SECURITY

Network Security with NetFlow and IPFIX

Big Data Analytics for Information Security

ciscopress.com

Omar Santos

Network Security with NetFlow and IPFIX

Big Data Analytics for Information Security

Omar Santos

Cisco Press

800 East 96th Street

Indianapolis, Indiana 46240 USA

Table 4-1 *continued*

Commercial Software	Description	Website
NetFlow Insight	Traffic analysis, NetFlow collection using HP Insight Network Performance Monitoring.	http://www.openview.hp.com/products/ovpi_net/
IBM NetFlow Aurora	NetFlow traffic profiling tool commercially available as Tivoli Netcool Performance Flow Analyzer (TNPFA).	http://www.zurich.ibm.com/aurora
IdeaData NetFlow Auditor	Tool used for network troubleshooting, security monitoring, and baseline trending.	http://www.netflowauditor.com
InfoVista 5View NetFlow	NetFlow monitoring tool.	http://www.infovista.com/products/NetFlow-Monitoring-Network-Traffic-Analysis
Lancope StealthWatch	Traffic analysis, NetFlow collection, and security monitoring tool suite part of Cisco's Cyber Threat Defense Solution.	http://lancope.com
Paessler PRTG	Network monitoring tool suite.	http://www.paessler.com
Plixer International Scrutinizer	Plixer offers free and commercial NetFlow reporting software. Scrutinizer is an incident response and network monitoring suite of tools.	http://www.plixer.com
SolarWinds NetFlow Traffic Analyzer	NetFlow traffic analyzer and performance management tool.	http://www.solarwinds.com/netflow-traffic-analyzer.aspx

Two of the most popular commercial products are Lancope's StealthWatch solution and Plixer Scrutinizer, as described in greater detail in the sections that follow.

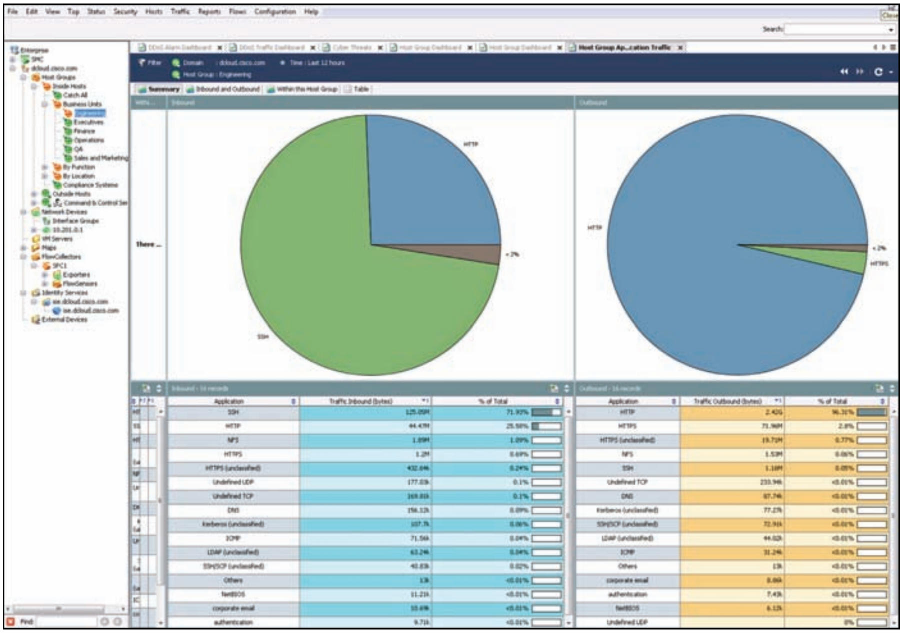
Lancope's StealthWatch Solution

Lancope's StealthWatch solution is a key component of the Cisco Cyber Threat Defense (CTD) Solution. One of the key benefits of Lancope's StealthWatch is its capability to scale in large enterprises. It also provides integration with the Cisco Identity Services Engine (ISE) for user identity information. Cisco ISE is a security policy management and control system that you can use for access control and security compliance for wired, wireless, and virtual private network (VPN) connections.

Note The Cisco CTD Solution is covered in detail in Chapter 6, "Cisco Cyber Threat Defense and NetFlow."

One other major benefit of Lancope's StealthWatch is its graphical interface, which includes great visualizations of network traffic, customized summary reports, and integrated security and network intelligence for drill-down analysis.

Figure 4-1 shows a screenshot of Lancope's StealthWatch Management Console (SMC).



Inbound - 16 records

Application	Traffic Inbound (bytes)	% of Total
SSH	125.05M	71.93%
HTTP	44.47M	25.58%
NFS	1.89M	1.09%
HTTPS	1.2M	0.69%
HTTPS (unclassified)	432.64k	0.24%
Undefined UDP	177.03k	0.1%
Undefined TCP	169.81k	0.1%
DNS	156.12k	0.09%
Kerberos (unclassified)	107.7k	0.06%
ICMP	71.56k	0.04%
LDAP (unclassified)	63.24k	0.04%
SSH/SCP (unclassified)	40.83k	0.02%
Others	13k	<0.01%
NetBIOS	11.21k	<0.01%
corporate email	10.69k	<0.01%
authentication	9.71k	<0.01%

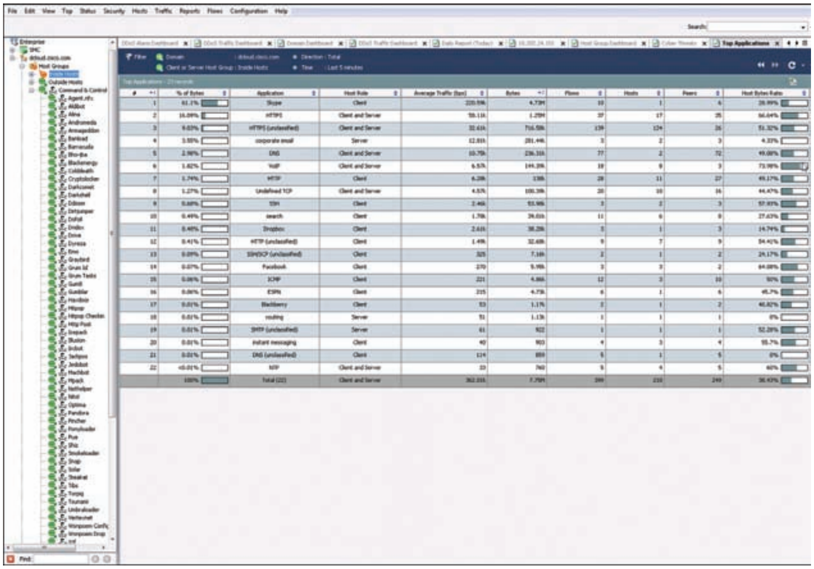
Outbound - 16 records

Application	Traffic Outbound (bytes)	% of Total
HTTP	2.42G	96.31%
HTTPS	71.96M	2.8%
HTTPS (unclassified)	19.71M	0.77%
NFS	1.53M	0.06%
SSH	1.18M	0.05%
Undefined TCP	233.94k	<0.01%
DNS	87.74k	<0.01%
Kerberos (unclassified)	77.27k	<0.01%
SSH/SCP (unclassified)	72.91k	<0.01%
LDAP (unclassified)	44.02k	<0.01%
ICMP	31.24k	<0.01%
Others	13k	<0.01%
corporate email	8.86k	<0.01%
authentication	7.43k	<0.01%
NetBIOS	6.12k	<0.01%
Undefined UDP		0%

Figure 4-1 *Lanscope's SMC Web Management Application*

In Figure 4-1, a summary report of inbound and outbound traffic for a predefined host group in the inside network (Engineering) is displayed.

Figure 4-2 shows a report of the top applications observed in the network for the client and server host group called Inside Hosts. In this report, you can see that the top application observed was Skype. You can drill down each application and host to get more detailed information about what is happening in the network.


File Edit View Top Status Security Hosts Traffic Reports Flows Configuration Help
Search:
Top Applications
Filter

Domain : dcloud.cisco.com
Client or Server Host Group : Inside Hosts
Direction : Total
Time : Last 5 minutes

#	% of Bytes	Application	Host Role	Average Traffic (bps)	Bytes	Flows	Hosts	Peers	Host Bytes Ratio
1	61.1%	Skype	Client	220.59k	4.73M	10	1	6	28.99%
2	16.09%	HTTPS	Client and Server	59.11k	1.29M	37	17	35	66.64%
3	9.03%	HTTPS (unclassified)	Client and Server	32.61k	716.59k	139	124	26	51.32%
4	3.55%	corporate email	Server	12.81k	281.44k	3	2	3	4.33%
5	2.98%	DNS	Client and Server	10.75k	236.31k	77	2	72	49.08%
6	1.82%	VoIP	Client and Server	6.57k	144.39k	18	9	3	73.98%
7	1.74%	HTTP	Client	6.28k	138k	28	11	27	49.17%
8	1.27%	Undefined TCP	Client and Server	4.57k	100.39k	20	10	16	44.47%
9	0.68%	SSH	Client	2.46k	53.98k	3	2	3	57.93%
10	0.49%	search	Client	1.78k	39.01k	11	6	8	27.63%
11	0.48%	Dropbox	Client	2.61k	38.28k	3	1	3	14.74%
12	0.41%	HTTP (unclassified)	Client	1.49k	32.68k	9	7	9	54.41%
13	0.09%	SSH/SCP (unclassified)	Client	325	7.16k	2	1	2	24.17%
14	0.07%	Facebook	Client	270	5.98k	3	3	2	64.08%
15	0.06%	ICMP	Client	221	4.86k	12	3	10	50%
16	0.06%	ESPN	Client	215	4.73k	6	1	6	45.7%
17	0.01%	Blackberry	Client	53	1.17k	2	1	2	40.82%
18	0.01%	routing	Server	51	1.13k	1	1	1	0%
19	0.01%	SMTP (unclassified)	Server	61	922	1	1	1	52.28%
20	0.01%	instant messaging	Client	40	903	4	3	4	55.7%
21	0.01%	DNS (unclassified)	Client	114	859	5	1	5	0%
22	<0.01%	NTP	Client and Server	33	760	5	4	5	60%
	100%	Total (22)	Client and Server	362.33k	7.79M	399	210	249	36.43%

Figure 4-2 *Lancope's SMC Top Applications Report*

Lancope has a security research initiative that tracks emerging threat information from around the world called the StealthWatch Labs Intelligence Center (SLIC). Figure 4-3 illustrates the major components of Lancope's StealthWatch solution.

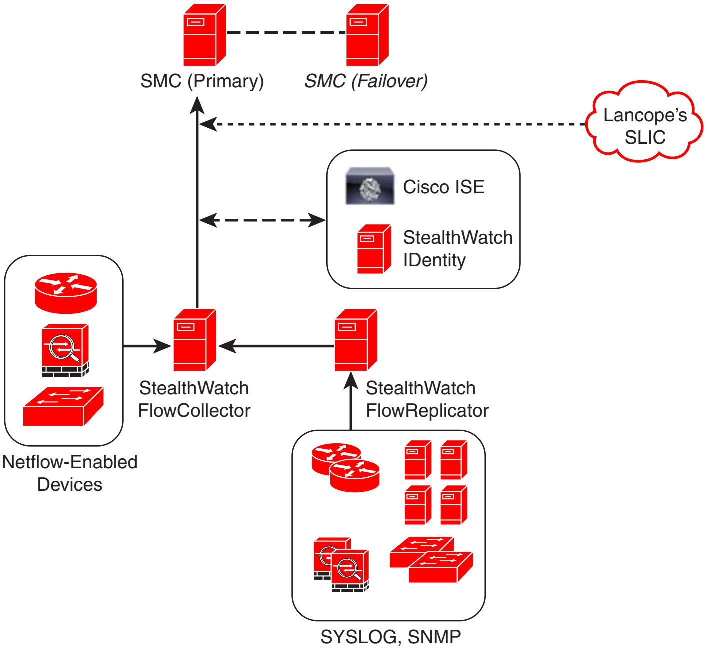


Figure 4-3 *The Lancope's StealthWatch Solution*

The following are the primary components of the Lancope StealthWatch solution shown in Figure 4-1:

- **StealthWatch Management Console:** Provides centralized management, configuration, and reporting of the other StealthWatch components. It can be deployed in a physical server or a virtual machine (VM). The StealthWatch Management Console provides high-availability features (failover), as shown in Figure 4-1.
- **FlowCollector:** A physical or virtual appliance that collects NetFlow data from infrastructure devices.
- **FlowSensor:** A physical or virtual appliance that can generate NetFlow data when legacy Cisco network infrastructure components are not capable of producing line-rate, unsampled NetFlow data. Alternatively, the Cisco NetFlow Generator Appliance (NGA) can be used.
- **FlowReplicator:** A physical appliance used to forward NetFlow data as a single data stream to other devices.
- **StealthWatch IDentity:** Provides user identity monitoring capabilities. Administrators can search on user names to obtain a specific user network activity. Identity data can be obtained from the StealthWatch IDentity appliance or through integration with the Cisco ISE.

Note Lancope StealthWatch also support usernames within NetFlow records from Cisco ASA appliances.

Lancope's StealthWatch solution supports a feature called *Network Address Translation (NAT) stitching*. NAT stitching uses data from network devices to combine NAT information from inside a firewall (or a NAT device) with information from outside the firewall (or a NAT device) to identify which IP addresses and users are part of a specific flow.

Note More information about Lancope's StealthWatch solution is covered in Chapter 6, "Cisco Cyber Threat Defense and NetFlow," and Chapter 8, "Case Studies."

Plixer's Scrutinizer

Plixer's Scrutinizer is another commercial NetFlow monitoring and analysis software package that has gone through interoperability tests by Cisco. Scrutinizer is used for incident response and network monitoring. Just like several components of Lancope's StealthWatch solution, Scrutinizer is available as a physical or virtual appliance.

Plixer also sells two other products that provide additional network visibility: FlowPro and Flow Replicator.

FlowPro is an appliance that can be deployed in a specific area of the corporate network to perform deep packet inspection (DPI) combining NetFlow/IPFIX data. Plixer's Flow Replicator allows several sources of network device and server log data to be replicated to different destinations. Flow Replicator can also be configured as a syslog to IPFIX gateway. It converts syslog messages and forwards them on inside IPFIX datagrams.

Open Source NetFlow Monitoring and Analysis Software Packages

The number of open source NetFlow monitoring and analysis software packages is on the rise. You can use these open source tools to successfully identify security threats within your network.

Table 4-2 lists the most popular open source NetFlow monitoring and analysis software packages.

Table 4-2 *Examples of Open Source NetFlow Monitoring and Analysis Software*

Open Source Software	Description	Website
cflowd	Traffic flow analysis tool provided by the Center for Applied Internet Data Analysis.	http://www.caida.org/tools/measurement/cflowd
flowtools	Tool set for collecting and working with NetFlow data created by Mark Fullmer.	http://www.splintered.net/sw/flow-tools
flowviewer	FlowViewer is a web-based interface to flow tools and SiLK.	http://sourceforge.net/projects/flowviewer
flowd	Small-packaged NetFlow collector.	http://www.mindrot.org/projects/flowd
IPFlow	NetFlow collector developed by Christophe Fillot of the University of Technology of Compiegne, France.	http://www.ipflow.utc.fr
NFdump	NetFlow analysis toolkit under the BSD license.	http://nfdump.sourceforge.net
NfSen	Web interface for NFdump.	http://sourceforge.net/projects/nfsen
Stager	Provides visualizations for NFdump.	https://trac.uninett.no/stager

Table 4-2 *Continued*

Open Source Software	Description	Website
Panoptis	NetFlow tool for detecting denial-of-service attacks. Development is fairly limited.	http://panoptis.sourceforge.net
Plixer's Scrutinizer NetFlow Analyzer	Scrutinizer NetFlow Analyzer a free version of Plixer's Scrutinizer.	http://www.plixer.com/Support/free-tools.html
SiLK	System for Internet-Level Knowledge (SiLK) is a NetFlow collector and analysis tool developed by the Carnegie Mellon University's CERT Network Situational Awareness Team (CERT NetSA).	https://tools.netsa.cert.org/silk
iSiLK	iSiLK is a graphical front end for the SiLK toolkit.	http://tools.netsa.cert.org/isilk
Elasticsearch, Logstash, and Kibana (ELK)	A distributed, scalable, open source big data analytics platform.	https://www.elastic.co/

Two of the most popular open source NetFlow collection and analysis toolkits are NFdump (sometimes used with NfSen or Stager) and SiLK, as described in greater detail in the sections that follow.

NFdump

NFdump is a set of Linux-based tools that support NetFlow Versions 5, 7, and 9. You can download NFdump from http://nfdump.sourceforge.net and install it from source. Alternatively, you can easily install NFdump in multiple Linux distributions such as Ubuntu using **sudo apt-get install nfdump**, as shown in Example 4-1.

Example 4-1 *Installing NFdump in Ubuntu*

```
omar@server1:~$ sudo apt-get install nfdump
[sudo] password for omar:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  linux-headers-3.13.0-53 linux-headers-3.13.0-53-generic
  linux-headers-3.13.0-54 linux-headers-3.13.0-54-generic
  linux-image-3.13.0-53-generic linux-image-3.13.0-54-generic
  linux-image-extra-3.13.0-53-generic linux-image-extra-3.13.0-54-generic
Use 'apt-get autoremove' to remove them.
```