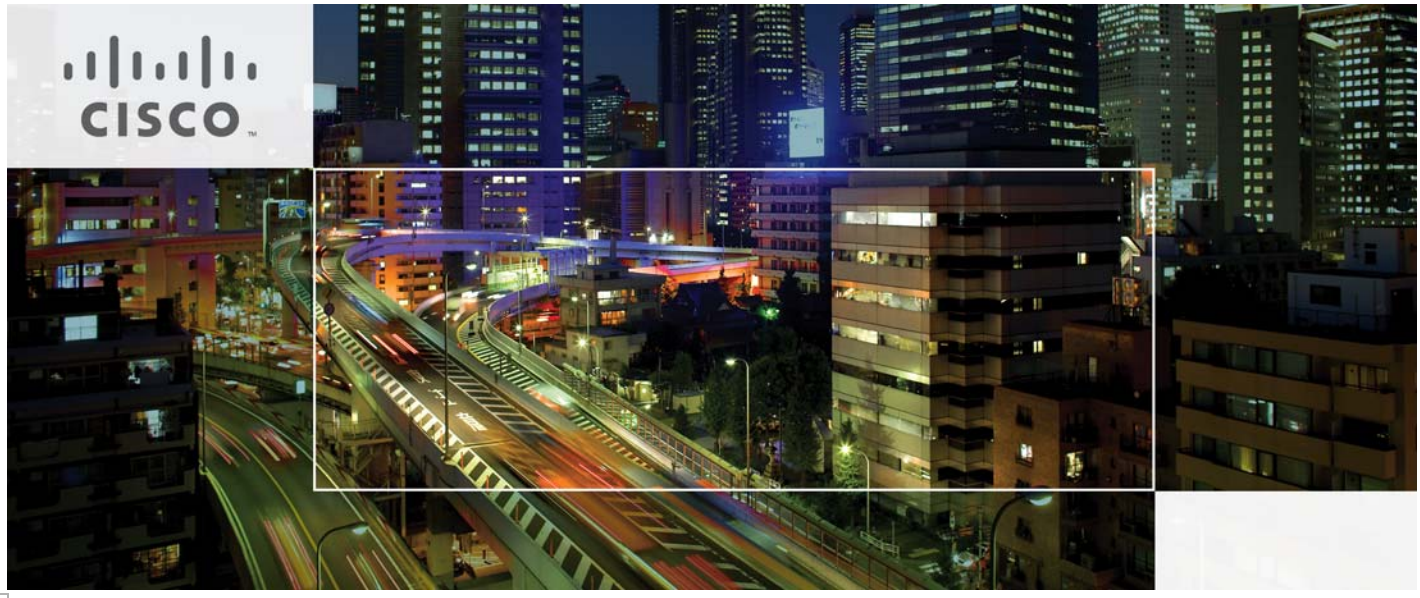


Cisco Cyber Threat Defense Solution 1.1 Design and Implementation Guide

Last Updated: July 28, 2013

Cisco Validated Design

About the Authors

Matt Robertson

Matt is a Technical Marketing Engineer in the Security Technology Group at Cisco Systems where he regularly works with Cisco's largest customers all over the world. Matt focuses on developing solutions for advanced threat detection and defense, and holds both a Bachelors and Masters degree in Computer Engineering from the University of Waterloo.

Brian MacMahon

Brian McMahon has been active in various computer and network security roles for much of the last 25 years, including education, testing, and technical support for institutions large and small. Currently, he is a Technical Marketing Engineer for Cisco Systems, working on network behavior-based threat detection systems.

CONTENTS

Cisco Cyber Threat Defense Solution 1.1

Introduction

The threat landscape has evolved; government organizations and large enterprises are being inundated with targeted, custom attacks known as advanced persistent threats (APTs). These APTs are often launched by motivated and well-financed attackers who are able to bypass the perimeter defenses of an organization to gain access to the network. In response, many government organizations and large enterprises are turning to tools that can help to identify and study the attacks that threaten their networks.

The Cisco Cyber Threat Defense Solution 1.1 provides a proactive capability for detecting threats already operating on an internal network. The solution uses telemetry from network devices to provide deep and pervasive visibility across the network interior, allowing the security operator to understand the "who, what, when, where, why, and how" of network traffic to discover anomalies. This approach gives the operator much more visibility into the nature of suspicious activity 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 1.1 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 1.1 across the entire network can provide the information and visibility to support the security operator in a wide spectrum of security tasks that include (but are not limited to):

- Detecting the occurrence of a data loss event
- Detecting network reconnaissance activity on the internal network
- Detecting and monitoring the spread of malware throughout the internal network
- Detecting botnet command and control channels on the internal network

The Cisco Cyber Threat Defense Solution 1.1 leverages Cisco networking technology such as NetFlow and 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 1.1. 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 1.1.

This guide describes design, deployment, and implementation details of the Cisco Cyber Threat Defense Solution 1.1.

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

Copyright © 2013 Cisco Systems, Inc. All rights reserved

Products and Releases

The Cisco Cyber Threat Defense Solution 1.1 is a tested system that has been demonstrated to achieve all stated objectives, using the components listed in Table 1.

Table 1 Cisco Cyber Threat Defense Solution 1.1 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)SE3	Universal and IP Services
Cisco Catalyst 4500E Series	Supervisor 7E	Cisco IOS Software Release 15.0(2)X0	Universal and IP Base
	Supervisor 7L-E	Cisco IOS Software Release 15.0(2)X0	Universal and IP Base
Cisco Catalyst 6500 Series	Supervisor 2T	Cisco IOS Software Release 15.0(1)SY2	Advanced Enterprise Services, Advanced IP Services and IP Base
Cisco ISR G2	Any	Cisco IOS Software Release 15.2(4)M2	Universal and IP Base
Cisco ASR 1000 Series Aggregation Services Routers	Cisco ASR 1000 Series Router Processor 1 or 2 (RP1/RP2), Cisco ASR 1001 Router, Cisco ASR 1002 Fixed Router, Cisco 1004, 1006, and 1013 Routers with • Embedded Services Processor (ESP) with 10, 20, or 40 Gbps • SPA Interface Processor (SIP) 10/40	Cisco IOS Software Release 15.2(1)S or XE3.5	Universal and IP Base
Cisco Adaptive Security Appliance	Any	Cisco ASA Software Release 8.4(4)1	Any
Cisco NetFlow Generation Appliance	3140	Cisco NGA Software Release 1.0	Any
Cisco Identity Services Engine	Any (incl. VM)	Cisco ISE Software Version 1.1.1	Any
Lancope StealthWatch Management Console	Any (incl. VM)	StealthWatch 6.3	Any
Lancope StealthWatch FlowCollector	Any (incl. VM)	StealthWatch 6.3	Any

Table 1 Cisco Cyber Threat Defense Solution 1.1 Components (continued)

Lancope StealthWatch FlowSensor	Any (incl. VM)	StealthWatch 6.3	Any
Lancope StealthWatch FlowReplicator	Any (incl. VM)	StealthWatch 6.3	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 Cisco Catalyst 3560-X/3750-X Series Switches, NetFlow services are supported only 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.

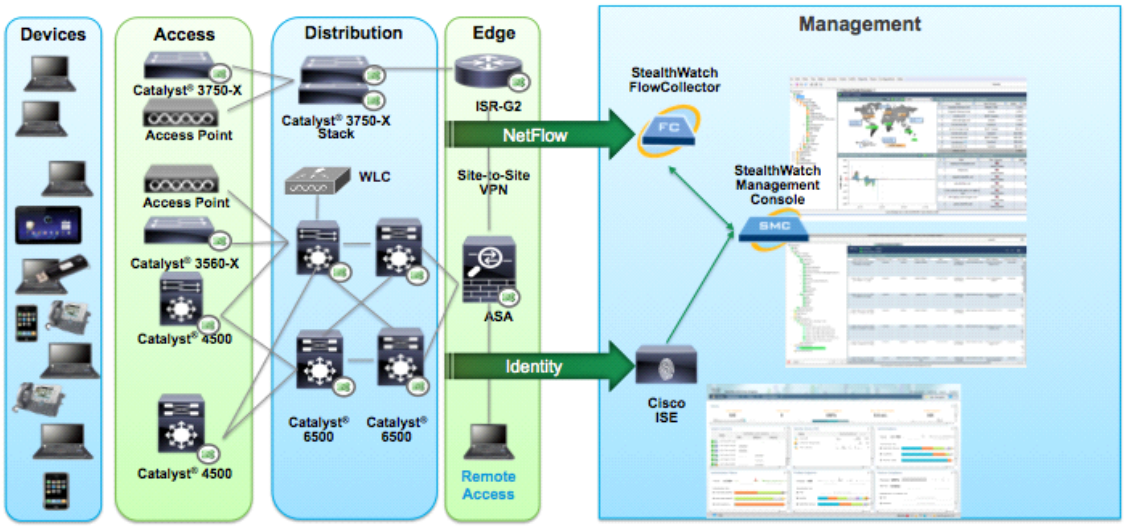
Note **Best Practice:** It may not be possible to build an entire network consisting solely of the listed Cisco network devices. To implement the pervasive visibility required by the solution in these situations, it may be necessary to use the Lancope StealthWatch FlowSensor to gain visibility into the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

Solution Overview

Architecture

The Cisco Cyber Threat Defense Solution 1.1 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. Figure 1 illustrates the high-level system architecture of the Cisco Cyber Threat Defense Solution 1.1.

Figure 1 Cyber Threat Defense Solution 1.1. Architecture



Visibility into network traffic is provided through NetFlow export from Cisco routers and switches. Identity services, including user name and profile information, are 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 1.1 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 ISE 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 gathers information about the traffic flow and reports on the information after the flow has occurred. NetFlow reporting has tremendous security applications as well, including the ability to provide non-repudiation, anomaly detection, and investigative capabilities.

NetFlow has gone through many versions since it was first introduced, as can be seen in Table 2. 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.

Table 2 NetFlow Versions

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

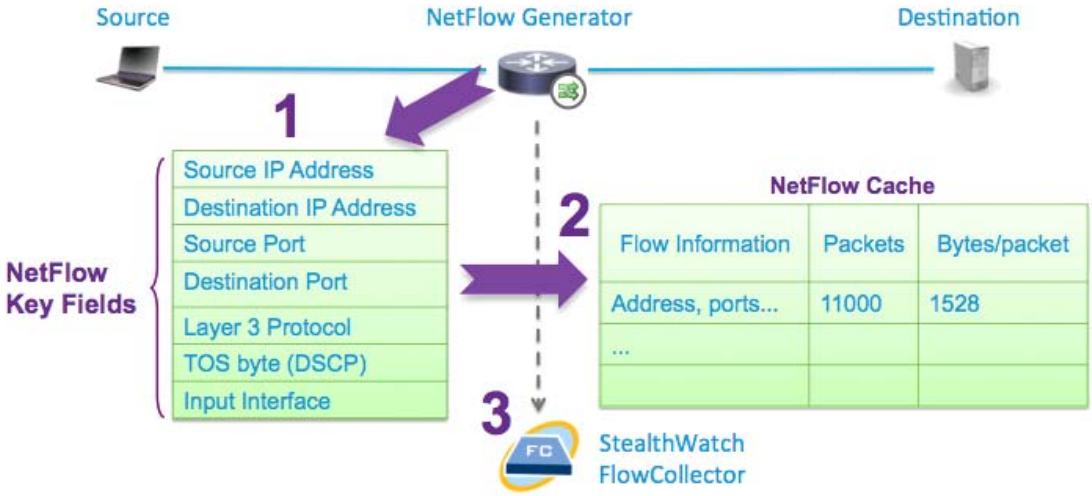
The Cisco Cyber Threat Defense Solution 1.1 takes advantage of the customization capability of the Flexible NetFlow Feature in Cisco IOS, allowing for customizable NetFlow v9 records. Using this approach, the Cisco Cyber Threat Defense Solution 1.1 has defined NetFlow records for each solution device 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; without them present, the advantages offered by some of the finely-tuned detection algorithms present in the Cisco Cyber Threat Defense Solution 1.1 would be lost.

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

Figure 2 illustrates NetFlow operation on a Cisco device.

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

Figure 2 NetFlow Operation on a Cisco Device



Selecting the Monitoring Locations

The Cisco Cyber Threat Defense Solution 1.1 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; that is, the malware that 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 that no network communication is missed.

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

A Cisco Cyber Threat Defense Solution 1.1 implementation should use NetFlow in a complete (non-sampled) manner. Sampled NetFlow leaves blind spots, because only a certain percentage of network flows have associated network records. This makes it difficult to detect the single traffic anomalies that indicate malicious activity.

Some older Cisco devices, as well as the Cisco Integrated Services Routers (ISRs) and Cisco Aggregated Services Routers (ASRs), support NetFlow services using a software implementation of the feature set. Give some consideration to a software router's current utilization when deploying software-supported NetFlow services, because NetFlow enablement can impact device performance; for instance, a fully loaded software router running Cisco IOS Software can experience an approximate 15 percent CPU uptick resulting from NetFlow enablement. When implementing software-supported NetFlow services, consult the Cisco NetFlow Performance Analysis whitepaper at the following URL: http://www.cisco.com/en/US/solutions/collateral/ns341/ns524/ns562/ns583/net_implementation_white_paper0900aecd80308a66.pdf.

Cisco devices with hardware-supported NetFlow suffer minimal performance degradation when NetFlow services are enabled. The most significant performance limitation in these devices is the size of the NetFlow cache supported by the hardware. Table 3 shows whether CTD 1.1 solution components are supported in hardware or software.

Table 3 NetFlow Support—Hardware or Software

Component	Hardware Support	Software Support
Cisco Catalyst 3560-X or 3750-X Series	X	
Cisco Catalyst 4500E Series	X	
Cisco Catalyst 6500 Series	X	
Cisco NetFlow Generation Appliance	X	
Cisco ISR G2		X
Cisco ASR 1000 Series		X
Cisco Adaptive Security Appliance		X[1]

1. The ASA NetFlow implementation, known as NetFlow Security Event Logging (NSEL) is different than most software supported NetFlow implementations. See the section regarding the ASA in this guide for more information.

Table 4 shows the cache size limitations of the solution devices with hardware-supported NetFlow. When the NetFlow cache on a device is full, the device does not generate NetFlow Records for new flows transiting the device.

Table 4 NetFlow Cache Size Limitations on Cisco Devices

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

Although every NetFlow generation device in the Cisco Cyber Threat Defense Solution 1.1 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. Table 5 lists flow record support across solution devices. Given the disparity in support, best results are obtained if there is a heterogeneous mix of solution components in the deployment to fill visibility gaps.

Table 5 Flow Record Support

Ideal Solution Flow Record	Cisco Catalyst 3560-X/ 3750-X	Cisco Catalyst 4500 Sup7-E/ Sup7L-E	Cisco Catalyst 6500 Sup2T	Cisco ISR	Cisco ASR 1000	Cisco NGA
match ipv4 tos	Yes	Yes	Yes	Yes	Yes	Yes
match ipv4 protocol	Yes	Yes	Yes	Yes	Yes	Yes
match ipv4 source address	Yes	Yes	Yes	Yes	Yes	Yes

Table 5 Flow Record Support (continued)

match ipv4 destination address	Yes	Yes	Yes	Yes	Yes	Yes
match ipv4 destination address	Yes	Yes	Yes	Yes	Yes	Yes
match transport destination-port	Yes	Yes	Yes	Yes	Yes	Yes
match interface input	Yes	Yes	Yes	Yes	Yes	Yes
match datalink mac source-address	Yes	No	No	No	No	No
match datalink mac destination-address	Yes	No	No	No	No	No
collect routing next-hop address ipv4	No	No	No	Yes	Yes	Yes
collect ipv4 dscp	No	Yes	No	Yes	Yes	Yes
collect ipv4 ttl minimum	match ipv4 ttl	Yes	No	Yes	Yes	Yes
collect ipv4 ttl maximum	match ipv4 ttl	Yes	No	Yes	Yes	Yes
collect transport tcp flags	No	Yes	Yes	Yes	Yes	Yes
collect interface output	Yes	Yes	Yes	Yes	Yes	No
collect counter bytes	Yes	Yes	Yes	Yes	Yes	Yes
collect counter packets	Yes	Yes	Yes	Yes	Yes	Yes
collect timestamp sys-uptime first	Yes	Yes	Yes	Yes	Yes	Yes
collect timestamp sys-uptime last	Yes	Yes	Yes	Yes	Yes	Yes
collect application name	No	No	No	Yes	Yes	No

Note **Best Practice**: Although not every Cisco network device needs to be present in the deployment for the solution to function, Cisco recommends that a heterogeneous mix of the listed devices be deployed because of the differences in NetFlow support across each platform.

After the monitoring location and the NetFlow generation device are selected, NetFlow must be enabled on that device. See 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 must be able to receive and analyze; this number must be taken into consideration when selecting the StealthWatch FlowCollector model (described in a subsequent section).

Determining the fps number before the deployment of the Cisco Cyber Threat Defense Solution 1.1 requires careful thought. Many factors can affect the volume of flows generated by the network devices, so predicting the exact number can be difficult. In general, a NetFlow generator generates between 1000 and 5000 fps per 1 Gbps of traffic passing through it; however, this is a general guideline and should be used only as a starting point.

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

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

- Flows per second
- NetFlow record size. The Cyber Threat Defense Solution 1.1 recommends NetFlow v9, which results in an average of 34 NetFlow Records per 1500-byte packet.
- Flow timers (active and inactive timeouts for a flow). The Cyber Threat Defense Solution 1.1 recommends an active timer of 60 seconds and an inactive timer of 15 seconds.

To predict the impact of enabling NetFlow, use the Lancope NetFlow Bandwidth Calculator, available at the following URL:
http://www.lancope.com/resource-center/netflow-bandwidth-calculator-stealthwatch-calculator/

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

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

After 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 1.1 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 1.1. Table 6 briefly introduces and describes each component in the Lancope StealthWatch System.

Table 6 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

Adding StealthWatch FlowSensors (Optional)

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 1.1. Additionally, the StealthWatch FlowSensor can be used to add packet-level application identification and performance metrics for key areas of the network.

Perform the following steps when considering adding a StealthWatch FlowSensor to a Cisco Cyber Threat Defense Solution 1.1 deployment.

Procedure

Step 1 Choose a StealthWatch FlowSensor.

When choosing a StealthWatch FlowSensor, consider the expected traffic profile of the monitoring point, because 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 1.1, Cisco recommends that the FlowSensor be deployed as close to the access layer as possible.

Table 7 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.

Table 7 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. Table 8 describes the requirements for the deployment of the StealthWatch FlowCollector VE.

Table 8 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. Sample deployment modes include using Test Access Ports (TAPs), Switched Port Analyzer (SPAN) ports, or a network hub. See the *System Hardware Installation Guide* on the Lancope StealthWatch Documentation CD for detailed information on how to integrate the StealthWatch FlowSensor into the network.

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 1.1. 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

Procedure

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), providing the benefit of a single collection location and possibly a single IP address globally for NetFlow collection. This deployment offers advantages in environments where NetFlow generators are far apart.

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

In an ideal implementation, every router that exports data related to a particular flow sends that data to the same FlowCollector. However, each unique host pair (or conversation) consumes additional resources on the FlowCollector. If the number of simultaneous connections gets too high, flow records are purged from memory. Take care during deployment planning to ensure that each FlowCollector has sufficient resources to keep state on all active conversations without purging records until after the conversations have been idle for some time.

Note **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 Table 9. However, also consider the following factors in the selection of a StealthWatch FlowCollector for the Cisco Cyber Threat Defense Solution 1.1:

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

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

Table 9 StealthWatch FlowCollector Appliance Specifications

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

Table 10 lists the support for a StealthWatch FlowCollector VE based on the amount of reserved memory and the number of CPUs for the VM.

Table 10 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

Choosing a StealthWatch Management Console

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

Table 11 shows the SMC models and the number of StealthWatch FlowCollectors they can support. Table 12 lists the number of FlowCollectors and concurrent users (based on reserved memory and CPUs) that the SMC VE can support.

Table 11 SMC Appliance Specifications

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

Table 12 SMC VE Specifications

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

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

Choosing a StealthWatch FlowReplicator (Optional)

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. Table 13 lists the StealthWatch FlowReplicator models and specifications.

Table 13 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 are dropped.

Deploying the Lancope StealthWatch System

This section describes the procedures necessary to deploy each appliance in the Lancope StealthWatch System and prepare it for operation in the Cisco Cyber Threat Defense Solution 1.1.

Install Each Appliance

To install each appliance, perform the following steps.

Procedure

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, Cisco recommends that the primary and secondary SMCs be installed in separate physical locations. See 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 1.1, the FlowSensor is most effective when placed such that it can monitor access layer traffic. See 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. See 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. See 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. See 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 into promiscuous mode for monitoring.

Configure the Firewall

If a firewall is present anywhere in the deployment, consult Figure 3 illustrating the data flows in the Cyber Threat Defense Solution 1.1 to ensure that the appropriate ports and services are allowed. Table 14 further highlights the required services. See the *System Hardware Installation Guide* on the Lancope StealthWatch Documentation CD for additional information.

Figure 3 Cisco Cyber Threat Defense Solution 1.1 Data Flows

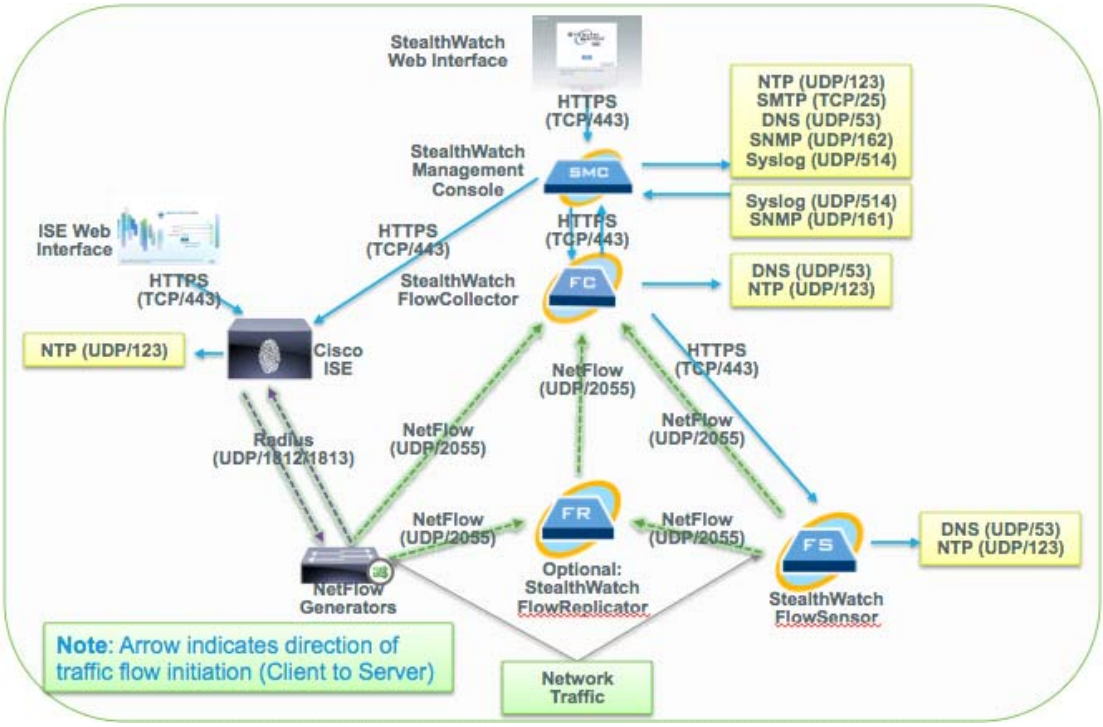


Table 14 Required Services

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)

Table 14 Required Services (continued)

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

Run the System Configuration on each Appliance

The system configuration dialog is used to initialize the networking and access information for each StealthWatch component. The dialog 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.

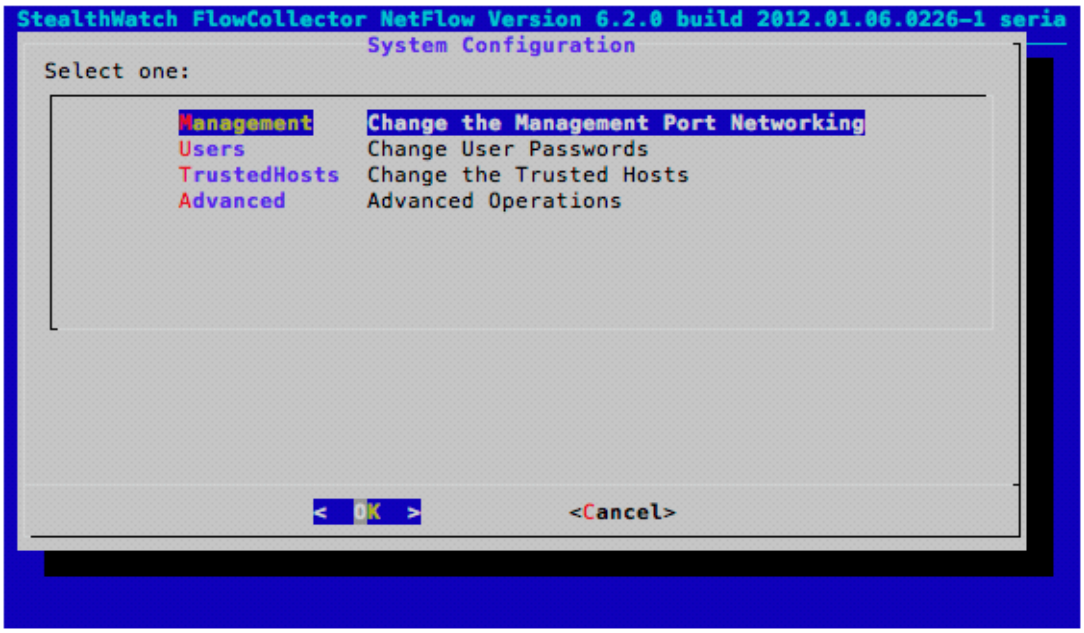
Procedure

Step 1 Log into the appliance through the console interface.

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

Step 2 Run the System Configuration program. A screen similar to the one in Figure 4 is displayed.

Figure 4 System Configuration Screen



Note See Chapter 1 of the StealthWatch *System Configuration Guide* for additional information.

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

Step 3 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 is used to access the appliance through the web interface.

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

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

Step 4 Change the user passwords.

Change the password that is used to access the console interface. This is also the password that is 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 5 Configure the trusted host settings (optional).

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

Log into the Web Interface of Each Appliance

Procedure

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.

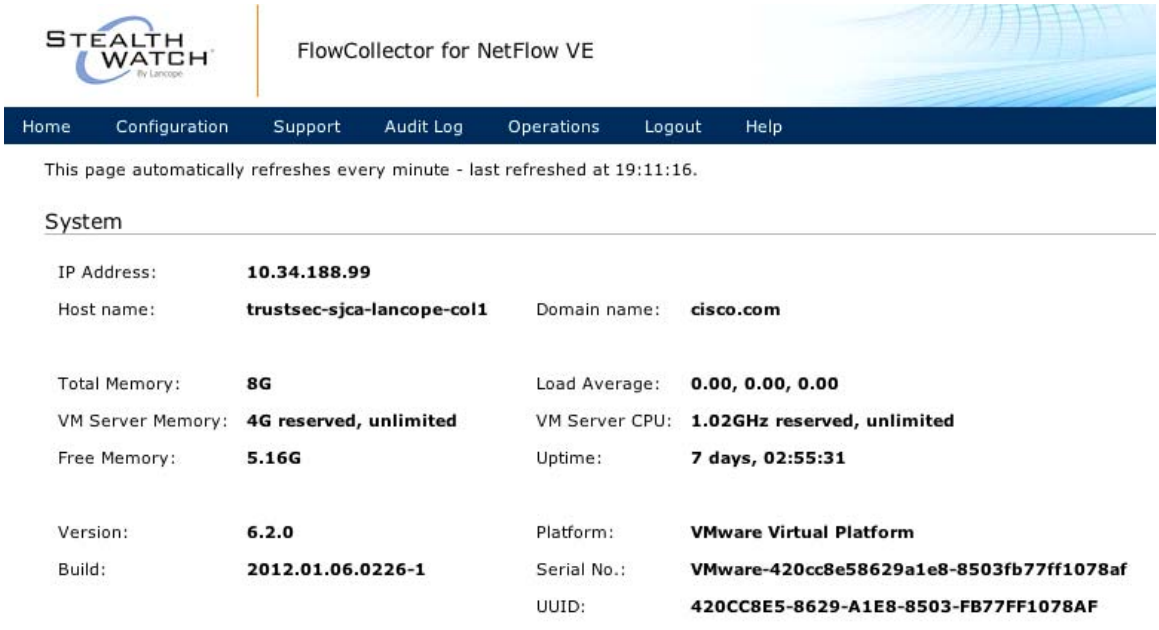
Step 2 Access the web interface of the SMC.

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 than 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 Figure 5.

Figure 5 StealthWatch FlowCollector Web Interface



Note See Chapter 6 of the *System Configuration Guide* for detailed information.

Configure the Host Name and DNS Settings

Procedure

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**.

Configure Time Settings

Procedure

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.

Note **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 in which the StealthWatch appliance is located.

Step 7 Click **Apply**.

Configure the Admin Password

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

Procedure

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**.

Configure the Certificate Authority Certificates

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

Note **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.

Procedure

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**.

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.

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**.

(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 1.1.

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

Procedure

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**.

Restart the Appliance

In the above procedures, changes were made to the host and time settings of the appliance. At this moment, Cisco strongly recommends restarting the appliance to ensure that 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

After completing the procedures in the previous section, the two mandatory Lancope StealthWatch appliances (FlowCollector and SMC) should now be deployed and 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 now receive NetFlow records from the NetFlow exporters and begin populating its database. If desired, you can skip ahead in this document and configure NetFlow export on the NetFlow exporters so they 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 preparing the StealthWatch System for NetFlow analysis.

Run the SMC Client Software

Procedure

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.

Step 3 Consider larger memory allocation if many open documents or large data sets (such as flow queries over 100,000 records) are expected. The local workstation should have at least twice the memory allocation selected.

Step 4 Click **Start** to download and install the SMC client software.

Configure the Domain

When first logging in to the SMC client, the Default Domain Properties Page is 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, and so on.

Note **Best Practice:** Use a single domain for the Cisco Cyber Threat Defense Solution 1.1 deployment for the enterprise.

Procedure

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

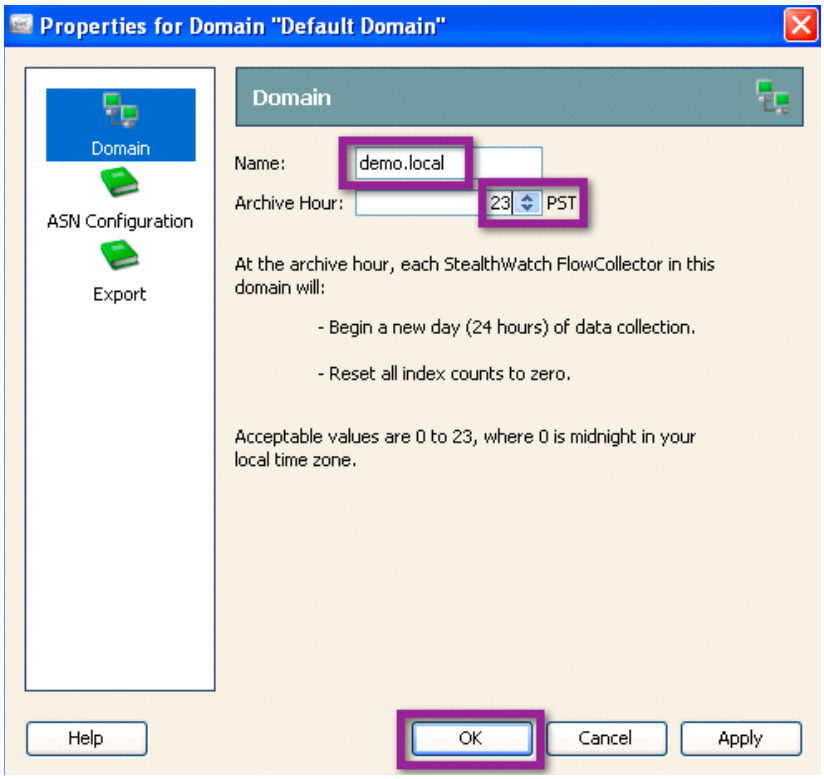
Step 2 In the Archive Hour Field, specify the archive hour.

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

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

Step 3 Click **OK**, as shown in Figure 6.

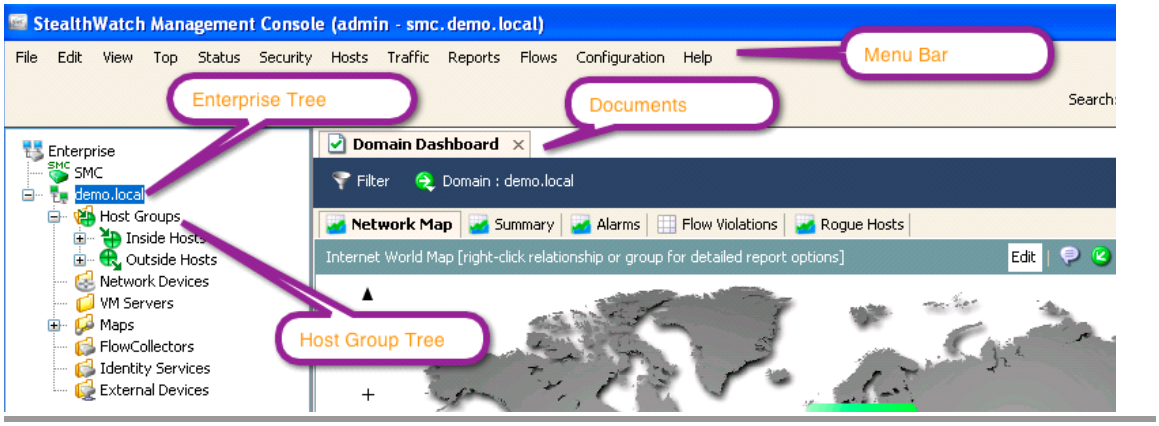
Figure 6 Setting the Archive Hour



Step 4 Become familiar with the SMC display (see Figure 7).

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 are displayed.

Figure 7 Setting the Archive Hour



Adding the StealthWatch FlowCollector

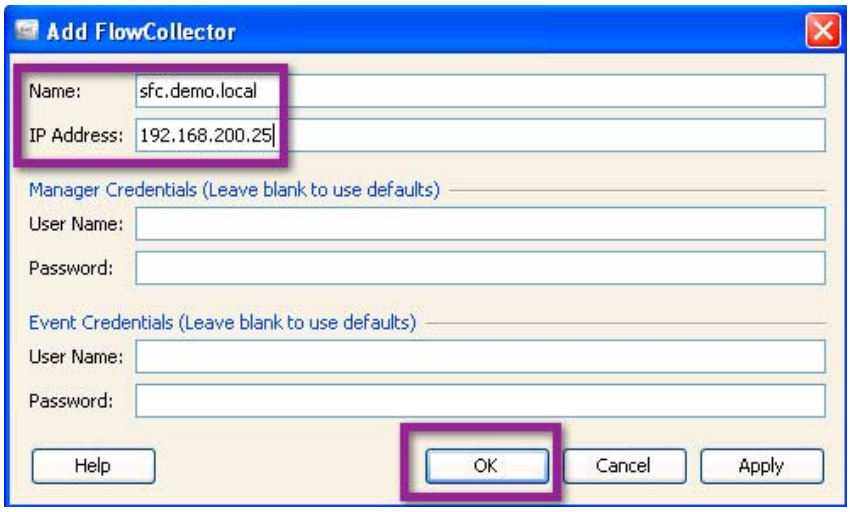
Procedure

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 (see Figure 8).

Figure 8 Add 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 opens. Verify the default configuration using Table 15.

Table 15 Default Configuration Details

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

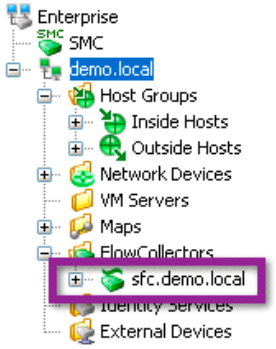
Table 15 Default Configuration Details (continued)

	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**, and then click **Close**.

Step 8 Expand the Enterprise Tree to view the FlowCollector (see Figure 9).

Figure 9 Viewing 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

As previously mentioned, the Cisco Cyber Threat Defense Solution 1.1 uses the Flexible NetFlow capabilities of specific Cisco platforms. This section provides a brief overview of the concepts and steps required to configure Flexible NetFlow on Cisco IOS, and then provides detailed configuration and troubleshooting guidance for the Cisco devices that are components of the Cisco Cyber Threat Defense Solution 1.1 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:

- Configure a Flow Record
- Configure a Flow Exporter
- Create the Flow Monitor
- Apply the Flow Monitor to one or more interfaces

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 NetFlow 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 1.1 defines a specific flow record for each supported device; Cisco strongly recommends that these flow records be 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.

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 1.1. Note that this configuration might differ from NetFlow configurations in older Cisco IOS and platform releases.

Create the Flow Monitor

A Flow Monitor describes the NetFlow cache or information stored in the cache. Additionally, the Flow Monitor links 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 (for example, no new packets received for the flow); or if the flow is long lived (active) and lasts greater than the active timer (for example, long FTP download). There are timers to determine whether a flow is inactive or long lived.

Note **Best practice:** The Cisco Cyber Threat Defense Solution 1.1 recommends an active timeout of 60 seconds and an inactive timeout of 15 seconds.

Apply the Flow Monitor to an Interface

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

Note **Best Practice:** The Cisco Cyber Threat Defense solution 1.1 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 Cisco 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 1.1. Previously, the visibility provided by NetFlow was available only 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 Cisco Catalyst 3500 Series are supported only on the Cisco Catalyst 3500-X Series (3560-X and 3750-X) platforms with the 10GE Service Module. Note that it is the service module that enables the NetFlow feature: NetFlow data is generated only for traffic that traverses the module. As such, the service module becomes a crucial component in the Cisco Cyber Threat Defense Solution 1.1.

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; for example, flows that enter or leave on a trunk port. The service module does not support “East-West” NetFlow; this means that NetFlow is not generated for traffic that does not traverse the service module; for example, traffic that is locally switched. Because one of the objectives of the Cisco Cyber Threat Defense Solution 1.1 is to gain visibility into locally switched traffic, consider deployment options carefully.

NetFlow is supported in hardware on the service module. The hardware is capable of supporting 32,000 flows in its resident cache. Note that this number does scale within a stack of Cisco 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

To operate correctly, the service module must be installed in a supporting hardware platform and have the correct Cisco IOS Software image and license. Table 16 lists the minimal requirements to enable Flexible NetFlow on the service module.

Table 16 Cisco Catalyst 3500-X Series Service Module Requirements

Component	Requirement
Minimum hardware	Version ID: 02 Revision: 0x03
Cisco IOS Software	15.0(1)SE3
License	IP Services

Note The service module has its own operating system. To function properly, the operating system on the service module must match the operating system on the switch itself.

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.

Procedure

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 is 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 provides 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 must be made when cabling the service module into a copper network.

Note **Best Practice:** Use standard 10GbE copper cables (requires the aggregation/core switches to have an available 10GbE port).

Note **Best Practice:** Use multi-mode Gigabit Ethernet Fibre SFP (GLC-SX-MM) with a media converter.

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 use the Flexible NetFlow capabilities of the Cisco Catalyst 3500-X Series as an access layer switch.

Configure the Flow Record

Procedure

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 sample 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.

Configure the Flow Exporter

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

Procedure

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 <SVI Interface>
```

This setting is the IP address from which the switch sources NetFlow records. Best practice is to define a loopback or SVI 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
```

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

Create the Flow Monitor

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

Procedure

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. Cisco recommends using a value of 60 seconds.

```
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. Cisco recommends that a value of 15 seconds be used.

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

Apply the Flow Monitor to the Interfaces

Procedure

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
```

Verify

Procedure

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

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

Verify that NetFlow records are being exported from the appliance and are being received by the FlowCollector. (Details are provided in the Flexible NetFlow Export Verification section below.)

Final Cisco 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 <SVI-interface>
 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?
!
```

Note For more details, see *Cisco Catalyst 3K-X Service Module: Enabling Flexible NetFlow in the Access* at the following URL: 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 Cisco 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 1.1 recommends deployment of the Cisco 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. Although 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 1.1.

The Cisco 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 (Cisco 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.

Because Cisco 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 1.1 recommends using the same configuration for both to keep the configuration as simple as possible while maintaining complete functionality.

Configure the Flow Record

Procedure

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

Configure the Flow Exporter

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

Procedure

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 <SVI Interface>
```

This setting is the IP address from which the switch sources NetFlow records. Best practice is to define a loopback or SVI 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
```

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

Create the Flow Monitor

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

Procedure

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. Cisco recommends 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. Cisco recommends that a value of 15 seconds be used.

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

Apply the Flow Monitor to the Interfaces

Procedure

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
```

Verify

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

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

Verify that NetFlow records are being exported from the appliance and are being received by the FlowCollector. (Details are provided in the Flexible NetFlow Export Verification section below.)

Final Cisco 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 <SVI-interface>
 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
!
```

Note For more details, see *Cisco Catalyst 4500 Series Switch Software Configuration Guide, Release IOS-XE 3.1.0 SG: Configuring Flexible NetFlow* at the following URL: 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 Cisco 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. Table 17 highlights the improved NetFlow feature set of the Supervisor Engine 2T.

Table 17 Cisco 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 6500 Series modules will support this ability.

Flexible NetFlow Configuration

This section describes the steps to implement the recommended level of flow visibility necessary for the Cisco Cyber Threat Defense Solution 1.1 on the Supervisor Engine 2T.

Because Cisco 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, this guide recommends using the same configuration for both to keep the configuration as simple as possible while maintaining complete functionality.

Configure the Flow Record

Procedure

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.

Configure the Flow Exporter

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

Procedure

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 <SVI-interface>
```

This setting is the IP address from which the switch sources NetFlow records. Best practice is to define a loopback or SVI 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
```

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

Create the Flow Monitor

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

Procedure

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. Cisco recommends 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. Cisco recommends that a value of 15 seconds be used.

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

Apply the Flow Monitor to the Interfaces

On a Cisco Catalyst 6500 Series Switch, a flow monitor can be applied only 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.

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

Procedure

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
```

Verify

Procedure

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

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

Verify that NetFlow records are being exported from the appliance and are being received by the FlowCollector. (Details are provided in the Flexible NetFlow Export Verification section below.)

Final Cisco 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 <SVI-interface>
```

```
  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
!
```

Note For more details, see *Cisco Catalyst 6500 Supervisor Engine 2T: NetFlow Enhancements* at the following URL:
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 Cisco 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. Take care when deploying software-supported NetFlow services, because the feature can affect device performance; for instance, a fully loaded ISR running Cisco IOS Software can experience an approximate 15 percent CPU uptick resulting from NetFlow enablement.

When implementing software-supported NetFlow services, consult the Cisco NetFlow Performance Analysis whitepaper at the following URL:
http://www.cisco.com/en/US/solutions/collateral/ns341/ns524/ns562/ns583/net_implementation_white_paper0900aecd80308a66.pdf

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 use the Flexible NetFlow and NBAR capabilities of the Cisco ISR G2.

Configure the Flow Record

Procedure

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 1.1 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 Using NBAR services on the router can affect the performance of the router. Although the collection of the application name is of great value in the Cisco Cyber Threat Defense Solution 1.1, enabling NBAR services must be done carefully.

Configure the Flow Exporter

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

Procedure

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 from which the switch sources NetFlow records. 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
```

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

Create the Flow Monitor

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

Procedure

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. Cisco recommends 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. Cisco recommends that a value of 15 seconds be used.

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

Apply the Flow Monitor to an Interface

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

Procedure

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
```

Verify

Procedure

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

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

Verify that NetFlow records are being exported from the appliance and are being received by the FlowCollector. (Details are provided 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
!
```

Note For more details, see the *NetFlow Configuration Guide, Cisco IOS Software Release 15.2 M&T* at the following URL: http://www.cisco.com/en/US/partner/docs/ios-xml/ios/fnetflow/configuration/15-mt/fnf-15-mt-book.html

Cisco ASR 1000 Series

Flexible NetFlow support on Cisco ASR 1000 Series routers adheres to the platform-independent implementation of NetFlow as documented in Cisco IOS guides. NetFlow support on the ASR takes the traditional NetFlow approach of collecting information and generating a NetFlow record for flows that cross a Layer 3 boundary. This makes the ASR a key component in providing visibility into flows that traverse different areas of the network.

Design Considerations

The Cisco ASR 1000 contains software-supported 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.

Because NetFlow and NBAR are implemented as software services on the ASR 1000 Series, care should be taken when deploying these features, as they can have an impact on device performance.

Configuring NetFlow Export

Configure the Flow Record

The flow record configuration defines which data fields are collected for each flow.

Procedure

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

```
ASR(config)#flow record CYBER_ASR_RECORD
ASR(config-flow-record)#match ipv4 tos
ASR(config-flow-record)#match ipv4 protocol
ASR(config-flow-record)#match ipv4 source address
ASR(config-flow-record)#match ipv4 destination address
ASR(config-flow-record)#match transport source-port
ASR(config-flow-record)#match transport destination-port
ASR(config-flow-record)#match interface input
```

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

Taking advantage of the NetFlow version 9 formatting and the ASR's role as a Layer 3 boundary allows the collection of many Layer 3 and 4 fields that are not always available on switch-based implementations of NetFlow, such as Time-To-Live values, TCP flags and next-hop addresses.

Note that the above flow record enables the collection of the name of the application from NBAR using the *collect application name* option. If NBAR is not being run, this line may be omitted.

Note NBAR services can affect the performance of the router; although the collection of the application name is of great value in the Cisco Cyber Threat Defense Solution, enabling NBAR services must be done carefully.

Configure the Flow Exporter

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

Procedure

Step 1 Define the exporter.

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

Step 2 (Optional) Add a description.

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

Step 3 Define the source.

```
ASR(config-flow-exporter)#source Loopback 1
```

This setting is the IP address that the switch will use as the source of the NetFlow export records. The best practice is to define a loopback interface (Loopback 1 in the example shown) with an IP address on a management VLAN and use that interface as the source. Note that the loopback interface must be configured before it can be used as a flow export source.

Step 4 Define the destination IP address.

```
ASR(config-flow-exporter)#destination ip-address-of-FlowCollector
```

Step 5 Define the transport protocol.

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

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

Create the Flow Monitor

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

Procedure

Step 1 Define the flow monitor.

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

Step 2 (Optional) Add a description.

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

Step 3 Configure the flow record.

```
ASR(config-flow-monitor)#record CYBER_ASR_RECORD
```

Step 4 Configure the exporter.

```
ASR(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.

```
ASR(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. Cisco recommends that a value of 15 seconds be used.

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

Apply the Flow Monitor to an Interface

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

Procedure

Step 1 Enter interface configuration mode.

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

Step 2 Apply the Flow Monitor on ingress traffic.

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

Verify

Procedure

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

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

Step 2 Verify that NetFlow records are being exported from the appliance and are being received by the FlowCollector. (Refer to the Design and Implementation Guide for details.)

Final Configuration

```
!
flow record CYBER_ASR_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_ASR_RECORD
 exporter CYBER_EXPORTER
 cache timeout active 60
?cache timeout inactive 15
!
!
interface GigabitEthernet0/0/0
 ip address <ip-address> <net-mask>
 ip flow monitor CYBER_MONITOR input
!
```

Note For more details, see the *NetFlow Configuration Guide, Cisco IOS XE Release 3S (ASR 1000)* at the following URL: http://www.cisco.com/en/US/docs/ios-xml/ios/netflow/configuration/xe-3s/asr1000/nf-xe-3s-asr1000-book.pdf

Cisco NetFlow Generation Appliance

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

Design Considerations

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

The NGA can be placed to receive data from the physical access, aggregation, and core layers. The objective is to ensure complete visibility of all traffic within the data center, as well as traffic that is leaving the data center. Traffic within the virtual environment (VM-to-VM traffic) can be monitored using the StealthWatch FlowSensor VE, while traffic entering and leaving the data center can be monitored using edge devices such as the ASA. Strategically placing the NGA in the aggregation and core layers ensures effective monitoring of traffic within the data center, as well as providing additional statistics for traffic leaving the data center. The Cisco NGA is very scalable and can support up to 64 million active flows. Refer to *Quick Start Guide for Cisco NetFlow Generation Appliance 3140* for more detailed information on the installation.

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

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

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

Flexible NetFlow Configuration

After the Cisco NGA has been deployed and it is receiving copies of network traffic (see the Cisco Cyber Threat Defense Solution 1.1 How-to Guide: *Gain Visibility in the Data Center with the Cisco NetFlow Generation Appliance* for details), it is necessary to configure Flexible NetFlow export. Flexible NetFlow configuration on the Cisco NGA can be done either through the web interface or directly from the CLI; this section describes a validated configuration using the Cisco NGA web Interface.

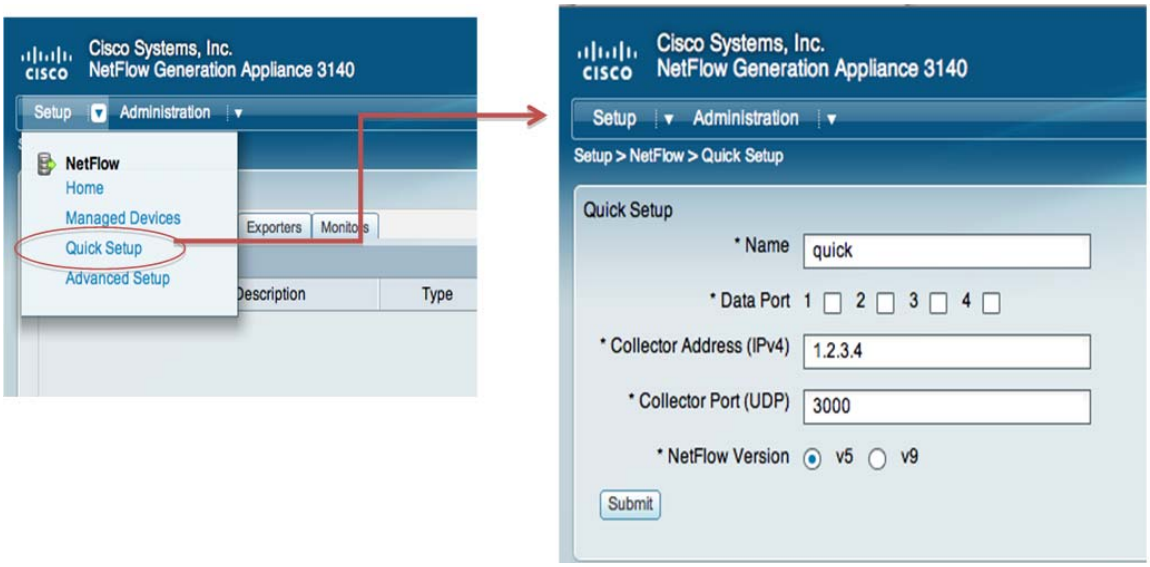
Perform Quick Setup NetFlow Configuration

This is the easiest and simplest configuration to export v5 or v9 NetFlow packets to a collector.

Procedure

Step 1 Click **Setup** > **Quick Setup**, as shown in Figure 10.

Figure 10 Quick Setup



Step 2 Define a name.

Enter a unique name to identify this configuration.

Step 3 Define one or more data ports.

Check the check box for each appliance data port that will accept incoming packets.

Step 4 Define a collector address.

Enter the IP address for the collector in the Collector Address field.

Step 5 Define a UDP collector port.

Enter the port on which the collector device is listening. This is typically configurable on the collector device. StealthWatch by default expects NetFlow on UDP port 2055.

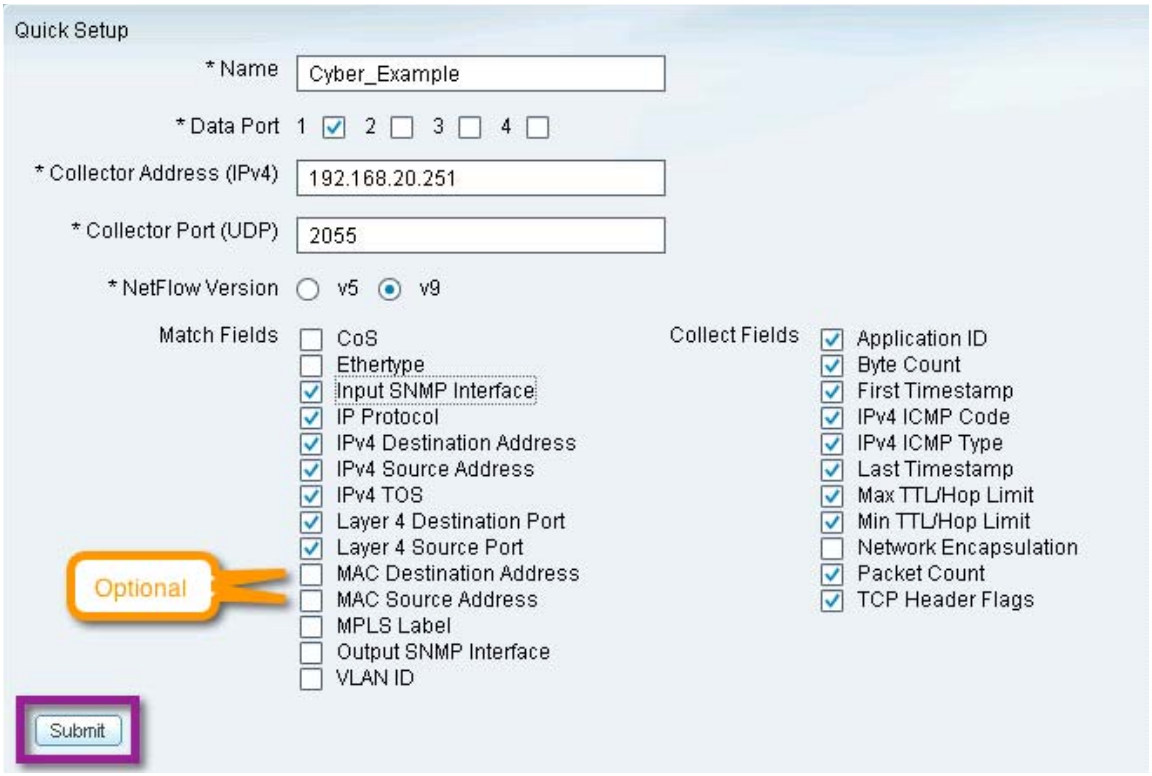
Step 6 Define the NetFlow version.

Select version 5 to configure the appliance to perform standard NetFlow version 5 monitoring and export. You do not need to select individual record fields because they are predetermined by the NetFlow version 5 standard.

Select which version 9 fields you want to include in your monitoring/collecting.

Note **Best Practice:** Use version 9 and select the fields as illustrated in Figure 11.

Figure 11 Quick Setup Window



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

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

- For V5:
  - A collector named *Cyber_Example_collector*
  - An exporter named *Cyber_Example_exporter*
  - A monitor named *Cyber_Example _monitor*
- For V9:
  - A collector named *Cyber_Example_collector*
  - An exporter named *Cyber_Example_exporter*
  - A monitor named *Cyber_Example_monitor*
  - A record named *Cyber_Example_record*

Step 8 Select **Cyber_Example_monitor** in the Monitor tab and click **Activate/Inactivate**.

This enables the newly created flow monitor to generate NetFlow information for the input traffic and send it to the StealthWatch FlowCollector.

Refer to *Cisco NetFlow Generation Appliance (NGA) 3140 User Guide* under section *Setting Up Multiple NetFlow Monitor Instances* for advanced information on creating filters, setting up multiple collectors, records, exporters and monitors.

Cisco ASA 5500 Series Adaptive Security Appliances

About NetFlow Security Event Logging

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

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

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

- Flow Create
- Flow Tear Down
- Flow Denied

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

- NSEL is bidirectional. A connection through a Cisco IOS device generates two flows, one for each direction, whereas NSEL sends a single flow per connection.
- NSEL reports a total byte count for the bi-directional flow, rather than a byte count for each direction.
- NSEL does not report a packet count.
- NSEL has predefined templates for the three event types. These templates are usually exported before any NSEL data records.

NSEL flow-export actions are not supported in interface-based policies; they can be applied only in a global service policy.

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

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

Configuring NSEL

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

Configure the NSEL Collector

Procedure

Step 1 Configure the NSEL collector.

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

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

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

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

Configure NSEL in the Global Policy

Procedure

Step 1 Enter the global_policy configuration.

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

Step 2 Enter class-default configuration.

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

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

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

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

(Optional) Tune the Template Timeout Interval

Procedure

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

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

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

(Optional) Disable Redundant Syslog Messages

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

Procedure

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
```

Verify

Procedure

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

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

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

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

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

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

Step 4 Open the Flow Table by right-clicking the ASA and selecting **Flows > Flow Table**.

Final Configuration

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

Note For more details, see *Configuring Network Secure Event Logging* (http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/monitor_nsel.html) and the Cisco ASA 5500 Series Implementation Note for NetFlow Collectors, 8.4, 8.5, and 8.6 (http://www.cisco.com/en/US/docs/security/asa/asa84/system/netflow/netflow.html)

Flexible NetFlow Export Verification

When NetFlow is configured on each device in the solution, it is necessary to verify 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 1.1. Use the following procedures to verify that the NetFlow configuration is operational.

Verify NetFlow Export on a Cisco IOS Software-based Device

Procedure

Step 1 Display the flow records present in the cache.

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

This command shows all flow records currently in the CYBER_MONITOR's memory. Assuming that 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 shows 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 that 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 shows 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.

Verify NetFlow Export on a Cisco ASA Appliance

Procedure

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

Verify NetFlow Records are being Received by the FlowCollector

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.

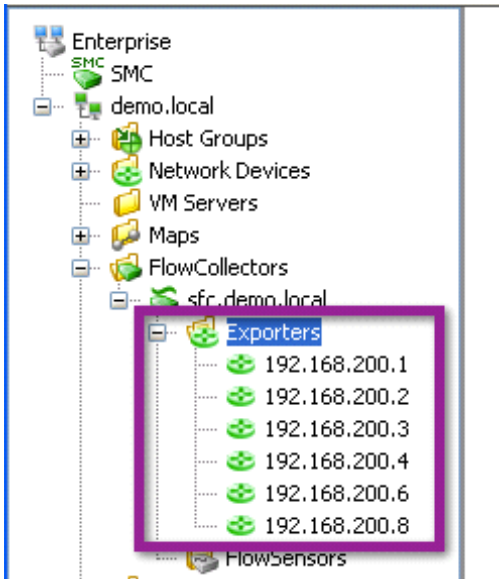
Procedure

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, as shown in Figure 12.

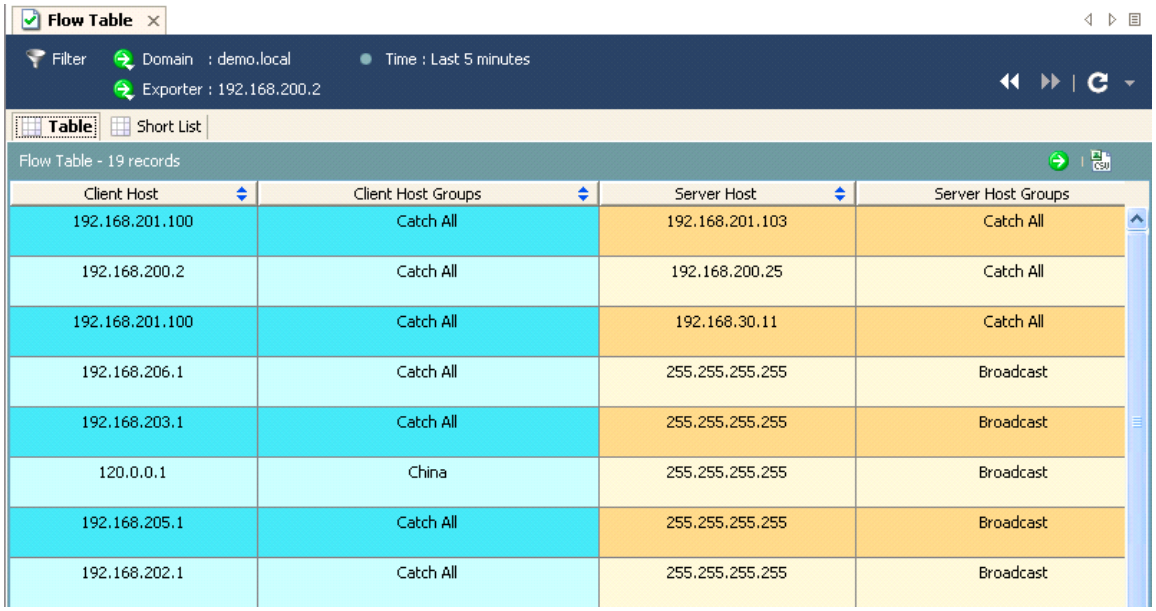
Figure 12 Expanded Tree



Step 4 Right-click the flow exporter and click **Flows > Flow Table**.

Step 5 Ensure that (expected) flow records are appearing in the table, as shown in Figure 13.

Figure 13 Flow 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

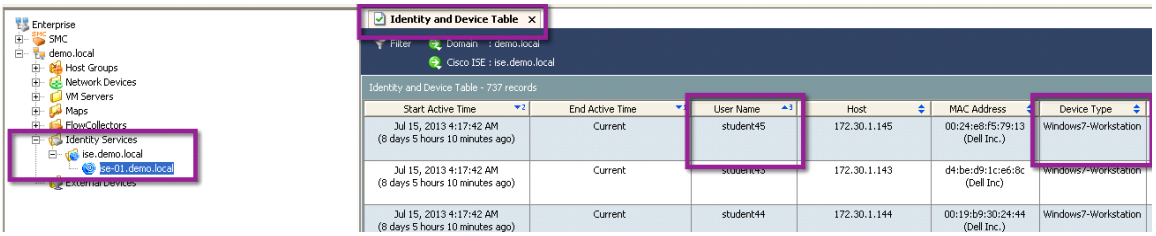
Overview

The Cisco Cyber Threat Defense Solution 1.1 is designed to operate cohesively with the Cisco TrustSec Solution, meaning that both solutions can be deployed simultaneously, and together offer administrators enhanced visibility and control over their network.

Note It is assumed that the reader is familiar with and has deployed the Cisco TrustSec Solution 2.0 or later to at least a Monitor Mode or better deployment. For more information about TrustSec, see the following URL: http://www.cisco.com/go/trustsec

Integration between the Lancope StealthWatch Management Console (SMC) and the Cisco Identity Services Engine (ISE) allows the administrator to quickly associate a user and device identity with a flow or set of flows from within the SMC console. Figure 14 shows this enhanced capability where the username, device type, and all other session information is available alongside all associated flows with an IP address. This section describes the process of integrating the Lancope SMC with a Cisco TrustSec Solution or Cisco ISE deployment to enhance the capabilities of the Cisco Cyber Threat Defense Solution.

Figure 14 Identity and Device Table



Integrating the Lancope SMC with the Cisco Identity Services Engine

StealthWatch 6.3 uses a Representational State Transfer (REST) API to collect identity information from a Cisco ISE Monitoring (MNT) node. The REST API calls are passed over a secure and authenticated HTTPS session.

Validate Identity Services Engine Monitoring Node Deployment

To successfully invoke the API call on a Cisco ISE node, the node must be deployed as a valid MNT node. This deployment can be verified by checking the ISE deployment configuration in the ISE dashboard.

Procedure

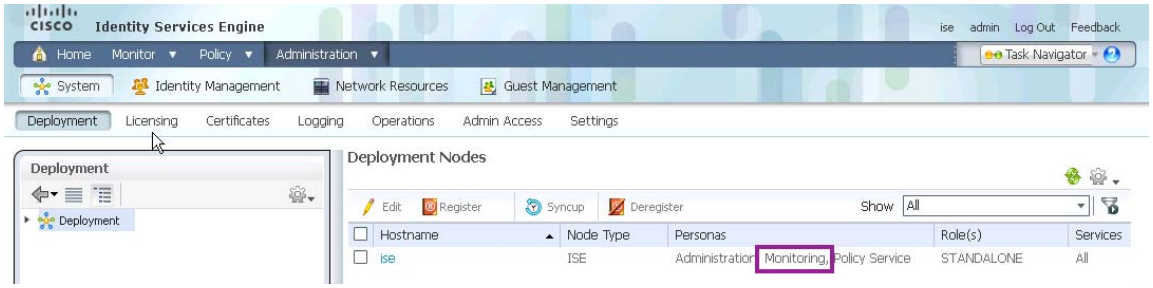
Step 1 Log in to the Cisco ISE dashboard.

Step 2 Go to **Administration > System > Deployment**.

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

Step 3 In the Role(s) 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 ISE node, as shown in Figure 15. (Note: The Standalone role includes MNT functionality.)

Figure 15 Deployment Nodes Screen



Create an Admin User on ISE for Monitoring Access

Note **Best Practice**: For the Cisco Cyber Threat Defense Solution and any deployment that makes use of the ISE REST APIs, the recommended practice is to create a separate user account on the ISE to authenticate API use.

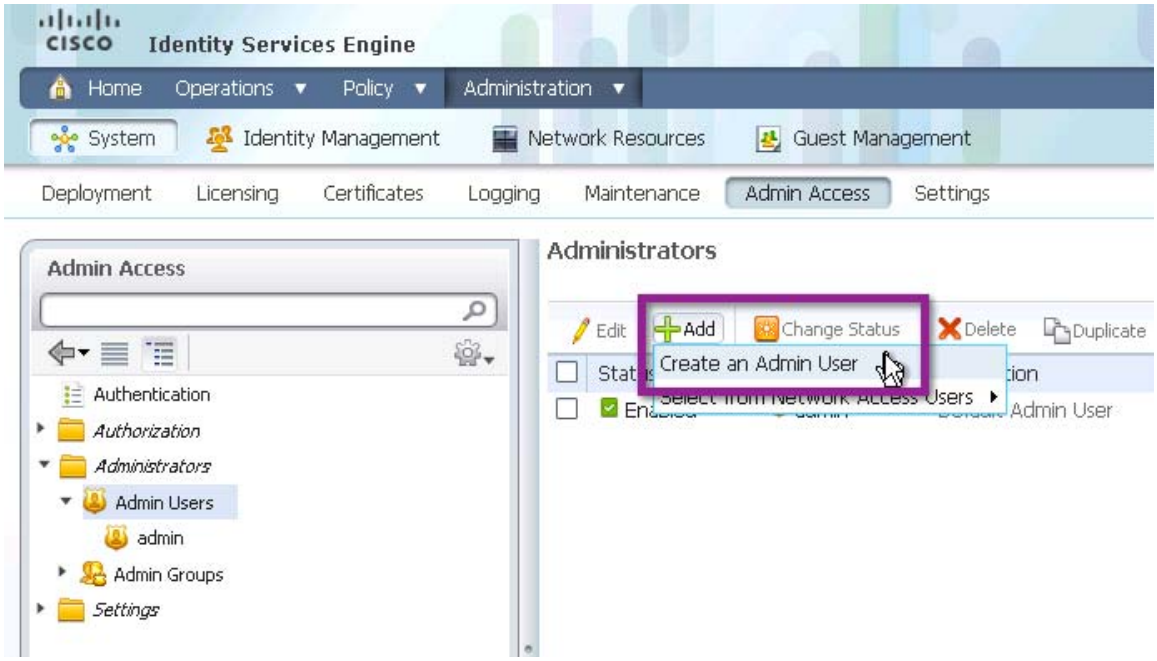
Procedure

Step 1 Log in to the ISE dashboard.

Step 2 Go to **Administration > System > Admin Access > Administrators**.

Step 3 Select **Admin Users**. Click **Add** and select **Create an Admin User**, as shown in Figure 16.

Figure 16 Creating an Admin User



Step 4 Fill out the Admin User, Password, User Information, Account Options, and Admin Groups sections (see Table 18).

Table 18 Admin User Information

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 Options	Optional: Add a meaningful description; for example: *Account used the StealthWatch 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**.

Ensure that there are Active Sessions in ISE

Procedure

Step 1 Log in to the ISE dashboard.

Step 2 Click **Operations** > **Authentications**.

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

Verify the ISE APIs are using a Web Browser

The integration between the Cisco ISE and the Lancope SMC utilizes two API calls supported by the Cisco ISE:

- Authenticated Sessions List—Retrieve a list of all currently active authenticated sessions
- Endpoint by IP Address—Retrieve authenticated session information for host by IP Address

Before continuing the integration, Cisco recommends that the Admin credentials and API operation be validated using a web browser.

Procedure

Step 1 Open a web 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

Note In this example, *ise.demo.local* is the DNS name of the ISE node. Substitute the correct DNS name or IP address of the ISE MNT node in your environment.

Step 3 Log in using the monitoring credentials from Procedure 2.

Step 4 Verify that the Authentication List is displayed.

Note The authentication list is empty if there are no active authenticated sessions maintained within the ISE. If no sessions are returned from the API, go to the ISE dashboard to validate that there are active sessions.

Step 5 Using an IP address from an active session in the ISE, call the *Endpoint 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 monitoring credentials from Procedure 2.

Step 7 Verify that the Authentication Session information is retrieved.

Configure the Certificate Authority Certificates

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

Procedure

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

Step 2 From the home page, 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**.

Register the Cisco ISE with the Lancope SMC.

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

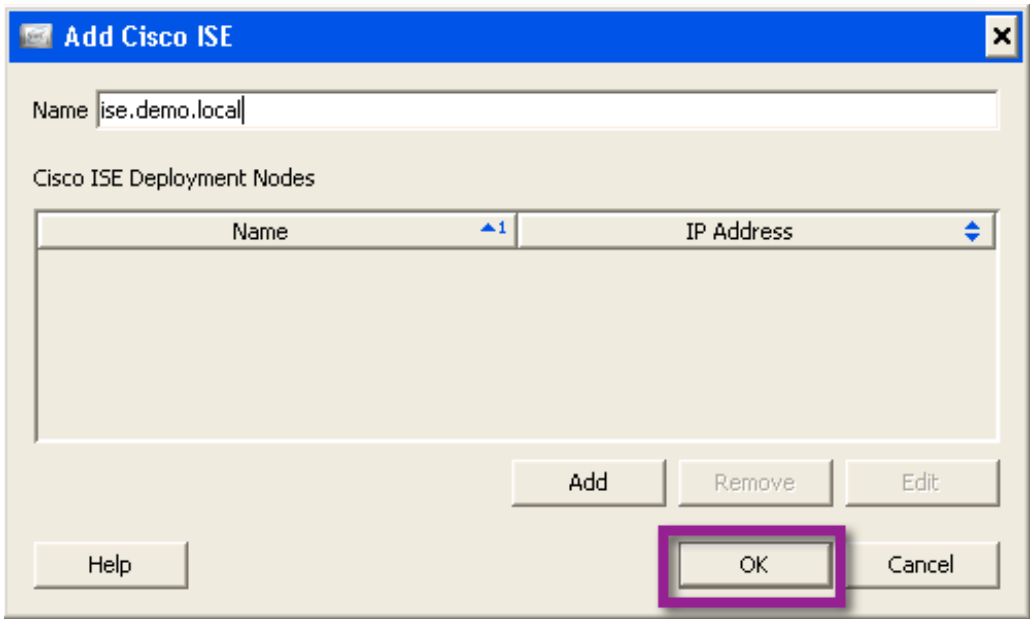
Procedure

Step 1 Log in to the SMC client software.

Step 2 Highlight the domain, then click **Configuration > Add Cisco ISE …**

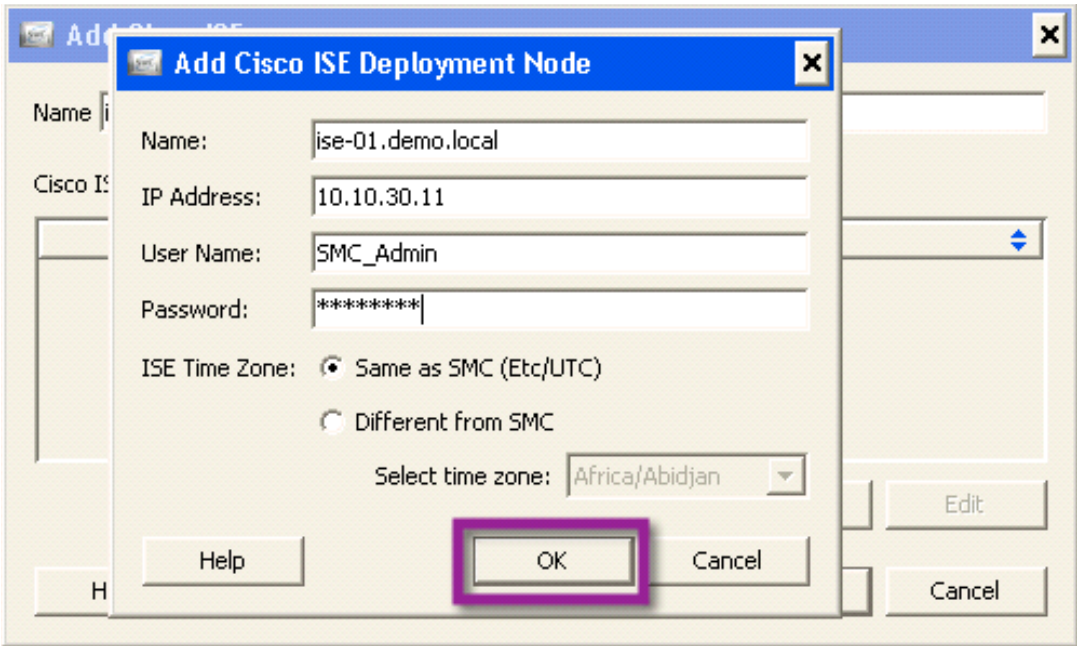
Step 3 Enter a name for the ISE deployment, as shown in Figure 17.

Figure 17 Adding Cisco ISE



Step 4 Click **Add**, and enter Name, IP Address, User Name, and Password; identify the time zone in which the Cisco Identity Services Engine is located, and then click **OK**. (See Figure 18.)

Figure 18 Adding Cisco ISE Deployment Node

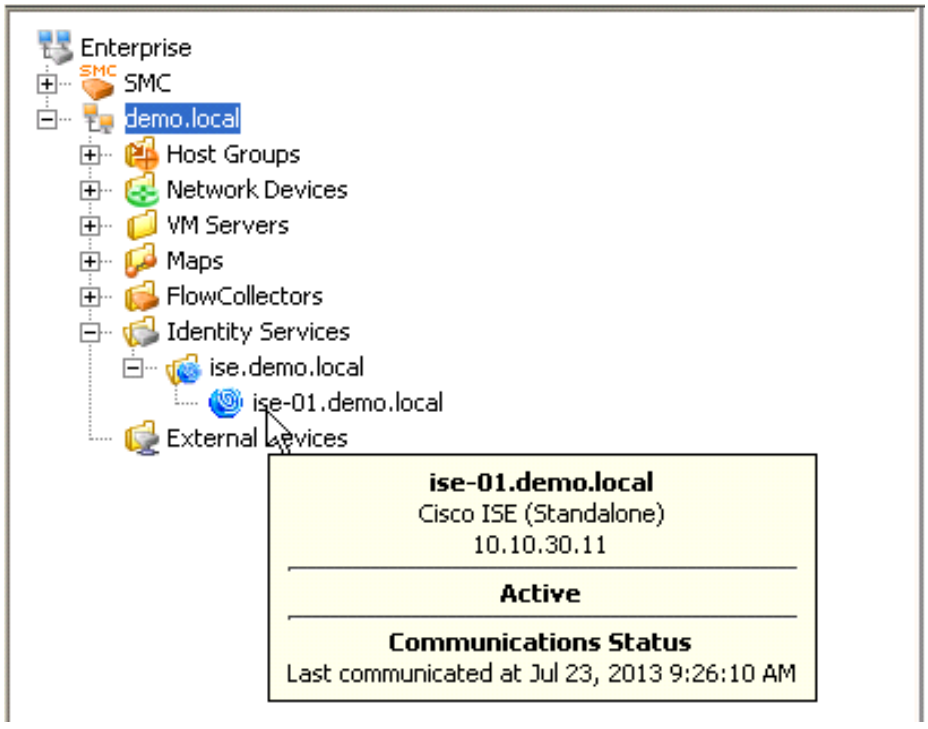


Step 5 To enter a second ISE MNT node for redundancy, repeat the previous step for the second node.

Step 6 Check the communication status with the Cisco Identity Services Engine.

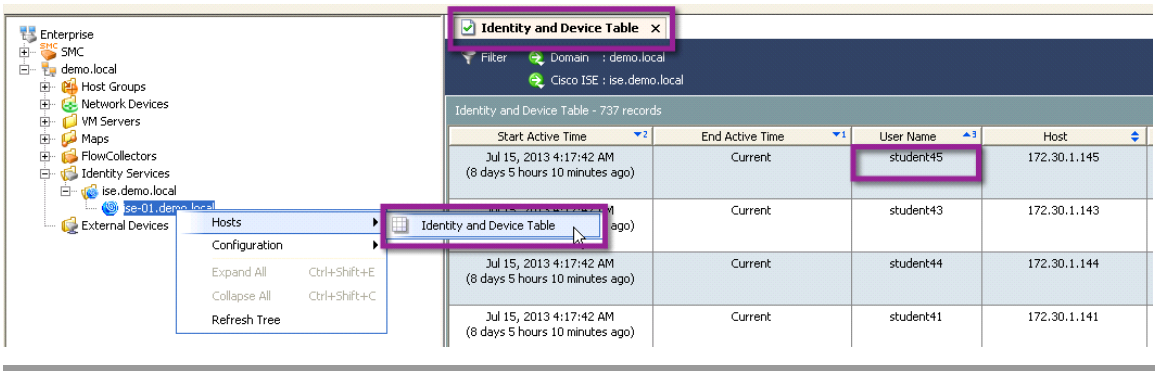
Expand the Identity Services menu and hover the mouse over the Identity Services Engine icon to see communication status, as shown in Figure 19.

Figure 19 Checking Communication Status



Step 7 Right-click the Identity Services Engine icon and go to **Hosts** > **Identity and Device Table**. This opens the Identity and Device Table, as shown in Figure 20. Verify that authenticated user names are present in the table.

Figure 20 Identity and Device Table



Conclusion

This guide describes the design, deployment, and implementation details of the Cisco Cyber Threat Defense Solution 1.1. An operational solution should now be present on the network and ready to aid in advanced threat defense detection and accelerating incident response. Consult other guides in the Cisco Cyber Threat Defense Guide Series on how to best leverage this solution for Cyber Threat Defense.

Appendix A: 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/solutions/collateral/ns341/ns524/ns562/ns583/net_implementation_white_paper0900aecd80308a66.pdf
- 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/partner/docs/ios-xml/ios/fnetflow/configuration/15-mt/fnf-15-mt-book.html
- Configuring Network Secure Event Logging (NSEL)—http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/monitor_nsel.html
- Cisco ASA 5500 Series Implementation Note for NetFlow Collectors 8.4, 8.5, and 8.6—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

About the Cisco Validated Design Program

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

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

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California. Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word *partner* does not imply a partnership relationship between Cisco and any other company. (1005R) Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.