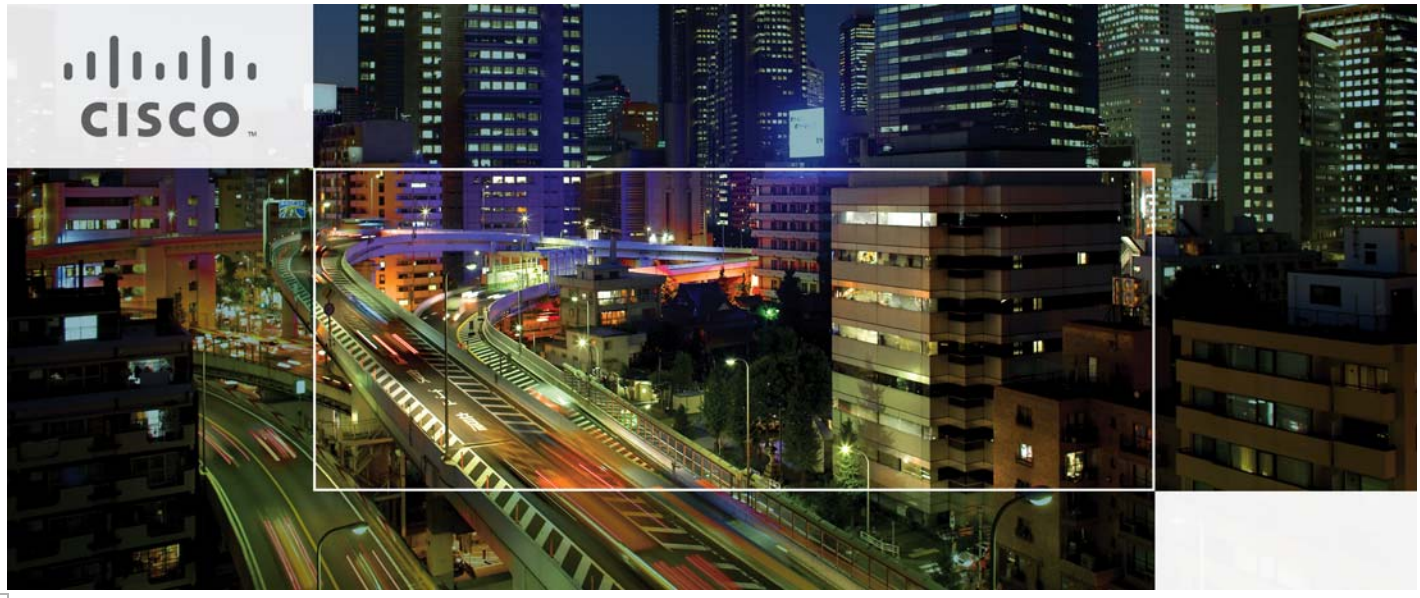


Cisco Cyber Threat Defense for the Data Center Solution: First Look Design Guide

Last Updated: November 4, 2013

Cisco Validated Design

About the Authors

Chris O'Brien

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

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 defense, and holds both a Bachelors and Masters degree in Computer Engineering from the University of Waterloo.

Terri Quinn

Terri is a Security Solutions Manager in the Security Business Group at Cisco Systems. She has been with Cisco for over 18 years, working in multiple areas during her tenure, including Product Management, Technical Marketing, Advanced Services, Compliance Solutions Management, and Marketing.

CONTENTS

Cisco Cyber Threat Defense for the Data Center Solution: First Look Design Guide

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. The APTs commonly focus on espionage of critically sensitive data or stealing specific types of information for financial gain. This information most likely resides in the data center, making it a primary target for APT attacks.

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

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

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

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

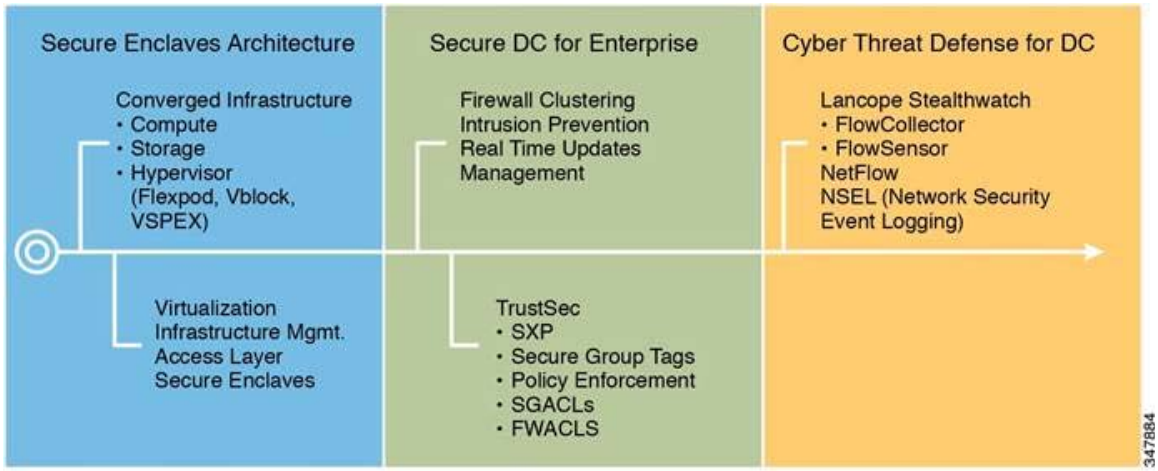
Cisco has partnered with Lancope to jointly develop and offer the Cisco Cyber Threat Defense Solutions. Available from Cisco, the Lancope StealthWatch System serves as the NetFlow analyzer and management system in the Cisco Cyber Threat Defense for the Data Center Solution.

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

Document Map

Figure 1 shows the relationship and focus areas for the Secure Enclaves, Secure Data Center for Enterprise, and the Cyber Threat Defense for the Data Center solutions. Please refer to the http://www.cisco.com/go/designzone for additional content outside the scope of this document.

Figure 1 Cyber Threat Defense Solution 1.1. Architecture



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

Products and Releases

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

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

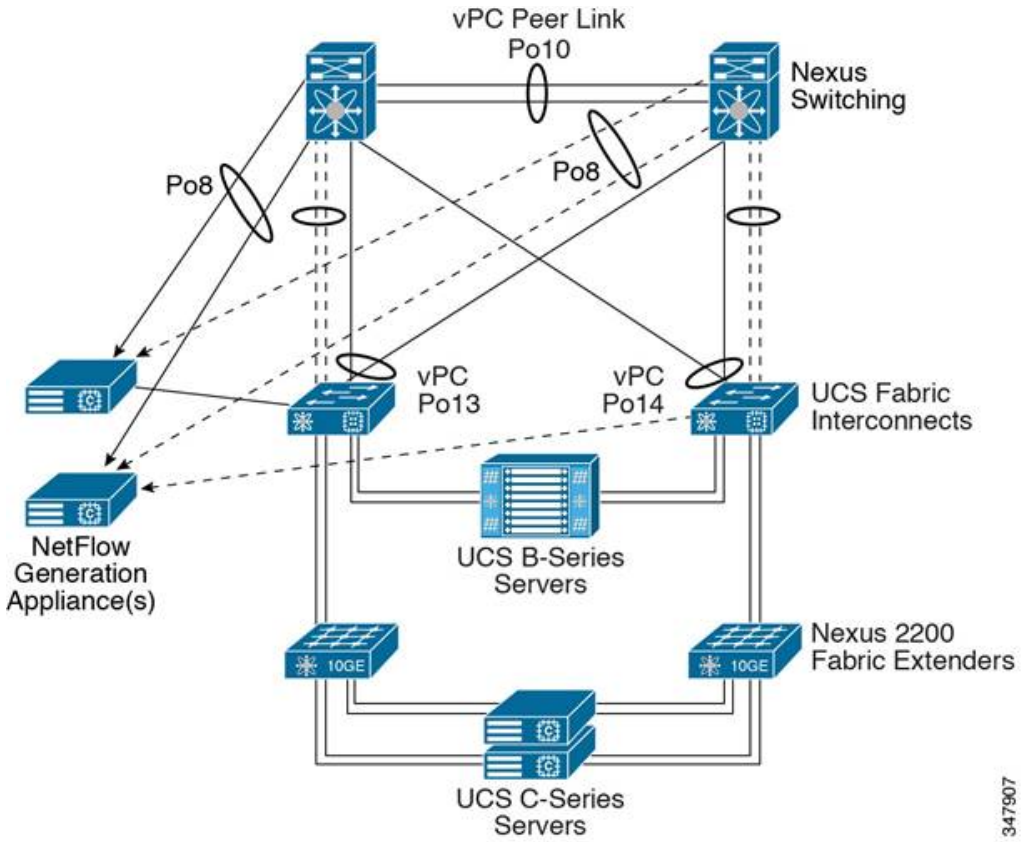
Component	Hardware	Release
Cisco Adaptive Security Appliance	ASA 5585-SSP60	Cisco ASA Software Release 9.1(2)
Cisco NetFlow Generation Appliance	3140	Cisco NGA Software Release 1.0(2)
Cisco Nexus 7000	7004	NX-OS Version 6.1(2)
Cisco Nexus 1000V Virtual Services Module (VSM)	Virtual machine	4.2(1)SV2(2.1)
Cisco Identity Services Engine	Virtual machine	Cisco ISE Software Version 1.2
Lancope StealthWatch Management Console	Virtual machine	StealthWatch 6.4
Lancope StealthWatch FlowCollector	Virtual machine	StealthWatch 6.4

Solution Overview

Architecture

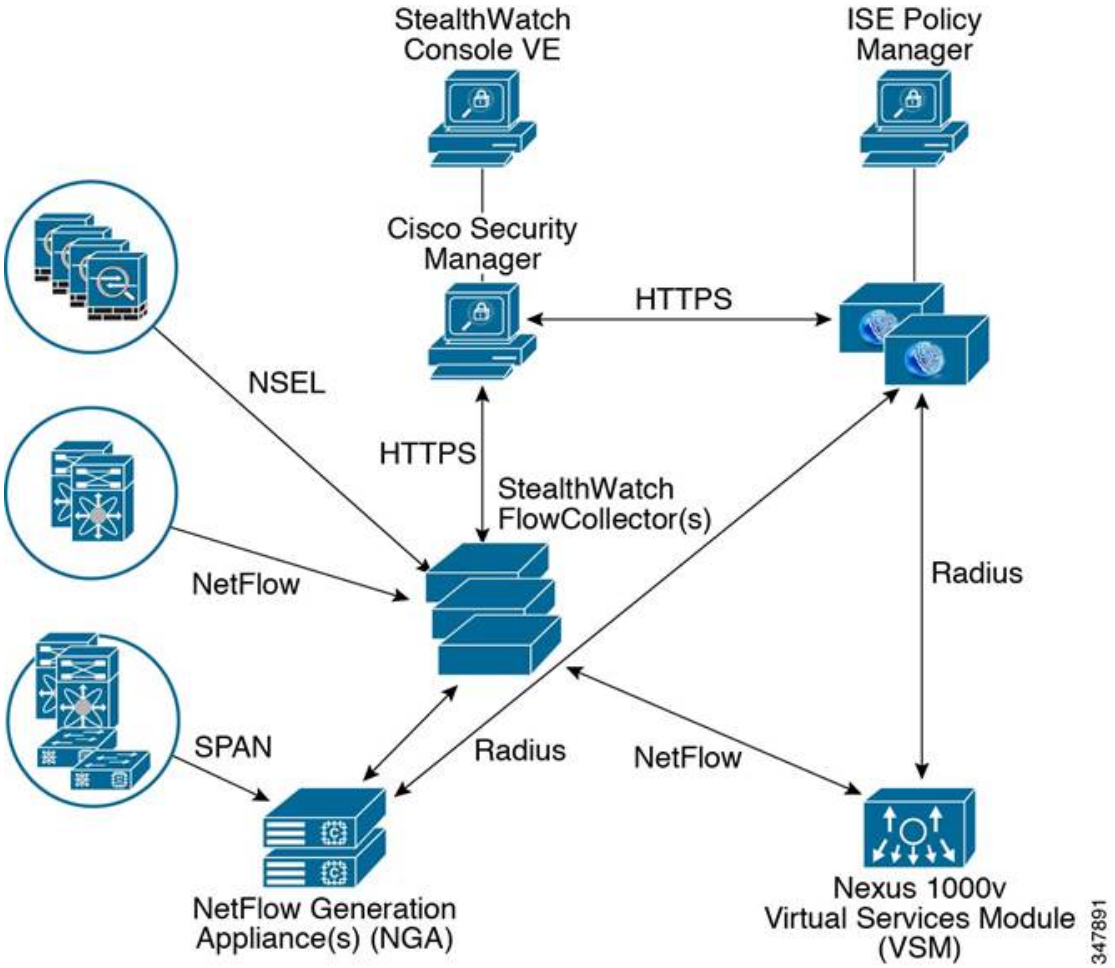
The Cisco Cyber Threat Defense for the Data Center Solution provides comprehensive visibility into all network traffic through the use of Cisco NetFlow technology. Cisco NetFlow technology is supported across Cisco data center switches and devices to enable telemetry to be implemented at all layers of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

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



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

Figure 3 Cisco Data Center Cyber Threat Defense TrustSec and StealthWatch Topology



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

The minimum system requirement to gain flow 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

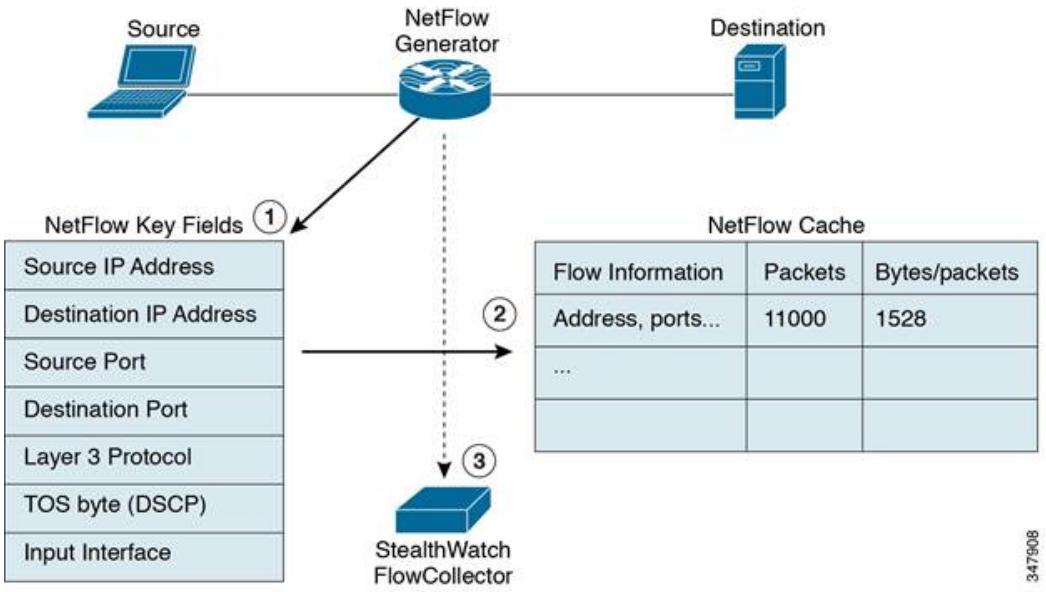
NetFlow is a Cisco application that measures the IP network traffic attributes of a traffic flow (a flow is identified as a unidirectional stream of packets between a given source and destination) as it traverses the Cisco device. NetFlow was initially created to measure network traffic characteristics 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.

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

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

Figure 4 illustrates NetFlow operation on a Cisco device.

Figure 4 NetFlow Operation on a Cisco Device



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

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

Some data center network devices support NetFlow via software, rather than hardware support, such as the Cisco Nexus 1000V. Give some consideration to a software device's current utilization when deploying software-supported NetFlow services, because NetFlow enablement can impact device performance.

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 2 shows whether Cisco Cyber Threat Defense for the Data Center Solution components support NetFlow in hardware or software.

Table 2 NetFlow Support—Hardware, Software, or SPAN

Component	Hardware Support	Software Support
Cisco NetFlow Generation Appliance	Yes	
Cisco Nexus 1000V Series		Yes
Cisco Adaptive Security Appliance (ASA)		Yes[1]
Cisco Nexus 7000	SPAN[2]	

1. The ASA NetFlow implementation, known as NetFlow Security Event Logging (NSEL), is different than most software-supported NetFlow implementations. See the ASA section in this guide for more information.
2. In this design, NetFlow is not enabled on the Nexus 7000 switches because it consumes CPU resources. Data is offloaded using SPAN to the NetFlow Generation Appliance (NGA) to perform NetFlow generation in hardware. NetFlow in hardware is supported using the F2 and Enhanced F2 Series modules. See the Nexus 7004 section in this guide for more information.

When the NetFlow cache on a device is full, the device does not generate NetFlow Records for new flows transiting the device.

Design Considerations

Customizable NetFlow Flow Record

Although NetFlow generation devices in the Cisco Cyber Threat Defense for the Data Center Solution support NetFlow v5 and v9, 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. 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.

Determining Flows-per-Second Volume

One necessary design task is to determine and measure the flows-per-second (fps) volume that will be generated. 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 for the Data Center Solution requires careful thought. Many factors can affect the volume of flows generated by the network devices, so predicting the exact number can be difficult. In general, a NetFlow generator generates between 1000 and 5000 fps per 1 Gbps of traffic passing through it; however, this is a general guideline and should be used only as a starting point.

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

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

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

- Flows per second.
- NetFlow record size. The Data Center Cyber Threat Defense Solution recommends NetFlow v9, which results in an average of 34 NetFlow records per 1500-byte packet.
- Flow timers (active and inactive timeouts for a flow). The Data Center Cyber Threat Defense Solution recommends an active timer of 60 seconds and an inactive timer of 15 seconds. To predict the impact of enabling NetFlow, use the Lancope NetFlow Bandwidth Calculator, available at the following URL: http://www.lancope.com/resource-center/netflow-bandwidth-calculator-stealthwatch-calculator/

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

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

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 restore flow visibility in these environments in a scalable and affordable manner.

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

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

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

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

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

Cisco ASA 5500 Series Adaptive Security Appliances

About NetFlow Security Event Logging

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

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

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

- Flow create
- Flow tear down
- Flow denied

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.

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

Cisco Nexus 7004

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

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

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

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

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

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

Cisco Nexus 1000V VSM

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

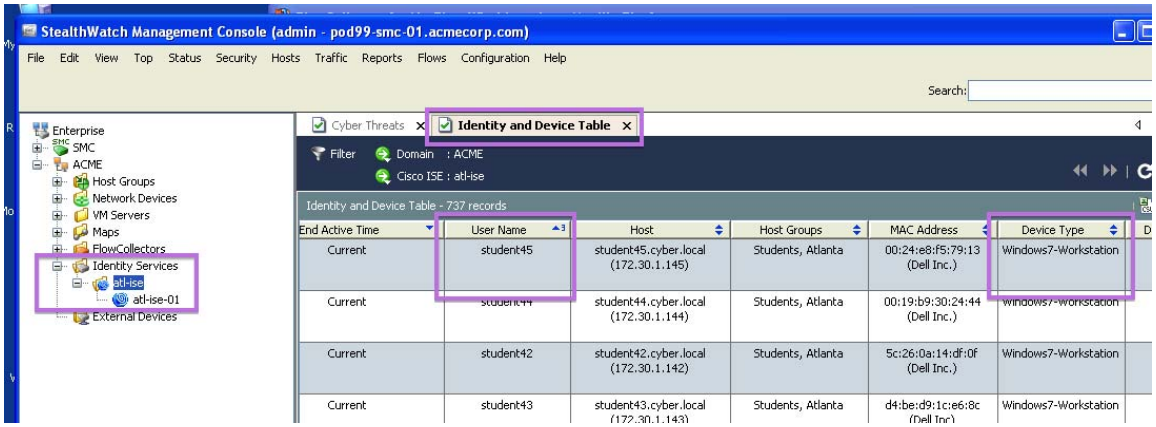
Cisco Identity Services Engine

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

Cisco Identity Services Engine (ISE), integral part of the Cisco TrustSec solution, provides visibility and control into who and what is connected to the network. Integration between the Lancope StealthWatch Management Console (SMC) and the 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 5 illustrates this enhanced capability where the username, device type, and all other session information is available alongside all associated flows with an IP address.

Figure 5 StealthWatch Management Console



StealthWatch 6.4 accepts and parses syslog messages from a primary or secondary ISE monitoring node to collect identity information. The Lancope SMC must be configured as a remote logging target on the ISE monitoring node with the RADIUS Accounting, Profiler, and Administrative and Operational Audit Logging categories set to log to the SMC target.

Authenticated session information from the Cisco ISE can be used to locate all of the flows based on authenticated session information.

Design Considerations for 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 for the Data Center Solution. Table 3 briefly introduces and describes each component used in this solution.

Table 3 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 ISE to correlate flow and identity.
StealthWatch FlowCollector	Serves as a central collector for flow data generated by NetFlow-enabled devices. The StealthWatch FlowCollector monitors, categorizes, and analyzes network traffic to create comprehensive security intelligence at both the network and host level.

Design Considerations for StealthWatch FlowCollector

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

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

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

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

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

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

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

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

Each StealthWatch FlowCollector can support a minimum guaranteed flow volume, as illustrated in Table 4. However, also consider the following factors in the selection of a StealthWatch FlowCollector for the Cisco Cyber Threat Defense for the Data Center Solution:

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

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

Table 4 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 5 lists the support for a StealthWatch FlowCollector VE based on the amount of reserved memory and the number of CPUs for the VM.

Table 5 StealthWatch FlowCollector VE Specifications

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

Design Considerations for StealthWatch Management Console

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

Table 6 shows the SMC models and the number of StealthWatch FlowCollectors they can support.

Table 6 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 7 lists the number of FlowCollectors and concurrent users (based on reserved memory and CPUs) that the SMC VE can support.

Table 7 SMC VE Specifications

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

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

Concluding Remarks

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

References

- 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 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
- Cisco Cyber Threat Defense Solution 1.1 Design and Implementation Guide—http://www.cisco.com/en/US/solutions/collateral/ns1015/ns1238/cyber_threat_defense_design_guide.pdf
- Gaining Visibility and Context Through NetFlow Security Event Logging—http://www.cisco.com/en/US/solutions/collateral/ns1015/ns1238/guide_c07-728135.pdf
- Gain Visibility in the Data Center with the Cisco NetFlow Generation Appliance—http://www.cisco.com/en/US/solutions/collateral/ns1015/ns1238/guide_c07-728136.pdf
- Secure Data Center for the Enterprise Solution—http://www.cisco.com/go/designzone

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.