Introduction to the Cisco Cyber Threat Defense Solution 1.0 How-To Documents

April 9, 2012

Introduction

Detecting threats on an internal network is a particularly difficult task for most security operations teams. Traditional network perimeter security products lack complete visibility to all traffic within the internal network. Therefore, detecting threats on the internal network is difficult—and sometimes impossible—due to the lack of visibility.

One of the main challenges to providing good internal network security is adequate visibility to the streams of data flowing through every corner of the enterprise network. Because there is simply no centralized location from data can be gathered, visibility is by default a distributed problem. However, distributed data collection could mean installing specialized data collection systems all over the network, which in turn complicates security management.

Security teams need to be able to collect data from the entire network without having to install specialized equipment. Furthermore, the data collected needs to be relevant to the problem of providing pervasive visibility for security.

The Cisco® Cyber Threat Defense Solution addresses this challenge.

Solution Overview

The Cisco Cyber Threat Defense Solution 1.0 is composed of multiple hardware and software components. These components fall into three broad categories:

NetFlow data generation devices, NetFlow is the de facto standard for acquiring IP operational data. Traditional IP NetFlow defines a flow as a unidirectional sequence of packets that arrive at a router on the same interface or sub-interface and have the same source IP address, destination IP address, Layer 3 or 4 protocol, TCP or UDP source port number, TCP or UDP destination port number, and type of service (ToS) byte in their TCP, UDP, and IP headers, respectively.

Flexible NetFlow is the next generation in flow technology and is supported by the Cisco Cyber Threat Defense Solution 1.0. Flexible NetFlow optimizes the network infrastructure, reducing operation costs and improving capacity planning and security incident detection with increased flexibility and scalability. Flexible NetFlow provides:

- Flexibility and scalability of flow data beyond traditional NetFlow
- Customized traffic identification
- Ability to focus and monitor specific network behavior

- Ability to monitor a wider range of packet information, producing new information about network behavior
- Enhanced network anomaly and security detection
- Convergence of multiple accounting technologies into one accounting mechanism

A flow record is created for each unique flow that passes through a NetFlow-enabled device. The information in a flow record expresses key details of the packet header, along with other statistical information such as the number of packets or bytes.

NetFlow can be enabled on most Cisco switches and routers, as well as some Cisco VPN and firewall devices. Packets used to generate NetFlow can be collected in two ways: by using every packet as part of a flow, or by sampling data. Unsampled NetFlow processes every single packet in the collection and generation of NetFlow data. This is the preferred method because it provides the most accuracy in NetFlow data reporting and security analysis. It is also the only supported method used in the Cisco Cyber Threat Defense Solution 1.0. An alternative method, sampled NetFlow, omits most packets in the collection and generation of NetFlow data. This method is not supported by the Cisco Cyber Threat Defense Solution 1.0. Although sampling data reduces the CPU overhead on the device generating the flows, the loss of accuracy seriously reduces the effectiveness of the security solution. Sampled NetFlow is most often used for network flow accounting, not network security.

To address the CPU overhead of NetFlow generation, select Cisco devices now employ special hardware acceleration to ensure NetFlow data collection does not have any performance impact on the forwarding plane of the device. This means NetFlow data can be collected pervasively throughout the network, even down to the user edge, ensuring every packet from every network segment and every device is completely visible.

Cisco Identity Services Engine. The Identity Services Engine delivers all the necessary identity services required by enterprise networks—AAA, profiling, posture, and guest management—in a single platform. In the context of the Cisco Cyber Threat Defense Solution 1.0, the Identity Services Engine can be deployed as either a network appliance or virtual machine and answers the “who” (user), “what” (device), and “where” (NetFlow-enabled device) questions that tie network flow data to the actual physical network infrastructure.

In an enterprise deployment, the Identity Services Engine is used to govern a network with central policy enforcement. It can provision and deliver cross-domain application and network services securely and reliably in enterprise wired, wireless, and VPN environments. This policy-based service enablement platform helps ensure corporate and regulatory compliance, enhances infrastructure security, and simplifies enterprise service operations. The Identity Services Engine can gather real-time contextual information from the network, users, and devices and make proactive governance decisions by enforcing policy across the network infrastructure.

The Cisco Identity Services Engine offers the following benefits:

- Security—Gain visibility into and control of all users and devices on your network
- Compliance—Create consistent policy across the infrastructure for corporate governance
- Efficiency—Increase IT staff productivity by automating labor-intensive tasks and simplifying service delivery

Product highlights include:

- Context-aware enforcement—Gathers information from users, devices, infrastructure, and network services to enable organizations to enforce contextual-based business policies across the network
- Business-relevant policies—Creates and enforces consistent policy from the head office to the branch office
- System-wide visibility—Enables IT to see who and what is on the network for advanced discovery and troubleshooting
- Flexible architecture—Combines authentication, authorization, and accounting (AAA), posture, profiling, and guest management

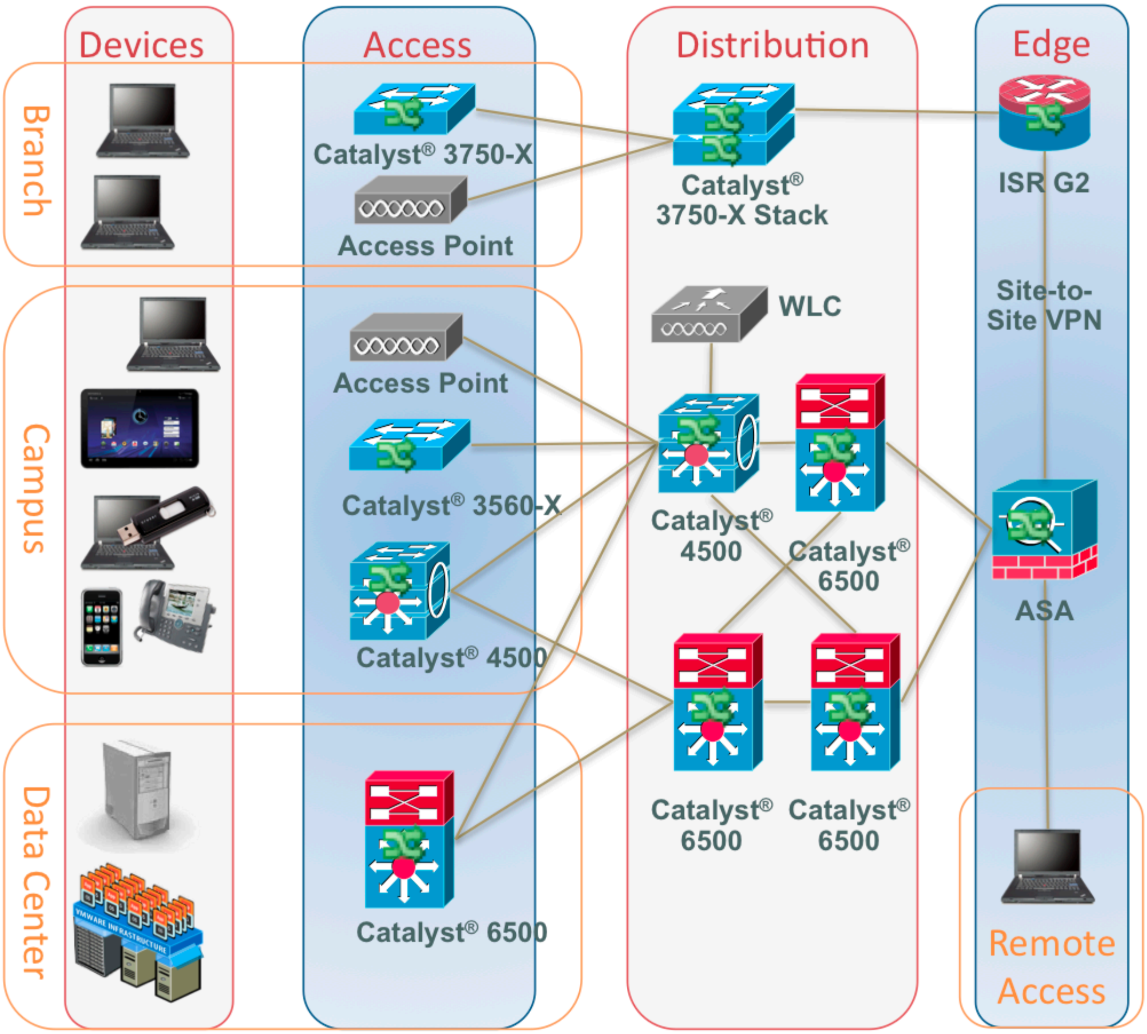
Lancope® StealthWatch® System. This NetFlow visibility, network performance, and threat detection solution provides an easy-to-use interface that enables both monitoring and detailed forensics. The solution is composed of two core components: the StealthWatch® Management Console and one or more StealthWatch® FlowCollectors. Additional optional components include a StealthWatch® Flow Sensor and a StealthWatch® Flow Replicator.

The Cisco Cyber Threat Defense Solution 1.0 provides the ability to detect a variety of security threats based on the analysis of NetFlow data. The StealthWatch® Management Console used to view the NetFlow data utilizes a technology called a *concern index* to reflect the severity of a security event. A *concern index* creates a point score for suspicious activities. This can be viewed as a raw numeric score, or as a percentage of acceptable activity (e.g. 150% of normal). The StealthWatch® detection engine examines each flow as it enters the FlowCollector and then applies a set of rules to each flow. The result of the comparison between the rule and the flow data determines whether various counters should be increased.

Independent of the collection process, StealthWatch® also constantly analyzes these flows to determine if thresholds have been exceeded or suspicious patterns have been detected. When a concern index value exceeds a defined threshold, StealthWatch® raises an alarm, indicating a potential problem.

Example Architecture

The Cisco Cyber Threat Defense Solution 1.0 can be deployed in a wide range of network architectures because it provides hardware-enabled NetFlow generation devices at the access, distribution, and edge layers, enabling pervasive network visibility. Following is a sample deployment that incorporates NetFlow generation in branch, campus, and data center networks, as well as in networks that need NetFlow generation at the distribution layer or for remote access or site-to-site VPNs.



Example Cisco Cyber Threat Defense Solution 1.0 Architecture

Supported Solution Components

Using the sample architecture as a reference, the Cisco Cyber Threat Defense Solution 1.0 supports the following hardware and software components:

Supported Hardware-Enabled NetFlow Devices

Component	Hardware	Release	Image Type and License
Catalyst 3560-X	Version ID: 02 Revision 0x03 10GE Service Module	Cisco IOS® Software Release 15.0(1)SE	Universal and IP Services
Catalyst 3750-X	Version ID: 02 Revision 0x03 10GE Service Module	Cisco IOS Software Release 15.0(1)SE	Universal and IP Services
Catalyst 4500E Series	Supervisor 7E or Supervisor 7L-E	Cisco IOS-XE Software Release 3.02.01.SG Cisco IOS-XE Software Release 3.02.00.XO	Universal and IP Base Universal and IP Base
Catalyst 6500 Series	Supervisor 2T	Cisco IOS Software Release 12.2(50)SY	Advanced Enterprise Services

Supported NetFlow-Enabled Security Devices

Component	Hardware	Release	Image Type and License
ISR G2	Any	Cisco IOS Software Release 15.1(2)T3	Universal and IP Base
Adaptive Security Appliance[1]	Any	Cisco ASA Software Release 8.4.3	Any
Identity Services Engine	Any	Cisco Identity Services Engine Software 1.1	Any

[1] The Cisco ASA Adaptive Security Appliance does not generate conventional NetFlow data. Instead, it generates NetFlow Secure Event Logging (NSEL) data. See below.

Information about NetFlow Secure Event Logging

The Cisco Cyber Threat Defense Solution 1.0 supports NetFlow Secure Event Logging (NSEL). The Cisco Adaptive Security Appliance implementation of NSEL is a stateful IP-flow-tracking method that exports only those records that indicate significant events in a flow. In stateful flow tracking, tracked flows go through a series of state changes. NSEL events are used to export data about flow status, and are triggered by the event that caused the state change. The significant events that are tracked include flow-create, flow-teardown, and flow-denied (excluding those flows that are denied by EtherType ACLs). Each NSEL record has an event ID and an extended event ID field that describes the event.

The Adaptive Security Appliance implementation of NSEL provides the following major functions:

- Keeps track of flow-create, flow-teardown, and flow-denied events and generates appropriate NSEL data records.

- Defines and exports templates that describe the progression of a flow. Templates describe the format of the data records that are exported through NetFlow. Each event has several associated record formats or templates.
- Delays the export of flow-create events.
- Tracks configured NSEL collectors and delivers templates and data records to these configured NSEL collectors through NetFlow over UDP only.
- Sends template information periodically to NSEL collectors. Collectors receive template definitions, normally before receiving flow records.
- Filters NSEL events based on the traffic and event type through Modular Policy Framework, and then sends records to different collectors. Traffic is matched based on the order in which classes are configured. After a match is found, no other classes are checked. The supported event types are flow-create, flow-denied, flow-teardown, and all. Records can be sent to different collectors. For example, with two collectors, you can do the following:
    - Log all flow-denied events that match access-list 1 to collector 1
    - Log all flow-create events to collector 1
    - Log all flow-teardown events to collector 2

NSEL may also be used with syslog messages that have an equivalent NSEL event, event ID, and extended event ID. The extended event ID provides more detail about the event (for example, which ACL—ingress or egress—has denied a flow).

The Adaptive Security Appliance supports NetFlow Version 9 services. For more information about NetFlow services, see RFC 3954. More information about NSEL on the ASA platform can be found at:
http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/monitor_nsel.html

Supported NetFlow Collection and Monitoring Components

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

Component Performance and Scaling

When deploying the Cisco Cyber Threat Defense Solution 1.0, it is important to select hardware and software that will provide the appropriate performance for your network and will scale to your specific needs. The following tables provide key information needed for selecting the right components based on your individual network requirements:

NetFlow Cache Size Limitations on Cisco Devices

Component	Hardware	Cache Size (flows)
Catalyst 3560-X	10GE Service Module	32,000
Catalyst 3750-X	10GE Service Module	32,000
Catalyst 4500E Series	Supervisor 7E	128,000
	Supervisor 7L-E	128,000
Catalyst 6500 Series	Supervisor 2T	512,000
	Supervisor 2TXL	1 million

StealthWatch® Management Console

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

Note: A single StealthWatch® Management Console can support up to 25 StealthWatch® FlowCollectors.

StealthWatch® FlowCollector Appliance

Model	Flows per Second	NetFlow Exporters
StealthWatch® FlowCollector 1000	30,000	500
StealthWatch® FlowCollector 2000	60,000	1000
StealthWatch® FlowCollector 4000	120,000	2000

StealthWatch® FlowCollector VE

Flows/sec.	Exporters	Hosts	Reserved Memory	Reserved CPUs
Up to 4,500	Up to 250	Up to 125,000	4 GB	2
Up to 15,000	Up to 500	Up to 250,000	8 GB	3
Up to 22,500	Up to 1,000	Up to 500,000	16 GB	4
Up to 30,000	Up to 1,000	Up to 500,000	32 GB	5

StealthWatch® FlowSensor Appliance

Model	Processing Capacity	Interfaces	Speed	Physical Layer	Form Factor	Power
250	100 Mbps	2	10/100/1000	Copper	1 RU-short	Non-redundant
1000	1 Gbps	3	10/100/1000	Copper	1 RU-short	Non-redundant
2000	2.5 Gbps	5	10/100/1000	Copper or fiber	1 RU	Redundant
3000	5 Gbps	1 or 2	10 GB	Fiber	1 RU	Redundant

StealthWatch® FlowSensor VE

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

StealthWatch® FlowReplicator

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

Key Deployment Use Cases

The initial release of the Cisco Cyber Threat Defense Solution 1.0 focuses on four deployment use cases commonly found in enterprise networks: network reconnaissance detection, data loss, internally spreading malware, and botnet command and control detection.

Network Reconnaissance Detection

A critical part of a strong security system is the ability to detect reconnaissance early in the threat lifecycle. When reconnaissance is coming from devices outside the corporate network, detection and prevention is a straightforward process involving an IPS and firewall. However, reconnaissance coming from an infected device that is inside the enterprise perimeter (where there is far less visibility to such traffic) can be much more difficult to detect.

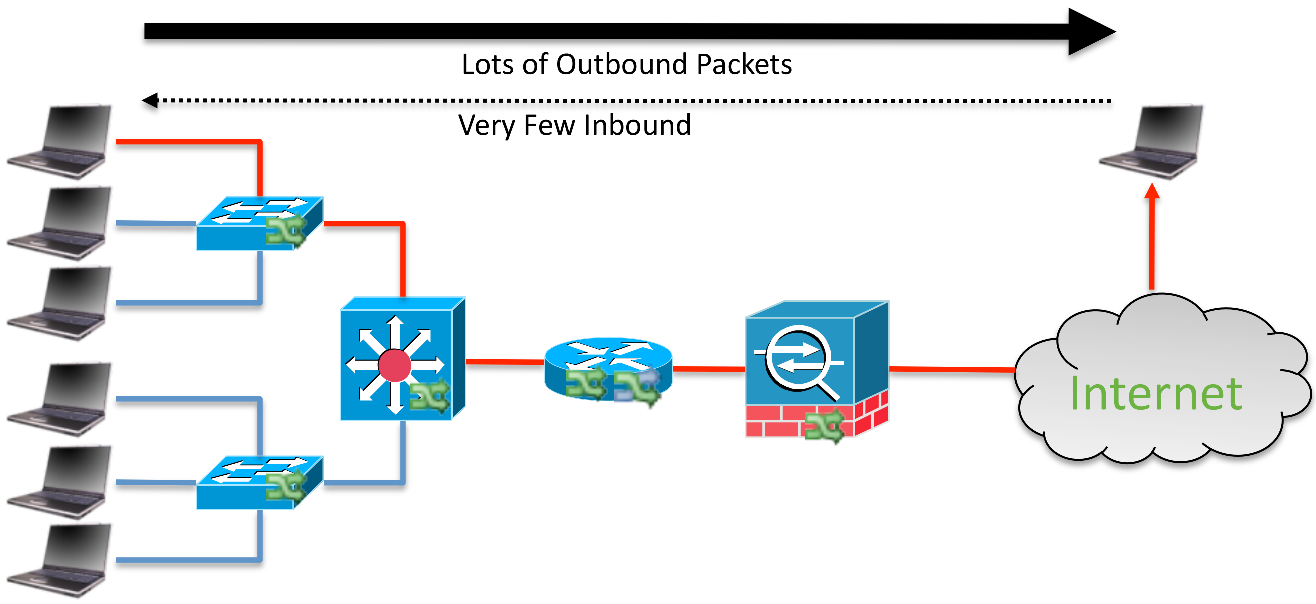
The Cisco Cyber Threat Defense Solution 1.0 provides a wide-ranging set of detection rules for network reconnaissance. These include detecting TCP and UDP scans in various forms (including unusual flag and flag configurations), stealth TCP scans, or the reuse of ports, low and slow scans, and ICMP scans.

Data Loss

Preventing persistent, widespread attacks against customer data, trade secrets, intellectual property, email, or financial data is a top priority for every IT organization. Unfortunately, detecting data loss (exfiltration) is one of the most difficult problems facing enterprise IT today. One of the critical aspects of detecting data loss in the enterprise is having a good visibility mechanism.

The Cisco Cyber Threat Defense Solution 1.0 detects data loss by using a customizable set of rules within StealthWatch® that detects *asymmetric outbound flows*.

An Asymmetric Flow



The rule within StealthWatch® that monitors for this behavior is called *Suspect Data Loss*.

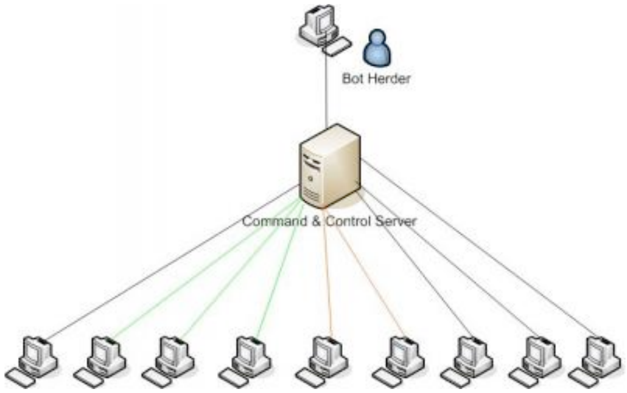
Internally Spreading Malware

One of the most common network defense strategies is to construct a hardened network perimeter to prevent attacks from reaching the internal network. While this is a good starting point, malware writers have adapted their techniques to compensate for this strategy, using polymorphic malware, encryption, obfuscation, and social engineering to bypass these traditional security measures. As a result, enterprise security professionals are now battling malware on their internal networks, where traditional perimeter defense technologies aren't easily deployed and don't scale well.

The Cisco Cyber Threat Defense Solution 1.0 provides the visibility mechanisms needed for detecting internally spreading malware—mechanisms that traditional perimeter security products lack. Cisco's solution integrates StealthWatch® with Cisco's hardware-supported NetFlow and the Identity Services Engine to provide a convenient and effective way to establish a baseline for host network behavior, monitor which internal devices a host is communicating with, and apply the behavior and communication to a set of rules and policies to determine if malware is spreading.

Botnet Command and Control Detection

Botnets have grown in sophistication and reach to the point where they are now responsible for a variety of activities, such as harvesting terabytes of sensitive information and denial of service attacks. Botnet-controlled computers are a particularly high risk for most enterprises because they can be controlled from anywhere in the world. This means an attacker could directly control a botnet-infected host inside a network for any number of purposes, including network reconnaissance, data exfiltration, or denial of service. Unfortunately, locating botnet hosts in a network can be difficult because the hosts are stealthy and often hide their communication to their controllers using standard protocols and ports like HTTP (port 80), HTTPS (port 443), or Internet Relay Chat servers.



Typical Botnet

The Cisco Cyber Threat Defense Solution 1.0 addresses the botnet problem by providing the visibility mechanisms needed for detecting infected hosts within a network. The solution offers three distinct methods for detecting botnets: IP address blacklisting, beaconing host detection, and IP address backtracking. The combination of these three methods provides a simple and convenient way to detect and manage this kind of malware.

Next Steps: Read the Detailed Use Case Documents

Cisco has produced a series of detailed "how-to" documents for each of the four use cases just described. These are:

- Detecting Network Reconnaissance with the Cisco Cyber Threat Defense Solution 1.0
- Detecting Data Loss with the Cisco Cyber Threat Defense Solution 1.0
- Detecting Internal Malware Spread with the Cisco Cyber Threat Defense Solution 1.0
- Detecting Botnet Traffic with the Cisco Cyber Threat Defense Solution 1.0

Now that you have a better understanding the components and architecture of the solution, your next step should be to select one the four use cases and read the in-depth discussion of how the Cisco Cyber Threat Defense Solution 1.0 can help secure your network.