Using Lancope StealthWatch for Information Security Monitoring

How the Cisco Computer Security Incident Response Team (CSIRT) uses Lancope StealthWatch to dig deep into Cisco IOS NetFlow.

EXECUTIVE SUMMARY

CHALLENGES

- High volume of global NetFlow
- IPv6 readiness

SOLUTION

- Deploy StealthWatch: store more NetFlow for incident look-back, enhanced detection capabilities, IPv6 capable
- Utilize the StealthWatch feature set: syslog export of events, Host Group-based detection, API queries, Host Alarms

RESULTS

- Retain 90+ days of full NetFlow records
- Provides unique interface for gaining insight into NetFlow and the information in contains
- Automate NetFlow analysis

LESSONS LEARNED

- Require Full NetFlow for security
- Tune StealthWatch Alarms to trim false positives

NEXT STEPS

- Expand StealthWatch hardware as network grows
- Upgrade StealthWatch to utilize new feature sets, including SLIC and Cisco ISE

Background

The Cisco® CSIRT is a global team of information security professionals responsible for 24-hour monitoring, investigating, and responding to cyber security incidents. With a variety of security tools, CSIRT is able to detect and analyze malicious traffic throughout the network, including virus propagation, targeted attacks, and commonplace exploits. The StealthWatch systems' ingestion and processing of NetFlow provides unique insight into network transactions, allowing investigators to dissect the finer details of security incidents.

CSIRT maintains a global deployment of StealthWatch hardware to forensically monitor traffic patterns in the vast Cisco network. The DMZ gateways are the thoroughfare for internal traffic to the Internet, and are a crucial NetFlow export point, because many of the threats to Cisco originate beyond the firewalls and must traverse those gateways. In addition, the most valuable information to Cisco is stored within the data center infrastructure, thus the data center gateways require strict monitoring for any malicious activity as well. These two gateways allow for pertinent insight into the network activity for maintaining a secure environment.

With StealthWatch, CSIRT is able to easily query stored NetFlow data and piece together the details and series of events of security incidents. Moreover, because StealthWatch comes equipped with algorithms designed to highlight specific activity, such as worm propagation, port scanning, and the like, CSIRT can quickly react to remediate such threats. In a world of advanced attacks, having a tool that can identify anomalies and suspicious activity is imperative to secure Cisco.

Challenges

The Cisco network is a large and complex environment that must be monitored extensively. While multitudes of technologies are used in this environment, NetFlow data is uniquely positioned to provide insight into the network. Because CSIRT continually identifies new security threats, the team needs some historical look-back at what occurred on the network.

NetFlow is a small package of metadata describing the "conversations" on the network. It contains the important details in network transactions endpoints of data communication, information about when the conversation occurred, how long it lasted, and what protocols were used. Even though it is a subset of the full conversations, it can become voluminous in a large environment. From the 180 exporting devices at the aforementioned gateways, CSIRT receives approximately 180,000 flows per second, which translates to 15.6 billion flows per day. A high priority for the security team is to maintain as much data as possible for tracing sources of incidents after they occur, while facing the ever-present restrictions with data storage.

Before deploying StealthWatch, CSIRT used the open source tool “OSU Flow-tools” for NetFlow capture. Use of this tool posed its own set of hardships, because it is a command-line process that requires manipulation to parse through raw NetFlow data. Administration of the NetFlow ingestion became cumbersome with port configurations and correctly distributing the data through the fan-out process. In addition, OSU Flow-tools did not support the IPv6-capable NetFlow v9, which left a large security gap for the up-and-coming IPv6 traffic.

Solution

StealthWatch provides an interactive interface for analyzing NetFlow data, while also manipulating raw flows for a decreased storage footprint, thus increasing retention. The resourceful StealthWatch feature of de-duplication, merging identical records into one, provides a concise set of data for analysis.

Deployment

The CSIRT StealthWatch deployment exists among the larger Cisco sites, housing the devices in data centers for optimal performance and support. With the intention of collecting NetFlow from data center and DMZ gateways, these selected locations limit latency because much of the traffic stems from within the very same theaters.

StealthWatch FlowReplicators receive NetFlow from 180 DMZ and data center gateways, the majority of which are Cisco Catalyst® 6500 Series devices. Acting as fan-out devices, the FlowReplicators then forward the traffic on to 15 StealthWatch FlowCollectors, which store all of the NetFlow for queries from the StealthWatch Management Console (SMC).

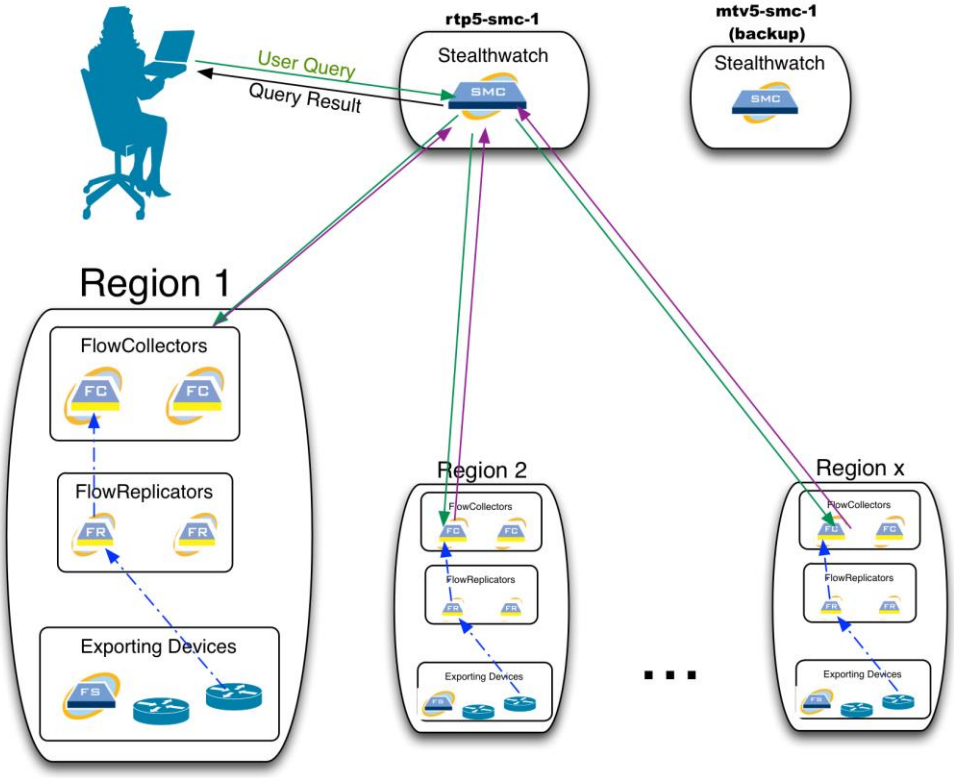
The CSIRT StealthWatch infrastructure consists of the following:

- Two SMC units (one primary, one failover – SMC2000)
- Ten FlowReplicators (FR2000)
- Fifteen FlowCollectors (seven FC2000, seven FC1000, one Virtual FlowCollector)
- Seven FlowSensors (two FS3000, five FS1000)

Each Cisco router sending NetFlow data to CSIRT is configured to use the CSIRT Enterprise Service Locator

record, which defaults to exporting NetFlow to the FlowReplicator nearest the router in terms of geography. CSIRT maintains the forwarding rules on the FlowReplicators, dividing the inbound router traffic among the FlowCollectors per geographic site. Not only does this minimize latency, but also investigators can refine queries by way of the collection point.

Figure 1. Centralized Query Interface with Localized Long-term NetFlow Storage



CSIRT also uses the StealthWatch virtual solutions to extend monitoring beyond the network with special engagements, such as security montioring at Cisco business events. CSIRT travels to external sites with compact racks housing multiple security tools such as Intrustion Detection System (IDS), Splunk, and the Cisco Web Security Appliance (WSA) to provide a mobile monitoring solution. Virtual FlowCollectors allow for NetFlow storage with no physical footprint and are easily managed through the primary SMC.

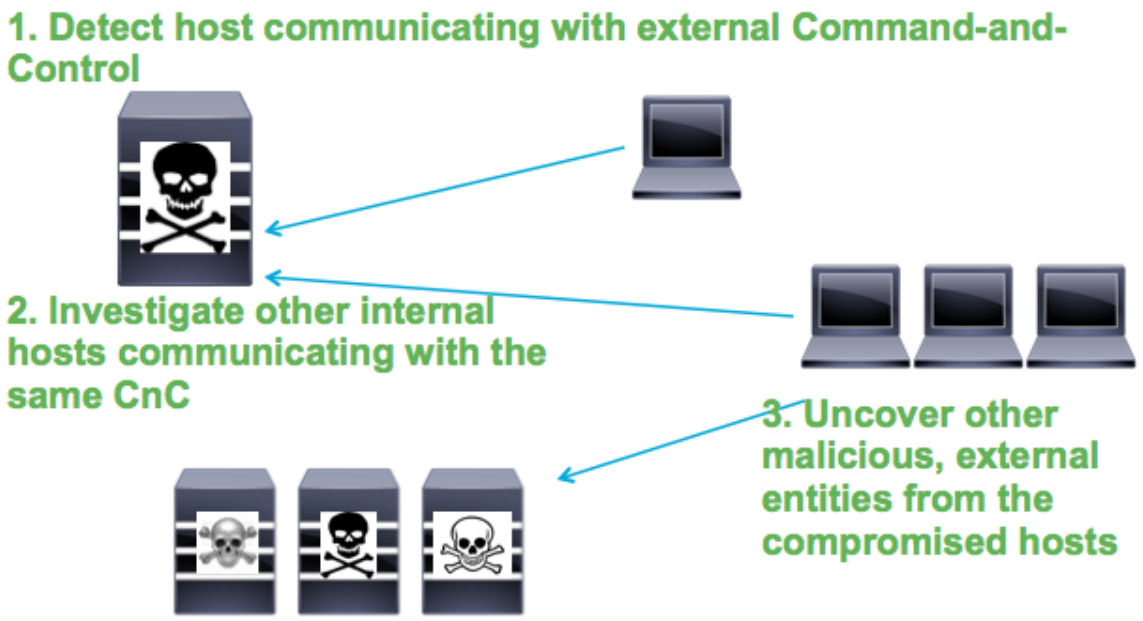
Utilization

Like any large enterprise, the Cisco network faces both serious and benign attacks from innumerable sources around the world. With a plethora of security monitoring tools, CSIRT maintains a vast amount of data and a methodical process by which to analyze the data for true breaches. NetFlow data inherently provides relevant, fundamental details of the network traffic, which is essential information for any security investigation. Using StealthWatch, CSIRT investigators have the necessary facts to augment evidence of any issues in the network. “Since deploying StealthWatch, we have been able to exceed our retention goal of 90 days across our entire

infrastructure and have significantly decreased the flow query time", says Paul Eckstein, Cisco Information Security Engineer.

CSIRT investigators use the StealthWatch Host Groups to detect command-and-control (CnC) behavior in the network, indicating one or more internal hosts have been compromised by an external entity. When an external CnC host is identified, the investigator can quickly query for all Inside Hosts that are communicating to this known bad agent. At that point, investigators use all devices found communicating with the CnC from the initial query to populate a new Host Group, and then pivot the query to find new external (bad) hosts with which these infected machines are communicating.

Figure 2. Responding to Identified CnC Host



Another feature that allows for dynamic monitoring is Host Locking groups. Investigators receive automatic updates from intelligence feeds such as the Lancope StealthWatch Labs Intelligence Center (SLIC) and also manually create and modify Host Groups based on intelligence from peer organizations and incidents. In both cases, CSIRT uses the Host Locking condition to alert when any traffic is seen going to or from these Host Groups. With this implementation, investigators quickly learn when a new connection is established to a confirmed malicious IP address, and can also look at historical connections to newly discovered malicious address space.

CSIRT heavily invests in flow-based detection for cyber threats, because Advanced Persistent Threats and malware are increasingly using encrypted network traffic for communication. Because StealthWatch was developed to function without relying on the data portion of the packets, all of the alarms and algorithms that work with traditional network traffic are not affected by encryption. Without independence of protocol-specific traffic, the security monitoring effort would be a constant struggle to confront the ever-evolving threats.

StealthWatch also has an Application Programming Interface (API), which allows for query and web interface

customization. This feature is useful to accommodate both regularly modified address space and infrastructure, in addition to specific needs of the CSIRT investigators to improve workflow. For example, the API allows for an automated Host Group update; a script gathers an exhaustive list of addresses for a particular network zone, and through the API, pushes the update to the SMC. Moreover, with the API, CSIRT easily investigates activity from a particular user when necessary. The API reduces multiple queries into one by stitching together time and IP address information pulled from an internal homegrown tool, and automatically extracts the flows with the information gathered.

In addition, in some instances, an investigator may need to retrieve more than 400,000 flows from the FlowCollectors (this is a current SMC restriction). By using the API, this query can be split into a series of smaller, automated *getFlow* requests, which are then concatenated into a single set of results that can exceed this limitation.

To simplify workflow even further, CSIRT sends specific StealthWatch alarms through syslog messages to Splunk for reporting and comparison with events from other security tools. StealthWatch Concern Index (CI) measures when suspicious activity is seen for a host, and once the High Concern Index threshold is exceeded, the system immediately triggers a syslog alert. For the Cisco network, this feature requires some tuning to avoid excessive false positives. With this information in Splunk, CSIRT can use StealthWatch information to augment any evidence of attack from the collection of events.

Results

StealthWatch provides multiple benefits for securing Cisco; with the ability to store and parse NetFlow data, CSIRT has a better understanding of interesting activity on the network. In addition, because StealthWatch has a unique set of algorithms, trend data, and network map capabilities, investigators can leverage the out-of-the-box features to assist analysis.

> "StealthWatch improves upon the inherent details in NetFlow with detection algorithms and an interface to visualize NetFlow in new ways."
> —Heather Pegram, Information Security Engineer, Cisco

In 2010, CSIRT deployed StealthWatch with the intention of aiding investigations by retaining at least 90 days worth of NetFlow data. With the former NetFlow collection solution, the retention policy was a best-effort, which proved to be lacking for multiple CSIRT use cases. After having StealthWatch deployed in the production environment for approximately three years, CSIRT maintains over 100 days worth of NetFlow data on each FlowCollector. Such retention is imperative for security investigations, in order to save as much data as possible for tracing sources of attacks and other malicious activity over time.

Moreover, as a Lancope consumer, CSIRT is freed from maintaining an open source tool with potential for misconfiguration and faulty software. Lancope provides licensing, software updates, and a responsive support team for hardware and configuration maintenance. After piloting StealthWatch with eight geographically dispersed devices, CSIRT has been able augment the deployment to its current capacity, and continues to use the StealthWatch solution for NetFlow consumption as the Cisco network grows.

One key value from StealthWatch is that a great deal of work has gone in to taking the difficulty out of NetFlow analysis and integrating that into the SMC. On nearly every NetFlow query, an analyst needs to perform a number

of actions, including determining flow start and stop time, total packets, directionality, GeoIP information, and network path. These actions can become error-prone and time-consuming tasks without a tool designed to parse the data correctly. These are only a few pieces of metadata analysis that StealthWatch automates.

Lessons Learned

The StealthWatch solution for consuming NetFlow provides CSIRT with a better grasp on securing Cisco; however, the deployment and migration presented several complications.

In 2012, CSIRT engaged Cisco IT to update the NetFlow exporting devices in preparation for IPv6 traffic. Previously with the OSU Flow Tools deployment, CSIRT worked solely with NetFlow v5 because Flow Tools could not manage NetFlow v9, and IPv6 was not yet a priority. CSIRT incorporated the existing NetFlow v5 traffic into the initial StealthWatch deployment, but also updated many of the router configurations to export NetFlow v9 to be ingested by StealthWatch as well.

Multiple platforms used in Cisco are geared towards Sampled NetFlow, which means that only a percentage of the traffic is sent as a NetFlow export. This arrangement hinders the CSIRT use case, because security incidents are constantly occurring and investigators need as much data as possible to pinpoint the source and activity of such incidents. In network spaces where devices do not support Full NetFlow, CSIRT uses StealthWatch FlowSensors to generate and export NetFlow. In addition, Cisco now also has its very own NetFlow sourcing device, the NetFlow Generation Appliance (NGA), which creates Full NetFlow for network devices. While CSIRT has not yet deployed the NGA, it is an available complement to both Cisco routers and FlowSensors to mitigate NetFlow gaps.

Because Cisco has a large, diverse network with a wide range of activity, the out-of-the-box alarms available in StealthWatch required tuning. While StealthWatch functioned as expected, it flagged traffic that was acceptable and had a business case in the Cisco environment; therefore, CSIRT worked with Lancope engineers to implement rules and exceptions to weed out the false positives. As a result, the unique alerts within StealthWatch now provide true insight into suspicious activity that requires CSIRT analysis.

Next Steps

CSIRT uses the StealthWatch toolset across the internal Cisco infrastructure, but CSIRT is also working to expand its use with Cisco diversified business units and acquisitions. With their own address space, Cisco Ironport® and Webex® require monitoring, and CSIRT is expanding the StealthWatch infrastructure to complete the coverage. As Cisco acquires more companies with diverse address space, CSIRT will utilize additional hardware as necessary.

Lancope's product and feature set is growing as well, and the latest software version, 6.4, has even more security innovations. SLIC integrates threat intelligence automatically into the SMC, and provides a visual indication of conversations with known "bad guys." This add-on feature has the potential to decrease threat activity within the network by providing the most up-to-date attack sources.

In addition, a highly beneficial feature on the horizon is the Cisco Identity Services Engine (ISE), which integrates with StealthWatch, providing attribution and granular event details. ISE matches user to device identity, as well as machine details, which lessens the time spent on pinpointing sources of infection. CSIRT is currently testing ISE with StealthWatch in a lab deployment and working closely with the ISE engineers on enhancements and testing as it is deployed across the greater Cisco network.

For More Information

- Cisco IOS NetFlow
- Lancope, Inc
- Validated Cyber Threat Defense designs

To read additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT.

Note

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

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.**