlow Feature wherever possible.

The following figure illustrates NetFlow operation on a Cisco device. As a flow traverses a Cisco device (NetFlow Generator) the NetFlow key fields are extracted (1). The key fields are used to identify the flow in the NetFlow cache (2), which is the database of flows maintained on the device. In addition to the Key Fields the Cisco device will collect additional configured collection fields, such as TCP flags, byte counters, and start and end times, and will store this information in the NetFlow cache entry for this flow. 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 Flow Collector (3).

Design Considerations

At a high level, the Cisco Cyber Threat Defense Solution 1.0 is an integration between the Cisco TrustSec 2.0 system and the Lancope StealthWatch 6.2 system and extensively leverages the increased NetFlow capabilities in Cisco's latest switches and routers. The deployment of the Cisco Cyber Threat Defense Solution 1.0 involves the following steps:

1. Select the monitoring locations

2. Determine the flows-per-second volume for the monitoring locations

3. Deploy the Cisco TrustSec solution (not covered in this guide)

4. Deploy the Lancope StealthWatch System

5. Integrate flow and identity services

Selecting the Monitoring Locations

The Cisco Cyber Threat Defense Solution 1.0 is most effective when NetFlow is enabled on network devices at all layers of the network. With this level of visibility, it is possible to record and

analyze all network traffic and identify threats such as malware that is spreading laterally through the internal network (i.e., the malware spreads to other hosts without leaving the VLAN and crossing a Layer 3 boundary). Visibility across the entire network and as close to the source of the traffic increases the accuracy of the behavioral algorithms and ensures no network communication is missed.

Best Practice: Enable NetFlow as close to the access layer as possible.

A Cisco Cyber Threat Defense Solution 1.0 implementation should implement NetFlow in a complete (non-sampled) manner. Sampled NetFlow will leave *blind spots*, as only a certain percentage of network flows will have associated network records. This makes it difficult to detect the single traffic anomalies that indicate malicious activity.

Some older Cisco devices, as well as the Integrated Services Routers and Adaptive Security Appliances, support NetFlow services using a software implementation of the feature set. Care should be taken when deploying software-supported NetFlow services as this can impact device performance; for instance, a fully loaded ISR running Cisco IOS Software can experience an approximate 15% CPU uptick resulting from NetFlow enablement. The Cisco NetFlow Performance Analysis white paper should be consulted when implementing software-supported NetFlow services.

Note: NetFlow Performance Analysis
http://www.cisco.com/en/US/technologies/tk543/tk812/technologies_white_paper0900aecd802a0eb9.html

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 that the hardware supports. The following table illustrates the cache size limitations of the solution devices with hardware-supported NetFlow. Once the NetFlow cache on a device is full the device will not generate NetFlow Records for new flows transiting the device.

NetFlow cache size limitations on Cisco devices

Component	Hardware	Cache Size (Flows)
Catalyst 3500-X	10 GE Service Module	32,000
Catalyst 4500E Series	Supervisor 7E	128,000
	Supervisor 7L-E	128,000
Catalyst 6500 Series	Supervisor 2T	512,000

Component	Hardware	Cache Size (Flows)
	Supervisor 2TXL	1 million

Note: NetFlow cache size on devices (such as the ISR) with software-supported NetFlow is limited by the amount of available memory.

While every NetFlow generation device in the Cisco Cyber Threat Defense Solution 1.0 supports the Flexible NetFlow Feature, customizable flow record support differs across platforms. This means that no universal flow record can capture all necessary security information and apply it to every device in the solution. The following table lists flow record support across solution devices. Given the disparity in support, best results will be obtained if there is a heterogeneous mix of solution components in the deployment to fill visibility gaps.

Ideal Solution Flow Record	Catalyst 3560-X/ 3750-X	Catalyst 4500 Sup7-E/ Sup7L-E	Catalyst 6500 Sup2T	ISR
match ipv4 tos	Yes	Yes	Yes	Yes
match ipv4 protocol	Yes	Yes	Yes	Yes
match ipv4 source address	Yes	Yes	Yes	Yes
match ipv4 destination address	Yes	Yes	Yes	Yes
match ipv4 destination address	Yes	Yes	Yes	Yes
match transport destination-port	Yes	Yes	Yes	Yes
match interface input	Yes	Yes	Yes	Yes
match datalink mac source-address	Yes	No	No	No
match datalink mac destination-address	Yes	No	No	No
collect routing next-hop address ipv4	No	No	No	Yes
collect ipv4 dscp	No	Yes	No	Yes
collect ipv4 ttl minimum	match ipv4 ttl	Yes	No	Yes
collect ipv4 ttl maximum	match ipv4 ttl	Yes	No	Yes

Ideal Solution Flow Record	Catalyst 3560-X/ 3750-X	Catalyst 4500 Sup7-E/ Sup7L-E	Catalyst 6500 Sup2T	ISR
collect transport tcp flags	No	Yes	Yes	Yes
collect interface output	Yes	Yes	Yes	Yes
collect counter bytes	Yes	Yes	Yes	Yes
collect counter packets	Yes	Yes	Yes	Yes
collect timestamp sys-uptime first	Yes	Yes	Yes	Yes
collect timestamp sys-uptime last	Yes	Yes	Yes	Yes
collect application name	No	No	No	Yes

Best Practice: Although not every Cisco network device needs to be present in the deployment for the solution to function, it is recommended that a heterogeneous mix of the listed devices be deployed due to the differences in NetFlow support across each platform. (This is discussed later.)

Once the monitoring location and the NetFlow generation device are selected, NetFlow will need to be enabled on that device. Refer to the device-specific NetFlow configuration section in this guide for more information.

Determining Flows-per-Second Volume

After identifying the monitoring locations, the next step is to determine and measure the flows per second (fps) volume that will be generated by the monitoring locations. The number (volume) of fps indicates how many records the StealthWatch FlowCollectors will need to be able to receive and analyze; this number will need to 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 Solution 1.0 requires careful thought. Many factors can have impact the volume of flows generated by the network devices, so predicting the exact number can be difficult. In general, a NetFlow generator will generate between 1,000 and 5,000 fps per 1 Gbps of traffic passing through it; however, this is a general guideline and should be used only as a starting point.

It should be noted that traffic throughput (Gbps) has no direct bearing on the fps number - the only measure that has 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 a 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 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)

While generally not a significant concern, some consideration should also be given to the impact that NetFlow records will have on network traffic. NetFlow generally adds very little traffic to the network, as a NetFlow record represents the reporting for an entire traffic flow, However, certain traffic sets can generate more NetFlow records than other sets. Here are some of the factors that can influence the network overhead introduced by NetFlow:

- Flows per second.

- NetFlow record size. The Cyber Threat Defense Solution 1.0 recommends NetFlow v9, which results in an average of 34 flow records per 1500-byte packet.

- Flow timers (active and inactive timeouts for a flow). The Cyber Threat Defense Solution 1.0 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.

Note: Lancope NetFlow Bandwidth Calculator: http://www.lancope.com/resource-center/netflow-bandwidth-calculator-stealthwatch-calculator/

Best Practice: If minimizing NetFlow overhead is a concern, NetFlow collection should be done as close to the NetFlow generator as possible.
Best Practice: In an asymmetric routing situation, all devices in the asymmetric route should send NetFlow records to the same FlowCollector.

Once the monitoring locations have been determined and design considerations have been made, the next step in the deployment of the Cisco Cyber Threat Defense Solution 1.0 is to select and deploy the Lancope StealthWatch System components.

Deploying the Lancope StealthWatch System

The Lancope 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 Solution 1.0. The following table briefly introduces and describes each component in the Lancope StealthWatch System.

Lancope 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 Identity Services Engine 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.
StealthWatch FlowReplicator	Aggregates NetFlow, syslog, and SNMP information in a single, high-speed appliance. This high-speed UDP packet replicator gathers essential network optimization and security information from multiple locations in the FlowReplicator, and then forwards this information in a single data stream to one or more StealthWatch FlowCollector appliances.
StealthWatch FlowSensor	Passively monitors all host and server communications and network traffic statistics, translating them into flow records, which are sent to FlowCollectors.
StealthWatch FlowSensor VE	A virtual appliance designed to run inside a virtual server. The FlowSensor VE passively monitors intra-VM traffic, translating it into flow records, which are sent to FlowCollectors.

Design Considerations

(Optional) Adding StealthWatch FlowSensors

Where NetFlow generation is not possible from the network equipment, the Lancope StealthWatch FlowSensor and FlowSensor VE can be used to translate the communications into flow records. This enables networking equipment not specified in this guide to participate in deployments of the Cisco Cyber Threat Defense Solution 1.0. Additionally, the StealthWatch FlowSensor can be used to add packet-level application identification and performance metrics for key areas of the network. The following steps should be performed when considering adding a StealthWatch FlowSensor to a Cisco Cyber Threat Defense Solution 1.0deployment.

Step 1 Choose a StealthWatch FlowSensor.

When choosing a StealthWatch FlowSensor, consideration must be made regarding the expected traffic profile of the monitoring point as the FlowSensor must be able to process the level of traffic being sent to it. As with any other NetFlow generation device in the Cisco Cyber Threat Defense Solution 1.0, it is recommended that the FlowSensor be deployed as close to the access layer as possible.

The following table lists the StealthWatch FlowSensor appliance models and their specifications. The processing capacity shown is the sustained rate supported. The FlowSensor can handle short bursts beyond the listed capacity. Like all NetFlow generators, the volume of NetFlow traffic generated by the StealthWatch FlowSensor varies based on the monitored traffic profile.

StealthWatch FlowSensor Appliance Specifications

Model	Processing Capacity	Interface	Speed	Physical Layer	Form Factor	Power
250	100 Mbps	2	10/100/100	Copper	1 RU-short	Non-redundant
1000	1 Gbps	3	10/100/1000	Copper	1 RU-short	Non-redundant
2000	60,000	5	10/100/1000	Copper or Fibre	1 RU	Redundant
3000	120,000	1 or 2	1GB	Fibre	1 RU	Redundant

Note: If the processing capacity of a single StealthWatch FlowSensor is reached, you can stack multiple FlowSensors using an appropriate Ethernet load balancer.

The StealthWatch FlowSensor VE is a virtual appliance that can be installed inside a vSphere/ESX host and used to generate NetFlow records for traffic between VMs in that host. The FlowSensor VE connects promiscuously to the virtual switches. It passively captures Ethernet frames from the traffic it observes and then creates flow records containing valuable session statistics that pertain to conversational pairs, bit rates, and packet rates. The FlowSensor VE then sends these records to the StealthWatch FlowCollector. The following table describes the requirements for the deployment of the StealthWatch FlowCollector VE.

StealthWatch FlowSensor VE Specifications

Disk Space Requirement	Flow Export Format	Minimum CPU Requirements	Minimum Memory Requirement	Interfaces
1.4 GB	NetFlow v9	2 GHz Processor	512 MB 1024 MB for application inspection	Up to 16 vnics

Step 2 Integrate the StealthWatch FlowSensor into the network.

The StealthWatch FlowSensor must be placed in a Layer 1 or Layer 2 adjacent manner to the monitoring point. Example deployment modes include using Test Access Ports (TAPs), Switch Port Analyzer ports (SPAN ports), or a network hub. Refer to the *System Hardware Installation Guide* on the Lancope StealthWatch Documentation CD for detailed information on how to integrate the StealthWatch FlowSensor into the network.

Procedure 2 Choosing a 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 Solution 1.0. 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

Step 1 Determine the StealthWatch FlowCollector deployment strategy.

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), giving 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.

There may be limitations in bandwidth between sites to consider as well (such as over a WAN). 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 will de-duplicate any duplicate flow records it receives, meaning that a single database entry will be 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 would send 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.

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

Step 2 Performance considerations.

Each StealthWatch FlowCollector can support a minimum guaranteed flow volume as illustrated in the table at the end of this step. However, the following factors should also be considered in the selection of a StealthWatch FlowCollector for the Cisco Cyber Threat Defense Solution 1.0.

- 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. It is recommended that the number of inside hosts not exceed 60% 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% reduction in the maximum data rate may occur at the maximum number of exporters.

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

The following table lists the support for a StealthWatch FlowCollector VE based on the amount of reserved memory and the number of CPUs for the VM.

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

Procedure 3 Choosing an SMC

The 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.

The first table below shows the SMC models and the number of StealthWatch FlowCollectors they can support. The second table lists the number of FlowCollectors and concurrent users (based on reserved memory and CPUs) that the SMC VE can support.

SMC Appliance Specifications

SMC Model	Maximum FlowCollectors	Size	Storage	Memory
SMC 500	1	1 RU	1.0 TB	8 GB
SMC 1000	5	1 RU	1.0 TB	8 GB
SMC 2000	25	2 RU	2.0 TB	16 GB

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 as the amount of data being sent to the SMC can increase in these deployments.

Procedure 4 (Optional) Choosing a StealthWatch FlowReplicator

The StealthWatch FlowReplicator receives or monitors UDP packets and generates copies of those packets to send to one or more new destinations, modifying the packets as they traverse the appliance to appear as though they came from the original source. Each FlowReplicator comes with two active interfaces: one is assigned an IP address for management, monitoring, and generation of packet copies; the other can be put into promiscuous mode for monitoring.

Each FlowReplicator is rated for a certain volume of input and output in terms of packets per second (pps). Each is tested against a generation of two to three copies per packet, but can support more destinations if required. The following table lists the StealthWatch FlowReplicator models and specifications.

StealthWatch FlowReplicator Appliance Specifications

FlowReplicator Model	Processing Capacity	Physical Layer	Form Factor	Power	Fault Tolerant
1000	10,000 pps input 20,000 pps output	Copper	1 RU-short	Non-redundant	No
2000	20,000 pps input 60,000 pps output	Copper or Fibre	1 RU	Redundant	Yes

Note: If the physical limits of the appliance are exceeded and too many copies are being generated for the link, packets will be dropped.

Deploying the Lancope StealthWatch System

This section describes the procedures necessary to deploy each appliance in the Lancope StealthWatch System and ready it for operation in the Cisco Cyber Threat Defense Solution 1.0.

Procedure 1 Install each appliance

Step 1 Install the StealthWatch Management Console (SMC).

As a management device, the SMC appliance should be installed in a location on the network that is accessible to all StealthWatch System components and management devices and is able to open an HTTPS connection to the Cisco Identity Services Engine. If a failover SMC is present, it is recommended that the primary and secondary SMCs be installed in separate physical locations. Refer to the *System Hardware Installation Guide* on the Lancope StealthWatch Documentation CD for detailed information.

Step 2 (Optional) Install any StealthWatch FlowSensors.

As a passive monitoring device the StealthWatch FlowSensor can be placed at any place in the network that currently does not have native NetFlow support to observe and record IP activity. As

with any NetFlow configuration in the Cisco Cyber Threat Defense Solution 1.0, the FlowSensor is most effective when placed such that it can monitor access layer traffic. Refer to the *System Hardware Installation Guide* on the Lancope StealthWatch Documentation CD for detailed information on the installation of the StealthWatch FlowSensor.

Step 3 (Optional) Install any StealthWatch FlowSensor VEs.

The StealthWatch FlowSensor VE is used to promiscuously monitor inter-VM communication inside of a single vSphere/ESX host. Refer to the *FlowSensor VE Installation and Configuration Guide* on the Lancope StealthWatch Documentation CD for detailed information.

Step 4 Install the StealthWatch FlowCollector(s).

As a collection and monitoring device, each StealthWatch FlowCollector appliance should be installed in a location on the network that is accessible to the devices that are generating and sending the NetFlow data to the FlowCollector. The FlowCollector should also be accessible to any devices that need to access the management interface, including HTTPS access from the SMC. Refer to the *System Hardware Installation Guide* on the Lancope StealthWatch Documentation CD for detailed information.

Step 5 (Optional) Install the StealthWatch FlowReplicator.

The only requirement for the placement of the StealthWatch FlowReplicator is that it has an unobstructed communication path to the rest of the StealthWatch System components. Refer to the next procedure (Configure the Firewall) and the *System Hardware Installation Guide* on the Lancope StealthWatch Documentation CD for detailed information.

The StealthWatch FlowReplicator has two active interfaces: One is assigned an IP address for management, monitoring, and generation of packet copies; the other can be put in to promiscuous mode for monitoring.

Procedure 2 Configure the firewall

If a firewall is present anywhere in the deployment, the following figure illustrating the data flows in the Cyber Threat Defense Solution 1.0 should be consulted to ensure that the appropriate ports and services are allowed. The table following the figure further highlights the required services. Refer to the *System Hardware Installation Guide* on the Lancope StealthWatch Documentation CD for additional information.

Cisco Cyber Threat Defense Solution 1.0 Data Flows
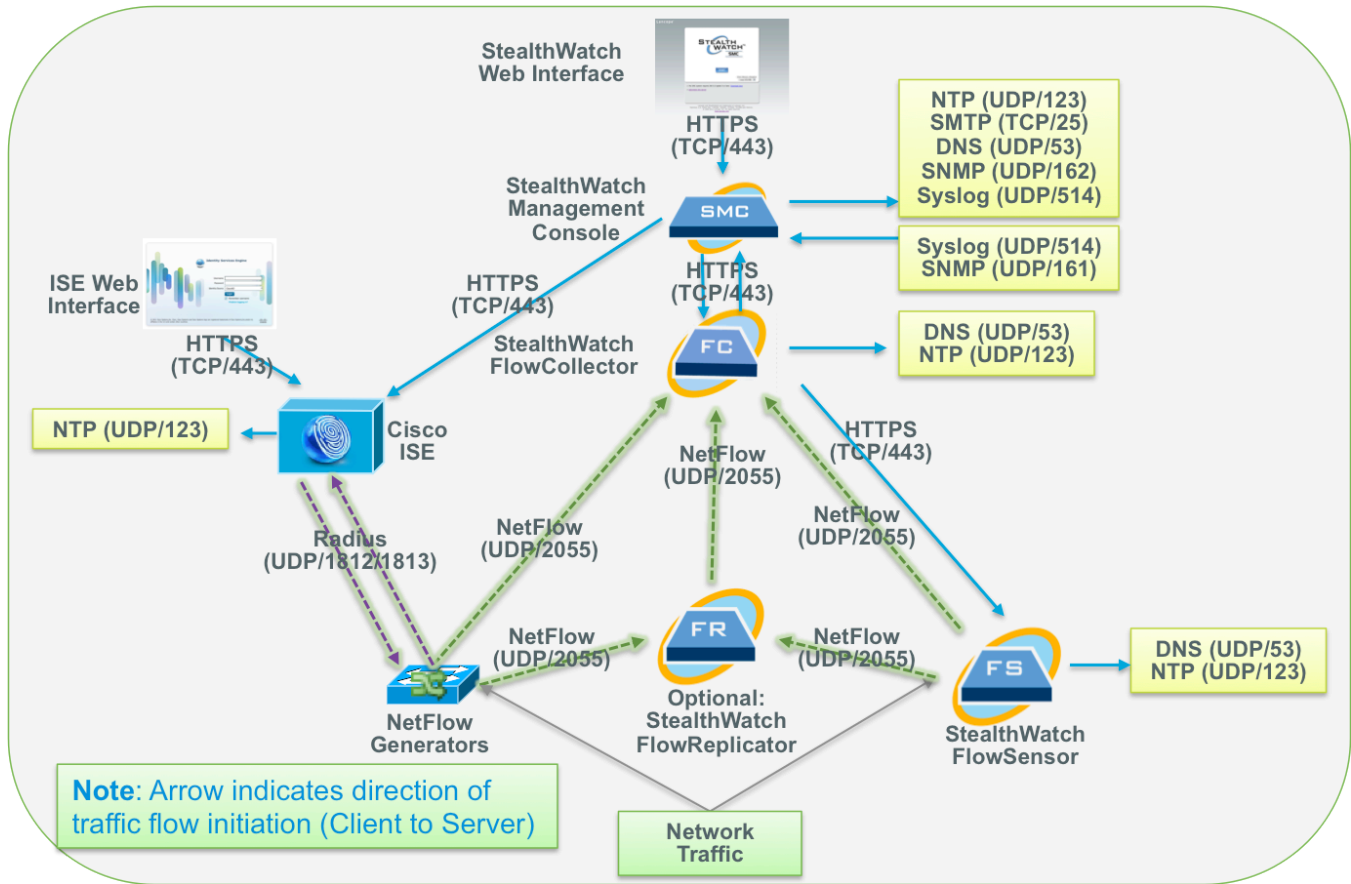
Client	Server	Port	Comment
SMC	FlowCollector	TCP/443	HTTPS
SMC	Cisco Identity Services Engine	TCP/443	HTTPS
SMC	Exporters	UDP/161	SNMP
SMC	–	UDP/123	NTP
SMC	–-	TCP/25	SMTP (optional)
SMC	-	UDP/53	DNS

SMC	-	UDP/162	SNMP-TRAP (optional)
SMC	-	UDP/514	SYSLOG (optional)
SMC	Identity Services Engine	TCP/443	HTTPS
–-	SMC	UDP/514	SYSLOG (optional)
–-	SMC	UDP/161	SNMP (optional)
SW Web Interface	SMC	TCP/443	HTTPS
FlowCollector	SMC	TCP/443	HTTPS
FlowCollector	FlowSensor	TCP/443	HTTPS
FlowCollector	–-	UDP/123	NTP
FlowCollector	–-	UDP/53	DNS
FlowSensor	–-	UDP/123	NTP
FlowSensor	–-	UDP/53	DNS
FlowSensor	FlowCollector	UDP/2055	NetFlow
Exporters	FlowCollector	UDP/2055	NetFlow

Procedure 3 Run the system configuration on each appliance

Step 1 The system configuration dialogue is used to initialize the networking and access information for each StealthWatch component. The dialogue and the configuration steps are the same for each StealthWatch appliance. Detailed information for this configuration is available in the *System Configuration Guide* on the Lancope StealthWatch Documentation CD.

Step 2 Log into the appliance through the console interface.

Note: The default console username is *sysadmin* with a password of *lan1cope.*

Step 3 Run the System Configuration program. A screen similar to the following will be displayed.

```
StealthWatch FlowCollector NetFlow Version 6.2.0 build 2012.01.06.0226-1 seria
                              System Configuration
   Select one:

                  Management     Change the Management Port Networking
                  Users          Change User Passwords
                  TrustedHosts   Change the Trusted Hosts
                  Advanced       Advanced Operations




                      <  OK  >              <Cancel>
```
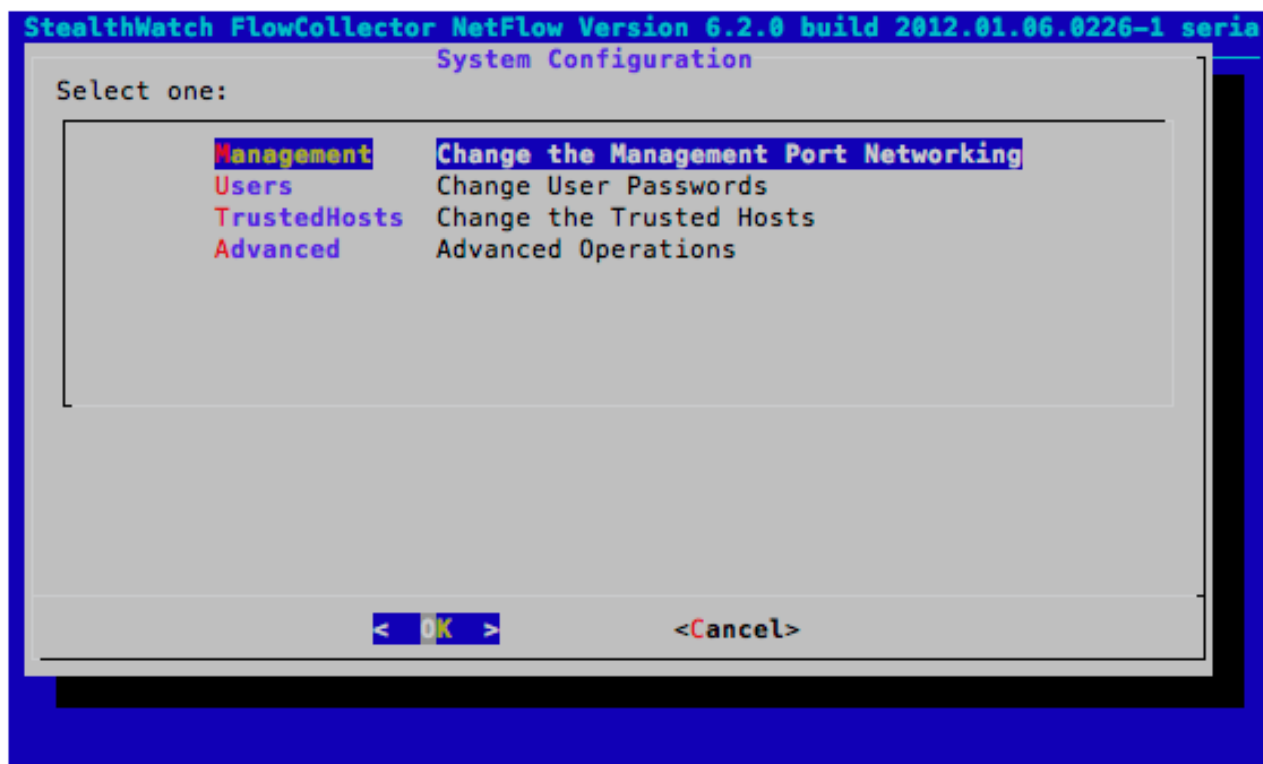
Note: Refer to Chapter 1 of the StealthWatch *System Configuration Guide* for additional information.

Note: Entering SystemConfig at the command prompt enters the system configuration.

Step 4 Configure the management port networking.

This is the IP address and subnet information necessary to allow the appliance to connect to the network. This is also the IP address that will be used to access the appliance through the web interface.

Note: Refer to Chapter 2 of the StealthWatch *System Configuration Guide* for additional information.

Best Practice: Configure a DNS entry for every StealthWatch System component.

Step 5 Change the user passwords.

Change the password that is used to access the console interface. This is also the password that would be used for SSH access to the appliance command prompt.

Note: Refer to Chapter 3 of the *System Configuration Guide* for detailed information.

Note: SSH access is disabled by default and can be enabled though the web interface; this is described in the next procedure.

Step 6 Configure the trusted host settings (optional).

These settings reflect the IP addresses of the hosts that are allowed to access the appliance. Refer to Chapter 4 of the *System Configuration Guide* for additional information.

Procedure 4 Log into the web interface of each appliance

Step 1 Access the web interface of the StealthWatch FlowCollector.

The web interface is accessed at **https://sfc.demo.local** where **sfc.demo.local** is the DNS entry for the IP address configured in the previous procedure.

Step 2 Access the web interface of the SMC.

The web interface is accessed at **https://smc.demo.local/smc/login.html** where **smc.demo.local** is the DNS entry for the IP address configured in the previous procedure.

Note: The web interface access credentials are different then the console access credentials. The default username is *admin* with a password of *lan411cope.*

Step 3 The web interface for each appliance will look similar to the following screenshot of the StealthWatch FlowCollector web interface:
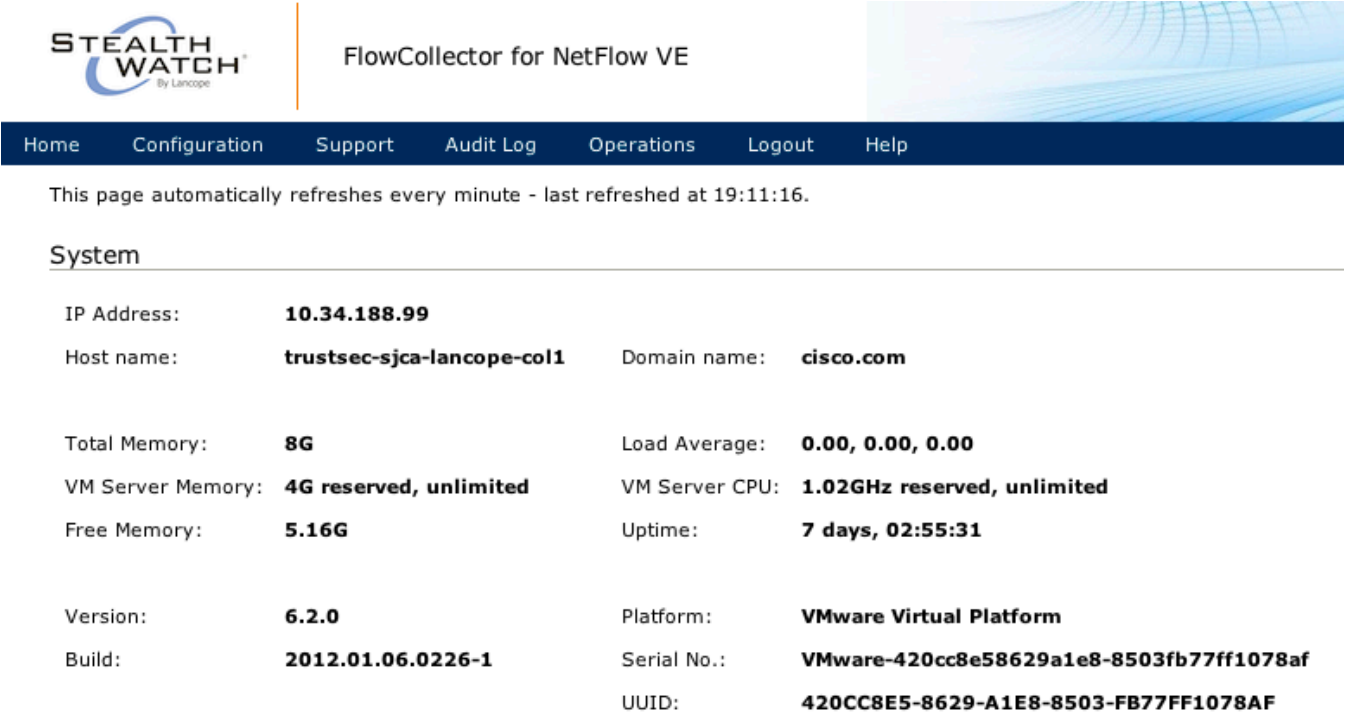
Note: Refer to Chapter 6 of the *System Configuration Guide* for detailed information.

Procedure 5 Configure the host name and DNS settings

Step 1 From the web interface homepage, click Configuration → Naming and DNS.

Step 2 Enter the host name and domain name for the appliance.

Step 3 Click *Apply.*

Step 4 Enter the address of the DNS server into the text box.

Step 5 Click *Add*.

Step 6 Click *Apply*.

Procedure 6 Configure time settings

Step 1 From the web interface homepage, click Configuration → System Time and NTP.

Step 2 Ensure the *Enable Network Time Protocol* check box is selected.

Step 3 Select a preferred NTP server from the drop-down menu or enter the IP address of a local NTP server into the text box.

Best Practice: Use the same time source for all the Cisco Cyber Threat Defence Solution components, including the NetFlow generators.

Step 4 Click *Add*.

Step 5 Click *Apply*.

Step 6 Configure the time zone settings to be the time zone the StealthWatch appliance is located in.

Step 7 Click *Apply*.

Procedure 7 Configure the admin password

Follow this procedure to change the password for the web interface admin account.

Step 1 From the web interface homepage, click Configuration → Password.

Step 2 Fill out the text boxes with the current and new password.

Step 3 Click *Apply*.

Procedure 8 Configure the Certificate Authority certificates

Note: The Certificate Authority certificate must be obtained and stored on the local disk before beginning this procedure.

Best Practice: The Certificate Authority certificate used here should be the same as the one used to issue the Identity certificate to the Cisco Identity Services Engine.

Step 1 From the web interface homepage, click Configuration → Certificate Authority Certificates.

Step 2 Click Choose File and then browse the local disk to locate the CA certificate.

Step 3 Give the certificate a name to identify it in the SMC configuration.

Step 4 Click *Add Certificate*.

Procedure 9 Configure the appliance Identity certificate

Note: A certificate and private key must be acquired from the Certificate Authority (added in the previous step) and stored on the local disk before beginning this procedure.

Step 1 From the web interface home page, click Configuration → SSL Certificate.

Step 2 Click the first Choose File and then browse the local disk to locate the appliance's identity certificate.

Step 3 (Optional) Click the second Choose File and then browse the local disk to locate the certificate chain used to issue the identity certificate.

Step 4 Click the third Choose File and then browse the local disk to locate the appliance's private key.

Step 5 Click *Upload Certificate*.

Procedure 10 (Optional) Configure the management systems

On a non-SMC StealthWatch component (such as the FlowCollector), the credentials used by the SMC to access the appliance can be modified from the default settings. The completion of this

procedure depends entirely on the requirements of the enterprise and does not affect the operation of the Cisco Cyber Threat Defense Solution 1.0.

Note: To complete this optional setup step, the SMC IP address must be known.

Step 1 From the web interface homepage, click Configuration → Management Systems Configuration.

Step 2 Click *Add New Management System*.

Step 3 Enter the IP address of the SMC.

Step 4 Check the *Is SMC* checkbox.

Step 5 Enter the *manager credentials*.

Step 6 Enter the *event credentials*.

Step 7 Click *Apply*.

Procedure 11 Restart the appliance

In the above procedures, changes were made to the host and time settings of the appliance. At this moment it is strongly recommended to restart the appliance to ensure all settings are properly operational.

Note: Detailed information for each configuration item in the web interface is available in the online help accessed by clicking *Help* in the web interface.

Initializing the Lancope StealthWatch System

In the previous section the two mandatory Lancope StealthWatch appliances (FlowCollector and SMC) were deployed and are operational. However, the appliances are not yet linked together and the StealthWatch System is not fully initialized.

The StealthWatch FlowCollector is fully deployed and operational and can at this moment begin receiving NetFlow records from the NetFlow exporters and begin populating its database. It is possible to skip ahead in the document and configure NetFlow export on the NetFlow exporters and have them begin generating NetFlow and sending it to the FlowCollector.

This section describes the process of integrating the Lancope StealthWatch FlowCollector into the Lancope SMC and readying the StealthWatch System for NetFlow analysis.

Procedure 1 Run the SMC client software

Step 1 Access the web interface of the SMC.

Step 2 Select the amount of memory to allocate to the SMC on the client computer.

Larger memory allocation should be considered if there is expected to be many open documents or large data sets (such as flow queries over 100,000 records). The local workstation should have at least twice the memory allocation selected.

Step 3 Click *Start* to download and install the SMC client software.

Procedure 2 Configure the domain

When first logging in to the SMC client, the *Default Domain Properties Page* will be displayed. The domain defines the set of related information for this deployment, including all hosts and host groups, network devices, FlowCollectors, the Cisco Identity Services Engine, etc.

Best Practice: Use a single domain for the Cisco Cyber Threat Defense Solution 1.0 deployment for the enterprise.

Step 1 In the *Name* field, enter a name for the domain.

Step 2 In the *Archive Hour Field*, specify the archive hour.

The archive hour is the time of day all StealthWatch FlowCollectors in the associated domain will begin a new day (24 hours) of data collection and reset all index counters to zero. All data received during the previous 24 hours will be archived in the database.

Best Practice: Set the archive hour to a time of day where network traffic is at a minimum.

Step 4 Click *OK.*
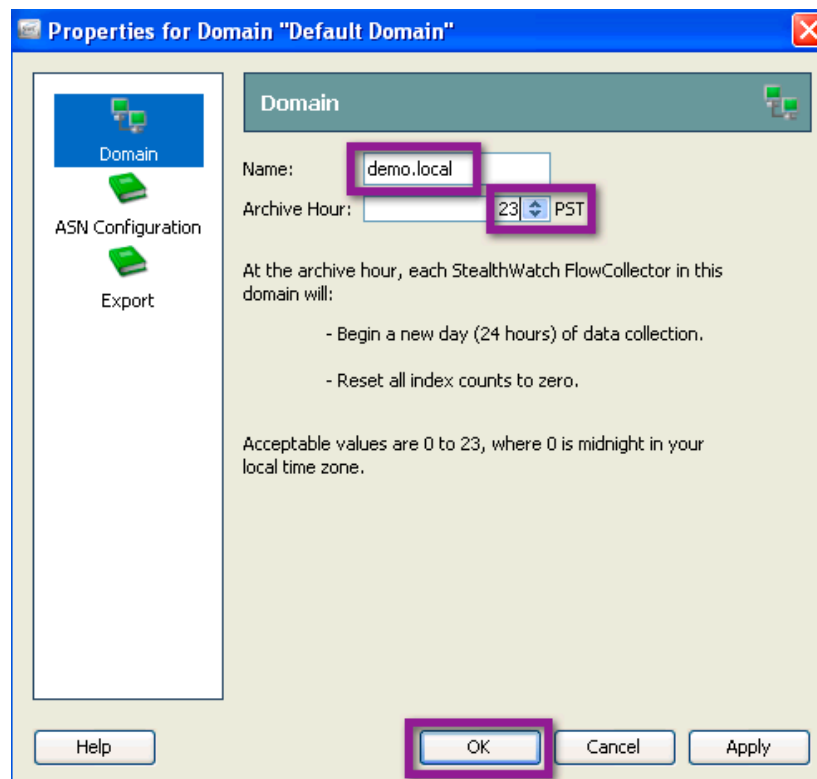
Step 5 Become familiar with the SMC display.

The top bar shows menu options. The left side shows the Enterprise Tree, which also contains the Host Group Tree. The right side is where documents will be displayed.
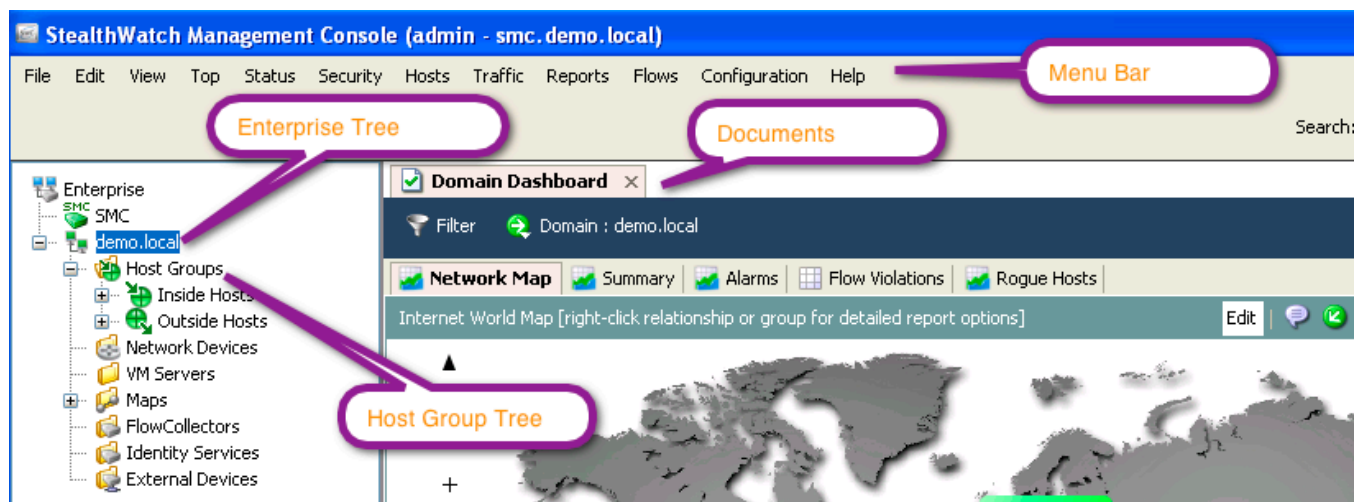
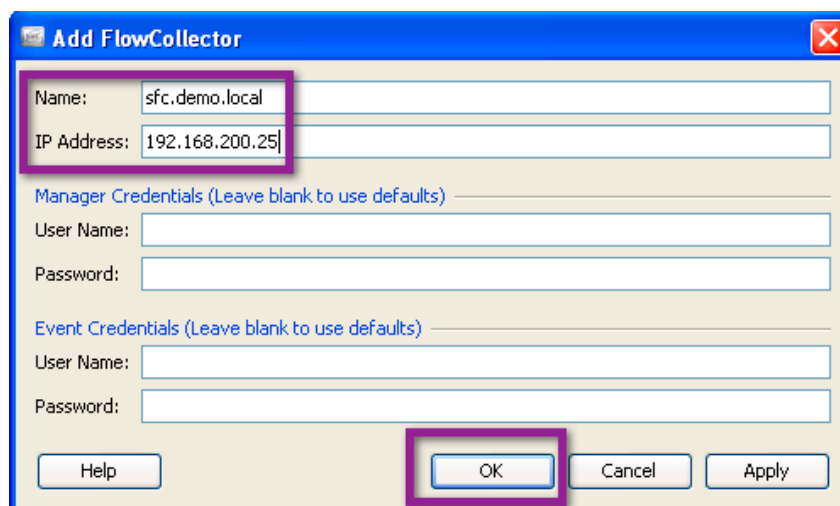**Procedure 3** Add the StealthWatch FlowCollector

Step 1 Highlight the domain in the Enterprise Tree.

Step 2 Click Configuration → Add FlowCollector.

Step 3 Enter the name and IP address of the StealthWatch FlowCollector.

Step 4 Enter the manager and event credentials (optional). Complete this step only if the credentials were changed from the default during the FlowCollector deployment.

Step 5 Click *OK*.

Step 6 The *Properties for FlowCollector* dialog will open. Verify the default configuration using the following table.

Configuration Item	Options	Setting
FlowCollector	Name	sfc.demo.local
Advanced	Ignore flows between inside hosts	Unselected
	Ignore flows between outside hosts	Unselected
	Ignore flow to and from non-routable addresses	Unselected
	Ignore flows between inside hosts when calculating File Sharing Index	Selected
	Ignore null0 flows	Unselected
	Seconds required to qualify a flow as long duration	32.4k
	Suspect long duration flow trust threshold	6
	Minimum number of asymmetric flows per 5-minute period to trigger Asymmetric_Route alert	50
	Minimum number of Class C subnets an infected host must contact before a worm alarm is triggered	8
	Store flow interface data	As much as possible
Watch List	Empty	
Broadcast List	Empty	
Ignore List	Empty	
Mitigation White List	IP ranges	SMC IP Address
	Domain names	Empty
Monitor Port	Port	2055
Exporters & Interfaces	Accept flows from any exporter	Selected
System Alarms	FlowCollector Data Deleted	Unselected
	FlowCollector Flow Data Lost	Selected
	FlowCollector Log Retention Reduced	Selected

	FlowCollector Management Channel Down	Selected
	FlowSensor Time Mismatch	Selected
	FlowSensor Traffic Lost	Selected
	FlowSensor VE Configuration Error	Selected
	Interface Utilization Exceeded Inbound	Selected
	Interface Utilization exceeded Outbound	Selected
	New VM	Selected
	V-Motion	Selected

Step 7 Click Synchronize → Synchronize.

Step 8 Click *Close.*

Step 9 Expand the *Enterprise Tree* to view the FlowCollector.
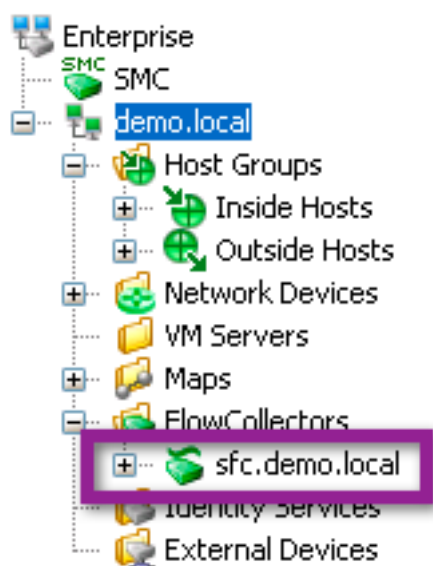
At this point in the deployment. the StealthWatch System is deployed and ready to begin receiving and analyzing NetFlow records.

Configuring Flexible NetFlow on Cisco Devices

Introduction

As previously mentioned, the Cisco Cyber Threat Defense Solution 1.0 makes use of the Flexible NetFlow capabilities of specific Cisco platforms. This section will first give a brief overview of the concepts and steps required to configure Flexible NetFlow on Cisco IOS and then provide detailed configuration and troubleshooting guidance for the Cisco devices that are components of the Cisco Cyber Threat Defense Solution 1.0 release.

Flexible NetFlow Configuration Overview

The configuration of Flexible NetFlow on a Cisco IOS device consists of the following four procedures described in detail below:

1. Configure a Flow Record

2. Configure a Flow Exporter

3. Create the Flow Monitor

4. Apply the Flow Monitor to one or more interfaces

Procedure 1 Configure a Flow Record

A flow record defines the information that will be gathered by the NetFlow process, such as packets in the flow and the types of counters gathered per flow. A custom flow record specifies a series of *match* and *collect* commands that tell the Cisco device which fields to include in the outgoing NetFlow record. The Cisco Cyber Threat Defense Solution 1.0 defines a specific flow record for each supported device; it is strongly recommended that these flow records are used to get the best possible results out of the deployment.

The *match* fields are the *key* fields, meaning that they are used to determine the uniqueness of the flow. The *collect* fields are extra information that is included in the record to provide more detail to the collector for reporting and analysis.

Procedure 2 Configure a Flow Exporter

The Flow Exporter defines where and how the NetFlow records will be sent. The configuration of the Flow Exporter is the same across all Cisco IOS devices used in the Cyber Threat Defense Solution 1.0. It should be noted that this configuration could differ from NetFlow configurations in older Cisco IOS and platform releases.

Procedure 3 Create the Flow Monitor

A Flow Monitor describes the NetFlow cache or information stored in the cache. Additionally, the Flow Monitor links together the Flow Record and the Flow Exporter. The Flow Monitor includes various cache characteristics such as the timers for exporting, the size of the cache, and, if required, the packet sampling rate.

As network traffic traverses the Cisco device, flows are continuously created and tracked. As the flows expire, they are exported from the NetFlow cache to the StealthWatch FlowCollector. A flow is ready for export when it is inactive for a certain time (e.g., no new packets received for the flow); or if the flow is long lived (active) and lasts greater than the active timer (e.g., long FTP download). There are timers to determine if a flow is inactive or if a flow is long lived.

Best practice: The Cisco Cyber Threat Defense Solution 1.0 recommends an active timeout of 60 seconds and an inactive timeout of 15 seconds.

Procedure 4 Apply the Flow Monitor to an interface

Until the Flow Monitor is applied to an interface, the Cisco device will not generate any NetFlow records. Once applied to an interface, the Flow Monitor will be activated and NetFlow records will be generated only for the interfaces to which the monitor is applied.

Best Practice: The Cisco Cyber Threat Defense solution 1.0 recommends that a Flow Monitor be applied to all interfaces where security visibility of flows is required.

Cisco Catalyst 3560-X and 3750-X Series

Flexible NetFlow is supported on Catalyst 3560-X and 3750-X (Cat3k-X) Series Switches on the 10GE Service Module. Previously unsupported on the platform, the service module can enable hardware-supported, line-rate NetFlow on all traffic `that traverses the module.`

The ability to generate NetFlow and gain flow visibility at the access layer is a key component of the Cisco Cyber Threat Defense Solution 1.0. Previously, the visibility provided by NetFlow was

only available at a Layer 3 boundary masking intra-LAN attacks. With NetFlow now available at the access layer, it is possible to detect suspicious behaviors present in the LAN.

Design Considerations

NetFlow services on the Catalyst 3500 Series are only supported on the Catalyst 3500-X Series (3560-X and 3750-X) platforms with the 10GE Service Module. It is important to note that it is the service module that enables the NetFlow feature: NetFlow data is only generated for traffic that traverses the module. As such, the service module and the ability to incorporate it into the network becomes a crucial component in the Cisco Cyber Threat Defense Solution 1.0.

The 10GE Service Module supports what is referred to as "North-South" NetFlow meaning that it generates NetFlow records for flows that traverse the switch (e.g., flows that enter or leave on a trunk port). The service module does not support "East-West" NetFlow; this means that NetFlow will not be generated for traffic that does not traverse the service module (e.g., traffic that is locally switched). As one of the objectives of the Cisco Cyber Threat Defense Solution 1.0 is to gain visibility into locally switched traffic, careful deployment considerations should be made.

NetFlow is supported in hardware on the service module. The hardware is capable of supporting 32,000 flows in its resident cache. It is important to note that this number does scale within a stack of Catalyst 3750-X switches. For example, a stack of four switches with four service modules can support 128,000 flows. There is no performance degradation in the switch when NetFlow is enabled on the service module.

Enabling the Service Module

In order to operate correctly, the service module must be installed in a supporting hardware platform and have the correct Cisco IOS Software image and license. The following are minimal requirements to enable Flexible NetFlow on the service module:

Component	Requirement
Minimum hardware	Version ID: 02 Revision: 0x03
IOS Software	15.0(1)SE
License	IP Services

Catalyst 3500-X Series Service Module Requirements

Note: The service module has its own operating system. In order to function properly, the operating system on the service module must match the operating system on the switch itself.

Enabling the Service Module

Note: The following procedure assumes you have met the hardware requirements and have already obtained an IP Services license and the appropriate Cisco IOS Software packages.

Step 1 Install the service module and turn on the switch.

Step 2 Upgrade the switch to the correct software image.

```
3560X# archive download-sw /overwrite /reload image-name
```

Step 3 Install the IP Services license.

```
3560X# license install license-name
```

Note: The switch may need to be restarted to make the license active.

Step 4 Ensure the license is active.

```
3560X# show license detail
Index: 1          Feature: ipservices                    Version: 1.0
        License Type: Permanent
        License State: Active, In Use
        License Priority: Medium
        License Count: Non-Counted
        Store Index: 1
        Store Name: Primary License Storage
```

Step 5 Upgrade the service module to the correct software image.

```
3560X# archive download-sw service-module-image-name
```

Step 6 Ensure the service module is operational.

```
3560X#show switch service-modules
Switch/Stack supports service module CPU version: 03.00.41
                        Temperature                   CPU
Switch#  H/W Status     (CPU/FPGA)      CPU Link      Version
---------------------------------------------------------------
  1       OK            67C/74C         connected     03.00.41
```

If not properly configured, a message similar to the following would be displayed:

```
3560X#show switch service-modules
```

```
Switch/Stack supports service module CPU version: 03.00.41
                           Temperature                    CPU
Switch#  H/W Status        (CPU/FPGA)      CPU Link        Version
        -------------------------------------------------------------
 1       LB-PASS-THRU *   71C/78C         notconnected    N/A
 *    Module services not supported on a Lanbase license
```

If the hardware status is in PASS-THRU mode, a misconfiguration has occurred. The error message will provide details on the cause of the error, which is that the hardware, software image, or license does not meet requirements. Review the checklist and the above steps to remediate.

Cabling

The 10GE Service Module has two dual-speed 10 Gigabit Ethernet SFP+ ports. As of the current release (15.01), these ports do not support a copper 1000BASE-T. Special consideration will need to be made when cabling the service module into a copper network.

Best Practice: Use standard 10GbE copper cables (requires the aggregation/core switches to have an available 10GbE port).
Best Practice: Multi-mode Gigabit Ethernet Fibre SFP (GLC-SX-MM) with a media converter.

NetFlow for Locally Switched Flows

As previously mentioned, locally switched traffic that does not traverse the service module is not monitored, and the switch will be unable to produce NetFlow records. If NetFlow is desired for locally switched traffic, there are two options available:

1. Deployment with PVLAN

2. Deployment with Remote SPAN and Flow-Based Span

Deployment with PVLAN

Private VLAN (PVLAN) can prevent local switching and force all traffic to go through the service module ports. The solution consists of the Cisco Catalyst 3560-X access switch or 3750-X stack acting as a Layer 2 device and the distribution switch as a Layer 3 gateway with local proxy Address Resolution Protocol (ARP) functionality enabled within the VLAN(s) used by directly connected devices.

The following figure is an example where PVLAN edge, or protected ports, is used. Locally switched traffic is exchanged between two workstations in the same subnet, both connected to a stack of Cisco Catalyst 3750-X switches.

Cyber Threat Defense Solution 1.0 Design and Implementation Guide

How to monitor locally switched traffic (left) with PVLAN (Right) for Layer 2 configured switch or stack
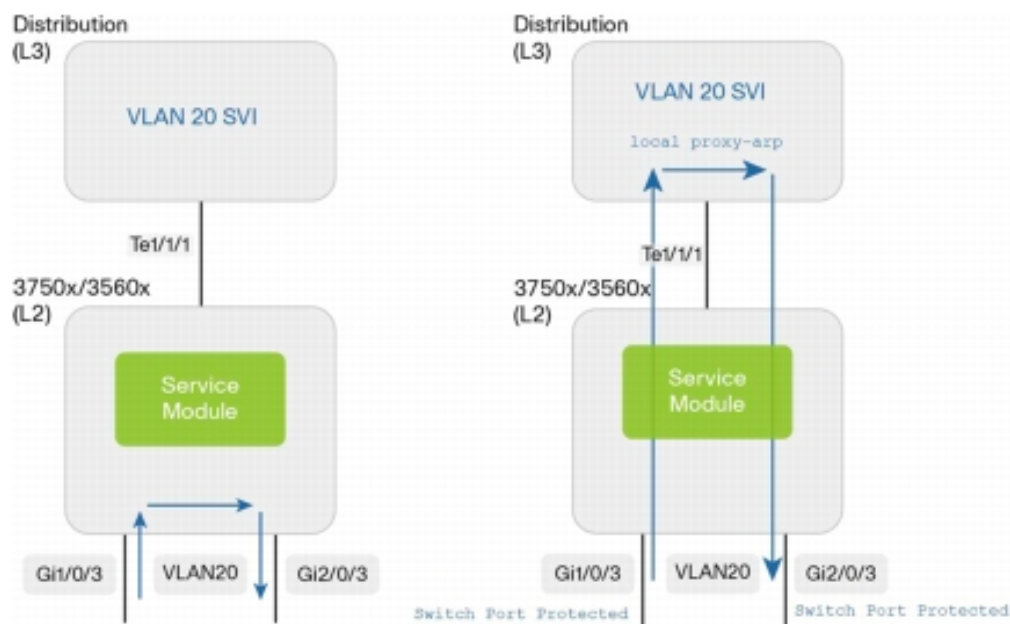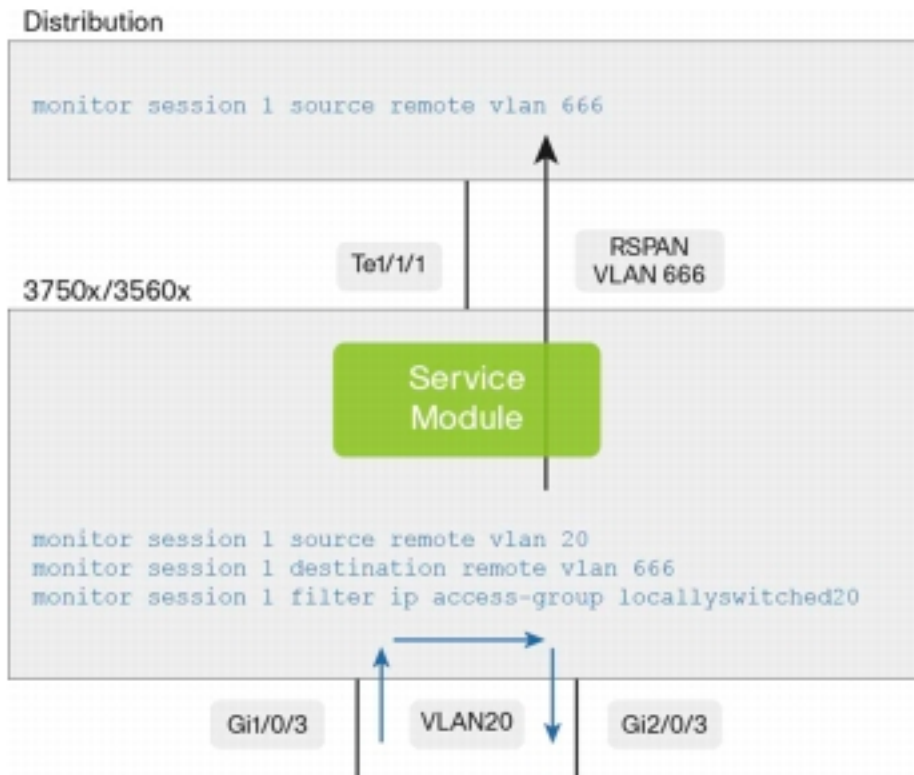

Deployment with Remote SPAN and Flow-Based Span

Another way to analyze locally switched or routed traffic is to send a copy of the traffic through the service module ports by enabling Switched Port Analyzer (SPAN) monitoring. Compared to the PVLAN deployment, this solution does not require the access switch to act as a Layer 2–only device. Furthermore, the mirrored traffic can also include CPU and ACL dropped traffic that would not reach the service module ASIC otherwise.

A remote SPAN (RSPAN) session is configured on the access and distribution switches to monitor the traffic received by the access VLAN(s). With flow-based SPAN, locally switched traffic characteristics can be exactly matched with an ACL filter applied to the RSPAN session. The locally switched traffic is mirrored on a remote SPAN destination VLAN and carried on the service module ports configured as trunks.

The following figure illustrates a deployment where locally switched traffic is exchanged between two workstations in the same subnet and a copy of the traffic is exported through the service module.

Flexible NetFlow Configuration

Cisco Catalyst 3500-X Series Switches are generally deployed in the access layer. This section describes how to implement the level of flow visibility necessary to best utilize the Flexible NetFlow capabilities of the Catalyst 3500-X Series as an access layer switch.

Procedure 1 Configure the flow record

Step 1 Create a flow record using the following commands:

```
3560X(config)#flow record CYBER_3KX_RECORD
3560X(config-flow-record)#match datalink mac source-address
3560X(config-flow-record)#match datalink mac destination-address
3560X(config-flow-record)#match ipv4 tos
3560X(config-flow-record)#match ipv4 ttl
3560X(config-flow-record)#match ipv4 protocol
```

```
3560X(config-flow-record)#match ipv4 source address
3560X(config-flow-record)#match ipv4 destination address
3560X(config-flow-record)#match transport source-port
3560X(config-flow-record)#match transport destination-port
3560X(config-flow-record)#collect interface input snmp
3560X(config-flow-record)#collect interface output snmp
3560X(config-flow-record)#collect counter bytes
3560X(config-flow-record)#collect counter packets
3560X(config-flow-record)#collect timestamp sys-uptime first
3560X(config-flow-record)#collect timestamp sys-uptime last
```

The above example record takes advantage of the fact that, as an access layer switch, it can help uniquely identity the end-user device and traffic set.

The data-link MAC destination/source address provides the unique identifier of the user device receiving/sending traffic to the switch, along with information about the device vendor available from its organizationally unique identifier (OUI).

The input/output interface value reports the Simple Network Management Protocol (SNMP) interface index value for the physical interface through which the traffic is entering/exiting the switch. For example, in the case of a downstream flow, the input interface value refers to a port on the service module, while the output interface value refers to a downlink port. The latter can be used to track the location of the user device, when integrated with information coming from a wired location database.

Procedure 2 Configure the flow exporter

The flow exporter describes the FlowCollector, including the destination IP address and port.

Step 1 Define the exporter.
```
3560X(config)#flow exporter CYBER_EXPORTER
```

Step 2 (Optional) Add a description.
```
3560X(config-flow-exporter)#description Lancope StealthWatch FlowCollector for the
Cisco Cyber Threat Defense Solution
```

Step 3 Define the source.
```
3560X(config-flow-exporter)#source loopback 1
```

This setting is the IP address that the switch will source NetFlow records from. Best practice is to define a loopback interface with an IP address on a management VLAN and use that interface as the source.

Step 4 Define the destination IP address.

```
3560X(config-flow-exporter)#destination <ip-address>
```

Step 5 Define the transport protocol.

```
3560X(config-flow-exporter)#transport udp 2055
```

Best Practice: NetFlow is usually sent over UDP port 2055.

Procedure 3 Create the flow monitor

The flow monitor represents the device's NetFlow database and links together the flow record and the flow monitor.

Step 1 Define the flow monitor.

```
3560X(config)#flow monitor CYBER_MONITOR
```

Step 2 (Optional) Add a description.

```
3560X(config-flow-monitor)#description Main NetFlow Cache for the Cisco Cyber Threat
Defense Solution
```

Step 3 Configure the flow record.

```
3560X(config-flow-monitor)#record CYBER_3KX_RECORD
```

Step 4 Configure the exporter.

```
3560X(config-flow-monitor)#exporter CYBER_EXPORTER
```

Step 5 Define the active timeout.

The active timeout refers to how often NetFlow records are generated for flows that are still active. It is recommended that a value of 60 seconds be used.

```
3560X(config-flow-monitor)#cache timeout active 60
```

Step 6 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. It is recommended that a value of 15 seconds be used.

```
3560X(config-flow-monitor)#cache timeout inactive 15
```

Procedure 4 Apply the flow monitor to the interfaces

Step 1 Enter interface configuration mode.

```
3560X(config)#interface range tenGigabitEthernet 1/1-2
```

Step 2 Apply the flow monitor on ingress traffic.

```
3560X(config-if-range)#ip flow monitor CYBER_MONITOR input
```

Step 3 Apply the flow monitor on egress traffic.

```
3560X(config-if-range)#ip flow monitor CYBER_MONITOR output
```

Procedure 5 Verify

Step 1 Verify the configuration using *show* commands.

```
3560X#show run flow [exporter|monitor|record]
```

Verify NetFlow records are being exported form the appliance and are being received by the FlowCollector. (Details available in the

Flexible NetFlow Export Verification section below.)

Final Catalyst 3500-X Series NetFlow Configuration

```
!
flow record CYBER_3KX_RECORD
 match datalink mac source-address
 match datalink mac destination-address
 match ipv4 tos
 match ipv4 ttl
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 collect interface input snmp
 collect interface output snmp
 collect counter bytes
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
!
!
flow exporter CYBER_EXPORTER
 description Lancope StealthWatch FlowCollector for the Cisco Cyber Threat
Defense Solution
 destination <ip-address>
 source loopback 1
 transport udp 2055
!
!
flow monitor CYBER_MONITOR
 description Main NetFlow Cache for the Cisco Cyber Threat Defense Solution
 record CYBER_3KX_RECORD
 exporter CYBER_EXPORTER
 cache timeout active 60
 cache timeout inactive 15
!
!
interface TenGigabitEthernet1/1/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 ip flow monitor CYBER_MONITOR input
 ip flow monitor CYBER_MONITOR output
!
interface TenGigabitEthernet1/1/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

```
 ip flow monitor CYBER_MONITOR input
 ip flow monitor CYBER_MONITOR output
!
```

Additional information: Cisco Catalyst 3K-X Service Module: Enabling Flexible NetFlow in the Access
http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps10745/white_paper_c11-691508_ps10744_Products_White_Paper.html

Cisco Catalyst 4500 Series Supervisor Engine 7-E/7-LE

Native Flexible NetFlow support was introduced to the Cisco Catalyst 4500 Series with the release of the Supervisor Engine 7-E and 7-LE; previously, the Catalyst 4500 Series had supported NetFlow with an optional NetFlow Services Card.

The modular Cisco Catalyst 4500 Series has a presence in both the access and aggregation layers and includes NetFlow services in the IP-base image and license.

Design Considerations

The Cisco Cyber Threat Defense Solution 1.0 recommends deployment of the Catalyst 4500 Supervisor 7-E/7-LE as both an access layer and aggregation layer switch. The Supervisor 7-E and 7-LE support a 128,000-entry hardware flow table that is shared across all flow monitors. While it is possible to limit the cache entries in a flow monitor (using the **cache entries** *numbers* command in the flow monitor configuration), this deployment guide assumes a single flow monitor for the entire switch and that the complete flow cache is allocated to the Cisco Cyber Threat Defense Solution 1.0.

The Catalyst 4500 Series does not support the selection of both Layer 2 and Layer 3 fields within a single flow record. This differs from the other access layer switches in the solution (Catalyst 3500-X Series).

Flexible NetFlow Configuration

As previously mentioned, the Supervisor 7-E and 7-LE support a wide range of NetFlow services and can be used effectively in both the access and aggregation layers. This section describes the procedures to implement the recommended level of flow visibility necessary on the Supervisor 7-E/7-LE.

Since Catalyst 4500 Series Switches can act as both access layer and aggregation layer switches, it is possible to define different flow records and flow monitors for the access ports and trunk ports. However, the Cisco Cyber Threat Defense Solution 1.0 recommends using the same configuration for both to keep the configuration as simple as possible while maintaining complete functionality.

Procedure 1 Configure the flow record

Step 1 Create a flow record using the following commands:

```
4500sup7e(config)#flow record CYBER_4K_RECORD
4500sup7e(config-flow-record)#match ipv4 tos
```

```
4500sup7e(config-flow-record)#match ipv4 protocol
4500sup7e(config-flow-record)#match ipv4 source address
4500sup7e(config-flow-record)#match ipv4 destination address
4500sup7e(config-flow-record)#match transport source-port
4500sup7e(config-flow-record)#match transport destination-port
4500sup7e(config-flow-record)#collect ipv4 dscp
4500sup7e(config-flow-record)#collect ipv4 ttl minimum
4500sup7e(config-flow-record)#collect ipv4 ttl maximum
4500sup7e(config-flow-record)#collect transport tcp flags
4500sup7e(config-flow-record)#collect interface output
4500sup7e(config-flow-record)#collect counter bytes
4500sup7e(config-flow-record)#collect counter packets
4500sup7e(config-flow-record)#collect timestamp sys-uptime first
4500sup7e(config-flow-record)#collect timestamp sys-uptime last
```

Note: The Catalyst 4500 Series does not allow the selection of both Layer 2 and Layer 3 fields in a single flow record.

Procedure 2 Configure the flow exporter

The flow exporter describes the FlowCollector, including the destination IP address and port.

Step 1 Define the exporter.

```
4500sup7e(config)#flow exporter CYBER_EXPORTER
```

Step 2 (Optional) Add a description.

```
4500sup7e(config-flow-exporter)#description Lancope StealthWatch FlowCollector for
Cisco Cyber Threat Defense Solution
```

Step 3 Define the source.

```
4500sup7e(config-flow-exporter)#source loopback 1
```

This setting is the IP address that the switch will source NetFlow records from. Best practice is to define a loopback interface with an IP address on a management VLAN and use that interface as the source.

Step 4 Define the destination IP address.

```
4500sup7e(config-flow-exporter)#destination <ip-address>
```

Step 5 Define the transport protocol.

```
4500sup7e(config-flow-exporter)#transport udp 2055
```

Best Practice: NetFlow is usually sent over UDP port 2055.

Procedure 3 Create the flow monitor

The flow monitor represents the device's NetFlow database and links together the flow record and the flow monitor.

Step 1 Define the flow monitor.

```
4500sup7e(config)#flow monitor CYBER_MONITOR
```

Step 2 (Optional) Add a description.

```
4500sup7e(config-flow-monitor)#description Main NetFlow Cache for the Cisco Cyber
Threat Defense Solution
```

Step 3 Configure the flow record.

```
4500sup7e(config-flow-monitor)#record CYBER_4K_RECORD
```

Step 4 Configure the exporter.

```
4500sup7e(config-flow-monitor)#exporter CYBER_EXPORTER
```

Step 5 Define the active timeout.

The active timeout refers to how often NetFlow records are generated for flows that are still active. It is recommended that a value of 60 seconds be used.

```
4500sup7e(config-flow-monitor)#cache timeout active 60
```

Step 6 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. It is recommended that a value of 15 seconds be used.

```
4500sup7e(config-flow-monitor)#cache timeout inactive 15
```

Procedure 4 Apply the flow monitor to the interfaces

Step 1 Enter interface configuration mode.

```
4500sup7e(config)#interface GigabitEthernet 1/1
```

Step 2 Apply the flow monitor on Layer 2 switched input traffic.

```
4500sup7e(config-if)#ip flow monitor CYBER_MONITOR layer2-switched input
```

Procedure 5 Verify

Step 1 Check the configuration using show commands.

```
4500sup7e#show run flow [exporter|monitor|record]
```

Verify NetFlow records are being exported form the appliance and are being received by the FlowCollector. (Details available in the

Flexible NetFlow Export Verification section below.)

Final Catalyst 4500 Series Supervisor 7-E/7-LE NetFlow Configuration

```
!
flow record CYBER_4K_RECORD
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface input
 collect ipv4 dscp
 collect ipv4 ttl minimum
 collect ipv4 ttl maximum
 collect transport tcp flags
 collect interface output
 collect counter bytes
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
!
!
flow exporter CYBER_EXPORTER
 description Lancope StealthWatch FlowCollector for the Cisco Cyber Threat
Defense Solution
 destination <ip-address>
 source loopback 1
 transport udp 2055
!
!
flow monitor CYBER_MONITOR
 description Main NetFlow Cache for the Cisco Cyber Threat Defense Solution 1
 record CYBER_4K_RECORD
 exporter CYBER_EXPORTER
 cache timeout active 60
 cache timeout inactive 15
!
interface GigabitEthernet1/1
 ip flow monitor CYBER_MONITOR input
!
```

Additional Information: Catalyst 4500 Series Switch Software Configuration Guide, Release IOS-XE 3.1.0 SG: Configuring Flexible NetFlow

http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/01xo/configuration/guide/fnf.html

Cisco Catalyst 6500 Series Supervisor Engine 2T

Since the introduction of the Cisco Catalyst 6500 Series, NetFlow services have been available on the platform. The introduction of the Supervisor Engine 2T for the Cisco Catalyst 6500 Series continues the advancement of NetFlow services, including the introduction of Flexible NetFlow support and the complete hardware support of the NetFlow feature set.

Design Considerations

The Supervisor Engine 2T for the Catalyst 6500 Series supports an unprecedented level of NetFlow data collection for a single system: It is possible to scale the deployment to support 13 million flow entries. The following table highlights the improved NetFlow feature set of the Supervisor Engine 2T.

Catalyst 6500 Series Switch Supervisor Engine 2T NetFlow Support

Feature	Supervisor Engine 2T/2TXL
NetFlow Table Size	512,000/1 million
NetFlow Hash Efficiency	99%
Maximum Flow Entries (6513-E)	13 million
Egress NetFlow	Yes
TCP Flags	Yes

Note: Currently, only the WS-X6908-10G-2T/2TXL, WS-X6816-10T-2T/2TXL, WS-X6716-10G with DFC4/DFC4XL, and WS-X6716-10T with DFC4/DFC4XL line cards can perform NetFlow record export in a Supervisor Engine 2T-based system. All future 6900 Series modules will support this ability.

Note: NetFlow is currently unavailable in the Cisco IOS Software IP Base image; as of the current release, NetFlow is only available in the Advanced Enterprise Services image.

Flexible NetFlow Configuration

This section describes the steps to implement the recommended level of flow visibility necessary for the Cisco Cyber Threat Defense Solution 1.0 on the Supervisor Engine 2T.

Since Catalyst 6500 Series Switches can act as access, aggregation, or distribution layer switches, it is possible to define different flow records and flow monitors for the access ports and trunk ports. However, in this guide we recommend using the same configuration for both to keep the configuration as simple as possible while maintaining complete functionality.

Procedure 1 Configure the flow record

Step 1 Create a flow record using the following key and non-key fields.

```
6500sup2T(config)#flow record CYBER_6K_RECORD
6500sup2T(config-flow-record)#match ipv4 tos
6500sup2T(config-flow-record)#match ipv4 protocol
6500sup2T(config-flow-record)#match ipv4 source address
6500sup2T(config-flow-record)#match ipv4 destination address
6500sup2T(config-flow-record)#match transport source-port
6500sup2T(config-flow-record)#match transport destination-port
6500sup2T(config-flow-record)#match interface input
6500sup2T(config-flow-record)#collect transport tcp flags
6500sup2T(config-flow-record)#collect interface output
6500sup2T(config-flow-record)#collect counter bytes
6500sup2T(config-flow-record)#collect counter packets
6500sup2T(config-flow-record)#collect timestamp sys-uptime first
6500sup2T(config-flow-record)#collect timestamp sys-uptime last
```

Note: The Supervisor Engine 2T supports the collection of TCP flags; however, it does not support the collection of the TTL field in an ipv4 header.

Procedure 2 Configure the flow exporter

The flow exporter describes the FlowCollector including the destination IP address and port.

Step 1 Define the exporter.

```
6500sup2T(config)#flow exporter CYBER_EXPORTER
```

Step 2 (Optional) Add a description.

```
6500sup2T(config-flow-exporter)#description Lancope StealthWatch FlowCollector for
the Cisco Cyber Threat Defense Solution
```

Step 3 Define the source.

```
6500sup2T(config-flow-exporter)#source loopback 1
```

This setting is the IP address that the switch will source NetFlow records from. Best practice is to define a loopback interface with an IP address on a management VLAN and use that interface as the source.

Step 4 Define the destination IP address.

```
6500sup2T(config-flow-exporter)#destination <ip-address>
```

Step 5 Define the transport protocol.

```
6500sup2T(config-flow-exporter)#transport udp 2055
```

Best practice: NetFlow is usually sent over UDP port 2055.

Procedure 3 Create the flow monitor

The flow monitor represents the device's NetFlow database and links together the flow record and the flow monitor.

Step 1 Define the flow monitor.

```
6500sup2T(config)#flow monitor CYBER_MONITOR
```

Step 2 (Optional) Add a description.

```
6500sup2T(config-flow-monitor)#description Main NetFlow Cache for the Cisco Cyber
Threat Defense Solution
```

Step 3 Configure the flow record.

```
6500sup2T(config-flow-monitor)#record CYBER_6K_RECORD
```

Step 4 Configure the exporter.

```
6500sup2T(config-flow-monitor)#exporter CYBER_EXPORTER
```

Step 5 Define the active timeout.

The active timeout refers to how often NetFlow records are generated for flows that are still active. It is recommended that a value of 60 seconds be used.

```
6500sup2T(config-flow-monitor)#cache timeout active 60
```

Step 6 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. It is recommended that a value of 15 seconds be used.

```
6500sup2T(config-flow-monitor)#cache timeout inactive 15
```

Procedure 4 Apply the flow monitor to the interfaces

On a Catalyst 6500 Series Switch, a flow monitor can only be applied to a routed (Layer 3) port. However, if applied to a routed port, a NetFlow record is generated only for the traffic that crosses the Layer 3 boundary and not on intra-VLAN traffic.

Cyber Threat Defense Solution 1.0 Design and Implementation Guide

To monitor intra-VLAN traffic the flow monitor must be applied on a VLAN interface.

Step 1 Enter the VLAN interface configuration mode.

```
6500sup2T(config)#interface vlan 100
```

Step 2 Apply the flow monitor on ingress traffic.

```
6500sup2T(config-if)#ip flow monitor CYBER_MONITOR input
```

Step 3 Apply the flow monitor on egress traffic.

```
6500sup2T(config-if)#ip flow monitor CYBER_MONITOR output
```

Procedure 5 Verify

Step 1 Check the configuration using *show* commands.

```
6500sup2T#show run flow [exporter|monitor|record]
```

Verify NetFlow records are being exported form the appliance and are being received by the FlowCollector. (Details available in the

Flexible NetFlow Export Verification section below.)

Final Catalyst 6500 Series Supervisor 2T NetFlow Configuration

```
!
flow record CYBER_6K_RECORD
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface input
 collect transport tcp flags
 collect interface output
 collect counter bytes
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
!
!
flow exporter CYBER_EXPORTER
  description Lancope StealthWatch FlowCollector for the Cisco Cyber Threat
Defense Solution
  destination <ip-address>
  source loopback 1
  transport udp 2055
!
!
flow monitor CYBER_MONITOR
  description Main NetFlow Cache for the Cisco Cyber Threat Defense Solution
  record CYBER_6K_RECORD
  exporter CYBER_EXPORTER
  cache timeout active 60
  cache timeout inactive 15
!
!
interface Vlan 200
 ip flow monitor CYBER_MONITOR input
 ip flow monitor CYBER_MONITOR output
!
```

Additional information: Cisco Catalyst 6500 Supervisor Engine 2T: NetFlow Enhancements
  http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white_paper_c11-652021.html

Cisco Integrated Service Routers G2

The Flexible NetFlow support on Cisco ISR G2 Routers adheres to the platform-independent implementation of NetFlow as documented in Cisco IOS Software guides. On the ISR, NetFlow services support takes the traditional NetFlow approach of collecting information and generating a NetFlow record for flows that cross a Layer 3 boundary. This makes the ISR a key component in providing visibility into flows that traverse different areas of the network.

Additionally, the ISR G2 contains software-supported Network-Based Application Recognition (NBAR) fully integrated with NetFlow services. If enabled, NBAR can perform deep packet inspection on packets traversing an interface to recognize and classify the application that is generating the traffic (for supported protocols). The application classification of the traffic set can be exported in a NetFlow record.

Design Considerations

The Cisco ISR G2 platform supports NetFlow and NBAR services using a software implementation of the feature sets. Care should be taken when deploying software-supported NetFlow services, as the feature can impact device performance; for instance, a fully loaded ISR running Cisco IOS Software can experience an approximate 15% CPU uptick resulting from NetFlow enablement. The Cisco NetFlow Performance Analysis white paper should be consulted when implementing software-supported NetFlow services.

Note: NetFlow Performance Analysis
   http://www.cisco.com/en/US/technologies/tk543/tk812/technologies_white_paper0900aecd802a0eb9.html

Flexible NetFlow Configuration

The Cisco ISR G2 platform is generally deployed as the Layer 3 boundary between VLANs and often at the edge of a branch network. This section describes the steps to implement the recommended level of flow visibility to best utilize the Flexible NetFlow and NBAR capabilities of the Cisco ISR G2.

Procedure 1 Configure the Flow Record

Step 1 Create a flow record using the following key and non-key fields.
```
ISR(config)#flow record CYBER_ISR_RECORD
ISR(config-flow-record)#match ipv4 tos
```

```
ISR(config-flow-record)#match ipv4 protocol
ISR(config-flow-record)#match ipv4 source address
ISR(config-flow-record)#match ipv4 destination address
ISR(config-flow-record)#match transport source-port
ISR(config-flow-record)#match transport destination-port
ISR(config-flow-record)#match interface input
ISR(config-flow-record)#collect routing next-hop address ipv4
ISR(config-flow-record)#collect ipv4 dscp
ISR(config-flow-record)#collect ipv4 ttl minimum
ISR(config-flow-record)#collect ipv4 ttl maximum
ISR(config-flow-record)#collect transport tcp flags
ISR(config-flow-record)#collect interface output
ISR(config-flow-record)#collect counter bytes
ISR(config-flow-record)#collect counter packets
ISR(config-flow-record)#collect timestamp sys-uptime first
ISR(config-flow-record)#collect timestamp sys-uptime last
ISR(config-flow-record)#collect application name
```

The above flow record takes advantage of the NetFlow version 9 formatting and the ISR's location as a Layer 3 boundary and collects many Layer 3 and 4 fields that are not available on all switch-based implementations of NetFlow, such as Time To Live field, TCP Flags and the next-hop address.

The ISR is the only device in the Cisco Cyber Threat Defense Solution 1.0 that supports NBAR. The above flow record allows the collection of the name of the application that is creating the flow using the "collect application name" option.

Note: Utilizing NBAR services on the router can impact the performance of the router. While the collection of the application name is of great value in the Cisco Cyber Threat Defense Solution 1.0, enabling NBAR services must be done carefully.

Procedure 2 Configure the flow exporter

The flow exporter describes the FlowCollector, including the destination IP address and port.

Step 1 Define the exporter.

```
ISR(config)#flow exporter CYBER_EXPORTER
```

Step 2 (Optional) Add a description.

```
ISR(config-flow-exporter)#description Lancope StealthWatch FlowCollector for the
Cisco Cyber Threat Defense Solution
```

Step 3 Define the source.

```
ISR(config-flow-exporter)#source loopback 1
```

This setting is the IP address that the switch will source NetFlow records from. Best practice is to define a loopback interface with an IP address on a management VLAN and use that interface as the source.

Step 4 Define the destination IP address.

```
ISR(config-flow-exporter)#destination <ip-address>
```

Step 5 Define the transport protocol.

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

Best Practice: NetFlow is usually sent over UDP port 2055.

Procedure 3 Create the flow monitor

The flow monitor represents the device's NetFlow database and links together the flow record and the flow monitor.

Step 1 Define the flow monitor.

```
ISR(config)#flow monitor CYBER_MONITOR
```

Step 2 (Optional) Add a description.

```
ISR(config-flow-monitor)#description Main NetFlow Cache for the Cisco Cyber Threat
Defense Solution
```

Step 3 Configure the flow record.

```
ISR(config-flow-monitor)#record CYBER_ISR_RECORD
```

Step 4 Configure the exporter.

```
ISR(config-flow-monitor)#exporter CYBER_EXPORTER
```

Step 5 Define the active timeout.

The active timeout refers to how often NetFlow records are generated for flows that are still active. It is recommended that a value of 60 seconds be used.

```
ISR(config-flow-monitor)#cache timeout active 60
```

Step 6 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. It is recommended that a value of 15 seconds be used.

```
ISR(config-flow-monitor)#cache timeout inactive 15
```

Procedure 4 Apply the flow monitor to an interface

The flow monitor should be applied to all routing interfaces and sub-interfaces.

Step 1 Enter interface configuration mode.

```
ISR(config)#interface GigabitEthernet 0/0
```

Step 2 Apply the flow monitor on ingress traffic.

```
ISR(config-if)#ip flow monitor CYBER_MONITOR input
```

Procedure 5 Verify

Step 1 Check the configuration using show commands.

```
ISR#show run flow [exporter|monitor|record]
```

Verify NetFlow records are being exported from the appliance and are being received by the FlowCollector. (Details available in the

Flexible NetFlow Export Verification section below.)

Final Configuration

```
!
flow record CYBER_ISR_RECORD
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface input
 collect routing next-hop address ipv4
 collect ipv4 dscp
 collect ipv4 ttl minimum
 collect ipv4 ttl maximum
 collect transport tcp flags
 collect interface output
 collect counter bytes
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
 collect application name
!
!
flow exporter CYBER_EXPORTER
 description Lancope StealthWatch FlowCollector for the Cisco Cyber Threat
Defense Solution
 destination <ip-address>
 source loopback 1
 transport udp 2055
!
!
flow monitor CYBER_MONITOR
 description Main NetFlow Cache for the Cisco Cyber Threat Defense Solution
 record CYBER_ISR_RECORD
 exporter CYBER_EXPORTER
 cache timeout active 60
 cache timeout inactive 15
!
!
interface GigabitEthernet0/0
 ip address <ip-address> <net-mask>
 ip flow monitor CYBER_MONITOR input
!
```

Additional information: NetFlow Configuration Guide, Cisco IOS Software Release 15.2 M&T

http://www.cisco.com/en/US/docs/ios-xml/ios/fnetflow/configuration/15-2mt/fnf-15-2mt-book.html

Cisco ASA 5500 Series Adaptive Security Appliances

About NSEL

The Cisco ASA implementation of NetFlow is known as NetFlow Security Event Logging (NSEL). NSEL was designed to utilize the benefits of the NetFlow protocol and message system to act as a high performance alternative to Syslog in environments with high demand for message logging. As a message logging technology NSEL focuses only on three types of events: flow creation, flow teardown, and flow denial by ACLs.

Although the NSEL implementation conforms to the NetFlow version 9 standard, its implementation and operation differs from other Cisco devices:

Note: NSEL records are generated based on the three flow status events (creation, tear-down, and denial) rather than on activity timers.

- NSEL has predefined templates for the three event types. These templates are usually exported before any NSEL data records.

- NSEL is bidirectional. A connection through a Cisco IOS Software-based device generates two flows whereas NSEL treats it as a single flow.

- Flow-export actions are not supported in interface-based policies and can thus only be applied in a global service policy.

The ability to track flow state at the edge of the network is significant in the context of the Cisco Cyber Threat Defense Solution 1.0. NSEL should be considered a complementary technology to enhancing visibility into network traffic.

Configuring NSEL

NSEL is configured on the ASA appliance using the Modular Policy Framework (MPF). This requires seven procedures, two of which are optional.

Procedure 1 Configure the NSEL collector

Step 1 Configure the NSEL collector

```
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.

Procedure 2 Create a class map

Step 1 Create a class map to match the traffic to create NSEL records for.

Best Practice: Use a *match any* option to generate NSEL for all traffic.

```
ASA(config)# class-map CYBER_FLOW_CLASS
ASA(config-cmap)# match any
```

Procedure 3 Create a policy map

Step 1 **Create the policy map to apply flow-export actions to the defined classes**.

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

Step 2 Associate the defined class map with the policy.

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

Step 3 Define the action to be taken on matched traffic: Export all flow events.

```
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 4 Create the global service policy

Step 1 Apply the policy map globally.

```
ASA(config)# service-policy CYBER_FLOW_POLICY global
```

Procedure 5 (Optional) Tune the template timeout interval

Step 2 Modify the interval in which the template records are sent.

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

Best practice: Use the default interval of 30 minutes.

Procedure 6 (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 7 Verify

Step 1 Verify the configuration using *show* commands.

Verify NetFlow records are being exported from the appliance and are being received by the FlowCollector. (Details available in the

Flexible NetFlow Export Verification section below.)

Final Configuration

```
!
flow-export destination management <ip-address> 2055
class-map CYBER_FLOW_CLASS
 match any
!
policy-map CYBER_FLOW_POLICY
 class CYBER_FLOW_CLASS
   flow-export event-type all destination <ip-address>
!
service-policy CYBER_FLOW_POLICY global
!
```

Additional information:

NSEL configuration:
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

Flexible NetFlow Export Verification

Once NetFlow is configured on each device in the solution, it is necessary to validate that the flow monitor is operational and is exporting NetFlow records to the StealthWatch FlowCollector. In the preceding sections, the devices were configured with Flexible NetFlow and the configuration was verified to be consistent with the Flexible NetFlow configuration recommended by the Cisco Cyber Threat Defense Solution 1.0. Use the following procedures to verify that the NetFlow configuration is operational.

<div style="background-color:#d9e2c4">Procedure 1   Verify NetFlow export on a Cisco IOS Software-based device</div>

Step 1 Display the flow records present in the cache.

```
Cisco-IOS#show flow monitor CYBER_MONITOR cache
```

This command will show all flow records currently in the CYBER_MONITOR's memory. Assuming flows are transiting the configured interfaces, records should be displayed. If not, ensure that the flow monitor is applied to the correct interface, in the correct direction, and that traffic is present on the interface.

Step 2 Display the historical statistics of the flow monitor.

```
Cisco-IOS#show flow monitor CYBER_MONITOR statistics
  Cache type:                          Normal
  Cache size:                             128
  Current entries:                          0
  High Watermark:                           0

  Flows added:                              0
  Flows aged:                               0
    - Active timeout      (    60 secs)     0
    - Inactive timeout    (    15 secs)     0
    - Event aged                            0
    - Watermark aged                        0
    - Emergency aged                        0

  Cache type:                          Normal (Platform cache)
  Cache size:                          Unknown
  Current entries:                         19

  Flows added:                              0
  Flows aged:                          171593
    - Active timeout      (    60 secs)  171593
```

This command will show the historical statistics of the CYBER_MONITOR, including the number of flows currently in the cache and the number of flows that have been aged out of the cache. The size of the cache as well as the active and inactive timeouts can also be verified here.

Step 3 Ensure flow records are being exported from the device.

```
Cisco-IOS#show flow exporter CYBER_EXPORTER statistics
Flow Exporter CYBER_EXPORTER:
  Packet send statistics (last cleared 8w4d ago):
    Successfully sent:          702414                (147362340 bytes)

  Client send statistics:
    Client: Flow Monitor EXAMPLE_MONITOR
      Records added:            0
        - sent:                 1404828
      Bytes added:              0
        - sent:                 147362340
```

This command will show historical counts of packets and bytes exported from the flow exporter. The number of packets sent (and records sent) should be greater than zero and increasing. If not, ensure the flow exporter is appropriately applied to the flow monitor.

Note: NetFlow allows for multiple flow records to be sent in a single packet, so the record and packet counts in the above output can be different.

Procedure 2   Verify NetFlow export on a Cisco ASA appliance

Step 1 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 flows are traversing the device)

- Zero errors

The final step in ensuring the configuration is operational is to ensure that flow records for each exporter are being received by the FlowCollector.

Note: This procedure assumes that the previous steps were successful and that NetFlow is being exported from the NetFlow generation device

Step 1 Log into the SMC console.

Step 2 Expand the FlowCollector in the Enterprise Tree.

Step 3 Verify that the configured flow exporter appears in the expanded tree.
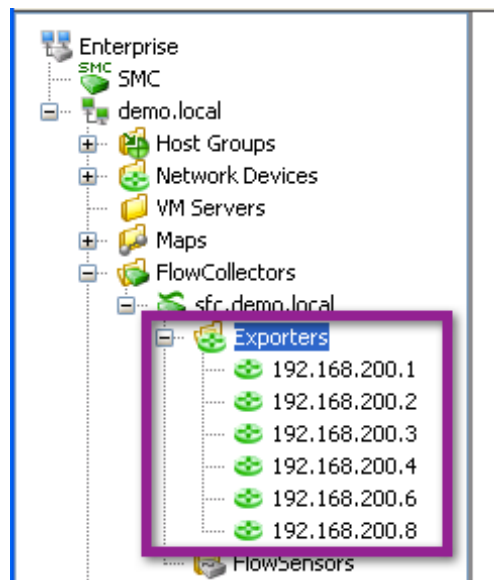
Step 4 Right-click the flow exporter and click Flows → Flow Table.

Step 5 Ensure that (expected) flow records are appearing in the table.

Client Host	Client Host Groups	Server Host	Server Host Groups
192.168.201.100	Catch All	192.168.201.103	Catch All
192.168.200.2	Catch All	192.168.200.25	Catch All
192.168.201.100	Catch All	192.168.30.11	Catch All
192.168.206.1	Catch All	255.255.255.255	Broadcast
192.168.203.1	Catch All	255.255.255.255	Broadcast
120.0.0.1	China	255.255.255.255	Broadcast
192.168.205.1	Catch All	255.255.255.255	Broadcast
192.168.202.1	Catch All	255.255.255.255	Broadcast

Integrating NetFlow Analysis with Identity, Device Profiling, and User Services

Overview

The Cisco Cyber Threat Defense Solution 1.0 operates cohesively with the Cisco TrustSec Solution, meaning that not only can the solutions be deployed simultaneously, but together they offer the administrator enhanced visibility and control into and over the network.

Note: Before beginning this section, it is assumed that the reader is familiar with and has deployed the Cisco TrustSec Solution 2.0 to at least a **Monitor Mode** or better deployment. Design and implementation information for Cisco TrustSec Solution 2.0 is available here: http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_2.0/trustsec_2.0_dig.pdf

Integration between the Lancope SMC and the Cisco Identity Services Engine allows the administrator to quickly associate a user identity, device type, user policy, and posture status with a flow or set of flows from within the SMC console. The figure below illustrates this enhanced capability where the username, device type, and all other session information are available alongside all the flows associated with an IP address. This section describes the process of integrating the Lancope SMC with Cisco TrustSec or the Cisco Identity Services Engine to enhance the capabilities of the Cisco Cyber Threat Defense Solution 1.0.

Integrating the Lancope SMC with the Cisco Identity Services Engine

Before beginning, it should be noted that the integration is accomplished through the use of a Representational State Transfer (REST) API exposed by the Cisco Identity Services Engine, which supports the gathering of real-time session and node-specific information from a Cisco Monitoring Identity Services Engine. The REST API calls are performed over a secure and authenticated HTTPS session. The Lancope SMC will call the Cisco Identity Services Engine API to retrieve identity information.

Note: Information about the Identity Services Engine REST API is available here:
   http://www.cisco.com/en/US/docs/security/ise/1.0/api_ref_guide/ise10_api_ref_guide.html

Procedure 1 Validate Identity Services Engine Monitoring Node Deployment

In order to successfully invoke the API call on a Cisco Identity Services Engine node, the node must be deployed as a valid Cisco Monitoring Identity Services Engine node. This deployment can be verified by checking the deployment configuration in the Identity Services Engine dashboard.

Step 1 Log into the Cisco Identity Services Engine dashboard.

Step 2 Go to Administration → System → Deployment.

   The *Deployment Node* page appears, which lists all configured nodes that are deployed.

Step 3 In the *Roles* column of the Deployment Nodes page, verify that the role for the target node that you want to monitor shows its type as a Cisco Monitoring Identity Services Engine node.
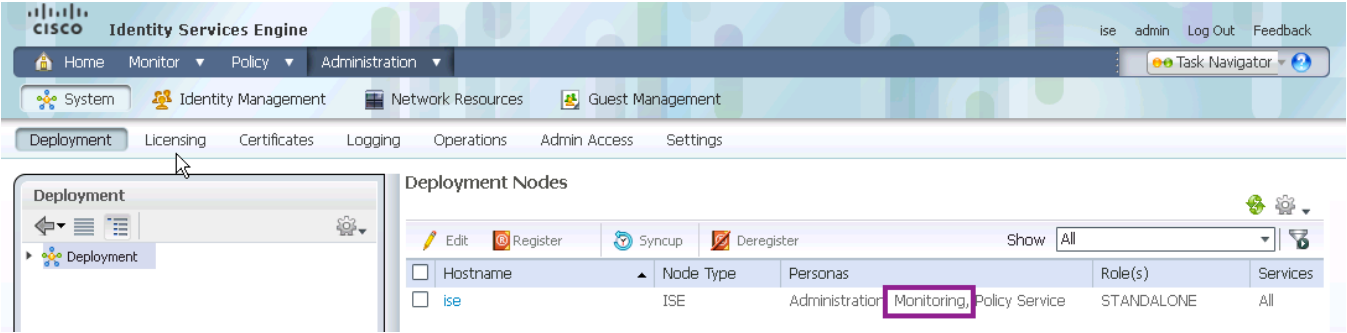
Procedure 2 Create an admin user on the Identity Services Engine for monitoring access

Best Practice: Create a dedicated user account on the Identity Services Engine for API use

Step 1 Log into the Identity Services Engine dashboard.

Step 2 Go to Administration → System → Admin Access → Administrators.

Step 3 Select *Admin Users*. Click *Add* and select *Create an Admin User.*
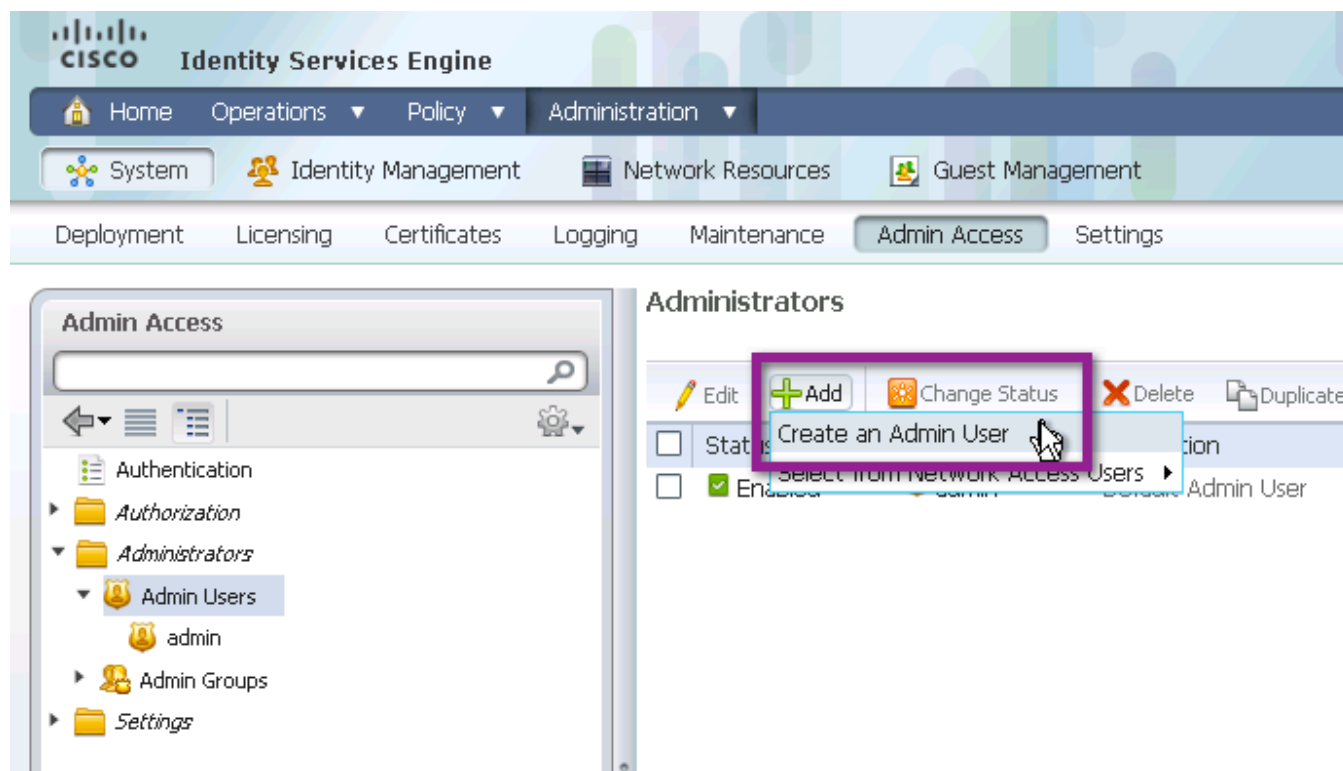
Step 4 Fill out the Admin User, Password, User Information, Account Options, and Admin Groups sections.

Configuration Item	Settings
Admin User	Name the admin user something easy to distinguish. Ensure the account status is set to *Enabled*.
Password	Create a password for the user.
User Information	Optional: Add information to describe the user.
Account	Optional: Add a meaningful description; for example:

Configuration Item	Settings
Options	*Account used the SteathWatch Management Console to access ISE Session information for the Cisco Cyber Threat Defense Solution.*
Admin Groups	Put the user in the predefined *Helpdesk Admin* group.

Step 5 Click *Submit*.

Procedure 3 Ensure there are active sessions in the Identity Services Engine

Step 1 Log into the Identity Services Engine dashboard.

Step 2 Click Operations → Authentications.

Step 3 Ensure that the *Live Authentications* table is not empty.

Procedure 4 Check the Identity Services Engine APIs using a web browser

The integration between the Cisco Identity Services Engine and the Lancope SMC utilizes two API calls supported by the Cisco Identity Services Engine:

- Authenticated Sessions List

    o Retrieve a list of all currently active authenticated sessions

- Endpoint by IP Address

    o Retrieve authenticated session information for host by IP address

Before continuing the integration, it is recommended that the admin credentials and API operation be validated using a web browser.

Step 1 Open an Internet browser. (Mozilla Firefox is recommended.)

Step 2 Call the *AuthList* API using the following URL:

https://ise.demo.local/ise/mnt/api/Session/AuthList/null/null

Step 3 Log in using the Cyber Threat Defense Solution monitoring credentials.

Step 4 Verify the *Authentication List* is displayed.

Note: The authentication list will be empty if there are no active authenticated sessions maintained within the Identity Services Engine. If no sessions are returned from the API, go to the Identity Services Engine dashboard to validate that there are active sessions.

Step 5 Using an IP address from an active session in the Identity Services Engine, call the *Endpoint Lookup by IP Address* API at the following URL:

> https://ise.demo.local/ise/mnt/api/Session/EndPointIPAddress/*<ip-address>*

Step 6 Log in using the Cyber Threat Defense Solution monitoring credentials.

Step 7 Verify the authentication session information is retrieved.

Procedure 5 Configure the Certificate Authority certificates

The SMC must be configured to trust the Certificate Authority that issued the Cisco Identity Services Engine'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.

Step 1 Log into the SMC (administration) web interface.

Step 2 From the homepage, click Configuration ➔ Certificate Authority Certificates.

Step 3 Click *Choose File* and then browse the local disk to locate the CA certificate.

Step 4 Give the certificate a name to identify it in the SMC configuration.

Step 5 Click *Add Certificate*.

Procedure 6 Register the Cisco Identity Services Engine with the Lancope SMC

Step 1 At this point in the deployment it has been verified that there are active authentication sessions in the Cisco Identity Services Engine and that they can be retrieved by an external entity using a configured username and password.

Step 2 Log into the SMC client software.

Step 3 Highlight the domain, then click Configuration ➔ Add Cisco ISE.

Step 4 Fill out the *Name*, *IP Address*, *User Name,* and *Password.*

Step 5 Identify the time zone the Cisco Identity Services Engine is located in.

Step 6 Click *OK*.

Step 7 Check the communication status with the Cisco Identity Services Engine.

Expand the Identity Services menu and hover the mouse over the Identity Services Engine icon to see communication status.
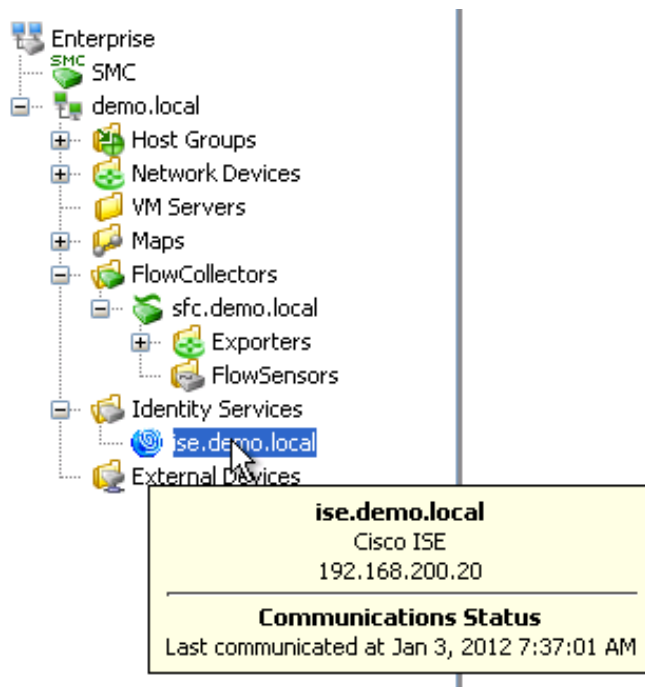
Step 8 Right-click the Identity Services Engine icon and go Hosts → Identity and Device Table.

This will open the Identity and Device Table. Verify that authenticated user names are present in the table.
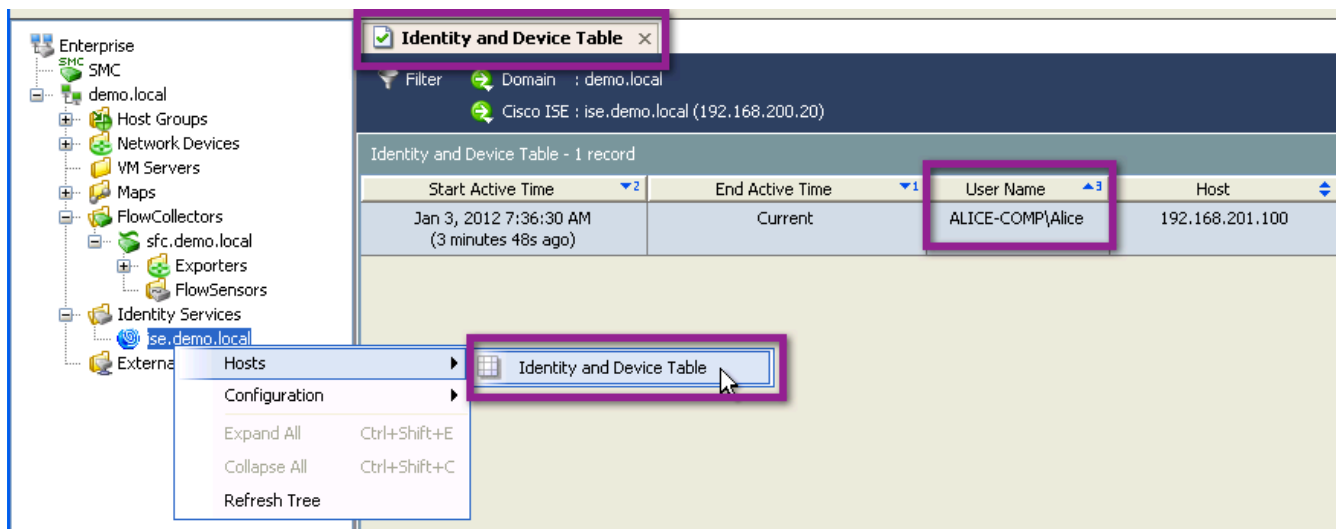
Procedure 7 (Optional) Check SMC logging

At this point it has been verified that authentication session information is available from the Cisco Identity Services Engine. If the information is not being displayed appropriately in the Lancope SMC, verify that the SMC is calling the Cisco Identity Services Engine using logging mechanisms on the SMC.

Step 1 Open the SMC Console.

Step 2 Go to: /etc/init.d

Step 3 Open the file: lc-tomcat

Step 4 Locate the following lines and uncomment the second line:

> #Uncomment following line for debugging
>
> JAVA_OPTS=$JAVA_OPTS" -Dcom.lancope.debug=2 -Xdebug -Xrunjdwp: transport=dt_socket, server=y,address=8000, suspend=n"

Step 5 Log files will be placed under: /lancope/var/smc/log. Check the logs to see if the SMC is appropriately calling the Identity Services Engine APIs.

Retrieving Authenticated Session Information in SMC

Authenticated session information from the Cisco Identity Services Engine is available in the Lancope SMC in the *Identity and Device Table*. This information can be used to locate all of the flows based on authenticated session information. Authenticated session information can also be viewed in the *Identity, DHCP & Host Notes* section of the host snapshot.

The following procedures describe two workflows highlighting the capabilities of the integration.

Procedure 1 Find all flows for a given user

Step 1 From the Enterprise Tree, right-click the Identity Services Engine icon. Go to Hosts → Identity and Device Table.

Step 2 In the Identity and Device Table, apply appropriate filters to locate the desired username of a Cisco Identity Services Engine authenticated user.
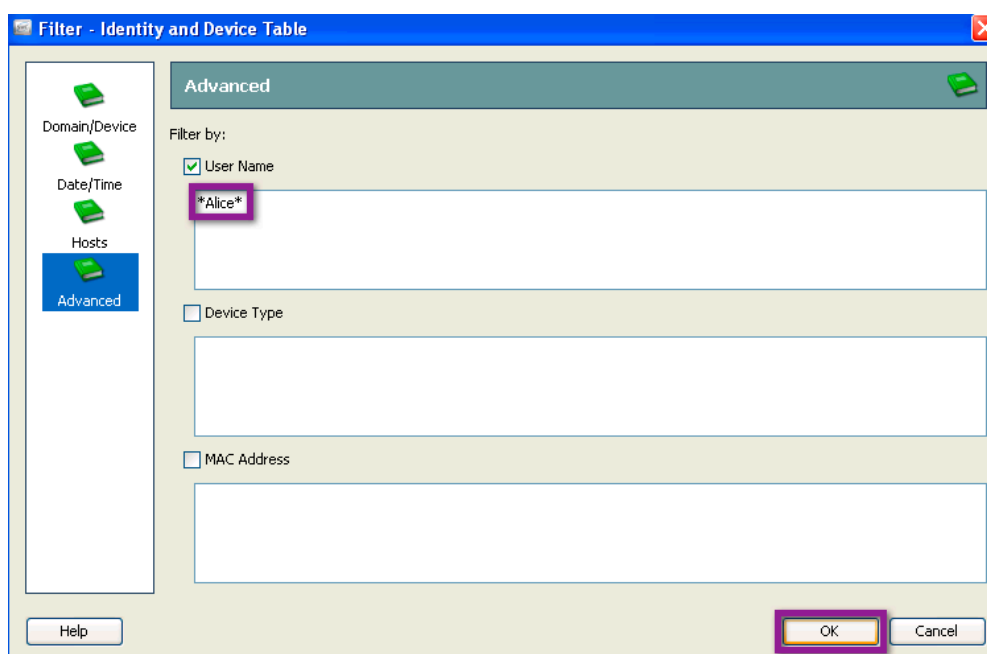
Note: Username filters can contain the wildcard character ("*").

Step 3 Right-click the username in the *Identity and Device Table* and click *Host Snapshot.*

Step 4 In the *Top Active Flows* tab, click the *Flow Table* icon.

Step 5 Apply the appropriate filters to locate the particular flow(s) of interest.

Procedure 2 Find the user responsible for a given flow

Note: This procedure assumes the reader has already identified a flow that needs further investigation and is interesting in locating the user responsible for it. For more on how to identify suspicious flows, consult the Cisco Cyber Threat Defense Solution How-To Guides.

Step 1 From the Flow Table, right-click the IP address requiring investigation and click *Host Snapshot.*

Step 2 In the Host Snapshot view for that IP address, select the *Identity, DHCP & Host Notes* tab.

Step 3 Locate the username and other authenticated session information in the *Identity and Device Table.*

Concluding Remarks

This guide described the deployment and implementation details on the Cisco Cyber Threat Defense Solution 1.0. An operational solution should now be present on the network and should be ready to aid in advanced threat defense operations. Consult other "how-to" guides in the Cisco Secure Network Services How-To Guide Series on how to best leverage this solution for Cyber Threat Defense.

Appendix X: References

Secure Network Services:

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

NetFlow:

Lancope NetFlow Bandwidth Calculator
http://www.lancope.com/resource-center/netflow-bandwidth-calculator-stealthwatch-calculator/

NetFlow Performance Analysis
http://www.cisco.com/en/US/technologies/tk543/tk812/technologies_white_paper0900aecd802a0eb9.html

Cisco Catalyst 3K-X Service Module: Enabling Flexible NetFlow in the Access
http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps10745/white_paper_c11-691508_ps10744_Products_White_Paper.html

Cisco Catalyst 4500 Series Switch Software Configuration Guide, Cisco IOS-XE Software Release 3.1.0 SG: Configuring Flexible NetFlow
http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/01xo/configuration/guide/fnf.html

Cisco Catalyst 6500 Series Supervisor Engine 2T: NetFlow Enhancements
http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white_paper_c11-652021.html

NetFlow Configuration Guide, Cisco IOS Software Release 15.2 M&T:
http://www.cisco.com/en/US/docs/ios-xml/ios/fnetflow/configuration/15-2mt/fnf-15-2mt-book.html

NSEL Configuration
http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/monitor_nsel.html

NSEL Implementation Note for NetFlow Collectors
http://www.cisco.com/en/US/docs/security/asa/asa84/system/netflow/netflow.html

Identity Services Engine

Cisco Identity Services Engine API Reference Guide, Release 1.0.4
http://www.cisco.com/en/US/docs/security/ise/1.0/api_ref_guide/ise10_api_ref_guide.html