



Mika Alatalo

# Cisco Secure Network Analytics (Stealthwatch)

Metropolia University of Applied Sciences

Master of Engineering

Information Technology

Master's Thesis

2 September 2022

## PREFACE

In this thesis I studied the Cisco Secure Network Analytics system and if it can be used to increase visibility into modern day network infrastructure for customers. When I chose this topic for my thesis, I thought it would be faster to do. However, there was first a period of time where there was no customer project available for this product through my employer. This delayed my graduation from the planned schedule.

There was a plan to modify my topic in a way that it would only have been done in the lab environment, but I got a stroke of luck with a help of my colleague. He was part of a project where the customer wanted to deploy this Secure Network Analytics system into their environment and my colleague remembered that I am waiting that kind of project to get my thesis done. So, he reached out to me and get me be part of the project to deploy this solution for the customer. During this project I learned lot more about of the Secure Network Analytics system and how it can be deployed into real network environments and how it can be used in there.

In the end I will want to thank my colleague Pekka about getting this project for me. Also want to thank Ville from Metropolia for the instructions and help when I was stuck with my thesis. And big thanks to my family for the understanding when I spend extra time after the work with my computer to get this thesis done.

It is finally done now.

Hyvinkää, 2.9.2022

Mika Alatalo

## Abstract

Author: Mika Alatalo  
Title: Cisco Secure Network Analytics (Stealthwatch)  
Number of Pages: 65 pages  
Date: 2 September 2022

Degree: Master of Engineering  
Degree Programme: Information Technology  
Professional Major: Networking and Services  
Supervisors: Ville Jääskeläinen, Principal Lecturer

---

This thesis studies the possibility to increase the visibility into the customer network environment by deploying the Cisco Secure Network Analytics system into the network. It also concentrates on actual installation procedure for the Secure Network Analytics system into the customer's network.

Today's network environments have new kind of threats which are not necessarily seen by firewalls in the network edge. When the networks get bigger in scale and lot of the hosts are sending traffic into the network, it gets harder to the customer to understand what really is happening inside their network. To get increased visibility for the customer's network, the Cisco Secure Network Analytics system was deployed into the customer's network infrastructure. Not all components of the Secure Network Analytics system were deployed into the customer environment. Installed components were the Secure Network Analytics Manager, the Flow Collector and two Flow Sensors. Also, one remote site core device was configured to work as a flow exporter for the Secure Network Analytics system in addition of their normal traffic forwarding activities. Other optional components of the Secure Networks Analytics system were not installed during this project but if there is need, they can be added later to the system.

After the system was installed and when one was able to analyse traffic flows generated by the hosts, it was seen that the visibility into the customer's network increased. To get gains from this increased visibility, the customer needs to have resources which use this system regularly and reacts to the alarms which the system is generating.

Keywords:

Cisco Secure Network Analytics, Visibility, Network

# Contents

## List of Abbreviations

1	Introduction	1
2	Cisco Secure Network Analytics System Overview	4
2.1	Secure Network Analytics Manager (SMC)	5
2.2	Flow Collector (FC)	6
2.3	Data Store	7
2.4	Flow Sensor (FS)	9
2.5	Cisco Telemetry Broker (CTB)	10
2.6	UDP Director	12
2.7	Licenses for the Secure Network Analytics system	13
3	Installation of Cisco Secure Network Analytics	15
3.1	Preparations for the Virtual Environment	16
3.2	Preparing Network for Secure Network Analytics system	20
3.3	Virtual Appliances Installations	25
3.4	Setup with AST (Appliance Setup Tool) and system patching	32
3.5	Licensing, Configuring System and Application installations	38
3.6	Configuring SPAN (Switch Port Analyzer) and NetFlow Exporters	46
4	System Testing and Initial Usage after installation	50
4.1	Working with Host Classifier	51
4.2	Working with Visibility Assessment	52
4.3	Working with Alarms on Network Security Dashboard	54
4.4	Working with the reports on the SMC	58
5	Conclusions	62
	References	65

## List of Abbreviations

AST	Appliance Setup Tool
AWS	Amazon Web Services
CPU	Central Processing Unit
CSV	Comma-separated value
CTB	Cisco Telemetry Broker
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EULA	End user License Agreement
FC	Flow Collector
FPS	Flows Per Second
FS	Flow Sensor
GB	Gigabyte
GUI	Graphical User Interface
HSRP	Hot Standby Router Protocol
IDS	Intrusion Detection System
IPAM	IP Address Management
IPFIX	Internet Protocol Flow Information Export
IPS	Intrusion Prevention System
NGFW	Next Generation Firewall
NIC	Network Interface Card
NTP	Network Time Protocol
NVM	Network Visibility Module for Anyconnect
OVF	Open Virtualization Format
RTT	Round Trip Time
SIEM	Security Information and Event Manager
SLR	Specific License Reservation
SMC	Secure Network Analytics Manager
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SPAN	Switch Port Analyser
SOC	Security Operation Center

SRT	Server Response Time
TAP	Ethernet Test Access Port
TB	Terabyte
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VE	Virtual Edition appliance
VLAN	Virtual Local Area Network
XML	Extensible Markup Language

## 1 Introduction

In recent years customers have developed their network perimeter security by using Next Generation Firewall (NGFW) solutions and these solutions have increased security and visibility in the network perimeter for customers. However, this increased security and visibility in the network perimeter doesn't create totally secured network for customers as it only shows what happens in the network perimeter and not what happens in the whole network.

This network perimeter security doesn't catch any traffic which stays inside network and doesn't go through those perimeter security devices. Among this traffic there could be so called bad traffic such as malware or traffic which is using customer resources incorrectly. As customer doesn't see or know about this bad traffic, their visibility into their network is not in a good state.

To increase visibility and security, some customers have added either Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) into their network. This can add more visibility but as they are mostly signature-based solutions, they usually see traffic which is already known to be bad and not catching traffic which they don't recognize. Also, they don't expose traffic which is misusing network resources. Difference between IDS and IPS is that IDS system only warns about security issues and customer must do preventive measures manually when IPS make preventive measures automatically. IDS and IPS systems efficient use would require customers to study and learn how to use them.

After adding those NGFW and IDS/IPS solutions into customer networks there is still lot of traffic inside their networks which are unknown to them. This traffic needs to be made visible so that potential security threats and network misuse (intended or accidental) can be found, and corrective measures can be made. One way to make this traffic visible is to collect flow data from network and analyze that flow data with different tools.



Flow data can be collected from different network devices such as routers, switches and firewalls. As there are different types of flow data from different vendors products it is crucial that a solution to be used analyze these needs to understand different types of flow data. Examples of these different types of flow data solutions are NetFlow, j-flow and s-flow. The NetFlow solution is Cisco Systems proprietary protocol and used in Cisco devices.

Cisco System has a solution called Cisco Secure Network Analytics (formerly known as Stealthwatch), which is built to gather flow data from different sources and analyse that flow data to find security or other network issues. This solution has several components such as The Secure Network Analytics Manager (SMC), Flow Sensor (FS), Flow Collector (FC) and UDP director. Not all components included in the solution are mandatory to do the actual flow collection and analysis in customer network. There is also cloud version of this solution called Secure Cloud Analytics (formerly known as Stealthwatch Cloud) but this thesis concentrates only on the on-premises solution.

This study will concentrate on installation of Cisco Secure Networks Analytics and what can be learned about the solution during installation. Also, one important part of the study is the usage of the solution after installation and getting initial feedback based on its usage. That feedback could give more information about how suitable this Secure Network Analytics solution is to improve visibility into the customer network and what kind of requirements it will make for customer IT department for using this solution effectively.

This study is done to Telia Cygate and one of its current customer. Telia Cygate is Telia owned company which is concentrating networking, security and data center solutions for business customers. Telia Cygate also offers managed services to business customers in these same areas. Part of their managed services offering is also Security Operation Center (SOC) which could have new service offering based on Secure Network Analytics solution. However, deciding if this could create new service offering for Telia Cygate SOC is not part of this study.

For security reasons the customer to whom this Secure Network Analytics solution was build is named only Customer X in this study. When going through the installation and usage of the solution in this study big part of the pictures are taken from Cisco materials and their live demo environment. Also, when there is configurations for network devices and information like IP addresses and VLAN id, those are not taken from actual customer environment. This is done to keep Customer X data in secret so that those pictures don't show any information which could help to identify the actual customer.

This thesis has been divided into 5 sections. The first section introduces the problem why this thesis was important to do. In the second section this thesis goes through the Cisco Secure Network Analytics solution and its components on general level. The third section of the thesis is the actual installation part of the Cisco Secure Network Analytics into customer X network. The fourth section of the thesis is reserved for initial feedback after the installation and system testing part. Finally, the fifth section of the thesis includes conclusions and discussions of this study.

## 2 Cisco Secure Network Analytics System Overview

The Cisco Secure Network Analytics system has several different components and these components will be discussed in this part of the thesis. Part of the components are mandatory for the solution and other are optional components which can be added to give more broader visibility into the customer network. Mandatory parts of the solution are The Secure Network Analytics Manager (SMC), Flow Collector (FC) and Flow Rate License. Optional parts of the solution are Flow Sensor (FS), the Cisco Telemetry Broker, the UDP (User Datagram Protocol) Director and the Data Store.

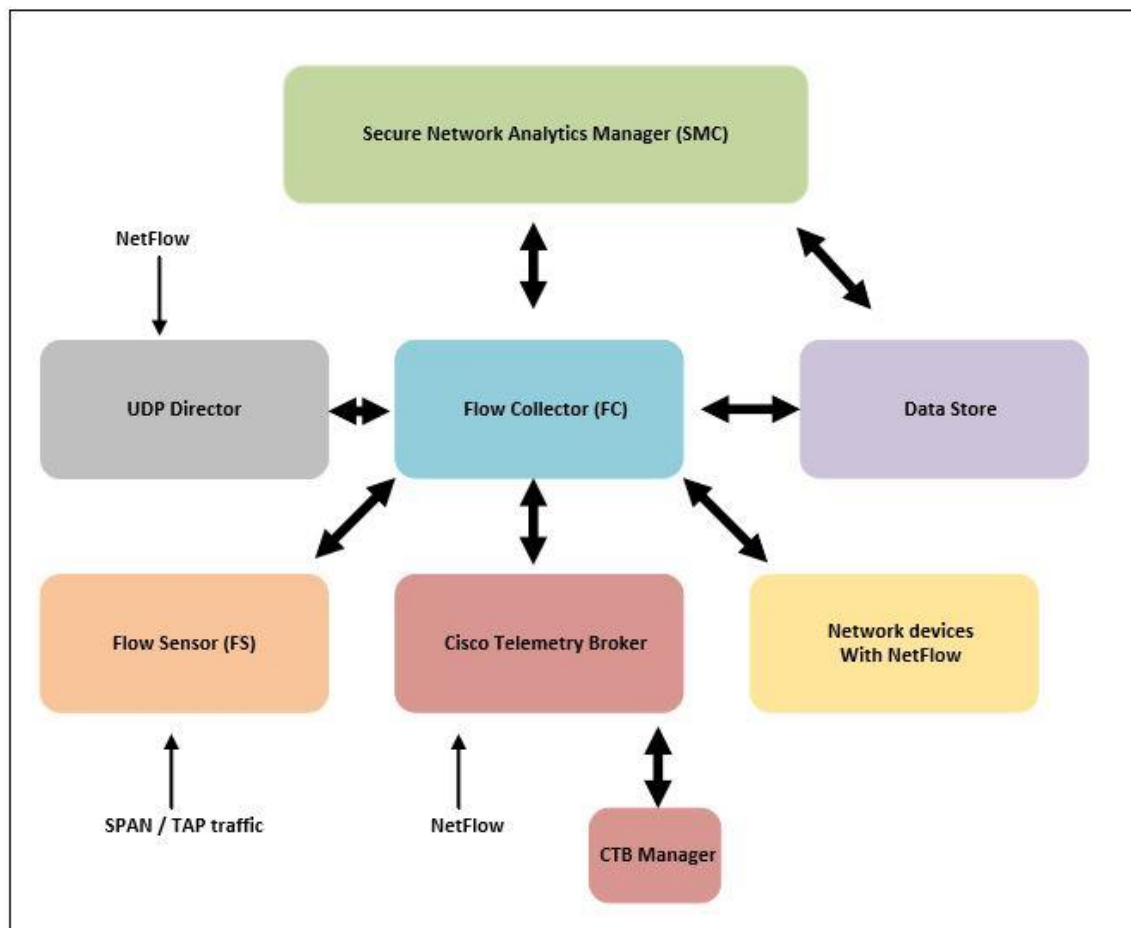


Figure 1: Overview of Secure Network Analytics system components.

In Figure 1 there is an overview of Secure Network Analytics system components and how do they communicate with each other. Flow Rate License is not in the

Figure 1 as it is only a license component inside the system even though this license is a mandatory part of the system. To have flows in Flow Collector there needs to be a device or devices which will feed flows to the Flow Collector. These can be Flow Sensors, Cisco Telemetry Broker and network devices which are capable of NetFlow collection and sending functions. Data Store is an optional component but if it is in place then data traffic flow is from Flow Collector to Data Store and the SMC then communicates with Data Store to show data in its GUI (Graphical User Interface). System components for Secure Network Analytics will be discussed in more detailed one by one in following subsections.

## 2.1 Secure Network Analytics Manager (SMC)

The Secure Network Analytics Manager (SMC) is working as a control center for the whole Secure Network Analytics system. The SMC is a mandatory part of the system and it is responsible for managing, coordinating, configuring and organizing different components of the Secure Network Analytics system. The SMC also provides a single point for network administrator where he/she can see contextual information about all activities across their network. If issues are spotted, then administrator can investigate them with the help of the SMC. The SMC is used through graphical user interface (GUI) which can be reached by using web browser from local computer.

The SMC can use up to 25 Flow Collectors and other sources to gather telemetry data for its network analysis function. This analysis is then created by using network traffic, identity information, customized summary reports, and integrated security and network intelligence. The volume of telemetry data which can be analysed and presented is based on the capacity of the SMC. This also affects the amount of Flow Collectors which can be deployed into customer network. The SMC can be deployed either a physical appliance or a virtual appliance. [1]

Benefit	Description
Real-time, up-to-the-minute data	Delivers data flow for monitoring traffic across hundreds of network segments simultaneously so that you can spot suspicious network behavior. This capability is especially valuable at the enterprise level.
Capability to detect and prioritize security threats	Rapidly detects and prioritizes security threats, pinpoints network misuse and suboptimal performance, and manages event response across the enterprise, all from a single control center.
Management of appliances	Configures, coordinates, and manages Cisco Network Analytics appliances, including the Flow Collector, Flow Sensor, and UDP Director.
Use of multiple types of flow data	Consumes multiple types of flow data, including NetFlow, IPFIX, and sFlow. The result: cost-effective, behavior-based network protection.
Scalability	Supports even the largest of network demands. Performs well in extremely high-speed environments and can protect every part of the network that is IP reachable, regardless of size.
Audit trails for network transactions	Provides a complete audit trail of all network transactions for more effective forensic investigations.
Real-time, customizable relational flow maps	Provides graphical views of the current state of the organization's traffic. Administrators can easily construct maps of their network based on any criteria, such as location, function, or virtual environment. By creating a connection between two groups of hosts, operators can quickly analyze the traffic traveling between them. Then, simply by selecting a data point in question, they can gain even deeper insight into what is happening at any point in time.
Flexible delivery options	You can order the Physical Appliance, a scalable device suitable for any size organization.  Or you can order the Virtual Edition, designed to perform the same functions as the appliance edition, but in a VMware or KVM Hypervisor environment.

Figure 2: Major benefits of the SMC [1]

Figure 2 lists the major benefits which can be achieved by using the Secure Network Analytics Manager (SMC).

## 2.2 Flow Collector (FC)

The Flow Collector (FC) is used for gathering and storing different type of telemetry data from network infrastructure devices. These devices can be routers, endpoints, switches, firewalls, Cisco Telemetry Broker, UDP Director and Flow Sensor. Collected telemetry data can be from NetFlow, IPFIX (Internet Protocol Flow Information Export), NVM (Network Visibility Module for Anyconnect) and other flow types such as J-Flow. After collecting these telemetry data, FC then analyses these telemetry data to provide a complete picture of network activity. [1]

Depending on the capacity of the FC and amount of the telemetry data it gathers, the FC can store months or years of data. This stored data can then be used to create audit trail for improving forensic investigations and compliance initiatives. Secure Network Analytics system can have multiple Flow Collectors installed. When several FC appliances are installed, then their combined capacity will increase the volume of telemetry data which can be collected from the network compared to only a single FC appliance installation. Flow Collector can be deployed either a hardware appliance or a virtual appliance. [1]

Benefit	Description
Threat detection	Ingests proxy records and associates them with flow records to deliver the user application and URL information for each flow to increase contextual awareness. This process enhances your organization's ability to pinpoint threats and shortens your Mean Time to Know (MTTK).
Flow traffic monitoring	Monitors flow traffic across hundreds of network segments simultaneously so that you can spot suspicious network behavior. This capability is especially valuable at the enterprise level.
Extended data retention	Allows organizations and agencies to retain large amounts of data for long periods.
Scalability	Performs well in extremely high-speed environments and can protect every part of the network that is IP reachable, regardless of size.
Deduplication and stitching	Performs deduplication so that any flows that might have traversed more than one router are counted only once. It then stitches the flow information together for complete visibility of a network transaction.
Choice of delivery methods	You can order the Appliance Edition, a scalable device suitable for any size organization. Or you can order the Virtual Edition, designed to perform the same functions as the appliance edition, but in a VMware or KVM Hypervisor environment. This solution scales dynamically according to the resources allocated to it.

Figure 3: Major benefits of the Flow Collector [1]

Figure 3 lists the major benefits which can be achieved by using Flow Collector (FC).

### 2.3 Data Store

The Data Store is one of the newest components in Secure Network Analytics system. It is aimed for environments where a volume of telemetry data is at high level or there is need to have telemetry data available for long time, exceeding capacity of one or more Flow Collectors. The Data Store is a cluster which

includes minimum of three Data Node appliances and received data is distributed equally across these nodes. In the Secure Network Analytics system Data Store can be deployed between Flow Collectors and the Secure Network Analytics Manager. [1]

Flow Collectors send their gathered flow data and their flow data analysis results to the Data Store. This way Data Store has all customers telemetry data in one centralized location. The Secure Network Analytics Manager has then access to telemetry data stored in Data Store for reporting and responding to threats and alerts. With Data Store and its centralized model customers can have greater storage capacity, flow rate ingestion and better resiliency when compared to a system where customers have several Flow Collectors and no Data store. The Data Store can be either a physical or a virtual solution. [1]

Benefit	Description
<b>Increases data ingest capacity</b>	Data Stores can be combined to create a single cluster of data nodes capable of monitoring over 3 million flows per second (FPS) to aid in relieving ingestion bandwidth challenges for organizations with high flow volumes.
<b>Enterprise-class data resiliency</b>	Telemetry data is stored redundantly across nodes to allow for seamless data availability during single node failures, helping to ensure against the loss of telemetry data. Deployments with two Data Stores or more can support up to 50% of data node loss and continue to operate.* The Data Store also supports redundant interconnection switches to remain fully operational during network upgrades and unplanned outages.  *Depending on your hardware configuration and installation.
<b>Significant query and reporting response time improvements</b>	The Data Store provides drastically improved query performance and reporting response times that are at least 10x faster than those offered by other standard deployment models. It can also perform an increased number of concurrent queries, whether through APIs or the Secure Network Analytics Manager web UI. These query improvements stand to deliver substantial operational efficiency gains. Through the ability to run reports and get answers more quickly, the Data Store enables practitioners to pinpoint and respond to threats more quickly to expedite triage, investigation, and remediation workflows.
<b>Storage scalability</b>	The Data Store offers organizations with growing networks enhanced flexibility around data storage scalability through the ability to add additional database clusters.
<b>Long-term data retention</b>	Scalable and long-term telemetry storage capabilities enable long-term flow retention of up to 1 to 2 years' worth of data with no need to add additional Flow Collectors. This aids in satisfying regulatory requirements and reducing costs and complexity associated with purchasing and integrating third-party storage solutions or extra Flow Collectors.

Figure 4: Major benefits of the Data Store [1]

Figure 4 lists the major benefits which can be achieved by adding the Data Store as part of the Secure Network Analytics system.

## 2.4 Flow Sensor (FS)

The Flow Sensor is an optional component of the Secure Network Analytics system. The Flow Sensor is used to create telemetry data in network segments where switches and routers can't generate NetFlow data by themselves. It can also be used in a situation where customer don't want to configure NetFlow in large number of devices in order to keep device configurations simple as possible. Visibility into the application layer data can also be achieved with the help of Flow Sensors. With this application layer visibility, the Flow Sensor can provide information about round trip time (RTT), server response time (SRT) and packet loss for TCP sessions (retransmissions). [1]

The Flow Sensor can be connected to customer network by using SPAN (switch port analyser) port, mirror port or TAP (Ethernet test access port) in network device. The Flow Sensor captures Ethernet frames from the traffic which it gets into its sensor port and based on those captured Ethernet frames the Flow Sensor creates flow records. These flow records are then sent from Flow Sensor to Flow Collector for analysis. The Secure Network Analytics system can include multiple Flow Sensors. The Flow Sensor can be either a physical appliance or a virtual appliance. [1]



Benefit	Description
Layer 7 application visibility	Provides true Layer 7 application visibility by gathering application information. This includes data features like RTT (Round Trip Time), SRT (Server Response Time), and Retransmissions.
Packet-level performance and analysis	Provides true Layer 7 application visibility by gathering application information. This includes data features like RTT, SRT, and Retransmissions.
Alerts on network anomalies	Additional telemetry from the Flow Sensor, such as URL information for web traffic and TCP flag detail, helps generate alarms with contextual intelligence so that security personnel can take quick action and mitigate damage.
Lower costs	Enhances operational efficiency and reduces costs by identifying and isolating the root cause of an issue or incident within seconds.
Choice of delivery methods	You can order the Appliance Edition, a scalable device suitable for any size organization. Or you can order the Virtual Edition, designed to perform the same function as the appliance edition, but in a VMware or KVM Hypervisor environment.

Figure 5: Major benefits of the Flow Sensor [1]

Figure 5 lists the major benefits which can be achieved if the Flow Sensor is added as a component into Secure Network Analytics system.

## 2.5 Cisco Telemetry Broker (CTB)

The Cisco Telemetry Broker is an optional component in Secure Networks Analytics system. It was made available for customers during spring 2021. The Cisco Telemetry Broker is built with at least two virtual nodes. These nodes are Management Server and Brokering Node. The CTB Management Server is only used for management of CTB Brokering Nodes and it doesn't manage any other component in Secure Network Analytics system. Below in Figure 6 there are resources which need to be reserved for virtual CTB Management Server and CTB Brokering Node. [2]

	Distributed	
	Management Server	Brokering Node
CPU	4 CPUs	1 Gbit/s: 2 CPUs 10 Gbit/s: 5 CPUs Transformation Capable: 8 GB
Memory	8 GB	1 Gbit/s: 4 GB 10 Gbit/s: 8 GB Transformation Capable: 12 GB
Storage	80 GB	70 GB

Figure 6: CTB virtual device resources [2]

The network telemetry data from various sources can be send to the Cisco Telemetry Broker. After the CTB has received the telemetry data, it can transform telemetry data to wanted data format and then forward it to one or multiple destinations. When the CTB is used in Secure Network Analytics system, then telemetry data is forwarded into the Flow Collector for analysis. Other additional telemetry data sources, for example, can be analytics platforms such as Hadoop and Security Information and Event Management (SIEM) platforms. Telemetry data sources for the CTB can be either on-premises or cloud-based. On-premises telemetry data for the CTB can include IPFIX, NetFlow and SYSLOG. Cloud based telemetry data for the CTB can include AWS VPC flow logs and Azure NSG flow logs. [1]

Benefit	Description
Brokering data	The ability to route and replicate telemetry data from a source location to multiple destination consumers to facilitate quick onboarding of new telemetry-based tools.
Filtering data	The ability to filter data that is being replicated to consumers for fine-grain control over what consumers can see and analyze. This can also help users save money by removing the need to send data to expensive tools.
Transforming data	The ability to transform data protocols from the exporter to the consumer's protocol of choice. This enables Secure Network Analytics and other tools to consume multiple and prior, noncompatible data formats.

Figure 7: Major benefits of the Cisco Telemetry Broker [1]

Figure 7 lists the major benefits gained with Cisco Telemetry Broker component when it is added into Secure Network Analytics system.

## 2.6 UDP Director

The UDP Director is an optional component in Secure Network Analytics system. It can be either a physical or a virtual appliance. Major difference between a physical and a virtual appliance is that only a physical appliance supports high availability setup between UDP directors in Secure Network Analytics system. The UDP Director provides a single destination for all UDP based telemetry data such as NetFlow, sFlow, Syslog and SNMP (Simple Network Management Protocol). Received telemetry data is then forwarded by UDP Director to a single or multiple destination. In Secure Network Analytics system destination to telemetry data traffic from UDP Director is the Flow Collector. [1]

The UDP Director is beneficial in large environments where infrastructure devices can be told to send telemetry data into the UDP Director and it forwards the telemetry data to the Flow Collector. If there is a need to add an additional destination for the telemetry data, then the only needed change is done in UDP Director configuration and all other network infrastructure don't need to have any changes. This way changes done in large environments don't cause a lot of additional work for network administrators.

Benefit	Description
Reduces unplanned downtime and service disruption	UDP Director high availability applies to the UDP Director 2210 appliance.
Simplifies network security and monitoring	UDP Director aggregates and provides a single standardized destination for NetFlow, sFlow, Syslog, and Simple Network Management Protocol (SNMP) information. UDP Director appliances can receive data from any connectionless UDP application and then retransmit it to multiple destinations, duplicating the data if required.
Can direct UDP data from any source to any destination	Receives data from any connectionless UDP application and then retransmits it to multiple destinations, duplicating the data if required.
Removes the need to reconfigure infrastructure	Directs point log data (NetFlow, sFlow, Syslog, SNMP) to a single destination without the need to reconfigure the infrastructure when new tools are added or removed.

Figure 8: Major benefits of the UDP Director [1]

Figure 8 lists the major benefits which can be achieved when the UPD Director is added as a component into Secure Network Analytics system.

## 2.7 Licenses for the Secure Network Analytics system

The Flow Rate License is a mandatory part of the Secure Network Analytics System. The SMC uses this license for collecting, managing and analysing flow data. The Flow Rate license is based on Flows Per Second (FPS) and defines the number of flows which can be collected into the system. The Flow Rate licenses can be bought with different sizes and combined to get the desired level of flow capacity. If FPS exceeds the current license level, then the SMC alerts that system is not at authorized level for Flow Rate license and to get rid of this alert an additional license needs to be purchased. In this case this alert is informational in a way that system does work normally and flows which exceeds FPS limit are also analysed. [1]

The Cisco Secure Network Analytics Endpoint license is an additional license. It is used to extend visibility to end-user devices and it helps to secure remote workers. For this license to work, also needed are Cisco Anyconnect client with the Network Visibility Module (NVM) and Endpoint Concentrator. This works in a way that NVM generates flow data (nvzFlow) from endpoints both on and off premises. Then NVM sends this nvzFlow to Endpoint Concentrator which is a virtual appliance. The Endpoint Concentrator collects telemetry data from all the endpoint devices which uses the NVM and this collected data is then sent to the Flow Collector for analysis. [3]

The Cisco Secure Network Analytics Threat Feed license is also an additional license for Security Network Analytics system. With this license customer gets a global threat intelligence feed from Cisco Talos. Cisco Talos is a threat intelligence group which researchers, analysts and engineers are working to defend Cisco customers for known and unknown vulnerabilities. This Threat Feed license can provide protection against botnets and other attacks. As for Cisco Talos it sees 1,5 million unique malware samples and blocks 20 billion threats

per day. If Threat Feed license is planned to be included, then it needs to be bought for each Flow Collector which are present in the Secure Network Analytics system. [1]

### 3 Installation of Cisco Secure Network Analytics

This part of the thesis concentrates on installation of the Secure Network Analytics system. The system installation was done for one of the Telia Cygate's customer. For security reasons that customer is called Customer X in this thesis. Because of this also pictures related to installation part are either created during installation part without customer info or taken from Cisco System's general guides. The Secure Network Analytics system, which was installed to Customer X network, doesn't include all system components as it was fitted for Customer X current needs. Also, components which were not installed this time, can be added later to the system.

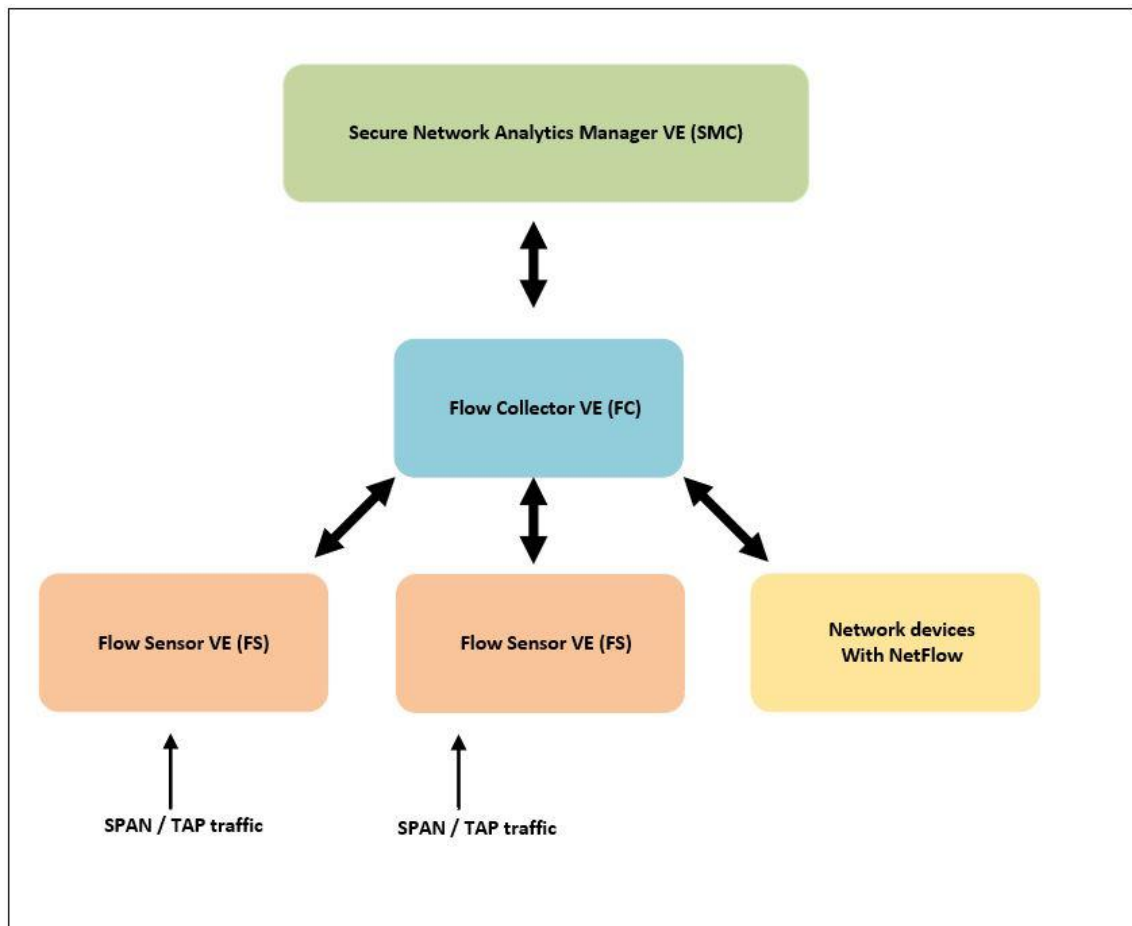


Figure 9: Customer X installed Secure Network Analytics components

Figure 9 shows the Secure Network Analytics system which was installed for Customer X network infrastructure. For this Customer X solution, it was decided that all the appliances are virtual editions. In this Customer X system there is one SMC VE installed and one Flow Collector VE installed. Then there is two Flow Sensors VE installed and some network devices were configured to send NetFlow data to Flow Collector. The Customer X network is present in several locations in Finland and two main sites are Helsinki and Turku. As these two main sites are also the sites where almost all customer networks can be seen, it was decided to install the solution components to Helsinki and Turku as well.

On Helsinki site there is the SMC, the Flow Collector and one Flow Sensor installed. On Turku site there is only one Flow Sensor installed. Network devices which will sent the NetFlow traffic to the Flow Collector, where chosen based the fact that they might have inter VLAN traffic in a way that inter VLAN traffic won't reach either Helsinki or Turku site. If traffic won't reach Helsinki or Turku site, then it won't be seen with the Flow Sensors installed on those sites. With configuring the network devices to send the NetFlow traffic to the Flow Collector, blind spot created by inter VLAN traffic in those network devices is avoided. Installation procedure on order for this Secure Network Analytics system for the Customer X is gone through following sub-sections of this thesis.

### 3.1 Preparations for the Virtual Environment

Before virtual appliances can be installed, there is need to do some preparation work for the Customer X virtual environment. In this part needed resources are reserved for the different virtual appliances from underlying hardware infrastructure. When reserving resources for the virtual appliances, it is important to reserve at least required resources so that the virtual appliances can run properly. As the Customer X has people who are responsible to run virtual server infrastructure, they made needed reservations based on following provided resource needs for the Secure Network Analytics Manager, the Flow Collector and the Flow Sensors.

The Secure Network Analytics Manager (SMC) has following resource requirements as shown in Figure 10 based on Cisco's guidance in their Stealthwatch Virtual Edition Installation Guide 7.3.0.

Flow Collectors	Concurrent Users*	Required Reserved Memory	Required Reserved CPUs
1	2	24 GB	3
3	5	32 GB	4
5	10	32 GB	4

\*Concurrent users include scheduled reports and people using the SMC client at the same time.

Figure 10: The SMC required resources for Virtual Appliance [4]

In the Customer X current system there is only one Flow Collector, but it is decided to reserve more resources for the SMC virtual appliance.

```
*****
* Stealthwatch Management Console (Helsinki) *
* 4 x CPU, 32GB Memory, 100GB Disk Space *
*****
```

Figure 11: Actual reserved resources for the virtual SMC

Actual resources reserved for the SMC virtual appliance is shown in Figure 11. With these resources the Customer X's SMC is capable to manage additional Flow Collector if there is need to add one into the system. It will also allow more concurrent users to log into the SMC same time with scheduled reports running.

The resource reservations for the Flow Collector are based on how many hosts it is expected to be monitored by the Flow Collector, the number of the exporters in the system and amount of the flows per seconds received into the Flow Collector. The following Figure 12 shows resource requirements for the Flow



Collector based on the Cisco's Stealthwatch Virtual Edition Installation Guide 7.3.0.

Flows per second	Exporters	Hosts	Required Reserved Memory	Required Reserved CPUs	Flow Collector VE Model
Up to 4,500	Up to 250	Up to 125,000	16 GB	2	FCVE
Up to 15,000	Up to 500	Up to 250,000	24 GB	3	FCVE
Up to 22,500	Up to 1000	Up to 500,000	32 GB	4	FCVE
Up to 30,000	Up to 1000	Up to 500,000	32 GB	6	FCVE
Up to 60,000	Up to 1500	Up to 750,000	64 GB	8	2000
Up to 120,000	Up to 2000	Up to 1,000,000	128 GB	12	4000

Figure 12: Resource requirements for the Flow Collector [4]

As there is no specific information about the number of the flows per seconds the Flow Collector will receive from the sensors and the exporters, it is decided to reserve resources which could handle up to 22500 flows per second.

```
*****
* Flow Collector VE resources (Helsinki)                               *
* 5 x CPU, 32GB Memory, 1 TB Disk Space                               *
*****
```

Figure 13: Actual reserved resources for the Flow Collector

Figure 13 shows actual resources reserved for The Flow Collector virtual appliance. This Flow Collector will also be able to monitor up to 500000 hosts and receive telemetry data from up to 1000 exporters, which is more than enough in the Customer X case.

The Flow Sensor virtual appliances have resource requirements based on Stealthwatch Virtual Edition Installation Guide 7.3.0 shown in following Figure 14.

NICs - monitoring ports (1 Gb)	Required Reserved CPUs	Required Minimum Reserved Memory	Estimated Throughput	Flow Cache Size (maximum number of concurrent flows)
1	2	4 GB	850 Mbps	32,766
2	4	8 GB	1,850 Mbps Interfaces configured as PCI pass-through (igb/ixgbe compliant or e1000e compliant)	65,537
4	8	16 GB	3,700 Mbps Interfaces configured as PCI pass-through (igb/ixgbe compliant or e1000e compliant)	131,073

**Optional:** One or more 10G NICs may be used on the physical VM host.

Figure 14: Resource requirements for The Flow Sensor virtual appliance [4]

As there is two Flow Sensors installed into the Customer X's network, important requirement is the flow cache size per installed sensor. It is estimated that 32766 maximum concurrent flows per sensor is more than enough for this installation.

```
*****
* Flow Sensor VE resources (Helsinki and Turku) *
* 2 x CPU, 4GB Memory, 50GB Disk Space (10G NIC for monitoring) *
*****
```

Figure 15: Actual reserved resources for the Flow Sensors virtual appliances

Both Flow Sensors have one dedicated network interface card port for getting the traffic from the Customer X's LAN switch port. This monitoring port speed is decided to be 10 Gbit/s in Flow Sensors. With these resource reservations the Flow Sensors virtual appliances can provide telemetry data to the Flow Collector in the Customer X environment.

### 3.2 Preparing Network for Secure Network Analytics system

Important part for the Secure Network Analytics system is to prepare the network to provide connectivity for the virtual appliances. As system is divided into two sites (Helsinki and Turku), there is need to make network configurations on both sites as well. The network configurations include planning the IP addressing, VLAN id reservations, network device configurations and needed firewall rule planning and deployment.

Local routing in the Helsinki and the Turku site is handled by pair of Cisco switches which can do both routing and switching. Having pair of switches in one site is done for enabling the high availability solution for that site. If one device breaks, then another device will handle the routing and the switching for the traffic and keeping the site functionally in the Customer X's network. High availability between two switches is built with configuring the HSRP (Hot Standby Router Protocol) to both switches. The HSRP needs to be kept in mind when planning the IP addressing for the IP subnets in both the Helsinki and the Turku site.

IP address needs in the Helsinki site are 3 IP addresses for the HSRP switch pair, one IP address for the SMC, one IP address for the Flow Collector and one IP address for the Flow Sensor. This gives six IP addresses for the devices in subnet in the Helsinki site. For fulfilling this six IP address need, the network 192.168.10.0 with subnet mask /29 is chosen for the devices in the Helsinki site as this gives six IP addresses for the devices. Also, the VLAN id 2001 is given to this network for separating it from other VLAN's in the Helsinki site.

```

*****
* Helsinki: ip addressing for vlan 2001 (Secure Network Analytics vlan) *
* * *
* 192.168.10.0/29 (subnet for Secure Network Analytics) *
* 192.168.10.1 HSRP standby virtual address (default gateway for hosts in vlan) *
* 192.168.10.2 Primary router address in HSRP *
* 192.168.10.3 Backup router address in HSRP *
* 192.168.10.4 Flow Sensor virtual appliance - hostname: fsve-helsinki01 *
* 192.168.10.5 Flow Collector virtual appliance - hostname: fcve-helsinki01 *
* 192.168.10.6 SMC (manager) virtual appliance - hostname: smcve-helsinki01 *
* 192.168.10.7 Broadcast address in subnet *
*****

```

Figure 16: IP addressing for the devices in the Helsinki site

Figure 16 show how the IP addresses are divided from the network 192.168.10.0/29 between different devices in the VLAN id 2001 for the Helsinki site and for the Secure Network Analytics system in there.

IP addresses needs in the Turku site are 3 IP addresses for the HSRP switch pair and one IP address for the Flow Sensor. This gives four IP addresses for the devices in subnet in the Turku site. For fulfilling this four IP address need, the network 192.168.40.0 with subnet mask /29 is chosen for the devices in the Turku site. This gives six IP addresses for the Turku site usage as well. Also, the VLAN id 3001 is given to this network for separating it from other VLAN's in the Turku site.

```

*****
* Turku: ip addressing for vlan 3001 (Secure Network Analytics vlan) *
* * *
* 192.168.40.0/29 (subnet for Secure Network Analytics) *
* 192.168.40.1 HSRP standby virtual address (default gateway for hosts in vlan) *
* 192.168.40.2 Primary router address in HSRP *
* 192.168.40.3 Backup router address in HSRP *
* 192.168.40.4 Flow Sensor virtual appliance - hostname: fsve-turku01 *
* 192.168.40.5 not used - free *
* 192.168.40.6 not used - free *
* 192.168.40.7 Broadcast address in subnet *
*****

```

Figure 17: IP addressing for the devices in the Turku site

Figure 17 shows how IP addresses are divided from the network 192.168.40.0/29 between different devices in the VLAN id 3001 for the Turku site and for the Secure Network Analytics system in there.

These planned IP addressing can be then used to built needed configurations in the switches both in the Helsinki and the Turku site.

```
*****
* Primary HSRP switch configuration in Helsinki site.      *
* !                                                         *
* vlan 2001                                                *
* name SNA                                                 *
* !                                                         *
* interface Vlan2001                                       *
* description Secure Network Analytics                     *
* ip address 192.168.10.2 255.255.255.248                 *
* standby version 2                                        *
* standby 10 ip 192.168.10.1                               *
* standby 10 priority 110                                  *
* standby 10 preempt                                       *
* standby 10 authentication md5 key-string HKI-SNA-HSRP   *
* !                                                         *
*****
* Backup HSRP switch configuration in Helsinki site.      *
* !                                                         *
* vlan 2001                                                *
* name SNA                                                 *
* !                                                         *
* interface Vlan2001                                       *
* description Secure Network Analytics                     *
* ip address 192.168.10.3 255.255.255.248                 *
* standby version 2                                        *
* standby 10 ip 192.168.10.1                               *
* standby 10 priority 105                                  *
* standby 10 preempt                                       *
* standby 10 authentication md5 key-string HKI-SNA-HSRP   *
* !                                                         *
*****
```

Figure 18: Added configurations in Primary and Backup HSRP switch in Helsinki

Added configurations for both the primary HSRP switch and the backup HSRP switch in the Helsinki site are shown in Figure 18. With these configurations the VLAN 2001 and the VLAN interface 2001 with related HSRP configuration is added. Both the primary HSRP switch and the backup HSRP switch are running dynamic routing protocol for advertising their networks to other part of the Customer X's network. In dynamic routing part of the configuration, it is defined

that when the new connected network is added, it will be also added into routing advertising automatically. When new VLAN interface is created and IP subnet is added under that then that same IP subnet will be part of the connected networks in the device automatically.

```
*****
* Primary HSRP switch configuration in Turku site.      *
* !                                                    *
* vlan 3001                                           *
*   name SNA                                          *
* !                                                    *
* interface Vlan3001                                  *
*   description Secure Network Analytics              *
*   ip address 192.168.40.2 255.255.255.248         *
*   standby version 2                                 *
*   standby 10 ip 192.168.40.1                      *
*   standby 10 priority 110                          *
*   standby 10 preempt                               *
*   standby 10 authentication md5 key-string TKU-SNA-HSRP *
* !                                                    *
*****
* Backup HSRP switch configuration in Turku site.     *
* !                                                    *
* vlan 3001                                           *
*   name SNA                                          *
* !                                                    *
* interface Vlan3001                                  *
*   description Secure Network Analytics              *
*   ip address 192.168.40.3 255.255.255.248         *
*   standby version 2                                 *
*   standby 10 ip 192.168.40.1                      *
*   standby 10 priority 105                          *
*   standby 10 preempt                               *
*   standby 10 authentication md5 key-string TKU-SNA-HSRP *
* !                                                    *
*****
```

Figure 19: Added configurations in Primary and Backup HSRP switch in Turku

Added configurations for both the primary HSRP switch and the backup HSRP switch in the Turku site are shown in Figure 19. With these configurations the VLAN 3001 and the VLAN interface 3001 with related HSRP configuration is added. Also, in the Turku site both the primary HSRP switch and the backup HSRP switch are running dynamic routing protocol for advertising their networks to other part of the Customer X's network. In these devices dynamic routing protocol is also advertising connected networks, which means that when IP

network is added into the VLAN 3001 then that IP network is also advertised out from the Turku site.

The firewall rules are also needed to allow the traffic to and from the Secure Network Analytic system. The Customer X has team that is responsible to monitor and manage all firewalls in the network. This means that this firewall team will deploy new needed firewall rules based on requests which are delivered to them. For this deployment part the required firewall rules needs to be defined.

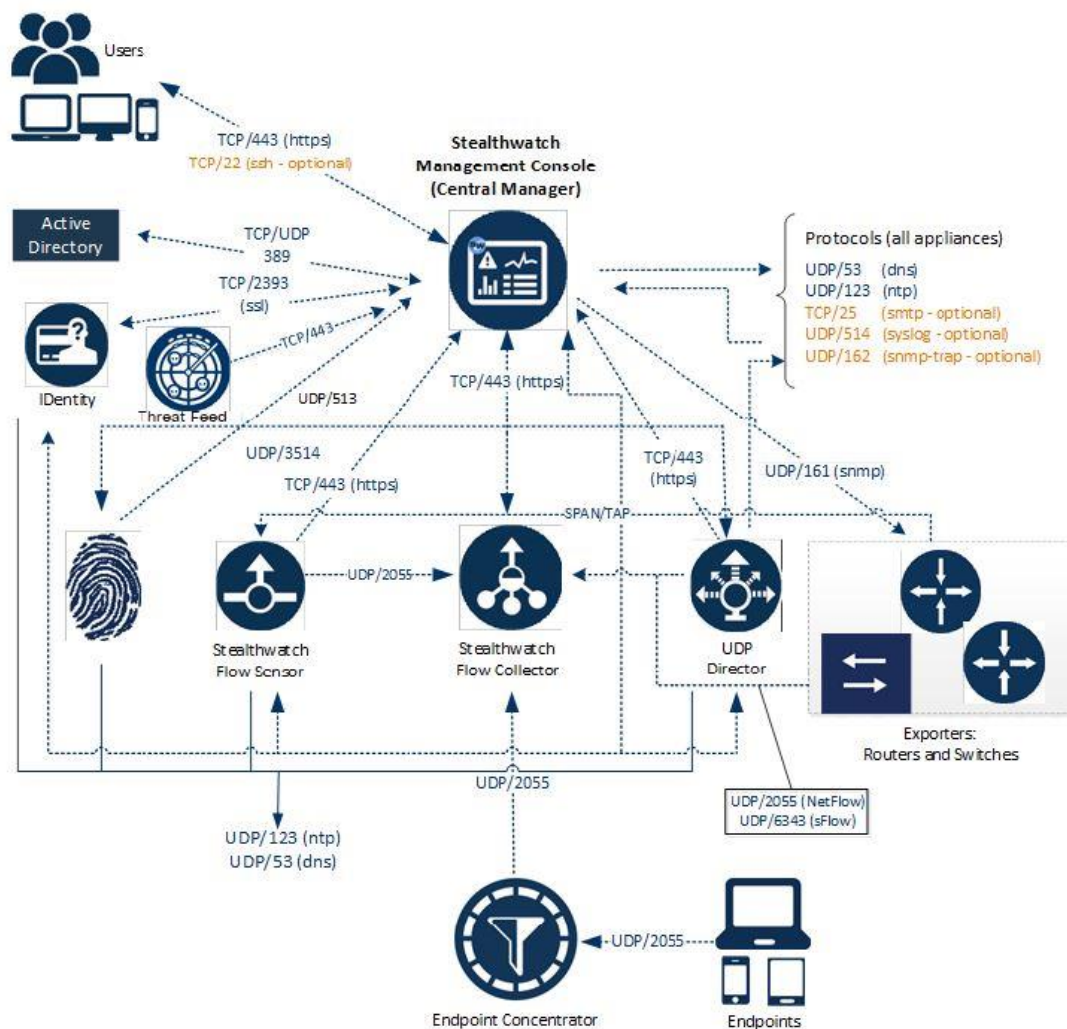


Figure 20: Connections in system for firewall rule creation needs [4]

The Figure 20 shows all connections related to the Secure Network Analytics system which might need firewall rules to allow the required traffic. In the

Customer X case there is no need to create all communications shown in Figure 20 as not all components are part of the installed system. The SMC, the Flow Collector and the Flow Sensor in the Helsinki site can communicate with each other without any firewall rules as their IP addresses are in the same network. In the Customer X network firewall rules don't affect traffic between devices which belong to the same IP network. The firewall rules need to be defined between devices which traffic passes the IP network boundaries.

```

*****
* From (client)          To (Server)          Port          Protocol      *
*                       *                       *           *
* Admin User PC         All appliances       TCP/443       HTTPS         *
* Admin User PC         All appliances       TCP/22        SSH           *
* All appliances        NTP server           UDP/123       NTP           *
* Flow Sensor Turku     SMC                  TCP/443       HTTPS         *
* Flow Sensor Turku     Flow Collector       UDP/2055      NetFlow       *
* NetFlow Exporters     Flow Collector       UDP/2055      NetFlow       *
* SMC                   DNS                  UDP/53        DNS           *
* SMC                   Flow Sensor Turku    TCP/443       HTTPS         *
* SMC                   NetFlow Exporters    UDP/161       SNMP          *
* SMC                   LDAP /AD             TCP/UDP/636   LDAPS         *
* SMC                   Monitoring servers   UDP/162       SNMP-trap     *
* SMC                   Monitoring servers   UDP/514       SYSLOG        *
* SMC                   Email gateway        TCP/25        SMTP          *
*****

```

Figure 21: Required firewall rules for the Customer X SNA system

The Figure 21 shows required firewall rules for the Customer X's Secure Network Analytics system needed communications. In the Figure 21 there is only shown object names and not the IP addresses belonging to those objects. This is because IP addresses are kept secret for security reasons. In the actual firewall rule request, there is also IP addresses with the object names. After these rules are implemented, then the Customer X's network is prepared for the Secure Network Analytics system for the firewall part also.

### 3.3 Virtual Appliances Installations

First thing to do on the virtual appliance installation is to get the correct software installation files. These can be gotten from the Cisco Systems software download web site. Access to the download section of Cisco's web site requires login with



the personal Cisco web site account. This account should also have enough access rights in that download web site before the actual software download can happen.

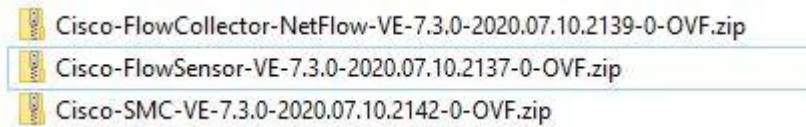


Figure 22: Virtual appliance software for SMC, Flow Collector and Flow Sensor

The Figure 22 shows virtual appliance software versions which are deployed for the SMC, the Flow Collector and Flow Sensor in the Customer X environment.

Both Flow Sensors virtual appliances are used for monitoring the traffic from the external data source. This external data source is switch port configured for the traffic mirroring both in the Helsinki and the Turku site switches. This approach requires dedicated PCI pass-through interface on a physical server which is then used by the Flow Sensor virtual appliance as a monitor port. The Customer X's server team prepared that PCI pass-through interface for the Flow Sensor virtual appliance usage.

Installing a virtual appliance starts with unzipping those earlier downloaded virtual appliance software. These downloaded files can be seen in Figure 22 above. Inside the zip files there are OVF file and VMDK file which will be used for virtual appliance installation. Zip files for both the SMC and the Flow Collector includes OVF files for other virtual appliance versions so when deploying these, correct OVF files needs to be chosen for installation. For the SMC deployment the SMCVE.ovf is the file which will be used and for the Flow Collector deployment the FCNFVE.ovf is the file which will be used from different versions inside Zip files.

The following steps can be used to install a virtual appliance on the Customer X's virtual environment hypervisor host. By right-click the host there will be option "Deploy OVF Template" which needs to be selected. This opens the Deploy OVF

template dialog box which has several steps for the virtual appliance installation. These steps will be gone through next with example figures. [4]



Figure 23: Select and OVF template [4]

Figure 23 shows the first step which is choosing the correct virtual appliance OVF and VMDK files.



Figure 24: Select a name and folder [4]

Figure 24 shows second step where the virtual machine is named and save location for the virtual appliance is selected.

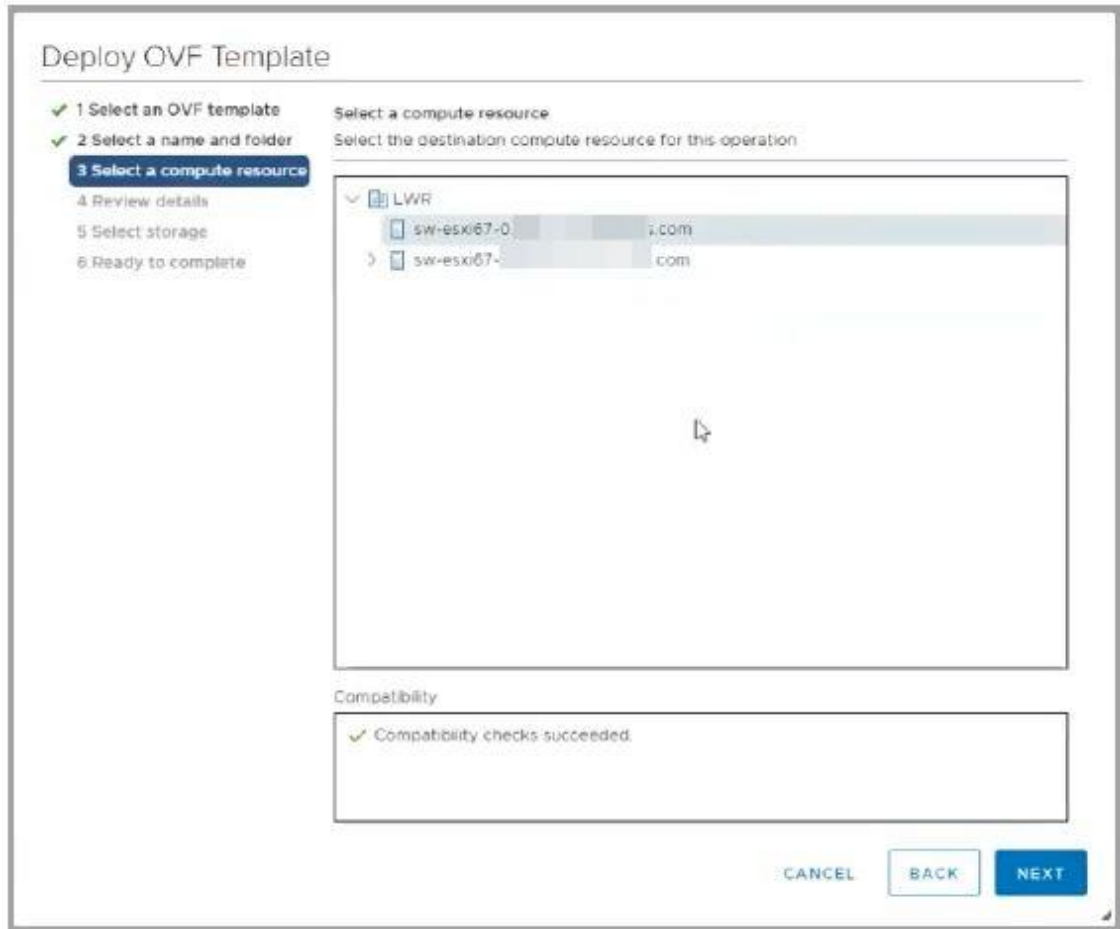


Figure 25: Select a compute resource [4]

Figure 25 shows the third step where destination compute resource is selected for the virtual appliance installation.

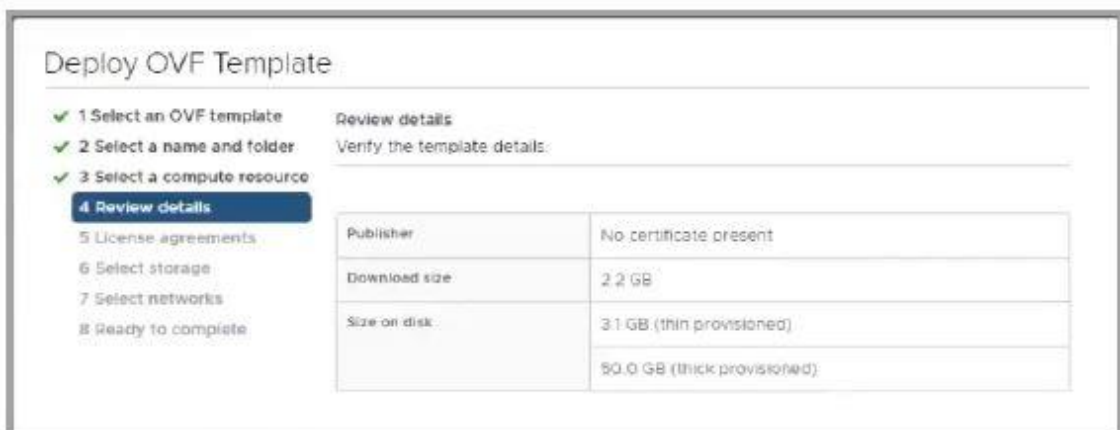


Figure 26: Review details [4]

Figure 26 shows the fourth step where details of the OVF deployment can be reviewed. After this is fifth step where the End User License Agreement (EULA) is reviewed and accepted.



Figure 27: Select storage [4]

Figure 27 shows the sixth step where location to the store data files is selected. Virtual disk format can be the Thick Provision Lazy Zeroed, the Thick Provision Eager Zeroed or the Thin Provision. The Thin Provision format should only be used if the disk space is limited.

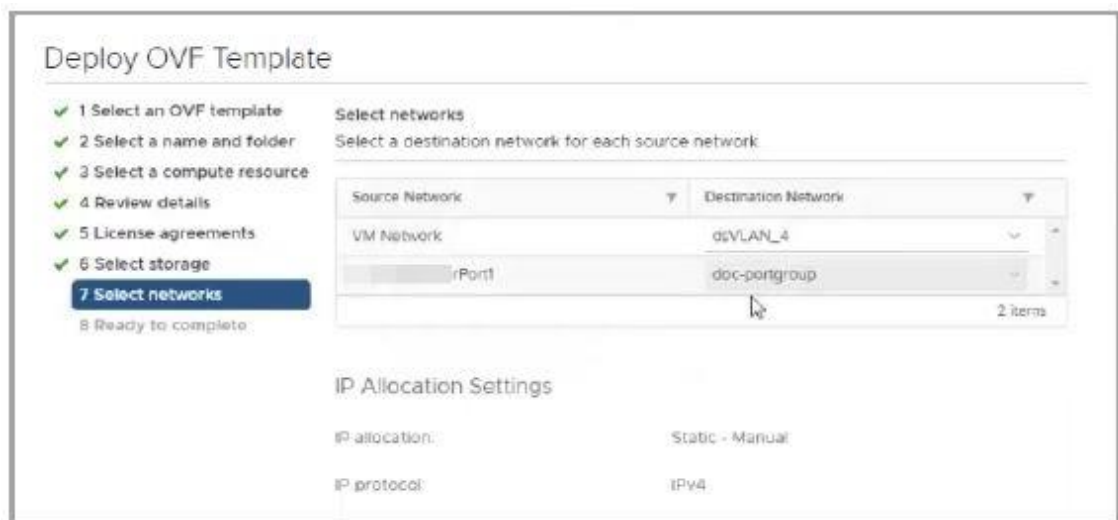


Figure 28: Select networks [4]

Figure 28 shows the seventh step where networks used for the virtual appliance is chosen. In the Flow Sensor virtual appliance case, there is need to add that PCI passthrough interface here as well. After this step there is Ready to complete

step of OVF template deployment where summary of settings can be reviewed. If all settings seem to be correct, then Finish button is pressed. This starts the deployment in the background. Deployment progress can be monitored through Recent Tasks section. After the deployment is completed and shown in the inventory tree then next step with configuring the IP addresses can be progressed. These OVF template deployment steps need to be repeated for all the virtual appliances. In Customer X case this means four OVF template deployments with above steps. [4]

Next part of the virtual appliance installation is the IP address configuration for the virtual appliances. This is done through the virtual machine console located in the Hypervisor host. From the Hypervisor host can be verified that the virtual machine is powered on and from there the virtual machine console can be accessed. After the virtual appliance has booted up then Administrative IP Address page opens. If there is need to log in through console, then default username is sysadmin and default password is lan1cope. These will be changed later stage. [4]

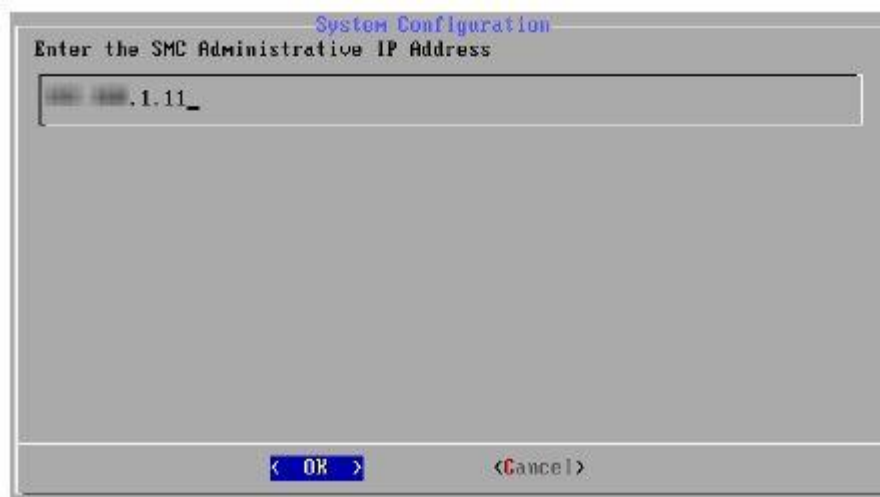


Figure 29: Enter appliance IP address [4]

Figure 29 shows the page where you enter the IP address for the virtual appliance. After the correct IP address is in place then select OK and press Enter.

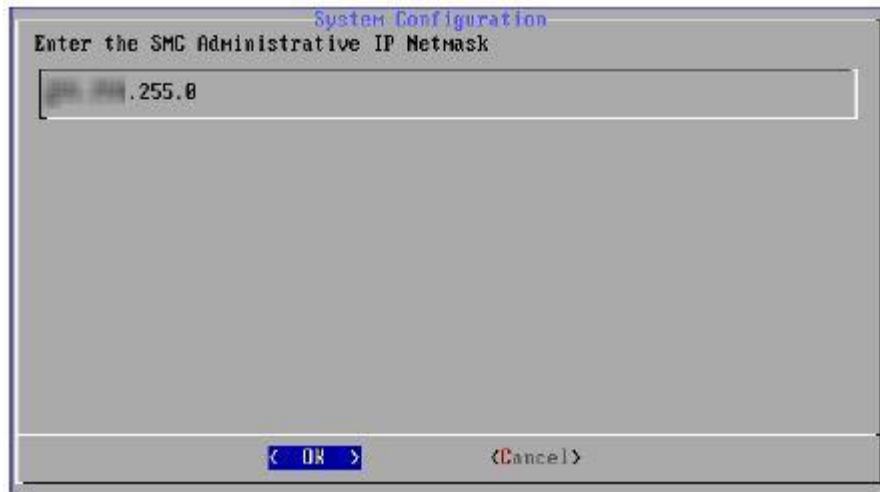


Figure 30: Enter network mask [4]

Figure 30 shows next page where the network mask for the virtual appliance IP address is given. When the correct mask is entered, then OK is selected and Enter is pressed to continue. After this is page where the broadcast IP address for the virtual appliance is given. When this is done then page for giving the IP address for the gateway server opens as shown in Figure 31.

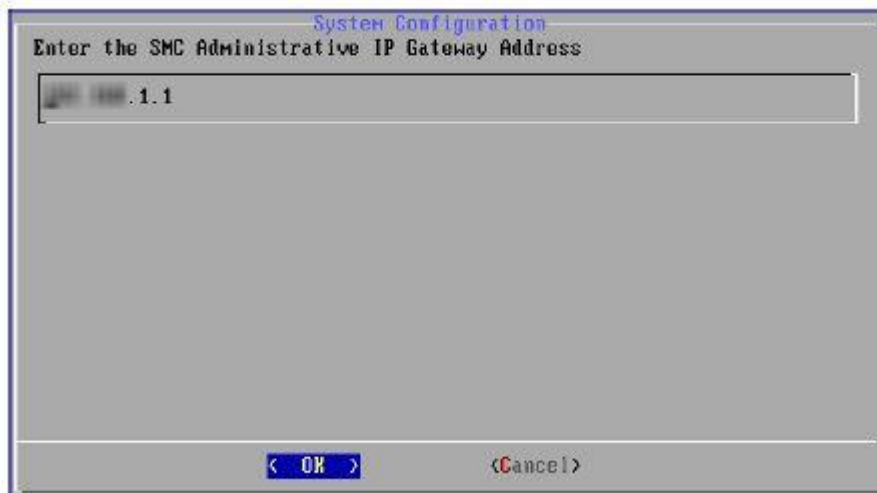


Figure 31: Enter gateway address [4]

After the gateway IP address is given then opens page for giving the hostname for the virtual appliance. The virtual appliance hostname needs to be unique. After the hostname is given then opens page for giving domain name for the virtual

appliance to use. Then next page to open is the page where given configuration settings can be reviewed and accepted as shown in the Figure 32.

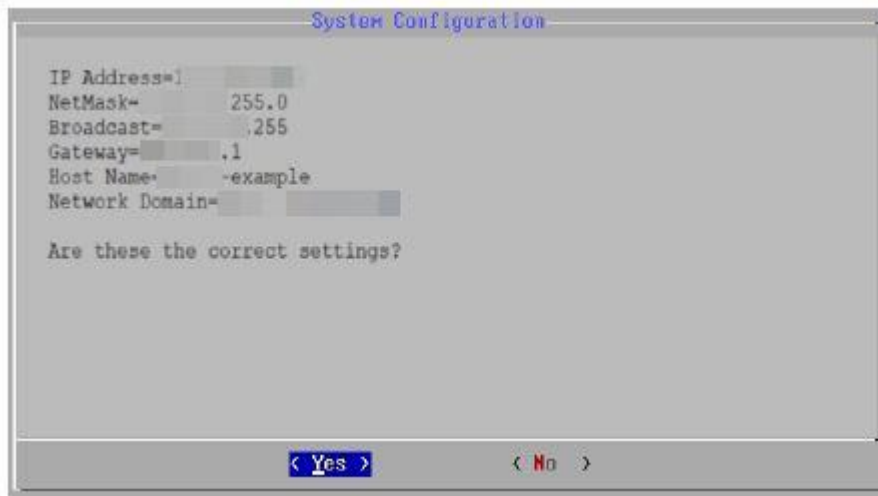


Figure 32: Review of configuration settings for virtual appliance [4]

If all settings are correct, then Yes is selected and Enter is pressed. There will be some on-screen prompts to finish the virtual environment and after these prompts the appliance will restart. Installation of the virtual appliance is complete after the restart has happened. These IP address configuration steps need to be repeated for all virtual appliances in the Customer X's environment. [4]

### 3.4 Setup with AST (Appliance Setup Tool) and system patching

Before the Secure Network Analytics system appliances can communicate with each other, their configuration needs to be finalised with the Appliance Setup Tool (AST). The AST can be launched by logging into appliance's IP address first time with the web browser. With the help of the AST all appliances will be configured to be managed by the Secure Network Analytics Manager. When appliances are configured with the AST, it is important that only one appliance is configured at a time. Before moving to configure the next appliance, it is also important to verify that just configured appliance is shown as Up status. [5]

The Secure Network Analytics appliances need to be configured in specific order with the Appliance Setup Tool. In the Customer X's environment first appliance to configure is The SMC virtual appliance. Second appliance to configure is the Flow Collector virtual appliance. Last appliances to configure are the Flow Sensor virtual appliances. Between two Flow Sensor virtual appliances it does not matter which one of them is configured first.

To start with the SMC virtual appliance configuration with AST, in web browser address `https://192.168.10.6` is typed into the address field. This opens AST into the web browser window. Default credentials are used to log in. After login welcome page is shown.

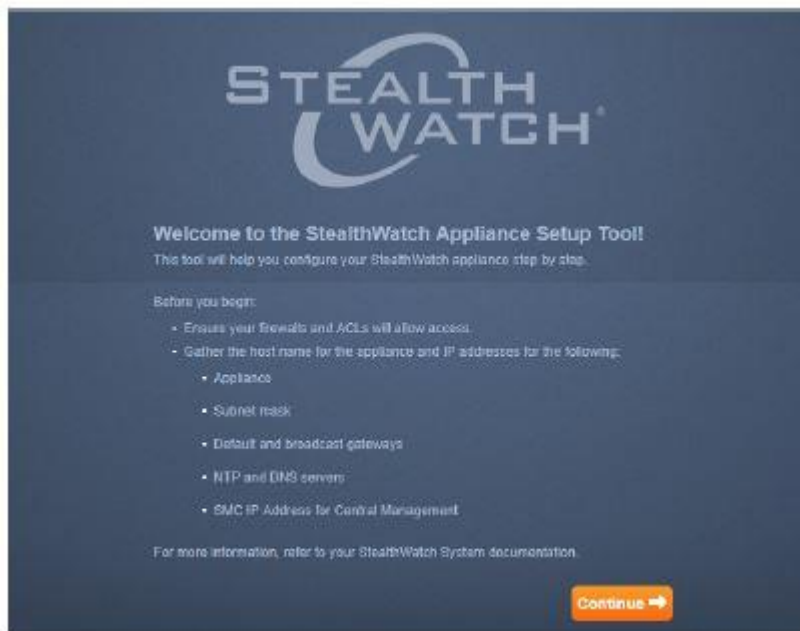


Figure 33: the AST welcome page [5]

Figure 33 shows the AST welcome page. Before moving on from this page, it is good to verify that all mentioned information on this page are available so that they can be filled in the next steps. By pressing continue button on this page the AST moves to next steps.



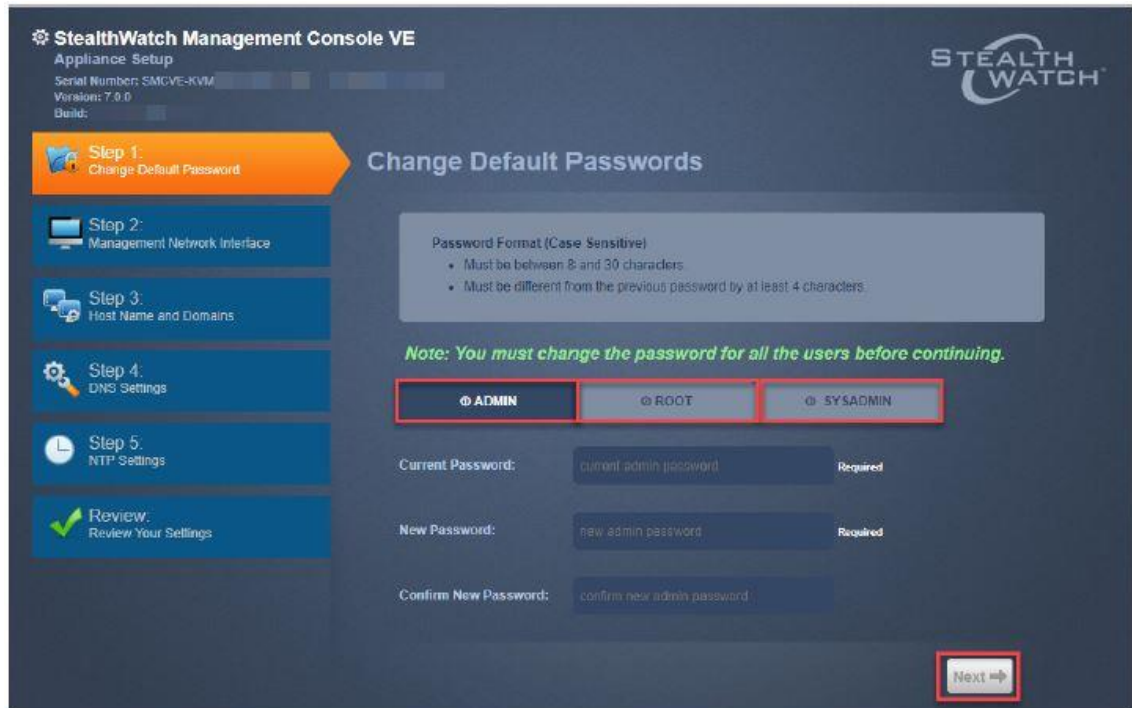


Figure 34: AST configuration steps. [5]

Figure 34 shows configuration steps with AST. In the first step passwords need to be changed to replace default passwords for the admin, the root and the sysadmin users with new passwords. In the second step, the management IP address for the appliance and the network interface field are reviewed. Third step is for filling the virtual appliance host name and the domains. In the SMC only, this also includes filling the Stealthwatch domain for virtual appliances and IP address range for the monitored networks. Fourth step is for filling the DNS server settings. In the fifth step the NTP server settings are filled. Last step is to review the settings which were given to the AST. After the review Apply button is pressed and the virtual appliance is also restarted. These above steps are also done for the Flow Collector virtual appliance and the Flow Sensor virtual appliances except that Stealthwatch domain and IP address range part.

After the SMC has restarted, new login is done. This opens the AST again for the appliance registering part for the management. In the Register Your Appliance tab shown IP address is verified and Save button pressed. This operation installs central management function on the SMC. After the virtual appliance setup is complete, Go to Dashboard button can be pressed. This will open the SMC

dashboard and from here can be verified that the SMC is Up state from Central Management page as shown in Figure 35.

The screenshot shows the 'Appliance Manager' tab in the Cisco Stealthwatch Central Management interface. Under the 'Inventory' section, it indicates '1 Appliance found'. A search filter is set to 'Appliance Inventory Table'. The table below shows the status of the SMC appliance.

APPLIANCE STATUS	LICENSE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Up	Up to date	SMC01	SMC SMC/UE-V/Name-C238a057dof685ad- 9eb9bb447903a367	198.18.128.136	[Refresh]

Figure 35: The SMC status shown as Up [6]

The next appliance to configure is the Flow Collector virtual appliance. First there is same steps as shown in the Figure 34 for the Flow Collector. After virtual appliance is restarted then new login for the AST is done for configuring the Central Management Settings. In this part the IP address of the SMC is given and saved. In the next step, window opens which requests the admin account credentials for the managing SMC. Then Central Management Settings screen updates and Stealthwatch Domain can be selected. In this part the flow collection port is set to 2055. After this part is done the Flow Collector starts synchronization process with the SMC. The Appliance Setup Complete page is displayed after this initial synchronization is done. The Flow Collector virtual appliance status can be checked from the Central Management page as shown in Figure 36.

The screenshot shows the 'Appliance Manager' tab in the Cisco Stealthwatch Central Management interface. Under the 'Inventory' section, it indicates '2 Appliances found'. A search filter is set to 'Appliance Inventory Table'. The table below shows the status of both the Flow Collector and SMC appliances.

APPLIANCE STATUS	LICENSE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Up	Up to date	FCNF01	Flow Collector FCNF/E-Name- 423946c934527161- 0e9d3949e116f528	198.18.128.137	[Refresh]
Up	Up to date	SMC01	SMC SMC/UE-V/Name-C238a057dof685ad- 9eb9bb447903a367	198.18.128.136	[Refresh]

Figure 36: The Flow Collector status shown as Up [6]

The last appliances to configure are the two Flow Sensor virtual appliances. First there is same steps as shown in Figure 34 for the Flow Sensors. After virtual

appliance are restarted then new login for the AST is done for configuring the Central Management Settings. In this part IP address of the SMC is given and saved. In the next step window opens which requests the admin account credentials for the managing SMC. Then Central Management Settings screen updates and Stealthwatch Domain can be selected. Also, in this part the Flow Collector is selected. This selected Flow Collector will receive telemetry data from the Flow Sensors. The Flow Collector here is same device which was configured in previous step. After this part is done the Flow Sensors starts synchronization process with the SMC and the Flow Collector. The Appliance Setup Complete page is displayed after this initial synchronization is done. The Flow Sensor virtual appliance status can be checked from Central Management page as shown in Figure 37.

Inventory  
3 Appliances found

Q Filter Appliance Inventory Table

APPLIANCE STATUS	LICENSE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Up	Up to date	FDNF01	Flow Collector FCNF/E-VMware-423845c70a45710c-0e843940e110f328	198.18.126.107	⊕
Up	Up to date	FS01	Flow Sensor FSVE-VMware-4238d79c7df8d73c-0e5a1521b2046a07	198.18.126.138	⊕
Up	Up to date	SMC01	SMC SMC/E-VMware-42389c055ad480a05-8abeb447038a367	198.18.126.138	⊕

Figure 37: The Flow Sensor status shown as Up [6]

At this point the SMC and the Flow Collector installation is done for the Customer X's environment. For the Flow Sensor virtual appliance there is need to do the application ID and payload configuration step. This is configured through the Flow Sensors appliance admin interface which can be reached with web browser from <https://192.168.10.4> (the Helsinki Site) and <https://192.168.40.4> (the Turku Site). Both Flow Sensors need same additional configuration. After login is done for the Flow Sensors admin interface, then under Configuration menu there is the Advanced Settings item which need to be selected. This opens Advanced Settings window.

### Advanced Settings

Export Packet Payload

Export Application Identification

Include IPv6

Include HTTPS Header Data *(Applies only to IPFIX exports.)*

Include HTTP Header Data *(Applies only to IPFIX exports.)*

Export  bytes of the HTTP Request Path.

Enable X-Forwarded-For Processing

Flow Export Format:

<input checked="" type="radio"/>	IPFIX
<input type="radio"/>	NetFlow v9

### Cache Mode

Use single, shared, cache for all monitoring ports

Use independent caches for each monitoring port

Figure 38: The Flow Sensor Advanced Settings [6]

Figure 38 shows Advanced Settings which need to be checked for the Flow Sensor virtual appliances. This finalises the Flow Sensor installation part as well.

Next step in this part is patching for all installed virtual appliances. In the Customer X's environment, the SMC, the Flow Collector and the Flow Sensors needs the patch update. Download for the needed patches are done from the Cisco Systems software download web page.

Name	Date modified	Type	Size
patch-fcnf-ROLLUP002-7.3.0-04.swu	23.11.2020 15.13	SWU File	646 944 KB
patch-fsuf-ROLLUP001-7.3.0-01.swu	23.11.2020 15.16	SWU File	364 207 KB
patch-smc-ROLLUP003-7.3.0-01.swu	23.11.2020 15.02	SWU File	2 454 496 KB

Figure 39: Patches for virtual appliances

Figure 39 shows the software patches for the SMC, the Flow Collector and the Flow Sensors. These patches are uploaded one at a time through the SMC update manager page into system. Patching needs to be done in specific order for these virtual appliances. There is extra requirement in patching for the SMC and the Flow Collector. Both the SMC and the Flow Collector have specific window for the update in a way that they must be up more than one hour but less than seven days. If they have been up, for example, eight days, then they need to be rebooted and then wait more than an hour before patching can be started.

First device to be patched is The Flow Collector. When patching is done and the Flow Collector shows as Up state in the SMC, then next device to be patched is the SMC itself. After the SMC is patched and Up state then patching is done the Flow Sensors as well. When patching is done for both the Helsinki site Flow Sensor and the Turku site Flow Sensor, then this installation and patching part of the Secure Network Analytics system for the Customer X is done.

### 3.5 Licensing, Configuring System and Application installations

The Secure Network Analytics virtual appliances are running in the evaluation mode for the licenses after installation. The evaluation mode lasts 90 days and because of this, next step is licensing the system and its components. The system is using software version 7.3.0 and licensing on that is based on the Cisco smart licensing. This means that licenses are maintained in the Cisco smart licensing tool in the Cisco's cloud and the SMC communicate with that smart licensing tool. However, Customer X has some licenses in old format, so they first needed to be converted by the Cisco support to the smart license format. The Cisco support

authorized customer smart account for the Specific License Reservation (SLR). With this SLR functionality system can be licensed without devices need to have direct communication with the Cisco cloud.

First step in the SLR process is to log into the SMC with SSH connection as a root user. In the SMC command line below lines are typed.

- cd /lancope/manifests
- docker-compose run - -rm sw-licensing-reservation-client

This opens License reservation command line interface where option 1. Generate Reservation Request Code is selected. [7]

```

Smart Software Licensing

Reserve Licenses
Use the Reservation Request Code to reserve licenses on your Cisco Smart Software Manager. You can copy this code and paste it into your account, or download
the RequestCode.txt file (refer to Saved As) and upload it to your account.

Reservation Request Code: CB-25P... KI7V2H-Fr
Saved As: /lancope/var/services/cm/licensing/RequestCode.txt

- For instructions, refer to the Stealthwatch Smart Software Licensing Guide on Cisco.com.
- After you submit your Reservation Request Code and reserve licenses, return to this page to install your license reservations using the Reservation Authori
sation Code provided by the Cisco Smart Software Manager.

1. Install Reservation
2. Cancel Reservation Request
3. Exit
enter your selection (1,2,3): █

```

Figure 40: Reservation request code example [7]

Figure 40 shows the created request code which can be copied from the output in red triangle. Next step is for Customer X's admin person to log into the Cisco smart licensing tool and go to license section. In the license section admin selects Inventory and Licenses tab with pressing License Reservation.

**Smart License Reservation**

STEP 1 Enter Request Code    STEP 2 Select Licenses    STEP 3 Review and confirm    STEP 4 Authorization Code

You will begin by generating a Reservation Request Code from the product instance.  
To learn how to generate this code, see the configuration guide for the product being licensed.

Once you have generated the code:

- 1) Enter the Reservation Request Code below.
- 2) Select the licenses to be reserved.
- 3) Generate a Reservation Authorization Code.
- 4) Enter the Reservation Authorization Code on the product instance to activate the features.

Reservation Request Code:

Browse Upload

To learn how to enter this code, see the configuration guide for the product being licensed.

Cancel Next

Figure 41: Smart License reservation process [7]

Figure 41 shows the Smart License Reservation steps. In step 1 the earlier created Reservation Request code is added into the window. By following on-screen prompts final step is reached where the Authorization Code is generated. This code is then transferred to the SMC by first copying it to the txt-file. In the SMC command line interface, the SLR client is running and with in it option 1. Install Reservation is chosen. Then option entering the code is chosen and the Authorization code is copied into the SLR client. After this the license reservation is done.

```

Smart Software Licensing

License Reservation Completed Successfully

**IMPORTANT**: : If you have updated the license reservations for this product ins
download the ConfirmationCode.txt file and upload it to your account.

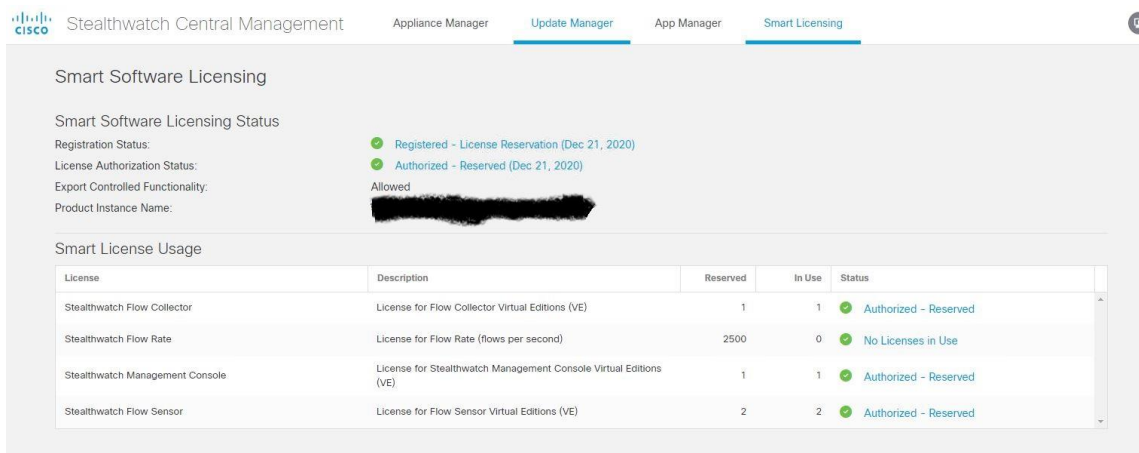
Confirmation Code: ██████████
Confirmation Code File: /lancope/var/services/cm/licensing/ConfirmationCode.txt

1. Continue
2. Exit
Enter your selection (1,2): █

```

Figure 42: License Reservation done successfully [7]

Figure 42 shows successfully completed License Reservation. After this the license situation can be verified also in the SMC gui as shown below in the Figure 43.



The screenshot shows the Cisco Stealthwatch Central Management (SMC) GUI. The top navigation bar includes 'Appliance Manager', 'Update Manager', 'App Manager', and 'Smart Licensing'. The main content area is titled 'Smart Software Licensing' and displays the following information:

- Smart Software Licensing Status:**
  - Registration Status: Registered - License Reservation (Dec 21, 2020)
  - License Authorization Status: Authorized - Reserved (Dec 21, 2020)
  - Export Controlled Functionality: Allowed
  - Product Instance Name: ██████████
- Smart License Usage:** A table with columns: License, Description, Reserved, In Use, and Status.

License	Description	Reserved	In Use	Status
Stealthwatch Flow Collector	License for Flow Collector Virtual Editions (VE)	1	1	Authorized - Reserved
Stealthwatch Flow Rate	License for Flow Rate (flows per second)	2500	0	No Licenses in Use
Stealthwatch Management Console	License for Stealthwatch Management Console Virtual Editions (VE)	1	1	Authorized - Reserved
Stealthwatch Flow Sensor	License for Flow Sensor Virtual Editions (VE)	2	2	Authorized - Reserved

Figure 43: Smart License Usage

The SMC is mainly managed through the web-based GUI but there are still some steps which needs old java-based desktop client usage. The Cisco's plan is to remove that old desktop client need in newer software versions but in the software version 7.3.0 it is still needed. Download for the desktop client can be done from the SMC GUI. In the Customer X system desktop client is used to



setup the SMTP relay and to setup couple automatic reports which are sent with the email which will use that SMTP relay. In the desktop client the SMC object is selected and with right-click the Configuration menu and below it, the Properties menu can be selected like Figure 44 shows.

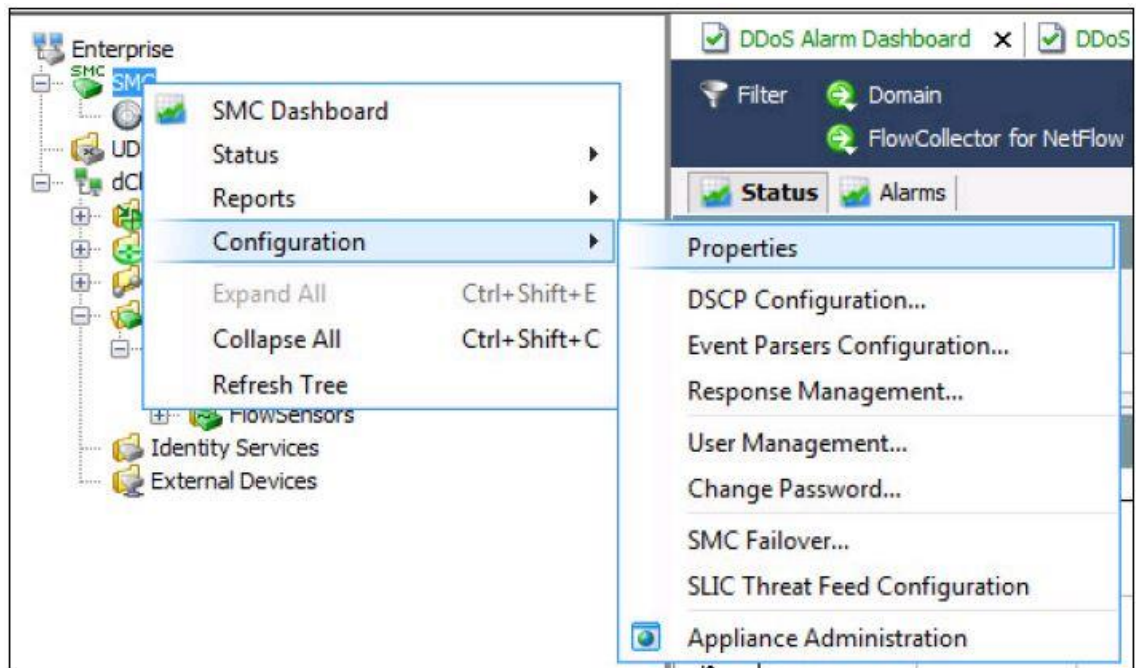


Figure 44: Desktop client Properties menu [6]

This opens the SMC properties window. In this properties window the email configuration is filled with from email address information and IP address of the SMTP relay server. The from email address is the address which is shown as email source when the SMC is sending email out from the virtual appliance. In Figure 45 below there is example of the SMC properties window where From Email Address and the SMTP Relay Address is filled.

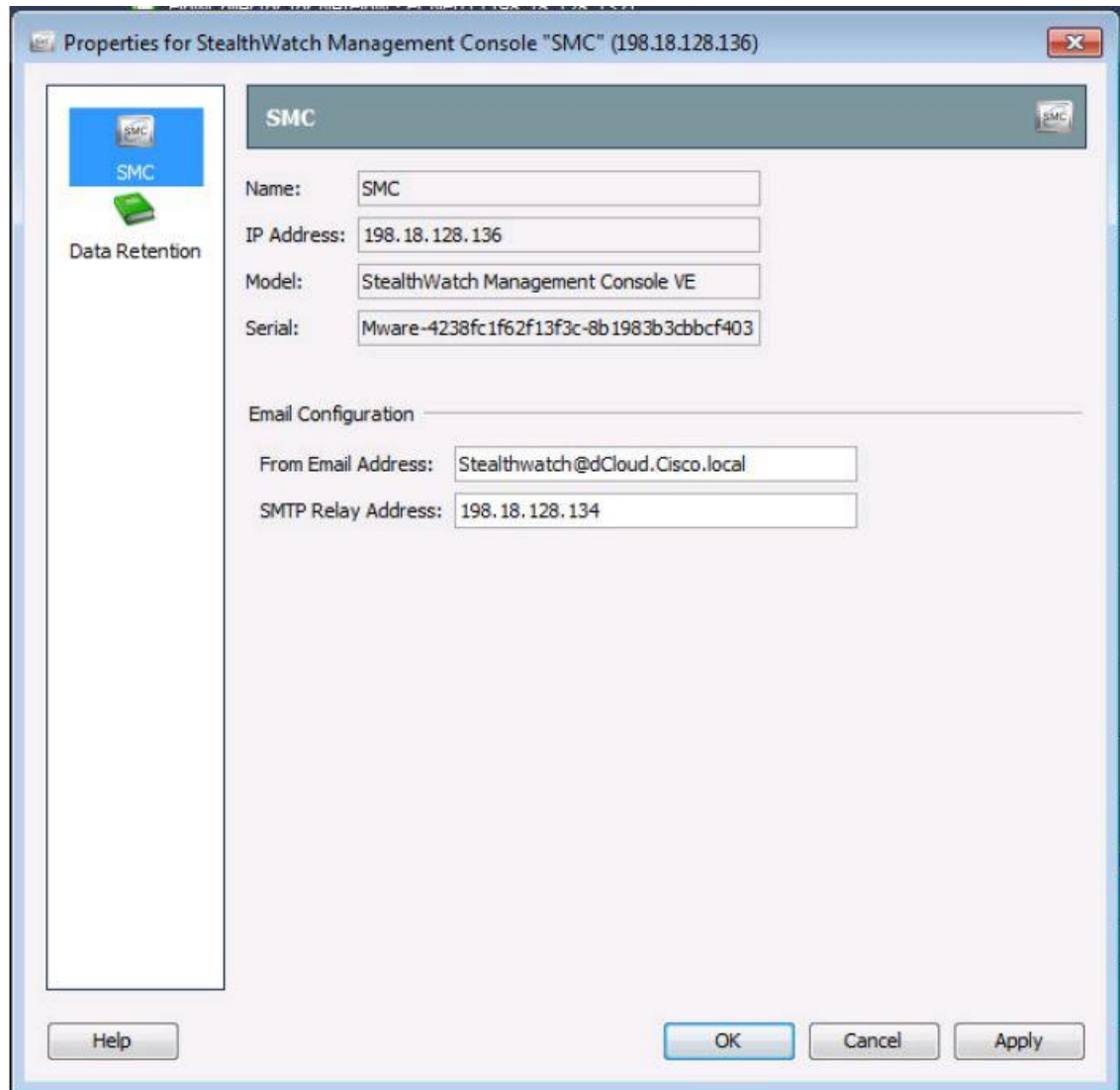


Figure 45: The SMC properties window [6]

Then in the desktop client two automatic reports are configured. These will be sent out in a weekly email in early Friday morning. In this email there is two pdf format reports which one of them including weekly Cyber Threats observed by system and other has the weekly alarms. With these reports the Customer X's security admins can see if there is something concerning happening in their network.

To make it easier to manage the information in the Secure Network Analytics system, it is a good practice to create the host groups. There is default catch all host group which includes private IP addresses but for addition to that customer

specific host groups are created. The Customer X's network has lot of hosts, so it is not good idea to create host groups manually. The Customer X has the IP Address Management (IPAM) system which already has tree like structure for the IP addresses. It is possible to get that data from the IPAM and import it to the SMC. However, it is not possible to transfer it directly as some modifications are needed. Data from the IPAM is gotten as the CSV (Comma-separated value) format. Then this is converted with the Cisco provided script into the XML format file. This XML file includes IP address information and hostname information if it was in place in IPAM system.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<sub-group-tree>
  <host-group id="20000" name="email relay" host-baselines="true" suppress-excluded-services="true" inverse-suppression="false" host-trap="false">
    <ip-address-ranges>10.100.1.10/32</ip-address-ranges>
  </host-group>
  <host-group id="20001" name="kamera serveri" host-baselines="true" suppress-excluded-services="true" inverse-suppression="false" host-trap="false">
    <ip-address-ranges>10.25.25.33/32</ip-address-ranges>
  </host-group>
  <host-group id="20002" name="kamerat" host-baselines="true" suppress-excluded-services="true" inverse-suppression="false" host-trap="false">
    <ip-address-ranges>10.30.1.0/28</ip-address-ranges>
    <ip-address-ranges>10.30.1.16/28</ip-address-ranges>
    <ip-address-ranges>10.30.1.32/28</ip-address-ranges>
    <ip-address-ranges>10.30.1.48/28</ip-address-ranges>
  </host-group>
</sub-group-tree>
```

Figure 46: Example of XML file

Figure 46 shows example of the XML file format which can be imported into the SMC as a host group file. This example would create three host groups with related IP addresses named the email relay, the kamera serveri and the kamerat. After actual converted XML file is imported into the SMC, then the host groups based on information from the IPAM is generated to the SMC.

Last thing for this part is installing the additional applications. With help of these additional applications, it is possible to enhance the usability of the SMC. These additional applications can be downloaded from the Cisco System software download web page. Then additional applications can be installed with the App manager inside the SMC GUI.

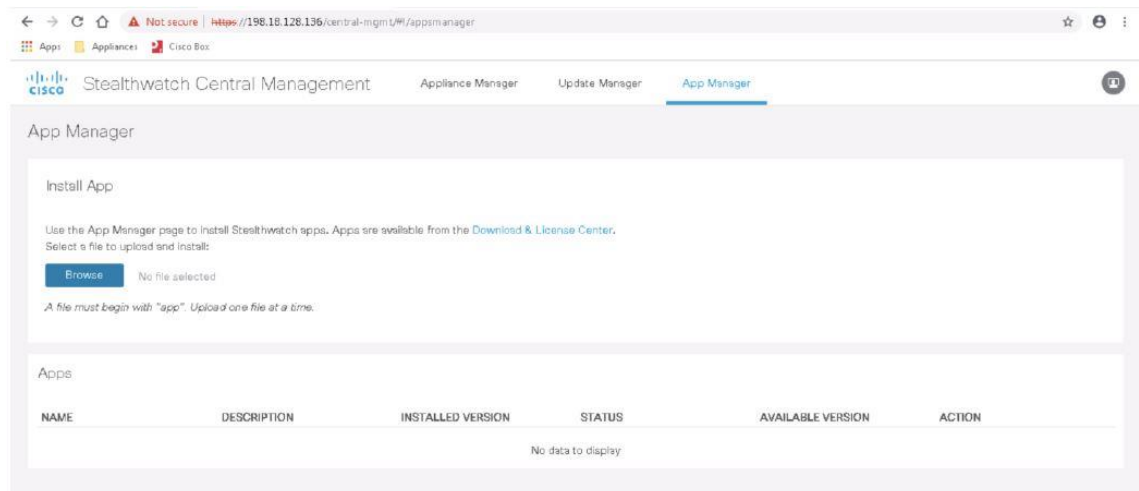


Figure 47: The SMC App manager screen [6]

Figure 47 shows the App manager screen which is used to install additional applications into the SMC. In the Customer X's case additional applications installed are the ETA Cryptographic Audit, the Host Classifier, the Network Diagrams and the Report Builder. The ETA Cryptographic Audit App identifies which traffic on the network is encrypted and which traffic is not encrypted. This App then extracts needed data elements from the encrypted traffic to analysis and to see if there is anomalous traffic inside encrypted traffic.

The Host Classifier App can be used to dynamic discovery and classification for the hosts in the network. In this App it can, for example, propose some hosts to be part of the DNS servers function host group. If administrator accept this classification, then the SMC adds that host part of the DNS server function host group. This helps with the maintenance of the deployed Host groups.

Network Diagram App enables users to graphically monitor the status of their environment. This happen almost real-time and active alarms and network traffic can be easily viewed. The Report Builder App allows creation and customization of reports. There are several report templates provided in the App and each report template includes parameters which can be used to defining the search criteria. After additional Apps are installed, then all is left to do is forward telemetry data into the system.

### 3.6 Configuring SPAN (Switch Port Analyzer) and NetFlow Exporters

Last part on this Secure Network Analytics system setup is to forward the telemetry data into the system for analysis. In the Customer X's network this telemetry data will be forwarded with two different ways to system. First option to gather the telemetry data is SPAN (Switch Port Analyzer), which is way to mirror traffic inside the switch to the port where the monitoring device is connected. Second option is to configure the network devices to work also as a NetFlow exporter as addition to their normal operation.

The SPAN works in a way that it copies traffic received or sent on source ports or source VLANs to a destination port or ports. Copying the traffic from source ports or VLANs doesn't affect the network traffic through these ports or VLANs. Destination port in the SPAN doesn't receive or forward any other traffic, it just receives the copied traffic and sends it out from that SPAN destination port to the device connected to that port. In the Customer X case the SPAN sources and the destination are in one switch both in the Helsinki and the Turku site.

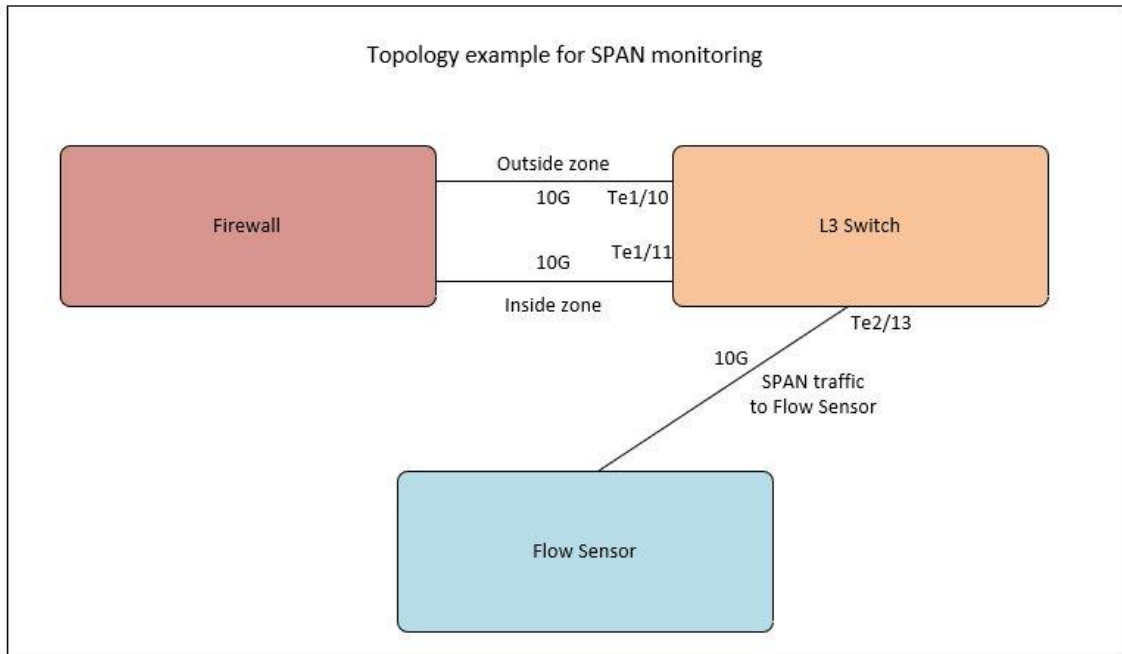


Figure 48: Network topology example for SPAN configurations

Figure 48 shows the example topology for creating the SPAN configurations. This same topology can be used for both the Helsinki site and the Turku site configurations and connections. Based on this topology source ports will be Te1/10 and Te1/11 which are connected to the firewall outside zone and inside zone. Destination port for the SPAN traffic will be port Te2/13 which is directly connected to the Flow Sensors physical 10G network interface. The needed SPAN configurations are created with below configuration lines in the switches located both in the Helsinki site and the Turku site.

```
Switch(config)# monitor session 5 source interface Te1/10 - 11 rx
```

```
Switch(config)# monitor session 5 destination interface Te2/13
```

```
Switch(config)# exit
```

```
Switch# write memory
```

With the first command ports Te1/10 and Te1/11 are defined as source ports and with rx in the command it is defined that only the received traffic in both ports is copied. With the second command port Te2/13 is defined as a destination port

for the copied traffic and all the copied traffic is sent out from this interface. With the last command changed configuration is saved. After this SPAN configuration, the Flow Sensor is getting the traffic from the network which the Flow Sensor then modifies to the flow data format and send out to the Flow Collector to analysis.

Next part is to configure selected network devices to be NetFlow exporters. When the network devices are working as a NetFlow exporter they will gather traffic from the selected interfaces and send it out to the Flow Collector in NetFlow format. Traffic which goes through the Helsinki site and the Turku site is already handled by the SPAN and the Flow Sensors in those sites. Smaller remote sites have switches with local routing enabled. By using this local routing, the remote switches have traffic between their VLANs which stays in the remote site and never reaches the Helsinki or the Turku site. As that local traffic is not place in the Helsinki site or the Turku site, it is not seen with the SPAN and the Flow Sensors. This creates the visibility gap on the network devices which offer that local routing. In the Customer X's network one remote site is chosen for the NetFlow exporter configurations.

```

*****
* flow export sw-export1
* destination 192.168.10.5
* source loopback 0
* transport udp 2055
* !
* flow record sw-record1
* match ipv4 source address
* match ipv4 destination address
* match ipv4 protocol
* match transport source-port
* match transport destination-port
* collect counter bytes long
* collect counter packets long
* collect timestamp sys-uptime first
* collect timestamp sys-uptime last
* !
* flow monitor sw-monitor1
* desc flow collection to Flow Collector
* record sw-record1
* exporter sw-export1
* !
* int vlan 200
* ip flow monitor sw-monitor1 input
* !
* int vlan 201
* ip flow monitor sw-monitor1 input
* !
* int vlan 202
* ip flow monitor sw-monitor1 input
* !
*****

```

Figure 49: Example NetFlow configuration to Cisco IE-5000 switch

Figure 49 shows example NetFlow configuration for the Cisco IE-5000 model switch. The remote site is using those Cisco IE-5000 switches as its core switches where local routing is enabled. In above example configuration there is only shown configuration lines which are added for enabling the NetFlow exporter functionality in the IE-5000 switches. With this configuration the NetFlow data is created from the traffic which is going input direction in the VLAN interfaces where ip flow monitor is enabled. Additional remote sites can be added as a NetFlow exporter sites later date.

After this NetFlow exporter configuration is done, it finalises the Secure Network Analytic system related installations and configurations for the Customer X.



## 4 System Testing and Initial Usage after installation

When logging into the Secure Network Analytics Manager (SMC) after all needed installations are done administrator will be entering on Network Security dashboard. This dashboard is landing page for configuration, monitoring, reporting and alarm investigation activities.

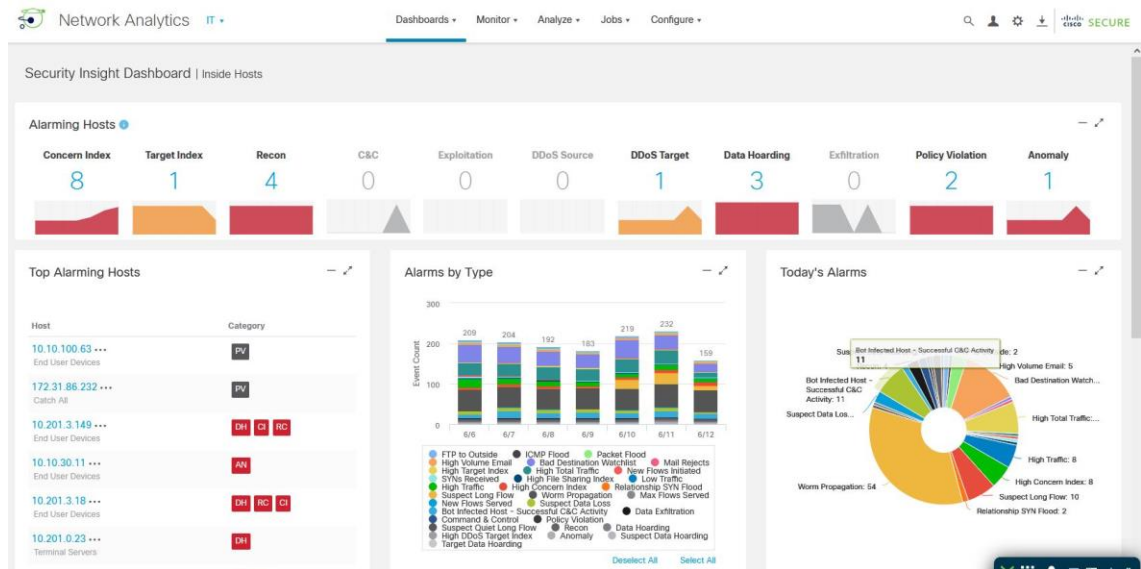


Figure 50: Example of Network Security Dashboard [8]

Figure 50 shows example output of Network Security dashboard taken from Cisco Systems dCloud demonstration and lab web page (<https://dcloud.cisco.com>). From this dashboard administrator can see for example top alarming hosts, alarms by different types and current day's observed alarms. If this Network Security dashboard doesn't show any data, then there is problem with telemetry data collection into system. In the Customer X's system data is present in the Network Security dashboard which shows that the telemetry data collection is working.

Although there is data available in the Customer X's Network Security dashboard, it might still be partial and not from all telemetry data sources. One way to verify telemetry data collection in the Customer X's system is with the Flow Collection status report from the SMC. In the Report Builder app there is template report for

the Flow Collection status. By choosing the Flow Collector as report source and setting correct date and then running report job, actual Flow Collection Status report is created.

Reports

All Reports **Flow Collection Status** x

Date: 6/13/2022 Save

Flow Collector: [Select]

Apply Filters to Total

Flow Collection Status (16)

Showing: 1 - 13 of 16

Status	Exporter	Flow Type	Average Flow Rate (fps)	Average NetFlow Traffic (bps)	Interface Count	Utilization Inbound (%)	Utilization Outbound (%)	Active Today
Active	198.18.133.23	IPFIX	367	232.63K	49	4	0	Yes
Error	172.16.16.1	NETFLOW_V9	211	74.2K	7	3	0	Yes
Error	172.16.16.3	NETFLOW_V9	92	38.13K	4	0	0	Yes
Active	198.18.133.39	IPFIX	3	7.09K	1	10	0	Yes

Figure 51: Example of Flow Collection Status report [8]

Figure 51 shows example of Flow Collection Status report taken from Cisco's dCloud. This report shows all the exporters delivering telemetry data to the Flow Collector and status of those exporters. Running the Flow Collection status report in the Customer X's SMC appliance, it shows that the Flow Collector is getting the telemetry data from both Flow Sensors and network switches configured to work as NetFlow exporters in remote site. As all the telemetry data sources are present as an active source in the report, this verifies that telemetry data collection is working as expected.

#### 4.1 Working with Host Classifier

Next step is to check dynamically learned hosts with Host Classifier app included in the SMC. In the Host Classifier app is seen that several Customer X's hosts are proposed to belong for different functional host groups in the system. There are several hosts proposed to belong to Mail Servers, NTP Servers, DNS Servers, Exchange Servers, Domain Controllers and DHCP Server functional groups.

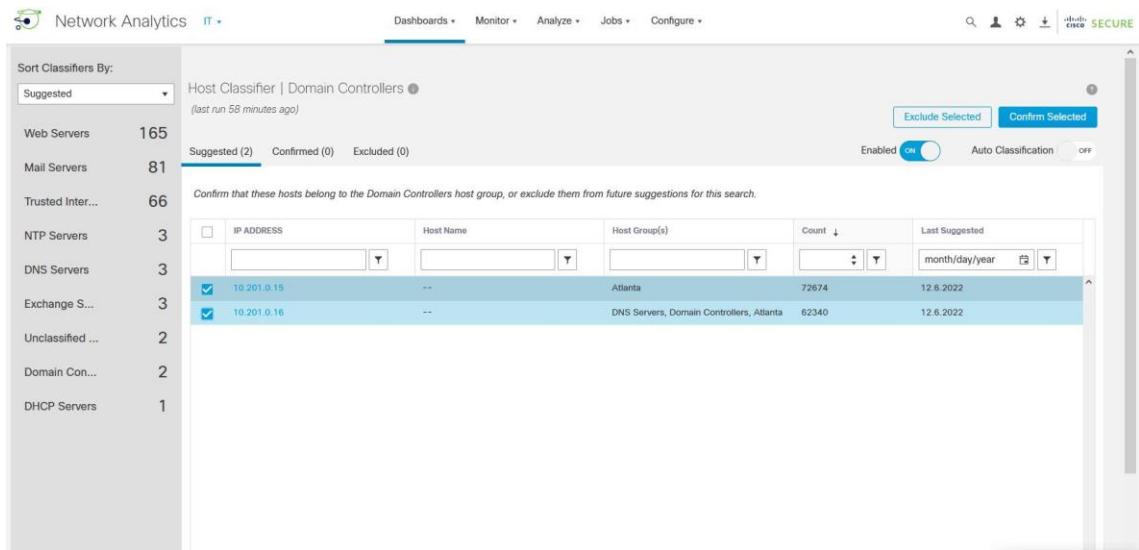


Figure 52: Example of Host Classifier [8]

Figure 52 shows example of Host Classifier taken from Cisco's dCloud. In this example there is two hosts suggested to be part of Domain Controllers group. Then they are selected by administrator and confirmed to be part of the Domain Controllers host group. Together with the Customer X's network administrator hosts found with the Host Classifier app are verified and valid hosts are confirmed to be part of the correct functional host groups. The hosts which are not part of the suggested host group are then excluded from that host group with Host Classifier. This way all the system suggested hosts are either confirmed or excluded to be part of the functional host groups.

## 4.2 Working with Visibility Assessment

On the SMC clicking the Dashboard menu and then choosing the Visibility Assessment opens The Visibility Assessment app's dashboard. From this dashboard the Customer X can see visual report which identifies potential security risks in their environment. The Visibility Assessment app was not installed separately because The Secure Network Analytics system in the Customer X's environment is in version 7.3.0 and software version 7.3.0 includes the Visibility Assessment app by default.

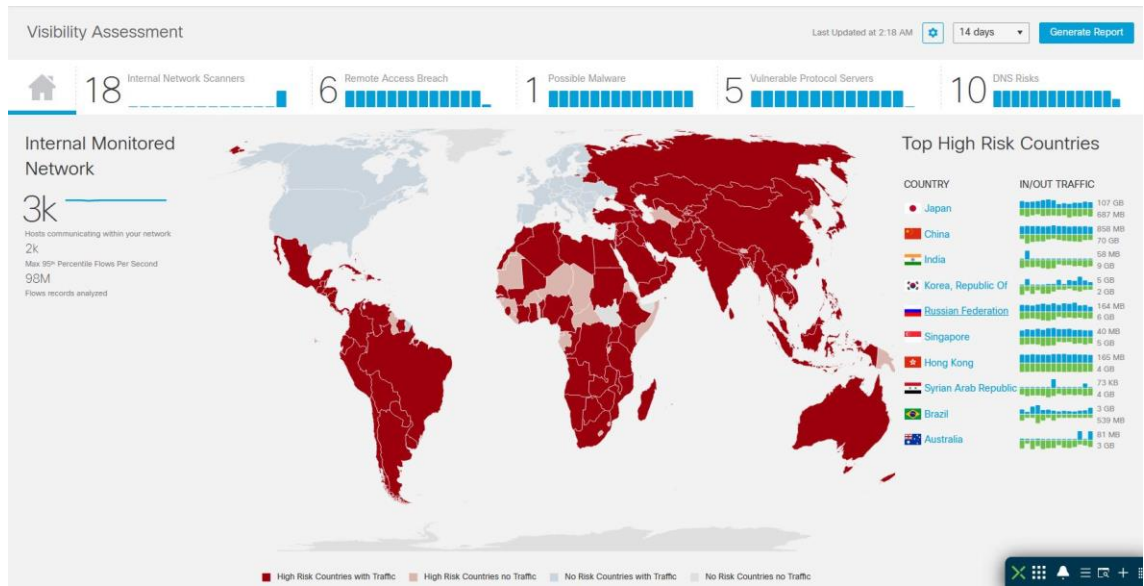


Figure 53: Example of the Visibility Assessment dashboard [8]

Figure 53 shows example of the Visibility Assessment dashboard taken from Cisco's dCloud. On the Customer X's dashboard first thing is to define High Risk Countries. As the Customer X's network should only communicate in Europe region then all other countries are marked as a High Risk country with exception of the United States and the Canada. This will help to first verify outgoing traffic which is for some reason going to those defined High Risk countries. In the world map presented in the Visibility Assessment dashboard dark red colour shows the High Risk countries which have received traffic from the Customer X's environment. The High Risk countries which haven't got traffic from the Customer X's network are presented with light red colour on the world map.

By clicking either the High Risk country on map or the top High Risk country on the list shown right on dashboard, gives more details about the traffic which is going or coming from that country. Customer X can then use this detailed data to check why that traffic is present in the network and then do possible modifications to hosts to stop that traffic related to the High Risk country.

The Visibility Assessment dashboard top menu has risk tabs which the Customer X can use to getting more detailed information about different risks such as Internal Network Scanners, Remote Access Breach, Possible Malware,

Vulnerable Protocol Servers and DNS risks. On the top right corner of the dashboard is Generate Report button for the Visibility Assessment. By pressing this Generate Report button, the Customer X can create PDF report which contains summary information about these risks shown in the Visibility Assessment dashboard. The report also has summary information about internal monitored network such as amount of the hosts communicating in the network. Time frame for the report can be decided in the dashboard between current day, last 7 days or last 14 days. This PDF report from the Visibility Assessment dashboard is good tool to help analyse risks in the Customer X's environment.

### 4.3 Working with Alarms on Network Security Dashboard

The Network Security dashboard which is shown earlier in Figure 50 has several alarm widgets which offers more information about alarms seen on Customer X's environment. On the right side of the Network Security dashboard there is the pie chart which shows Today's Alarms. That pie chart shows all the alarms which have been triggered during the current day in the Customer X's environment. From that pie chart is also easy to see which type of alarm has seen the most activity during the current day. It is wise to focus first on the alarm which have had most hits in this pie chart.

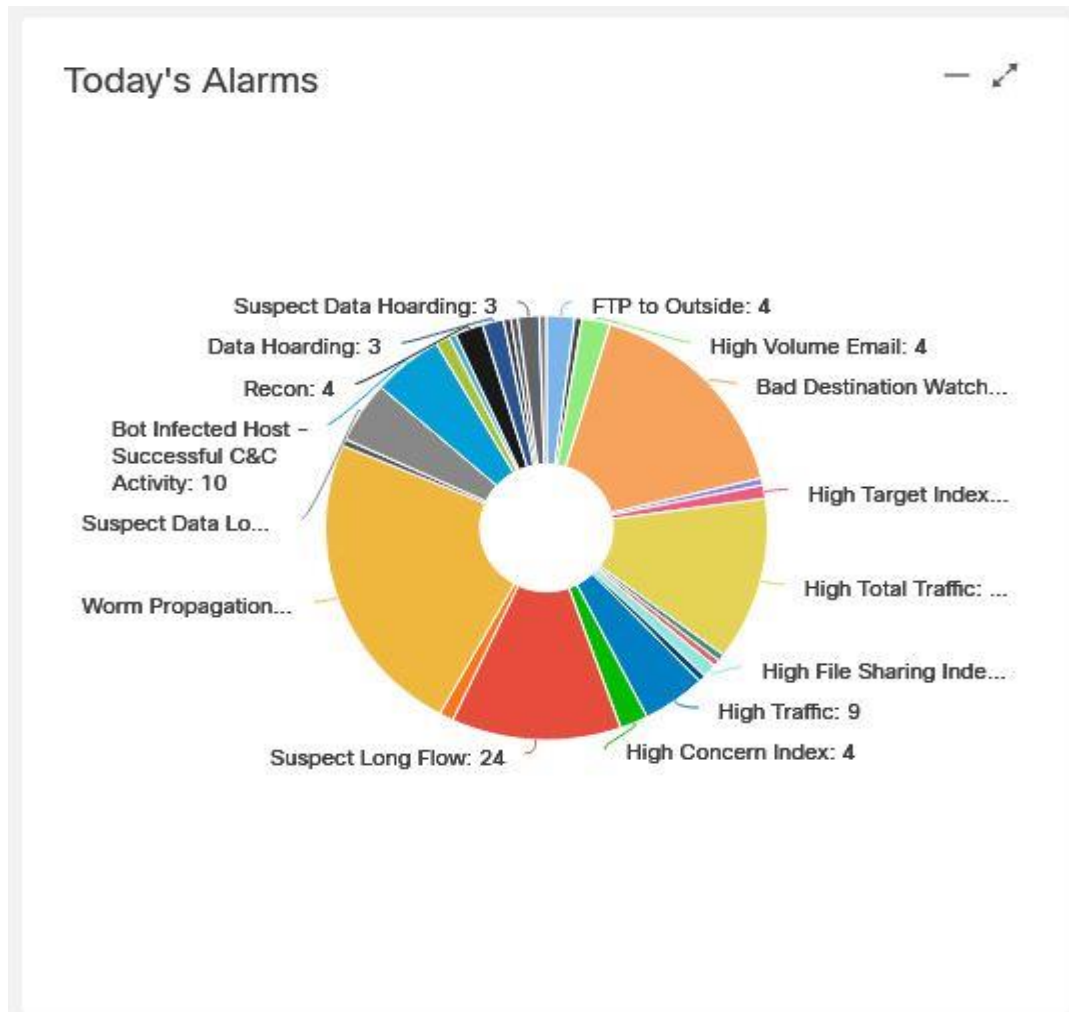


Figure 54: Example of Today's Alarm pie chart [8]

Figure 54 shows example of Today's Alarms taken from Cisco's dCloud environment. By using this as an example how to get more information about the alarms, can be seen that the Worm Propagation is currently most active alarm in the environment. Of course, all the alarms are important to study and solve all the issues in the environment which are found through those studies.

By clicking that Worm Propagation part from the pie chart, administrator moves to page which have only alarms related to the Worm Propagation in the environment. From this page can then be seen more information about individual Worm Propagation alarms.

Network Analytics IT-Data Store Data Store Dashboards Monitor Analyze Jobs Configure

Worm Propagation | 08/02/2022 (51)

Alarms

First Active	Source Host Groups	Source	Target Host Groups	Target	Alarm	Policy	Event Alarms	Source User	Details	Last Active	Active	Acknowledged	Actions
8/2/22 4:56 PM	End User Devices, Desktops, New York	10.100.10.254	End User Devices, Desktops, New York	10.110.100.254	Worm Propagation	Inside Hosts	--	UserAt10.100.10.254	Worm originating at 10.201.3.50, directly propagated from source host using vnc (5900/tcp).	8/2/22 4:56 PM	No	No	...
8/2/22 4:56 PM	End User Devices, Desktops, New York	10.110.10.254	End User Devices, Desktops, New York	10.120.100.254	Worm Propagation	Inside Hosts	--	UserAt10.110.10.254	Worm originating at 10.201.3.50, directly propagated from source host using vnc (5900/tcp).	8/2/22 4:56 PM	No	No	...
8/2/22 4:56 PM	End User Devices, Desktops, New York	10.80.10.254	End User Devices, Desktops, New York	10.90.100.254	Worm Propagation	Inside Hosts	--	UserAt10.80.10.254	Worm originating at 10.201.3.50, directly propagated from source host using vnc (5900/tcp).	8/2/22 4:56 PM	No	No	...
8/2/22 4:56 PM	End User Devices, Desktops, New York	10.90.10.254	End User Devices, Desktops, New York	10.100.60.254	Worm Propagation	Inside Hosts	--	UserAt10.90.10.254	Worm originating at 10.201.3.50, directly propagated from source host using vnc (5900/tcp).	8/2/22 4:56 PM	No	No	...
8/2/22 4:55 PM	End User Devices, Desktops, New York	10.40.10.254	End User Devices, Desktops, New York	10.50.100.254	Worm Propagation	Inside Hosts	--	UserAt10.40.10.254	Worm originating at 10.201.3.50, directly propagated from source host using vnc (5900/tcp).	8/2/22 4:55 PM	No	No	...
8/2/22 4:55 PM	End User Devices, Desktops, New York	10.50.10.254	End User Devices, Desktops, New York	10.60.90.254	Worm Propagation	Inside Hosts	--	UserAt10.50.10.254	Worm originating at 10.201.3.50, directly propagated from source host using vnc (5900/tcp).	8/2/22 4:55 PM	No	No	...
8/2/22 4:55 PM	End User Devices, Desktops, New York	10.60.10.254	End User Devices, Desktops, New York	10.70.100.254	Worm Propagation	Inside Hosts	--	UserAt10.60.10.254	Worm originating at 10.201.3.50, directly propagated from source host using vnc (5900/tcp).	8/2/22 4:55 PM	No	No	...
8/2/22 4:55 PM	End User Devices, Desktops, New York	10.30.10.254	End User Devices, Desktops, New York	10.40.30.254	Worm Propagation	Inside Hosts	--	UserAt10.30.10.254	Worm originating at 10.201.3.50, directly propagated from source host using vnc (5900/tcp).	8/2/22 4:55 PM	No	No	...

Figure 55: Example of Worm Propagation alarms page [8]

Figure 55 shows example page for the Worm Propagation alarms taken from the Cisco dCloud environment. From this page the administrator can get more info about source host and target host and their host groups. Also, there is details field which tells more about the alarm. By using those fields, the administrator can get more information about the alarm.

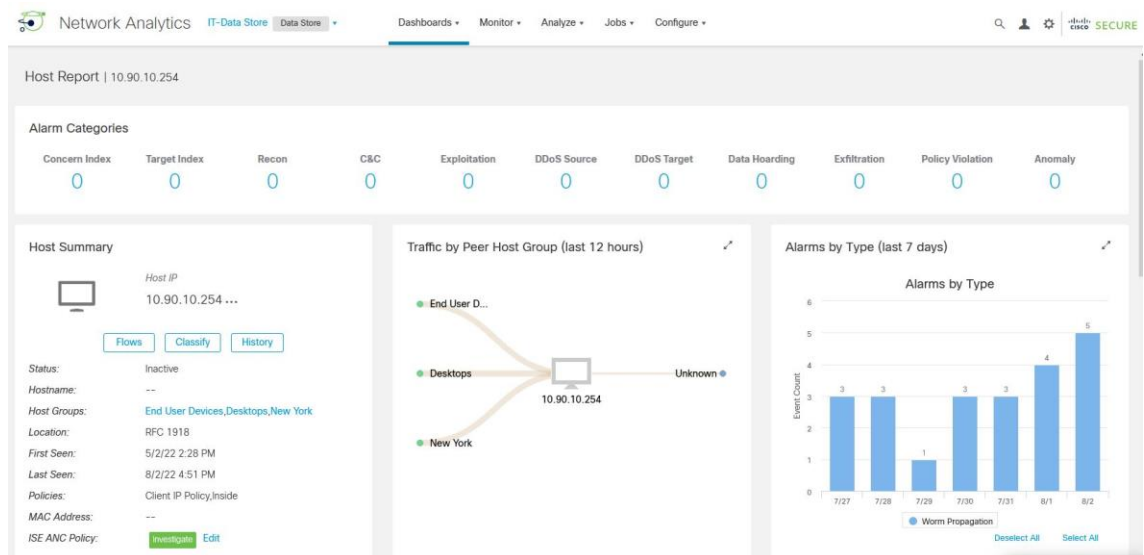
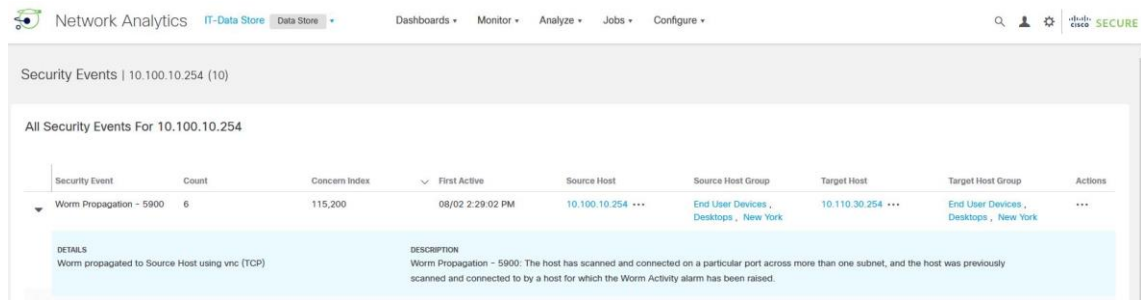


Figure 56: Example of source host related to worm alarm [8]

Figure 56 shows example of the source host information page related to the Worm Propagation alarm taken from the Cisco dCloud environment. From this

page can be seen that this host have the Worm Propagation alarms on last seven days. Also, from this page the administrator can go to look the flows related to this source host to solve issues in it.

By clicking details part for one alarm on the Worm Propagation alarm page, the administrator moves to page which shows all security events for that host.



Security Event	Count	Concern Index	First Active	Source Host	Source Host Group	Target Host	Target Host Group	Actions
Worm Propagation - 5900	6	115,200	08/02 2:29:02 PM	10.100.10.254	End User Devices , Desktops , New York	10.110.30.254	End User Devices , Desktops , New York	...

**DETAILS**  
Worm propagated to Source Host using vnc (TCP)

**DESCRIPTION**  
Worm Propagation - 5900: The host has scanned and connected on a particular port across more than one subnet, and the host was previously scanned and connected to by a host for which the Worm Activity alarm has been raised.

Figure 57: Example of the security event related to the worm alarm [8]

Figure 57 shows example of the security events information page related to the alarming host taken from the Cisco dCloud environment. From this page the administrator can see that the worm used the VNC port to propagate itself. It also informs that this host has propagated worm to target host and this host got the worm from host which also have raised the worm alarm. Below the Actions field are three dots and pressing those the administrator can look the Associated Flows to this event, Top Reports (Applications, Ports, Protocols, Hosts, Peers, Conversations and Services), External Lookup and Tune Event settings if needed.

Other alarm widgets on the Security Dashboard shown in Figure 50 are Alarm by Type, Top Alarming Hosts and Alarming Hosts trend. All these can be used by the administrator to investigate and create resolutions to issues seen in the Customer X's environment with the Secure Network Analytics system.



## 4.4 Working with the reports on the SMC

On the SMC dashboards drop down menu there is link to Report Builder app which can be used to create different reports related to environment. When reports page opens then the administrator can start by pressing the Create New Report button. This opens the page where several report templates are available to be used to create reports from the Customer X's environment. These templates include reports for Security, Network, and System functional areas.

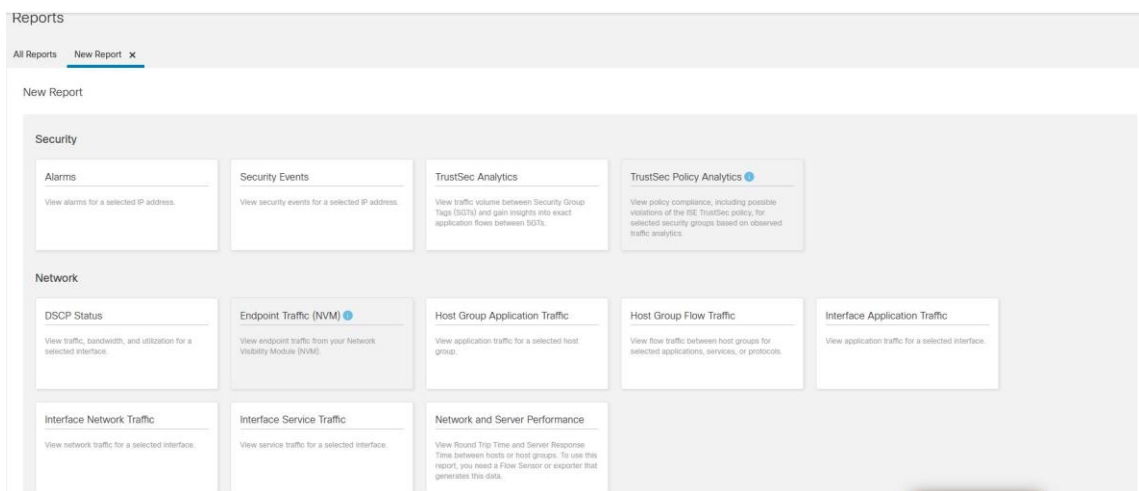


Figure 58: Example of Security and Network report templates [8]

Figure 58 shows different Security and Network report templates available in the Secure Network Analytics system in the Cisco dCloud demo environment. Not all templates shown in the Figure 58 are available in the Customer's X environment. These includes the TrustSec Analytics, the TrustSec Policy Analytics and the Endpoint Traffic (NVM) as these solutions are not used in the Customer X's environment.

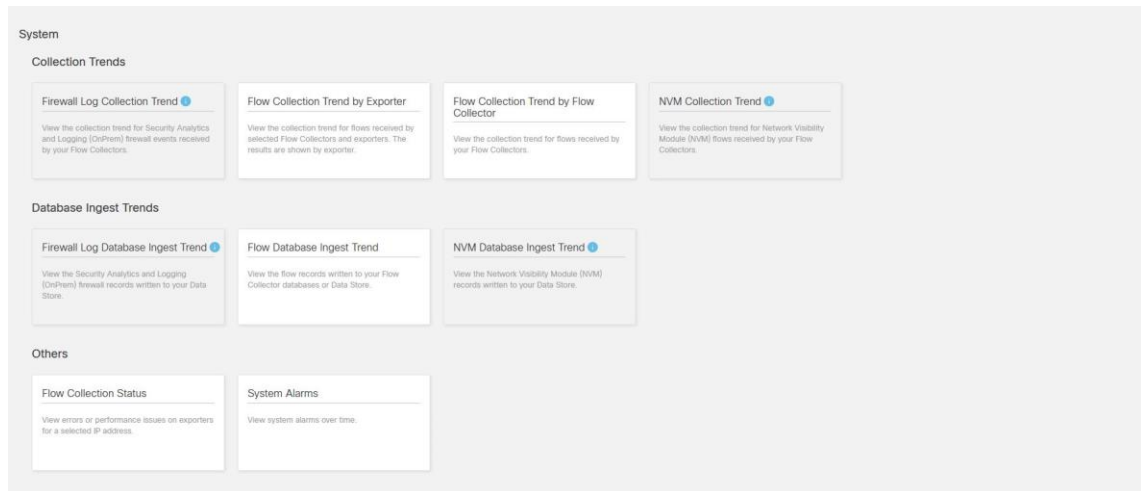


Figure 59: Example of System, Database and Others report templates [8]

Figure 59 shows different System related template reports available in the Secure Network Analytics System in the Cisco dCloud environment. In the Customer X's environment report templates available are the Flow Collection Trend by Exporter, the Flow Collection Trend by Flow Collector, the Flow Database Ingest Trend, the Flow Collection status and the System Alarms reports. The Firewall and the NVM related are not available as those are not used in the Customer X's environment.

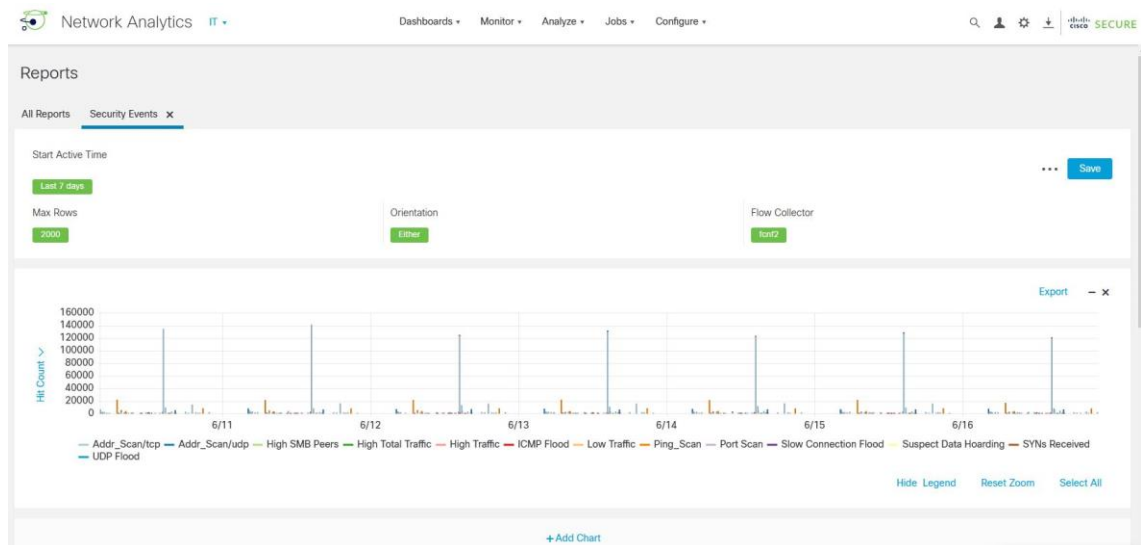


Figure 60: Example of Security Event report [8]

Figure 60 shows example of Security Event report taken from Cisco dCloud environment. Running this report in the Customer X's environment gives same kind of chart about the Security Events in the network. This report then can be exported to PDF format and then used to report events to the security team and/or upper management. Also, on this report can be used for selecting into interesting events like ICMP flood and then from there to deep dive analysis into related flows. Through these flows the administrator then can see source hosts and destination hosts and verify if they are valid traffic or something which needs to be fixed in the Customer X's environment.

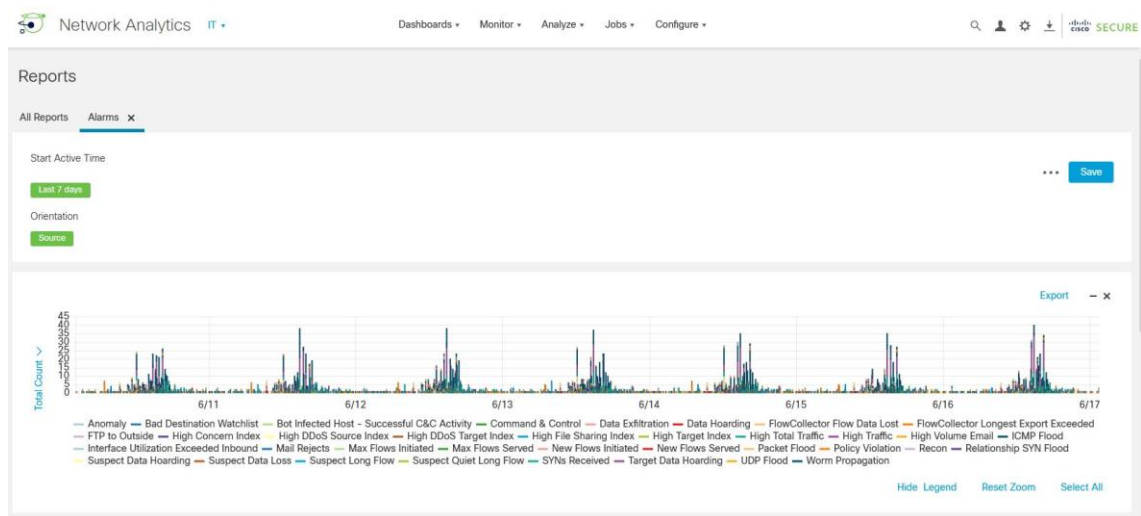


Figure 61: Example of the Alarms report [8]

Figure 61 shows the example of the Alarms report taken from the Cisco dCloud environment. Running the Alarms report in the Customer X's environment gives same kind of report about the Alarms seen in the network. Like earlier report this can also be exported to PDF format and then used to report alarms to the security team and/or upper management. From this report the administrator can select interesting alarm like the Data Hoarding and then see the flows related to that alarm. Again, these flows can be used by the administrator and security staff to determine if the traffic is valid traffic in the network or something which needs to be fixed in the Customer X's environment.

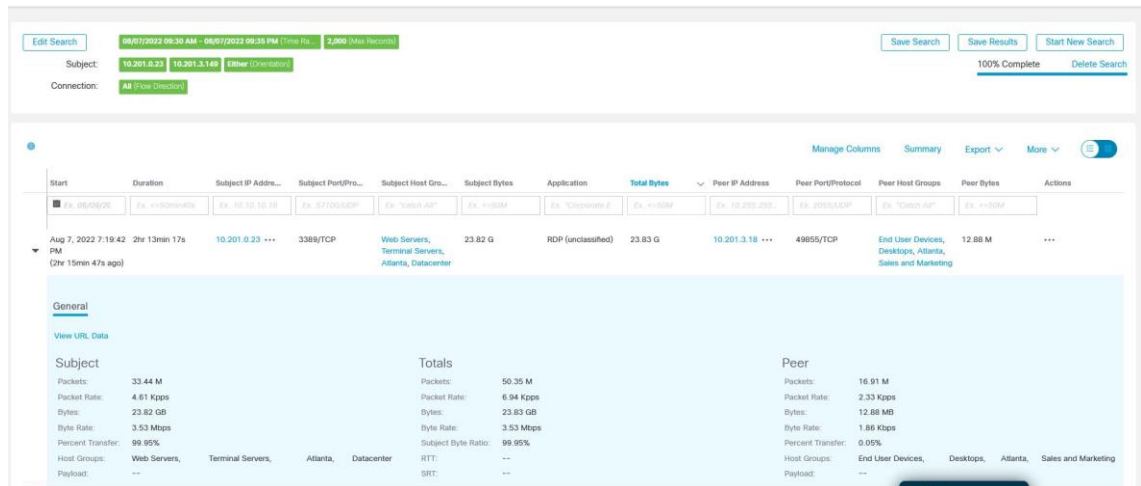


Figure 62: Example of flow information [8]

Figure 62 shows example of the flow data information taken from the Cisco dCloud environment by using the Alarm report.

Other report templates in the SMC Report Builder app can be used to build related reports and then use them to deep dive to investigate issues seen in the reports. Those report templates will be used by Customer X's administrators based on their needs for investigating seen issues or reporting those to other interested parties like upper management. Going through all the other report templates for this thesis is not feasible and this concludes the system testing and the initial usage chapter of this thesis.

## 5 Conclusions

This last chapter of the thesis goes through the observations and conclusions made during the installation process and during initial usage period of the Secure Network Analytics system. The Secure Network Analytics system was installed into the Customer X's network environment. The environment in the Customer X's case has several sites all over the Finland and number of the hosts communicating in the environment is also large. In this kind of large network, it is typical that not all the traffic is seen in the central site. This is usually caused by the local routing in the remote site which forwards traffic locally between the site hosts and no traffic related to local hosts is sent to the central site.

The local routing in the Customer X's environment made clear that deploying only the Flow Sensors in the central sites will left blind spots in the network for part of the traffic. Getting rid of all these blind spots would have required to configure all the remote sites routing devices to work as a flow exporter for the Secure Network Analytics system. When those remote sites routing devices were studied, it was seen that part of those devices are models which don't support the NetFlow configurations and can't be used as a flow exporter. This caused a situation where Customer X's network will have blind spots for network traffic seen by the Secure Network Analytic system until those older model devices are replaced with new models. Because of this it was accepted that big part of the locally routed traffic at the remote sites is not currently seen by the system leaving some blind spots in the network. However, it was estimated that traffic which is not seen is quite low as almost all the traffic from remote sites is destined to the central sites and can be seen with the Flow Sensors in the central sites. So, during initial installation phase only one remote site was configured to work as flow exporter for the system and the Flow Sensors were installed into two central sites to monitor all traffic through those central sites.

The capacity planning for the system was quite hard as there was no realistic estimation how many flows will be seen by the Secure Network Analytics system. The resources for the virtual devices were reserved in a way that they have plenty

of resources to handle large amount of flow data if needed. The reserved flow rate license for the system was 2500 flows per second and when the system was initially started it was seen that the flows from the two Flow Sensors and one flow exporter device was exceeding this 2500 flows per second. A good thing in the flow rate license is that even if the amount of the flows is exceeding the licensed level, the system won't stop handling the flow data. It gives warning to the administrator on the SMC and based on the flow rate seen in the SMC the Customer X can acquire additional license to expand licensed flow rate for the system.

Host group information creation for the SMC was a task which took quite long time in this environment. The Customer X has an IPAM solution which has all their IP address information available. From that IPAM solution the CSV file was exported and by using Cisco provided script it was changed to the XML file. In this case IPAM had some host groups with name formats which were not supported in the XML file, so they needed to be found manually from the CSV file and changed to format which was accepted by the XML file. For instance, using characters "<" or ">" in the host group name will break the XML file as they are used in the XML file body instead. After manual fixing for the CSV file was done then the script was able to create the correct XML file to be uploaded into the SMC. Other thing to note is that in the big environment such as Customer X's environment, the IP addressing scheme is changing all the time so keeping the SMC host group information up to date is a challenging task for the administrators. There needs to be an agreed process how administrators for the SMC get update information about IP addressing changes so that they can also update the host groups in the SMC. If the host group information is not updated, it will make harder to work with alarms and it will also make generated reports not reliable.

When the Secure Network Analytics system is switched on, it will start to learn hosts and traffic patterns from the environment. This learning phase will generate also alarms into the SMC and these alarms needs to be investigated by the administrator. In this phase there is usually quite lot of false alarms where hosts

are seen fresh in the system and no policies are in the system for hosts yet. When administrator goes through the alarms, he/she will need to check if the alarming hosts are working correctly. If the alarming hosts are working as they should, then there is need to create policies for them which removes those hosts from the alarming hosts. In these policies, currently alarming behavior is excluded by putting the host into the alarming host list. If the host start to do some other suspicious traffic, then it will be placed back into the alarming hosts. In the big environments the administrators, responsible of the alarms in the SMC, are probably not familiar with all the hosts which they see in the alarming host list. To solve these alarms, the administrators need to contact persons who are responsible of those hosts in order to solve if the alarm is a valid one or a false alarm. This needs a good cooperation and ways to communicate between different persons and organization groups in the Customer X's environment.

The main goal for the Secure Network Analytics system project was to increase visibility into the Customer X's network environment. With this system increased visibility for the network infrastructure was achieved. As mentioned earlier there are still some blind spots for the locally routed traffic in the remote sites but lot more information from the network and the host traffic behavior is now available for the Customer X to use. However, to use it effectively, Customer X need to have administrators who use the system regularly and react to alarms in the system. These administrators can be either internal personnel or a service provider can offer the Security Operating Center (SOC) functionality to handle the system on behalf of the Customer X. During the project it was seen that the Secure Network Analytics system is not so good fit for small or middle size businesses for their network visibility needs. Cost and resource needs for the system usage is pointing it to be used in the larger corporations either by themselves or by outsourcing it for the service providers.

## References

- 1 Cisco Secure Network Analytics (formerly Stealthwatch), Data Sheet July 2021.
- 2 Cisco Telemetry Broker, Data Sheet 2021
- 3 Cisco Secure Network Analytics Endpoint At-a-Glance
- 4 Stealthwatch Virtual Edition (VE) Installation Guide 7.3.0
- 5 Stealthwatch System Configuration Guide 7.3
- 6 Cisco-Stealthwatch-7.0-Deployment-Lab-v1.1-Guide-1.pdf
- 7 SW\_7\_2\_x\_Stealthwatch\_Smart\_Software\_Licensing\_Reservation\_Guid\_DV\_2\_0.pdf
- 8 Cisco dcloud Secure Networks Analytics 7.4.1 v1 – Instant Demo from [dcloud.cisco.com](https://dcloud.cisco.com)



