Cisco Cyber Threat Defense Solution: Delivering Visibility into Stealthy, Advanced Network Threats

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

Using NetFlow telemetry and contextual information from the Cisco network infrastructure, a network security analyst can, from a single pane of glass, identify suspicious activity, gather pertinent user information, identify the application, and collection of host information. With this information, the analyst can decipher the correct next steps to take concerning the threat in a timely, efficient, and cost-effective manner for advanced cyber threats such as:

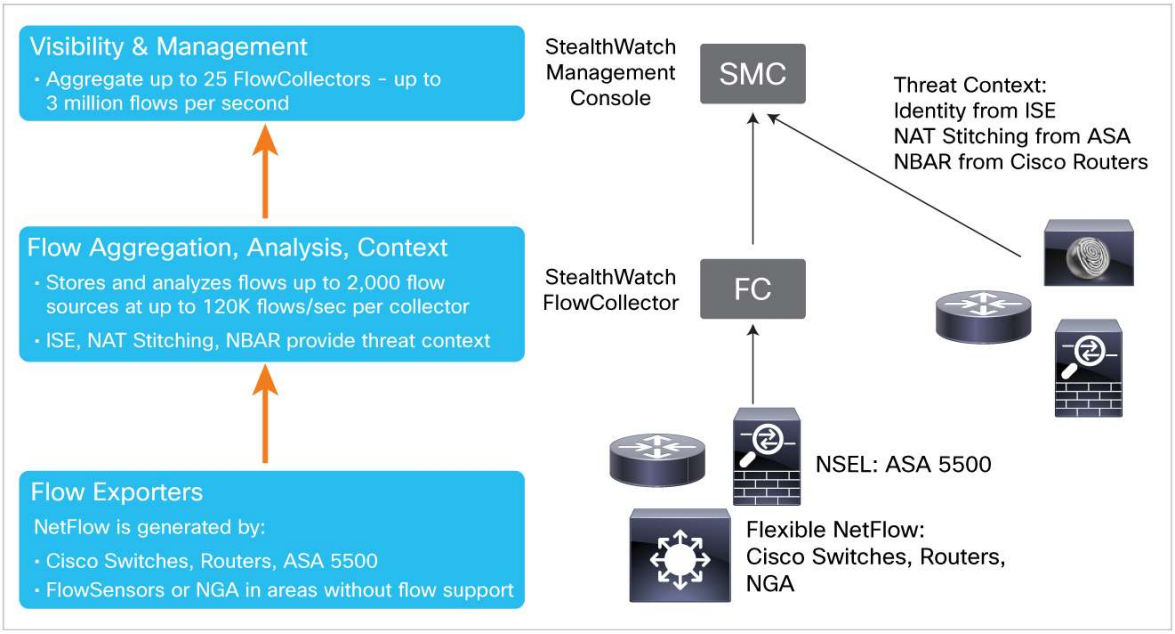
- Network reconnaissance - The act of probing the network looking for attack vectors that can be exploited by custom-crafted cyber threats
- Network interior malware proliferation - Spreading malware across hosts for the purpose of gathering security reconnaissance data, exfiltrating data, or creating back doors to the network
- Command and control traffic - Communications between the attacker and the compromised internal hosts
- Data exfiltration - Export of sensitive information back to the attacker, generally via command and control communications

This document outlines the specifications for the three main functional components of the Cisco Cyber Threat Defense Solution:

- Generating network-wide security telemetry - NetFlow export from Cisco Catalyst® switches, Cisco Integrated Services Routers, and Cisco ASA 5500 Series Adaptive Security Appliances
- Aggregating, normalizing, and analyzing NetFlow telemetry data to detect threats and suspicious behavior - Lancope StealthWatch System

- Providing contextual information to determine the intent and severity of the threat - User identity, endpoint device profiling, and posture information from the Cisco Identity Services Engine

Figure 1. Cisco Cyber Threat Defense Solution Components



Cisco Network Infrastructure: Generating Full Security Telemetry from the Network Interior

Recent advances in Cisco Catalyst switches enable the industry's first pervasive network traffic telemetry - from the user access edge to distribution to the core of the switching network. The line-rate, non-performance-impacting NetFlow telemetry capabilities of the Cisco Catalyst 3560-X, 3750-X, 4500, and 6500 Series provide insight into traffic patterns characteristic of threats that have bypassed the security perimeter and are attempting to remain below the detection radar. Key to delivering this visibility is Cisco's ability to generate unsampled NetFlow data in scale from these platforms.

Table 1 lists system requirements for generating line-rate, unsampled NetFlow data from Cisco Catalyst switches.

Table 1. Cisco Catalyst Switches Capable of Line-Rate, Unsampled NetFlow

Model	Hardware Required	Recommended Cisco IOS® Software Version
Catalyst 3560-X	Cisco Service Module	15.0(1)SE3
Catalyst 3750-X	Cisco Service Module	15.0(1)SE3
Catalyst 4500	Supervisor Engine 7-E or 7L-E	15.0(2)X0
Catalyst 6500	Supervisor Engine 2T	15.0(1)SY2

Additional information regarding Cisco Catalyst switches and Cisco NetFlow can be found at http://www.cisco.com/go/catalyst and http://www.cisco.com/go/netflow.

NetFlow telemetry is also generated at network borders from Cisco routers and Cisco ASA 5500 adaptive security appliances as well as the Cisco NetFlow Generation Appliance (NGA). Table 2 lists system recommendations for generating NetFlow data from these platforms.

Table 2. Cisco Router and ASA 5500 and NGA System Recommendations

Platform Series	Recommended Software Version
Cisco Integrated Services Routers	Cisco IOS Release 15.1(4)M2
Cisco Aggregated Services Router 1000 Series	Cisco IOS XE Release 3.5 Cisco IOS Release 15.2(1)S
Cisco ASA 5500 Series Adaptive Security Appliances	Cisco ASA Software Release 8.4(4)1
Cisco NetFlow Generation Appliance	Cisco NGA Software Version 1.0

Lancope StealthWatch System: Detecting Threats and Suspicious Activity

With the Cisco network infrastructure delivering ubiquitous NetFlow telemetry, the next step is to collect and analyze that data. The Lancope StealthWatch System, available from Cisco, is purpose-built to aggregate and normalize massive amounts of NetFlow data, and then apply security analytics to detect malicious and suspicious network traffic patterns as presented through the StealthWatch Management Console.

The primary components of the Lancope StealthWatch System are:

- FlowCollector - A physical or virtual appliance that aggregates and normalizes NetFlow and application-type data collected from up to 2,000 Cisco Catalyst switches, Cisco integrated services routers, or Cisco ASA 5500 adaptive security appliances per FlowCollector.
- StealthWatch Management Console - A physical or virtual appliance that aggregates, organizes, and presents analysis from FlowCollectors, the Cisco Identity Services Engine, and other network context via graphical representations of network traffic, user identity information, customized summary reports, and integrated security and network intelligence for drill-down analysis.
- Flow licenses - A Flow license is required to aggregate flows at the StealthWatch Management Console. Flow licenses also define the volume of flows that may be collected.

The optional components of the Lancope StealthWatch System are:

- FlowSensor - A physical or virtual appliance that Provides an overlay solution for generating NetFlow data for legacy Cisco network infrastructures not capable of producing line-rate, unsampled NetFlow data. Also for environments where IT security prefers a dedicated overlay architecture separate from the network infrastructure.
- FlowReplicator - A physical appliance that provides a single point for forwarding NetFlow data as a single data stream to other consumption devices.

StealthWatch FlowCollector

The volume of NetFlow telemetry collected from the network is defined by the capacity of the FlowCollectors deployed. Multiple FlowCollectors may be installed to scale the deployment. FlowCollectors are available as hardware appliances or as virtual machines (“VEs”). Table 3 lists FlowCollector specifications and capacities.

Table 3. StealthWatch FlowCollector Models

Model	Maximum Flows Per Second	Maximum NetFlow Exporters (e.g., Switches, Routers)	Maximum Hosts Monitored (IP Addresses)	Flow Storage Capacity
FlowCollector VE	30,000*	1000	500,000	1 TB
FlowCollector 1000	30,000	500	250,000	1 TB
FlowCollector 2000	60,000	1000	500,000	2 TB
FlowCollector 4000	120,000	2000	1,000,000	4 TB

* Dependent on resources of virtual machine.

Additional information regarding deployment sizing and hardware configurations can be found at http://www.lancope.com.

StealthWatch Management Console

The volume of NetFlow data analyzed and presented, as well as the number of StealthWatch FlowCollectors that can be deployed, is defined by the capacity of the StealthWatch Management Console. The console is available as a hardware appliance or as a virtual machine. Table 4 lists the specifications and capacities of the StealthWatch Management Console.

Table 4. StealthWatch Management Console Models

Model	Maximum FlowCollectors Supported	Flow Storage Capacity
StealthWatch Management Console VE	5*	1 TB
StealthWatch Management Console 1000	5	1 TB
StealthWatch Management Console 2000	25	2 TB

* Dependent on resources of virtual machine.

Additional information regarding deployment sizing and hardware configurations can be found at http://www.lancope.com.

StealthWatch Flow Licenses

A Flow license is required to aggregate flows at the StealthWatch Management Console. Flow licenses also define the volume of flows that may be collected. Licenses may be combined in any premutation to achieve the desired level of flow capacity. License capacities available are:

License Type
Flow Collection License - 1000 Flows
Flow Collection License - 10,000 Flows
Flow Collection License - 25,000 Flows
Flow Collection License - 50,000 Flows
Flow Collection License - 100,000 Flows

Note: FlowSensor traffic does not count against flow license capacities.

StealthWatch FlowSensor

The FlowSensor is an optional component that produces NetFlow data for segments of the switching and routing infrastructure that do not support NetFlow, or for environments where an overlay monitoring solution better fits the operations model of the IT organization. The FlowSensor can also provide Layer 7 application information for environments where Cisco Network-Based Application Recognition (NBAR) is not enabled.

The volume of NetFlow data generated from the network is defined by the capacity of the FlowSensors deployed. Multiple FlowSensors may be installed to scale the deployment. FlowSensors are available as hardware appliances or as software to monitor virtual machine environments. Table 5 lists the specifications and capacities of FlowSensors.

Table 5. StealthWatch FlowSensor Models

Model	Traffic Capacity
FlowSensor VE	1 per ESXi server
FlowSensor 250	100 Mbps
FlowSensor 1000	1 Gbps
FlowSensor 2000	2.5 Gbps
FlowSensor 3000	5 Gbps

Additional information regarding deployment sizing and hardware configurations can be found at http://www.lancope.com.

StealthWatch FlowReplicator

The FlowReplicator is an optional component that reduces telemetry generation and network overhead by aggregating network and security information from multiple locations into a single data stream to send to the FlowCollector or other devices. FlowReplicators are available as hardware appliances. Table 6 lists the specifications and capacities of FlowReplicators.

Table 6. StealthWatch FlowReplicator Models

Model	Traffic Capacity - Inbound	Traffic Capacity - Outbound
FlowReplicator 1000	10 KPPS	20 KPPS
FlowReplicator 2000	20 KPPS	60 KPPS

Additional information regarding deployment sizing and hardware configurations can be found at http://www.lancope.com.

Cisco Identity Services Engine, NAT Stitching, and Application Recognition: Providing Threat Context

Identifying suspicious traffic patterns is key to threat detection and visibility, but deciphering the intent and danger associated with those threats requires relevant contextual information. The Cisco Cyber Threat Defense Solution presents a unified view of the traffic pattern analysis via NetFlow and relevant contextual information regarding that traffic, such as user identity, posture, device type, user policy, application information, and firewall context. This information is presented in a single pane of glass via the StealthWatch Management Console.

Cisco Identity Services Engine

The Cisco Identity Services Engine provides a highly powerful and flexible attribute-based access control solution that combines authentication, authorization, and accounting (AAA), endpoint security posture assessment, and endpoint device-type profiling and identification on a single platform. The Cisco Identity Services Engine automatically discovers and classifies endpoints, provides the right level of access based on identity, and provides the ability to enforce endpoint compliance by checking a device's posture. These functions enable the Identity Services Engine to provide key identity, device, and posture information to provide threat context associated with suspicious network traffic patterns identified by the StealthWatch System. Furthermore, Cisco Identity Services Engine can be used to execute threat remediation actions for affected users.

The volume of users/sessions and devices that can be monitored is defined by the capacity of the Cisco Identity Services Engine model. Multiple Cisco Identity Services Engine devices may be installed to scale the deployment. The Cisco Identity Services Engine is available as a hardware appliance or as a virtual machine. Table 7 lists the specifications and capacity of the Identity Services Engine.

Table 7. Cisco Identity Services Engine Models

Model	Endpoints Supported	Storage Capacity	Cisco ISE Software Release
Cisco ISE 3315 Identity Services Engine	3000	500 GB	1.1
Cisco ISE 3355 Identity Services Engine	6000	600 GB	1.1
Cisco ISE 3395 Identity Services Engine	10,000	1.2 TB	1.1

Additional information regarding deployment sizing, hardware configurations, and licensing options can be found at http://www.cisco.com/go/ise.

NAT Stitching

Lancope StealthWatch uses NAT context from ASA 5500 appliances and ASR 1000 Series Routers to connect internal and external representations of the same traffic flow into one single deduplicated flow record. Along with the other identity and application information presented in StealthWatch, this can significantly speed the process of analysis and incident response by eliminating the time-consuming manual process of correlating inside to outside address information.

Cisco Network-Based Application Recognition (NBAR)

NBAR is a Cisco IOS® Software feature on Cisco Integrated Services Routers that performs stateful deep-packet inspection on a data flow to identify the packet type and the protocol that the flow belongs to. NBAR can distinguish more than 900 different protocols using protocol signatures inside the packet content. It can also inspect custom protocols by using a custom Protocol Description Language Module (PDLM) that has the protocol signatures.

The Lancope StealthWatch System uses NBAR information from Cisco Integrated Services Routers to provide additional threat context by identifying the application associated with suspicious traffic. This capability is included in the StealthWatch System.

For More Information

For more information about the Cisco Cyber Threat Defense Solution, visit http://www.cisco.com/go/threatdefense.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

Printed in USA C78-700868-01 05/13