VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Tuomas Anttila

SWOIS AUTOMATION SYSTEM MONITORING

School of Technology
2018

VAASAN AMMATTIKORKEAKOULU
Tieto- ja viestintätekniikka

TIIVISTELMÄ

Tekijä	Tuomas Anttila
Opinnäytetyön nimi	sWOIS-automaatiojärjestelmän valvonta
Vuosi	2018
Kieli	englanti
Sivumäärä	55 + 1 liite
Ohjaaja	Antti Virtanen

Opinnäytetyö tehtiin Wärtsilä Finland Oy:n Cyber Security -osastolle. Insinöörityön aiheena oli suunnitella ja implementoida verkon ja verkkoon liitettyjen laitteiden valvontajärjestelmä käyttäen PRTG Network Monitor -ohjelmaa Wärtsilän sWOIS-järjestelmässä (server based Wärtsilä Operator's Interface System). Valvontajärjestelmän tarkoituksena on saada keskitetty valvontapiste koko sWOIS-järjestelmän laitteistolle, jolloin reagoiminen laitteiston ja verkon toimintahäiriöihin on tehokkaampaa.

Wärtsilän sWOIS-järjestelmäkokonaisuus on suunniteltu ympäristöksi, johon liitetyillä laitteilla pystytään valvomaan eri tuotantolaitosten ja laivojen moottoreiden toimintaa. Se pohjautuu Wonderwaren InTouch HMI -sovellukseen, joka eri asiakkaille sovellettuna mahdollistaa tuotantolaitosten eri komponenttien tarkkailun valvomosta, jossa operaattorilla on näkymä koko järjestelmän toimintaan yhdeltä ruudulta.

PRTG Network Monitor -ohjelmalla on tarkoitus valvoa sWOIS-ympäristössä olevia laitteita käyttäen eri verkkoprotokollia. Ohjelman tarkoituksena on lähettää sWOIS-operaattorille ilmoitus, jos sovellukseen määritellyt vikasietorajat ylittyvät ja järjestelmän toiminta häiriintyy.

Opinnäytetyössä tutkittiin vaatimusluettelon avulla valvontasovellukselta vaadittavat ominaisuudet ennen työn aloittamista ja sopivan ohjelman valitsemista. Tämän luettelon perusteella valittu ohjelma asennettiin testiympäristöön ja suoritettiin varsinainen testaus, jonka tulosten perusteella pystyttiin tekemään päätös, jatketaanko projektin kehittämistä tuotantoympäristöön.

Projektin lopputuloksena on toimiva verkon valvontajärjestelmä sWOIS-ympäristöön.

Avainsanat sWOIS, PRTG, valvontajärjestelmä

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Tieto- ja viestintätekniikka

ABSTRACT

Author	Tuomas Anttila
Title	sWOIS Automation System Monitoring
Year	2018
Language	English
Pages	55 + 1 Appendix
Name of Supervisor	Antti Virtanen

This Bachelor's thesis was done for the Cyber Security department of Wärtsilä Finland Oy. The objective of the thesis was to design and implement a network monitoring solution using the PRTG Network Monitor software in Wärtsilä's sWOIS (server based Wärtsilä Operator's Interface System) automation system. The aim of this thesis is to provide a centralized monitoring solution for the sWOIS hardware and software. This allows a more efficient way to react to network and hardware malfunctions.

Devices connected to the Wärtsilä sWOIS Human Machine Interface environment are designed to monitor the operation of engines in different production facilities and ships. SWOIS enables the monitoring of different hardware components from a centralized control room and provides a view of the facility on a single computer screen.

PRTG Network Monitor software was implemented to sWOIS environment to monitor the hardware, software and network traffic running in sWOIS using various networking protocols. The main purpose of the software is to send an alarm to the sWOIS operator if the predefined failure thresholds are exceeded and the system is malfunctioning.

In this thesis requirement specifications were used to define the required properties of the monitoring software before any actual testing was done. The program selected using the specifications was installed to a test environment where the actual testing took place. Based on these tests and the final documentation, it is possible to make a profound decision on whether to continue this project to a production environment.

The result of the thesis is a working network monitoring solution implemented to the sWOIS environment.

Keywords sWOIS, PRTG and monitoring system

CONTENTS

LIST OF ABBREVIATIONS

CIM	Common Information Model
CLI	Command Line Interface
CPU	Central Processing Unit
DMZ	Demilitarized Zone, subnet that exposes the external-facing services to Internet
FGCP	Fortigate Clustering Protocol
GPS	Global Positioning System
GUI	Graphical User Interface
HA	Fortigate High Availability firewall cluster
HMI	Human Machine Interface
iDRAC	Integrated Dell Remote Access Controller
IIS	Internet Information Services
ISL	Cisco Inter-Switch Link protocol
LACP	Link Aggregation Control Protocol
MIB	Management Information Base, a database used for managing the entities in a communication network
PRTG	Paessler Router Traffic Grapher Network Monitor
PVST	Per VLAN Spanning Tree
RAM	Random-Access Memory
SFP	Small Form-factor Pluggable, optical module transceiver for data communication
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
sWOIS	Server based Wärtsilä Operator’s Interface System, control room operator’s user interface

UDP	User Datagram Protocol, minimal message-oriented transport layer protocol
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
WBEM	Web-Based Enterprise Management
WMI	Windows Management Instrumentation

LIST OF FIGURES AND TABLES

LIST OF APPENDICES

1 INTRODUCTION

1.1 Thesis Overview

This thesis was done for Wärtsijä Oyj, a global leader in smart technologies and complete lifecycle solutions for the marine and energy markets /1/.

The object of the thesis was to design and implement a network monitoring solution for Wärtsilä's served based Wärtsilä Operator's Interface System (later referred to as sWOIS) Human Machine Interface (HMI). The sWOIS project is the core of Wärtsilä's automation system solution provided for the company's customers worldwide. The majority of sWOIS installations are delivered to large production facilities which require a centralized control room to observe the operation of the site using the HMI. In collaboration with other industry leading companies, Wärtsilä is also providing the sWOIS project to marine vessels operating around the world seas.

The main purpose of the sWOIS HMI is to monitor and control devices and network in an automation system environment. The subject for this thesis was based on the need to monitor the sWOIS system itself. In a large-scale manufacturing or energy facility, all the critical data that is being generated by motors and generators is being transmitted through the network, which is controlled by sWOIS. If the network or devices connected to it fail, it compromises the operation of the facility. This was the main reason for this thesis; to study what options are available to prevent hardware and software malfunctions before they happen, or at least minimize the downtime when they do.

In this thesis a working network monitoring solution for sWOIS was studied, designed, installed and tested. At the beginning of this process, requirements specifications were used to outline the devices and network components that will be included in this thesis.

As the sWOIS project continues, Wärtsilä's customers will have the option to select a monitoring software for their customized sWOIS package.

1.2 Wärtsilä Oyj

Wärtsilä is an industry leader in marine and energy markets and it specializes in smart technologies and complete lifecycle solutions for its customers. In 2017, the company's net sales were EUR 4.9 billion and it has approximately 18000 employees. Wärtsilä's employees and operations are in over 200 different sites and more than 80 countries /1/. The company is divided into three different business units which all work together to maximize the company's result.

1.3 Marine Solutions

Wärtsilä's Marine Solutions produces a wide array of products to meet the demand of its customers. When designing new vessels or engines, Wärtsilä emphasizes environmental excellence to reduce polluting discharges and emissions. This ensures the company's customers to continue to operate in sensitive areas around the world. Wärtsilä is leading the way in improving performance and reliability for gas engines. Liquified natural gas has low levels of harmful emissions and the cost is relatively low, which makes it ideal for gas engines or dual-fuel vessels. Marine Solutions aim to find fully customizable solutions for their customers and reducing their environmental footprint in the process /1-3/.

1.4 Energy Solutions

The main focus of Energy Solutions is to design and build power plants for utilities. Wärtsilä can provide their customers numerous different types of solutions, ranging from gas or biofuel power plants to hydro and solar solutions. At the end of 2017, Wärtsilä had over 67 GW of installed power plant capacity in 177 different countries.

Wärtsilä has also introduced its Smart Power Generation power plants, which are based on multiple internal combustion engines that can run on any gaseous or liquid fuels. The possibility to run on different fuel types gives them more flexibility as well as energy efficiency in helping to integrate wind and solar power into the grid /1, 4/.

1.5 Services

Wärtsilä Services provide a variety of solutions for the company’s marine and energy customers. These services range from spare parts and support to providing lifecycle services that can enhance the customer’s business. In 2017, Services had a 45% share of Wärtsilä’s net sales /1, 5/.

2 PROJECT BACKGROUND AND PURPOSE

The sWOIS project in Wärtsilä is a widely used HMI solution for power plants, production facilities and marine vessels. It is an ongoing and continuously developing project, which can be tailored to suit Wärtsilä's customers' needs depending on the installation environment. SWOIS consists of everything that is needed to control any facility or vessel engines and auxiliary systems in a human readable format. This includes all the hardware (servers, firewalls, switches, etc.) and software (virtual machines, InTouch) already preconfigured and ready for installation for the customer. Every sWOIS project is assembled and tested by Wärtsilä and its partner companies before they are delivered to the customer.

As sWOIS monitors the on-site engines and auxiliary systems, the need for a network monitoring solution was introduced by one of the company's customers; "Who or what monitors the sWOIS itself?" This question presented the subject for this thesis. As all the hardware (and software) related to sWOIS are installed to a server cabin, which is not continuously observed by control room operators, the need for a software-based monitoring system with alerting and notification system was apparent. This would allow operators to react quickly and efficiently to any software failures or hardware malfunctions without causing any significant downtime in the HMI system or even prevent them before they occur.

The objective of this thesis was to implement a functioning network monitoring solution to sWOIS, which can be rolled out to production environment. This was done by studying different available network monitoring programs and based on a requirement specification, to select suitable candidates for testing.

The sWOIS environment used in this thesis is already available and therefore this project did not require any server or virtual machine configuration prior to starting. New server hardware and PRTG Network Monitoring software added to existing sWOIS are explained in detail in this document.

3 THEORETICAL BACKGROUND OF THE THESIS

A wide array of different software components and protocols are used in this thesis which are explained in this chapter as well as the overview of the sWOIS HMI.

3.1 sWOIS in General

The sWOIS HMI is used for monitoring and controlling the status and essential data of a power plant or a marine vessel. Its main purpose is to visualize the data received from engines and auxiliary systems. This allows the control room operators to monitor the facility or vessel more efficiently from a graphical user interface. /6/

3.2 The Operation of sWOIS

Figure 1 displays the overall view of the sWOIS system environment.

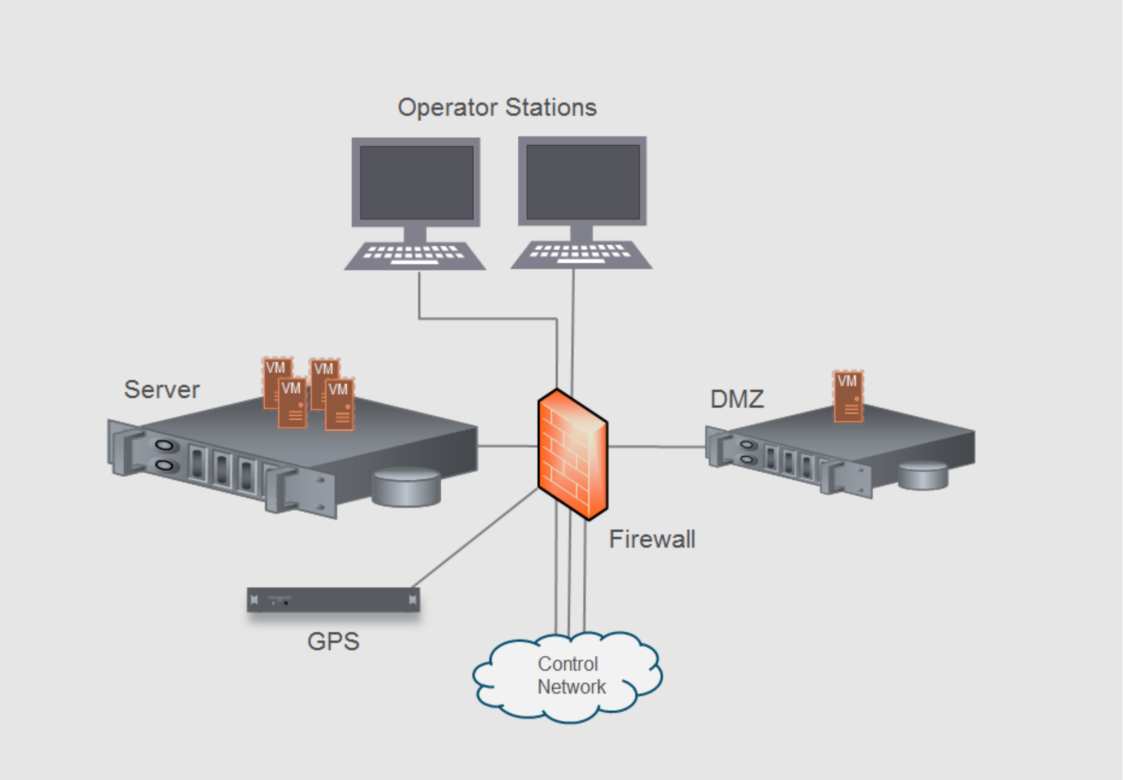


Figure 1. Simplified image of the sWOIS system /6/.

The engine data is received from the Control Network through the firewall to a server, which runs a virtual machine. The virtual machine runs a service that visualizes the engine data and sends it to the Operator Station located in the control room. The DMZ server is used for any outbound network connections and the GPS is used to keep all network devices synchronized in the same clock.

3.3 Software and Protocols

This section describes the different protocols and software used in this thesis.

3.3.1 Simple Network Management Protocol

The Simple Network Management Protocol (SNMP) is a set of standards that is used to exchange management information between the SNMP manager (server) and agents (managed devices) in a TCP/IP network (Figure 2). SNMP is mainly used for monitoring connected devices, but it can also be used as a remote configuration tool to change device settings from a distance. /15-17/

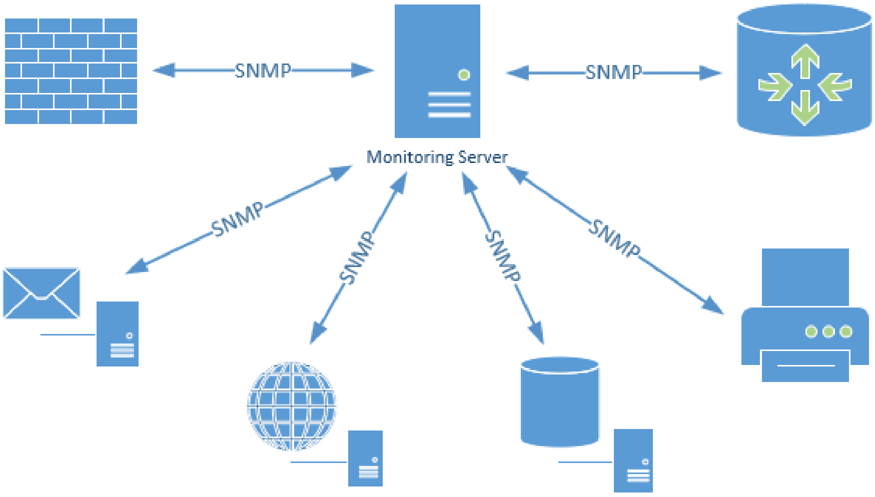


Figure 2. SNMP server communicating with managed devices.

SNMP has three different versions available; v1, v2c and v3. Version 1 was defined in 1988 and it is not currently widely used due its lack of cyber security. Version 2c is an enhanced version and is used in this thesis. This version uses a community string as a password between connected devices and can be used safely in intranets and closed networks. SNMP v3 adds more security but it also creates more complexity. Version 3 is recommended when using public networks such as the Internet. /17/

SNMP uses client-server communication between devices; a monitoring software (client) sends a UDP packet to the SNMP server, which in return sends an SNMP packet as a reply. This data exchange provides a result from the client device, such as core temperature, RAM usage or CPU-load /17/. Using a monitoring software, this information can be visualized to a human readable format.

3.3.2 Windows Management Instrumentation

Windows Management Instrumentation (WMI) is Microsoft's protocol for managing Windows based systems. It provides extensive monitoring and remote control to a computer running a Windows operating system. Everything can be monitored and changed on the target computer using login credentials (username and password). The downside of this protocol is that it can only be used on Windows operating systems. /18/

3.3.3 Web-Based Enterprise Management

Web-Based Enterprise Management (WBEM) is a set of specifications that define how resources can be discovered or accessed using the Common Information Model (CIM). It is used to unify the management of distributed computing environments /21/. In this thesis, WBEM based sensors are deployed to monitor the hardware information of an ESXi server using WBEM.

3.3.4 Simple Object Access Protocol

The Simple Object Access Protocol (SOAP) is a protocol used for exchanging information in computer networks. SOAP uses an XML-based way to encode requests and responses between in a client-server environment. In this project, SOAP sensors were used to transmit virtual machine data from ESXi to PRTG.

3.3.5 Inter-Switch Link Protocol

In sWOIS, two Fortiswitches are linked together using Inter-Switch Link (ISL). ISL is a Cisco proprietary protocol for interconnecting multiple switches and maintenance of VLAN information. The protocol also provides VLAN trunking capabilities with full wire-speed performance. As network traffic passes through the ISL interface, the original frame is encapsulated, and an additional header is added. On the receiving end, the header is removed, and the frame is forwarded to the assigned VLAN. ISL uses Per VLAN Spanning Tree (PVST), which is used to allow the optimization of root switch placement for each VLAN and to prevent the switches from creating an infinite loop. ISL also enables the load balancing of VLANs between the two switches used in sWOIS and adds a redundancy feature. If one of the switches fail, the other switch will continue to operate without any disturbance in the network. /8/

The topology and how both Fortiswitches are connected to each of the firewalls using the SFP ports in the switch and an optic cable is shown in Figure 3.

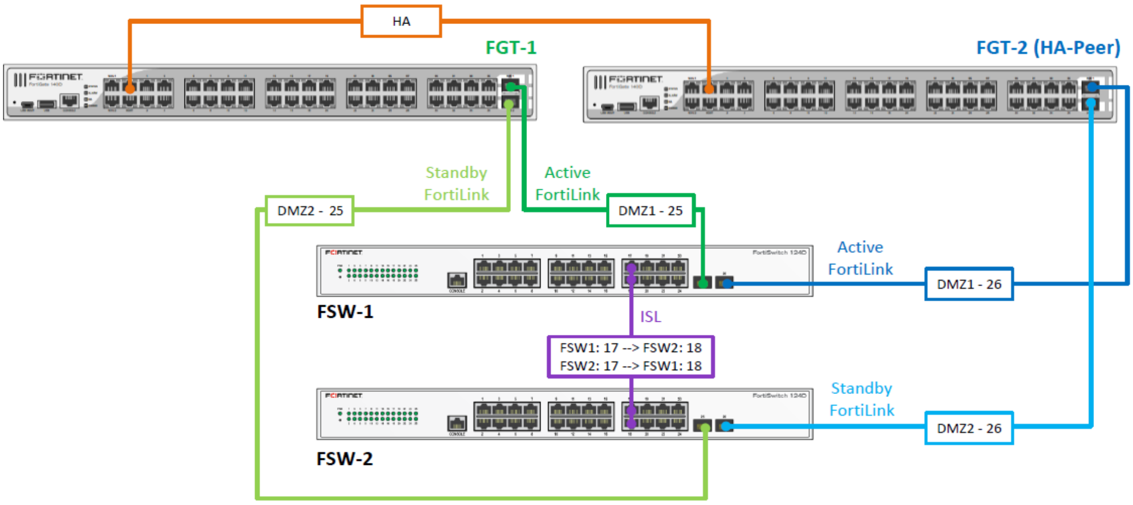
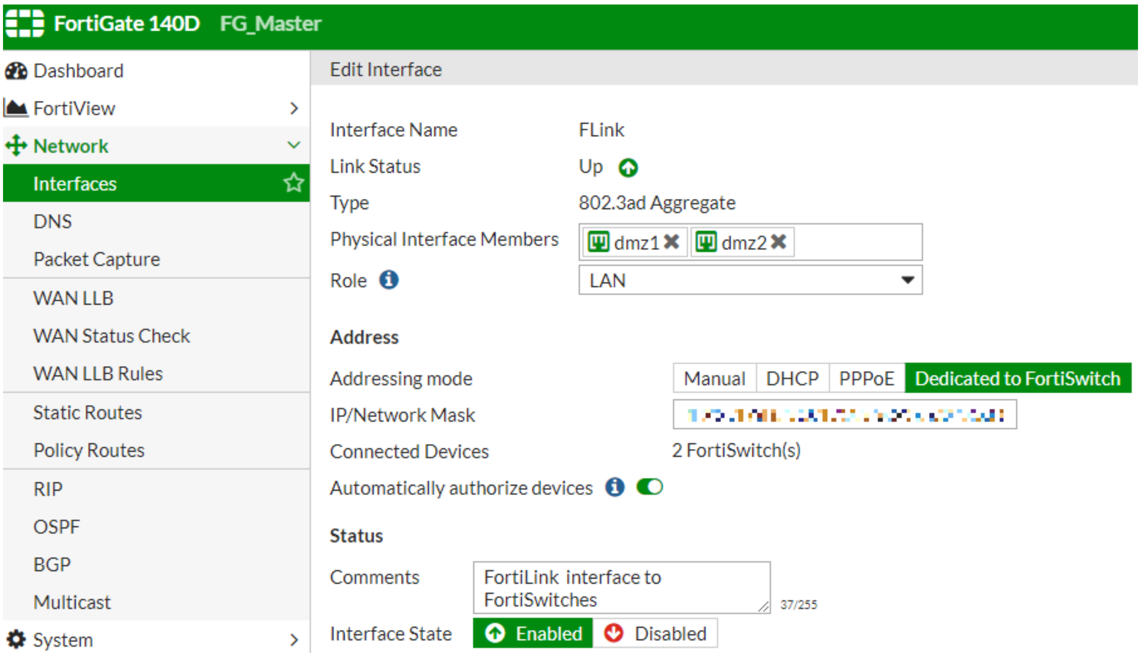


Figure 3. HA-mode Fortigate with two switches.

3.3.6 802.3ad Link Aggregation

In the Fortigate firewall, the link between the firewalls and switches is created using 802.3ad link aggregation and its management protocol Link Aggregation Control Protocol (LACP). This is a management protocol for combining multiple physical links into a single logical link. This enables the redundancy and it increases potential throughput between the devices. When LACP is being used, network traffic is distributed among the physical ports in the link, which increases performance /9/. In sWOIS, the physical interface members dmz1 and dmz2 are in the Fortigate firewall as shown in Figure 4.



Edit Interface

Interface Name FLink

Link Status Up

Type 802.3ad Aggregate

Physical Interface Members dmz1 ✖ dmz2 ✖

Role LAN

Address

Addressing mode Manual DHCP PPPoE [✓ Dedicated to FortiSwitch]

IP/Network Mask [redacted]

Connected Devices 2 FortiSwitch(s)

Automatically authorize devices ●

Status

Comments FortiLink interface to FortiSwitches 37/255

Interface State [✓ Enabled] Disabled

Figure 4. 802.3ad Aggregate interface in Fortigate GUI.

3.3.7 Integrated Dell Remote Access Controller

An integrated Dell Remote Access Controller (iDRAC) is embedded in every Dell PowerEdge Server used in sWOIS. It allows system administrators to update, monitor and maintain servers without any additional systems management software. As it is embedded in the servers, it requires no additional operating systems or hypervisors to work. Dell servers are equipped with specific iDRAC network ports, which can be accessed by any computer using a standard network cable /19/. The reason why this feature is used in this thesis is its simplicity to acquire hardware data from the server. Using iDRAC, administrators can see every hardware measurement (temperature, CPU, RAM usage, etc.) from the iDRAC GUI.

3.3.8 Wonderware InTouch

Wonderware’s InTouch is the HMI software that allows plant or facility operators to monitor engine and auxiliary data in a visualized format /14/. InTouch in sWOIS is accessed using a HP Thin Client running a HP ThinPro operating system.

As this is the main view for control room operators, one of the requirements for PRTG was to a have PRTG notification or alert integrated into InTouch to display any hardware or software malfunction in the sWOIS environment.

3.3.9 VMware ESXi

VMware ESXi is a bare metal hypervisor that installs directly to a server without having to install an operating system. This allows for more efficient use of the physical server resources. Figure 5 displays the role of the ESXi as a hypervisor /13/.

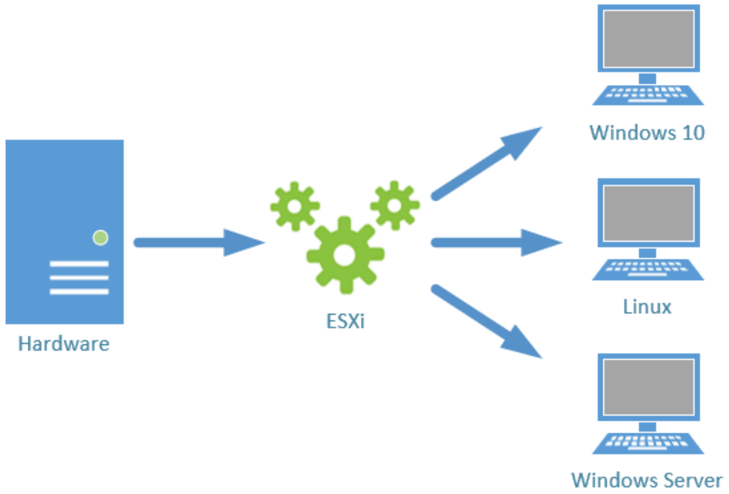


Figure 5. VMware ESXi bare metal hypervisor.

3.3.10 Paessler Router Traffic Grapher Network Monitor

The PRTG Network Monitor (later referred only as PRTG) is an “All-In-One Network Monitoring Software”. It allows system administrators to monitor and diagnose IT infrastructure quickly and efficiently. To analyze network traffic, PRTG uses mainly SNMP, packet sniffing, WMI and NetFlow /10/.

The software itself is a Windows based program, which is installed to a Dell PowerEdge server running Windows Server2012 R2 64-bit operating system. As the main reason for a network monitoring tool was to monitor and diagnose the sWOIS HMI, PRTG will be installed to a standalone server without any other virtual machines running on the same platform. It will also have its own subnet and VLAN with firewall policies created in the Fortigate firewall policy list. Figure 6 explains the segmentation used in this thesis.

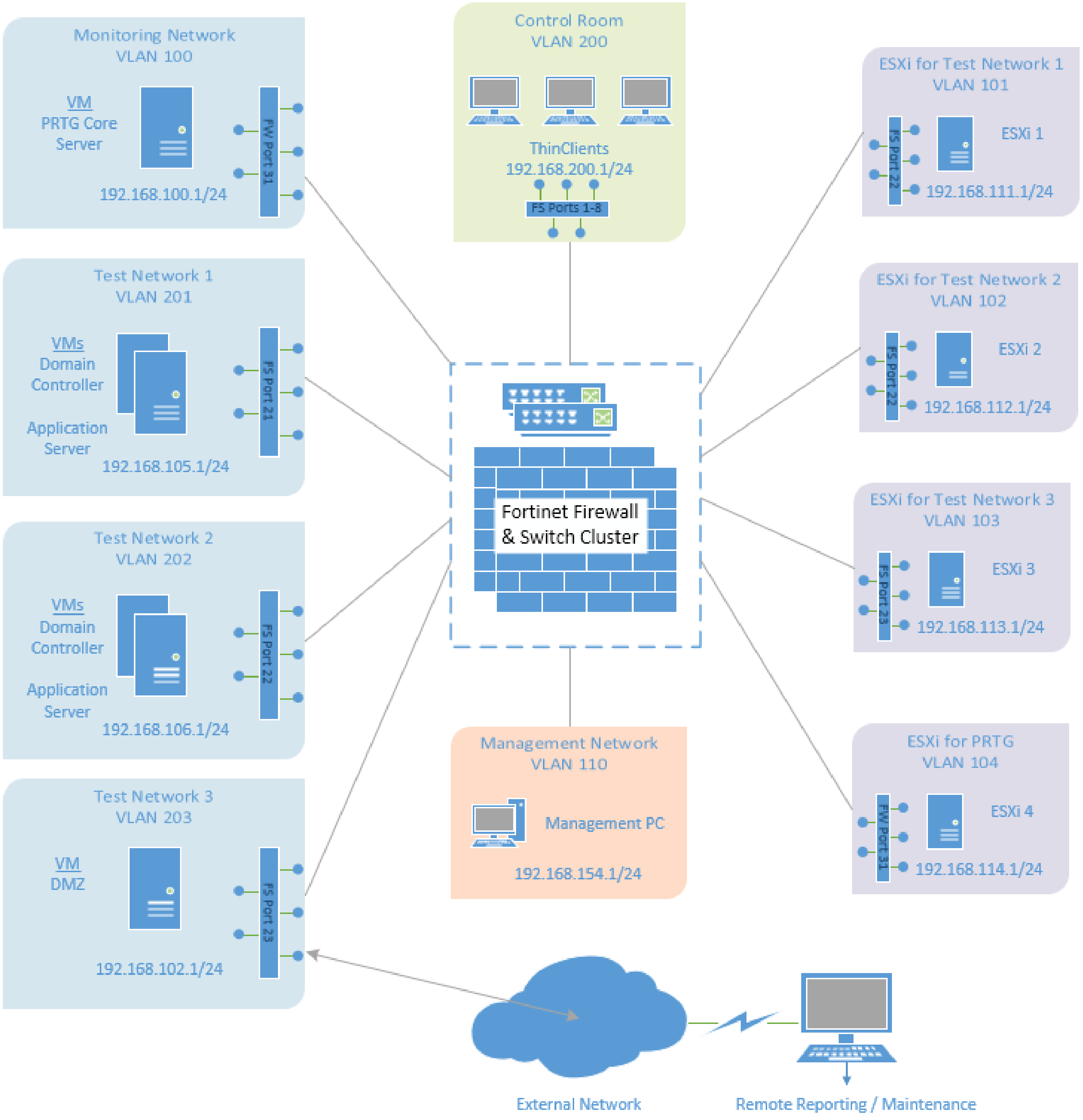
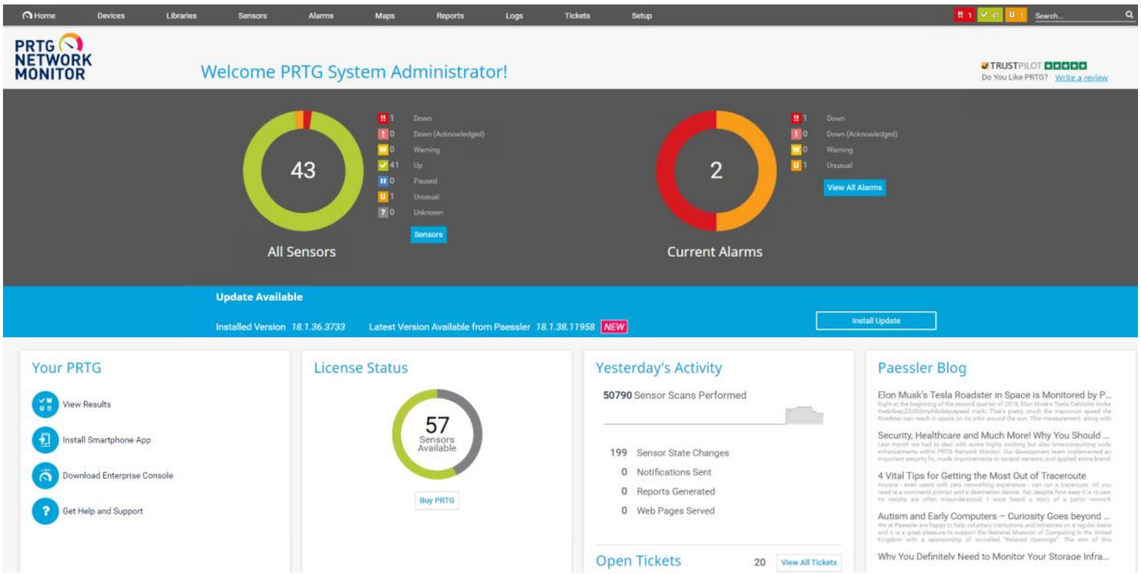


Figure 6. Network segmentation.

3.3.11 The Operation of PRTG

The main component of PRTG is the core server. The Windows installer installs the core services of PRTG, which also includes a web server. This enables system administrators to use the software from a web GUI using a browser. PRTG also offers the possibility to use its Enterprise Console, which is a native Windows application, or mobile applications for Android, iOS, Windows Phone and Blackberry /11/. In this thesis, all the configuration and testing are done using the web interface (Figure 7).



Welcome PRTG System Administrator!

Do You Like PRTG? Write a review

43

All Sensors

‼ 1	Down
! 0	Down (Acknowledged)
W 0	Warning
✓ 41	Up
⏸ 0	Paused
U 1	Unusual
? 0	Unknown

2

Current Alarms

‼ 1	Down
! 0	Down (Acknowledged)
W 0	Warning
U 1	Unusual

Update Available

Installed Version 18.1.36.3733 Latest Version Available from Paessler 18.1.38.11958 NEW

Your PRTG

- View Results
- Install Smartphone App
- Download Enterprise Console
- Get Help and Support

License Status

57 Sensors Available

Yesterday's Activity

50790 Sensor Scans Performed

199	Sensor State Changes
0	Notifications Sent
0	Reports Generated
0	Web Pages Served

Open Tickets 20

Paessler Blog

Elon Musk's Tesla Roadster in Space is Monitored by P...
Right at the beginning of the second quarter of 2018, Elon Musk's Tesla Cabriolet broke the 25,000mph speed mark. That's pretty much the maximum speed the Roadster can reach in space on its orbit around the sun. This measurement, along with

Security, Healthcare and Much More! Why You Should ...
Last month we had to deal with some highly exciting but also time-consuming code enhancements within PRTG Network Monitor. Our development team implemented an important security fix, made improvements to several sensors, and applied some brand-

4 Vital Tips for Getting the Most Out of Traceroute
Anyone - even users with zero networking experience - can run a traceroute. All you need is a command prompt and a destination device. Yet, despite how easy it is to use, its results are often misunderstood. I once heard a story of a junior network

Autism and Early Computers – Curiosity Goes beyond ...
We at Paessler are happy to help voluntary institutions and initiatives on a regular basis and it is a great pleasure to support the National Museum of Computing in the United Kingdom with a sponsorship of so-called "Relaxed Openings". The aim of this

Whv You Definitelv Need to Monitor Your Storage Infra...

Figure 7. Home screen of the PRTG web GUI.

The operating model of PRTG is shown in Figure 8. The core server sends SNMP, ping or WMI requests to network devices, if the connected device is configured to respond, they send a reply to PRTG, which then visualizes the result in the web interface (Figure 9).

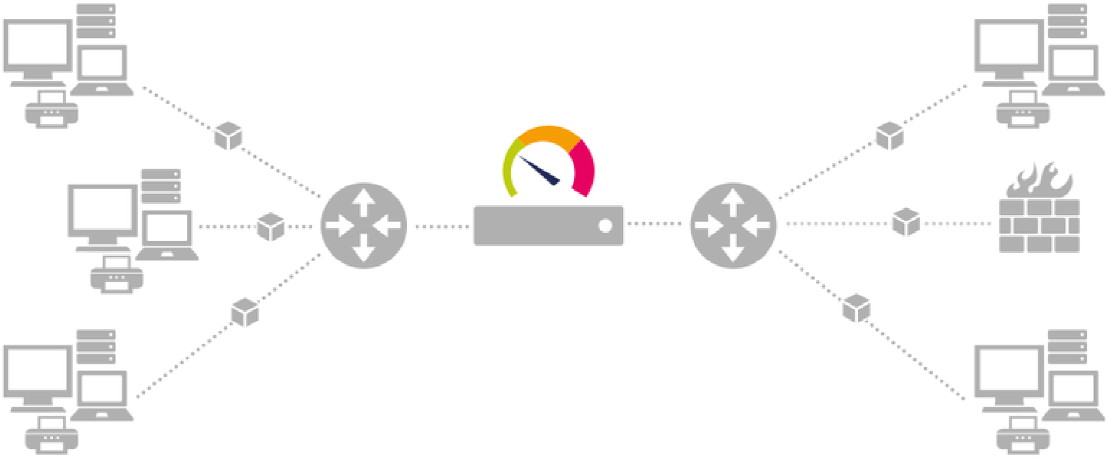


Figure 8. The operating model of PRTG /24/.

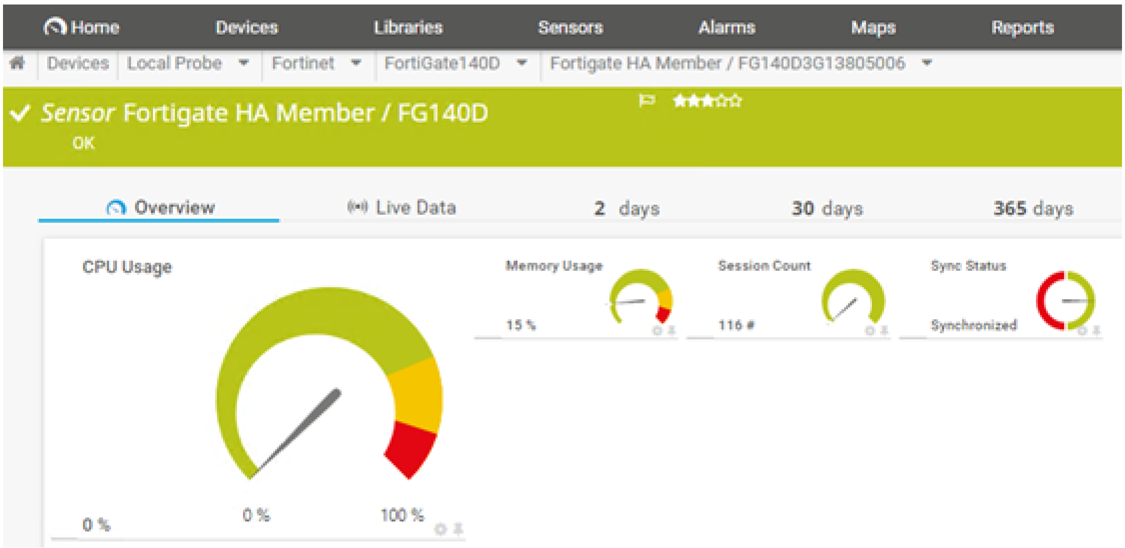


Figure 9. Fortigate firewall health status SNMP sensor.

3.3.12 PRTG Sensors

When using PRTG, the concept of a sensor is very important to understand. Sensors are the basic monitoring elements in PRTG and one sensor monitors a specific aspect of a device. Sensors are further divided into channels as displayed in Figure 9. The sensor “Fortigate HA Member / FG140D” has 4 channels; CPU Usage, Memory Usage, Session Count and Sync Status, which are combined into a single sensor. This sensor is a part of the Fortigate’s Management Information Base (MIB) file, which can be uploaded to PRTG. Using manufacturer specific MIB files to upload sensors into PRTG can save the number of sensors required to be created. This becomes important when moving from a trial version of PRTG to a licensed version as PRTG bases its licensing on the number of sensors used. Typically, any device uses between 5 and 10 sensors (CPU, RAM, disk space, etc.) but as explained, this number can be reduced by using existing MIB files /12/.

4 PRTG NETWORK MONITOR IN SWOIS

4.1 Planning Phase

The planning phase of the project started with a meeting with members from the Wärtsilä Cyber Security department where the requirements specifications were created. Based on these requirements, the planning of a new network segment as well as the new server hardware and monitoring software was done.

4.1.1 Requirements Specifications

This thesis was started in cooperation with Wärtsilä Cyber Security to form requirements specifications for the project. The requirements were divided into three different groups as shown in tables 1, 2 and 3.

Table 1. Required software functions.

Reference	Description	Priority
F1	Detect hardware failures	1
F2	Read virtual machine system status (ESXi)	2
F3	Collect hardware system status (On/Off)	2
F4	Basic reporting	2
F5	Alert WOIS operator on HW/SW/Network failures	3
F6	Fortinet monitoring / syslog / SNMP	2
F7	Hardware monitoring (CPU, RAM, temp, RAID)	2
F8	UPS (Eaton) monitoring	2
F9	iDRAC port monitoring (ESXi preferred)	3

Table 2. External interface. References on how the system is interfaced to other systems and environment.

Reference	Description	Priority
I1	Web interface / software GUI	1
I2	Remote access to system monitoring software	1
I3	Interface to customer monitoring system	3

Table 3. Other characteristics required from the selected monitoring software.

Characteristic	Description	Priority
Usability	GUI needs to be easy to operate	2
Safety	Only authorized personnel can operate the system	1
Price	Reasonable pricing options / free trial	2
Error detection	WOIS operator can detect HW errors easily	1
Segment	New network segment to sWOIS	1
Hardware	New hardware for monitoring system (server)	1
Network	Network traffic monitoring (SNMP / NetFlow …)	2
Scalability	Option to extend monitoring to higher level	3
Software patching	Option to update remotely	2

4.1.2 Software

PRTG Network Monitor was selected for testing based on these requirements and the compatibility PRTG has with already existing network devices in sWOIS (Fortigate, Dell servers, ESXi). Other software options were also considered but were discarded in the process of testing PRTG due to PRTG’s excellent properties.

As the sWOIS default environment used in this thesis is already in production, no other planning was required concerning the hardware or software used in implementation and testing phases.

4.1.3 Network

The planning for a new network segment for the monitoring software was done in cooperation with Wärtsilä. This also required planning for new firewall rules, port assignments and routes to be applied in the Fortigate configuration (Figures 10 and 11). IP addresses and VLAN IDs used in this document do not correlate the ones used in production.

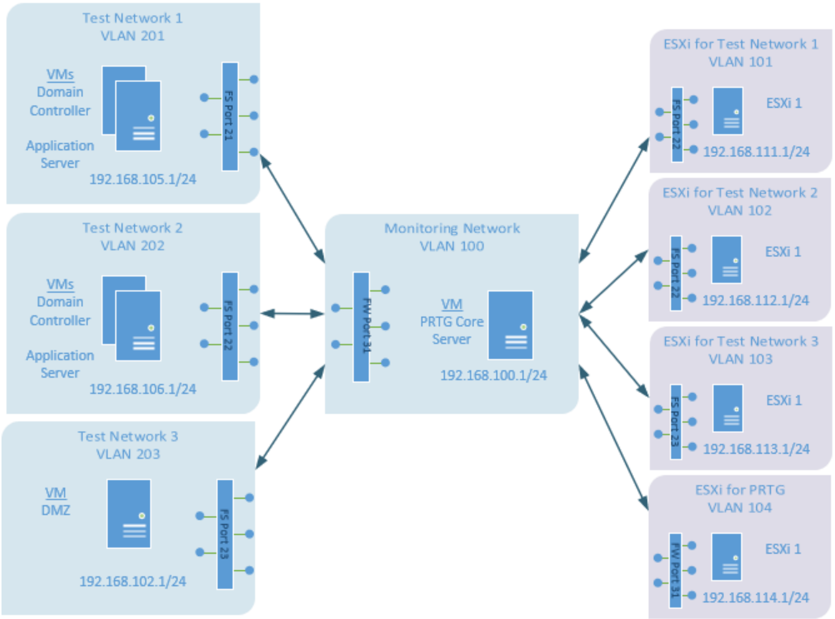


Figure 10. Network segments and routes created in Fortigate configuration.

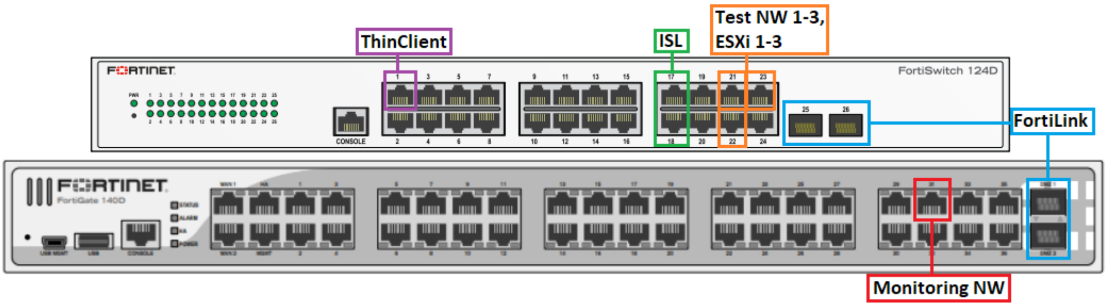


Figure 11. Fortigate and Fortiswitch port assignments.

4.1.4 Hardware

The hardware used in the future for the PRTG core server in production environment will be decided by Wärtsilä as it is not yet part of the default sWOIS. In this thesis the core server was installed to a Dell T630 desktop server running Windows Server2012 R2 64-bit operating system.

4.2 Implementation

To test the network monitoring solution successfully, a test version of the sWOIS setup had to be configured using the components and devices explained in this section.

4.2.1 Hardware

Table 4 lists all the hardware used in the test environment excluding network cables.

Table 4. sWOIS hardware components.

Device	**Operating System**	**Additional Information**
Fortigate 140D Firewall	FortiOS 5.4, build1138	2x firewalls in HA cluster
Fortiswitch 124D	S124DN-v3.6.2-build382	2x switches in ISL
Dell PowerEdge T630	Windows Server2012 R2	ESXi, PRTG core server
Dell PowerEdge R430	Windows Server2012 R2	ESXi, Test Network 1
Dell PowerEdge R430	Windows Server2012 R2	ESXi, Test Network 2
Dell PowerEdge R420xr	Windows Server2012 R2	ESXi, Test Network 3
HP Z440	Windows 10	Management PC

4.2.2 Fortigate 140D Firewall

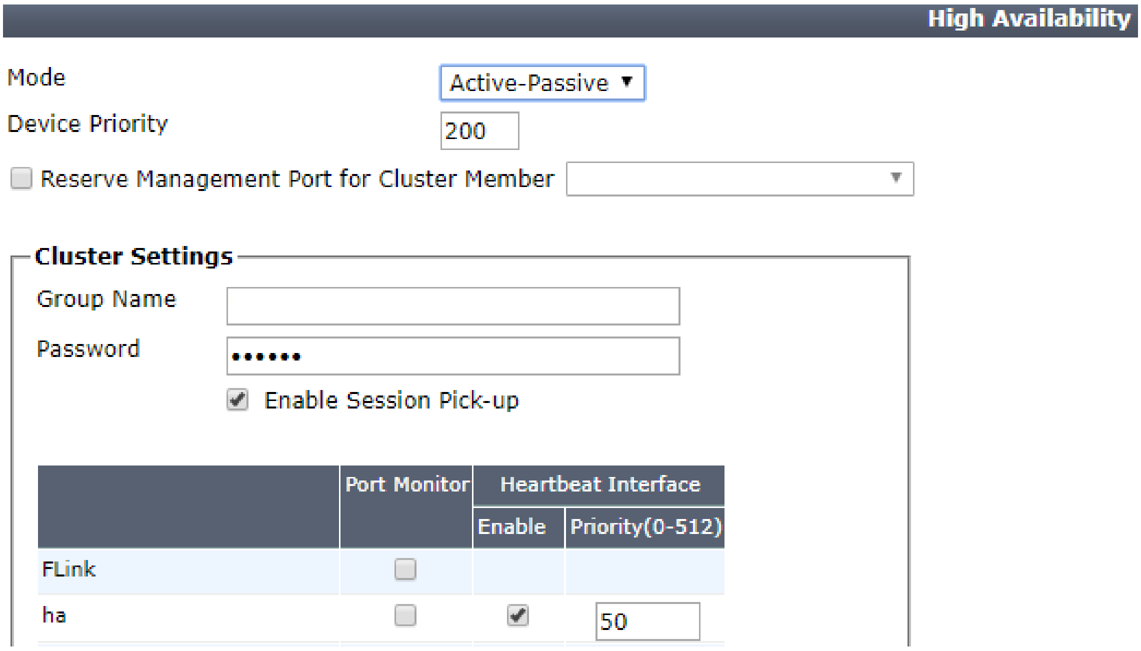
Figure 12. Fortigate 140D Firewall.

The main component of the network in sWOIS is the Fortigate 140D firewall. It is used to create firewall policies between network segments to route network traffic and it also blocks and logs any unauthorized connections. The firewall can be configured using a Graphical User Interface (GUI), Command Line Interface (CLI) or FortiExplorer software by connecting to the USB port of the device. This documentation uses only the GUI.

4.2.3 Fortigate High Availability Cluster

Using two of these firewalls, they form a high-availability (later referred as HA) cluster to improve network reliability. The main purpose of using a HA cluster is redundancy; if one firewall malfunctions or reboots, the other firewall will take its place without causing any downtime in the network. The two firewalls work in active-passive mode, which means that only one of the firewalls is actively routing network traffic while the other stays idle.

To form the HA cluster, the firewalls are linked using a RJ-45 Ethernet cable in their HA ports and the cluster settings are set on both firewalls (Group Name, Password and Device Priority). In this configuration, the HA ports are also set as heartbeat interfaces in the Fortigate settings (Figure 13).



High Availability

Mode: Active-Passive ▼

Device Priority: 200

□ Reserve Management Port for Cluster Member ▼

Cluster Settings

Group Name:

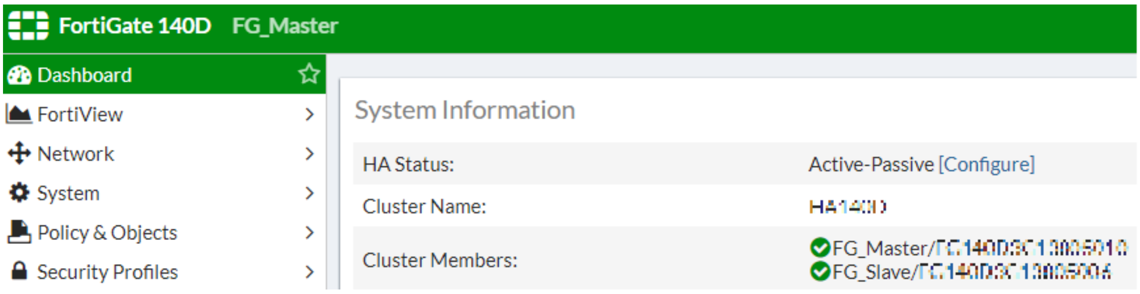
Password: ••••••

☑ Enable Session Pick-up

	Port Monitor	Heartbeat Interface	
		Enable	Priority(0-512)
FLink	□		
ha	□	☑	50

Figure 13. Fortigate High Availability cluster settings.

The heartbeat interface is used between the two firewalls to poll each other – if the active firewall stops responding to the standby unit, their roles are switched without causing any significant downtime. It is also possible to add more than one heartbeat interface if required, but this configuration does not use any additional ports for HA monitoring. After the settings have been edited and the HA cable connected, Fortigate will automatically form the HA cluster using Fortigate Clustering Protocol (FGCP) /7/. Figure 14 displays the Fortigate system information with a synchronized HA cluster.



System Information

HA Status: Active-Passive [Configure]

Cluster Name: HA140D

Cluster Members:
FG_Master/FG140D3C13005010
FG_Slave/FG140D3C13005004

Figure 14. Successfully created Fortigate High Availability Cluster.

4.2.4 Fortigate Network Interfaces

Every device or subnet requires its own network interface in the Fortigate firewall or Fortiswitch. One physical port in the firewall or switch can contain multiple logical interfaces or subnets. An overview of the network interfaces in the Fortigate GUI is shown in Figure 15.

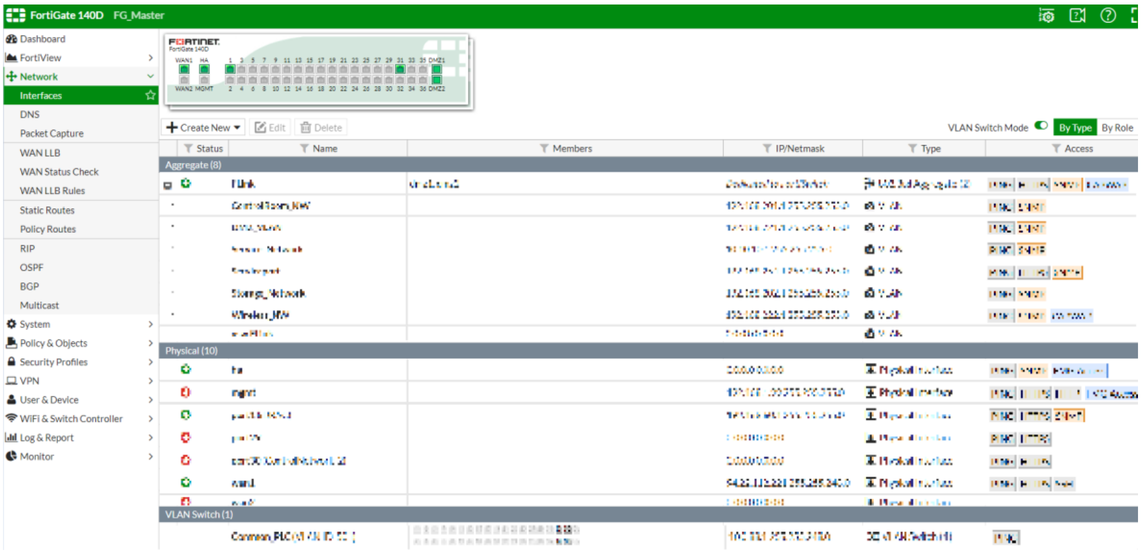


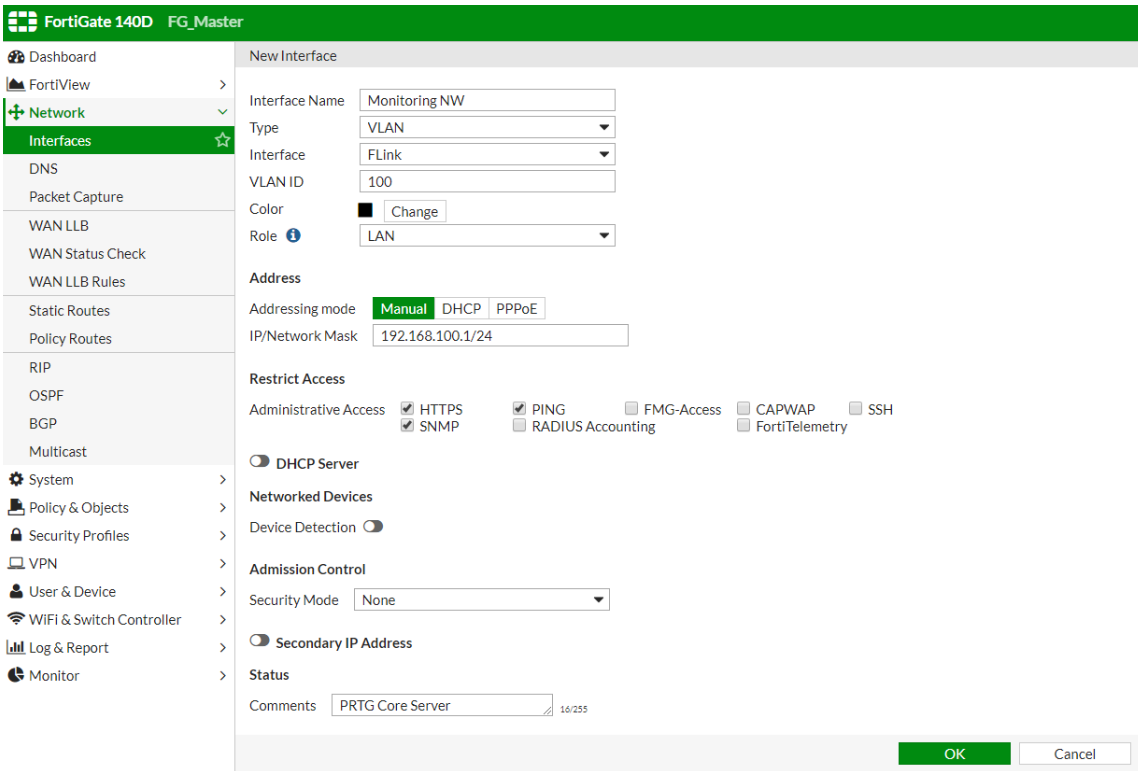
Figure 15. Fortigate Network Interfaces.

As Wärtsilä uses these interfaces and IP addresses in production, they will not be added to this document in full. Table 5 defines the IP addresses and network segments used in this thesis (with the IPs and VLAN IDs modified).

Table 5. IP addresses and network segments used in this thesis.

Network Segment	IP Address	VLAN ID	Information
Monitoring NW	192.168.100.1/24	100	PRTG core server
Test NW 1	192.168.105.1/24	201	Two VMs, IIS
Test NW 2	192.168.106.1/24	202	Two VMs, IIS
Test NW 3	192.168.102.1/24	203	DMZ VM
Management NW	192.168.154.1/24	110	Management PC
ESXi 1	192.168.111.1/24	101	ESXi for Test NW1
ESXi 2	192.168.112.1/24	102	ESXi for Test NW2
ESXi 3	192.168.113.1/24	103	ESXi for Test NW3
ESXi 4	192.168.114.1/24	104	ESXi for PRTG
InTouch NW	192.168.200.1/24	200	ThinClient

All the interfaces are created using the Fortigate GUI. System administrators can create or modify the interfaces as shown in Figure 16.



New Interface

Interface Name: Monitoring NW
Type: VLAN
Interface: FLink
VLAN ID: 100
Color: ■ Change
Role: LAN

Address

Addressing mode: [✓ Manual] DHCP PPPoE
IP/Network Mask: 192.168.100.1/24

Restrict Access

Administrative Access: ☑ HTTPS ☑ PING □ FMG-Access □ CAPWAP □ SSH ☑ SNMP □ RADIUS Accounting □ FortiTelemetry

○ DHCP Server

Networked Devices

Device Detection ○

Admission Control

Security Mode: None

○ Secondary IP Address

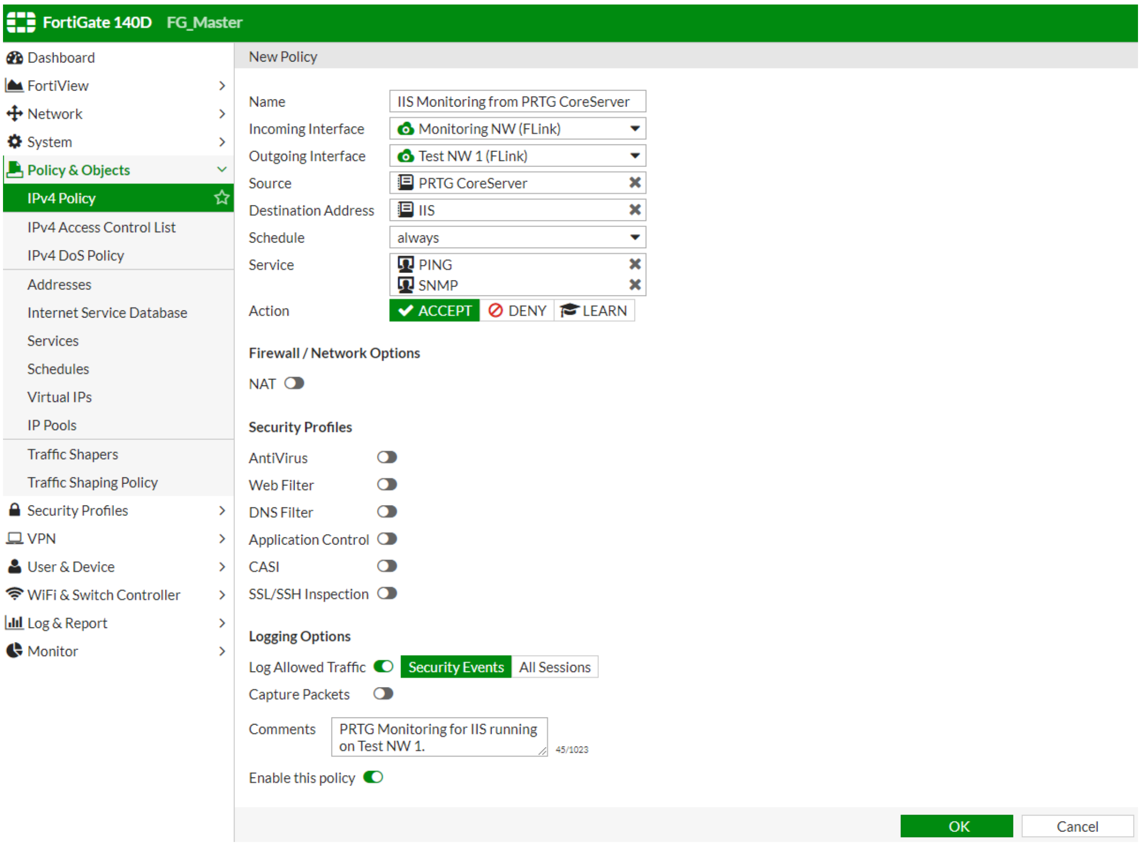
Status

Comments: PRTG Core Server 16/255

Figure 16. Creating a new interface in Fortigate GUI.

4.2.5 Fortigate Firewall Policies

Firewall policies are used to route traffic between network segments and it is the main function of the Fortigate firewall. This also enables network administrators to specify protocols, VLANs or services that are allowed to pass through the network. The new policy creation is displayed in Figure 17.



New Policy

Name: IIS Monitoring from PRTG CoreServer

Incoming Interface: Monitoring NW (FLink)

Outgoing Interface: Test NW 1 (FLink)

Source: PRTG CoreServer

Destination Address: IIS

Schedule: always

Service: PING
SNMP

Action: [✓ ACCEPT] DENY LEARN

Firewall / Network Options

NAT ○

Security Profiles

AntiVirus ○

Web Filter ○

DNS Filter ○

Application Control ○

CASI ○

SSL/SSH Inspection ○

Logging Options

Log Allowed Traffic ● [✓ Security Events] All Sessions

Capture Packets ○

Comments: PRTG Monitoring for IIS running on Test NW 1. 45/1023

Enable this policy ●

OK Cancel

Figure 17. Firewall policy for IIS monitoring from PRTG core server to Test NW 1 using SNMP.

The firewall policies in the network follow the process as shown in Figure 18.

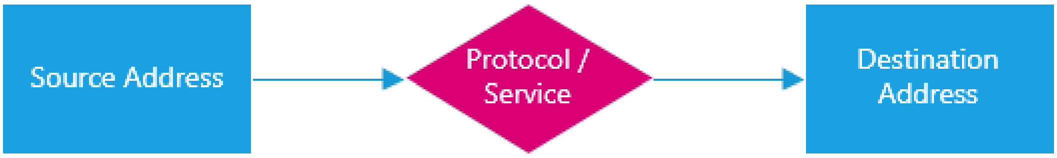
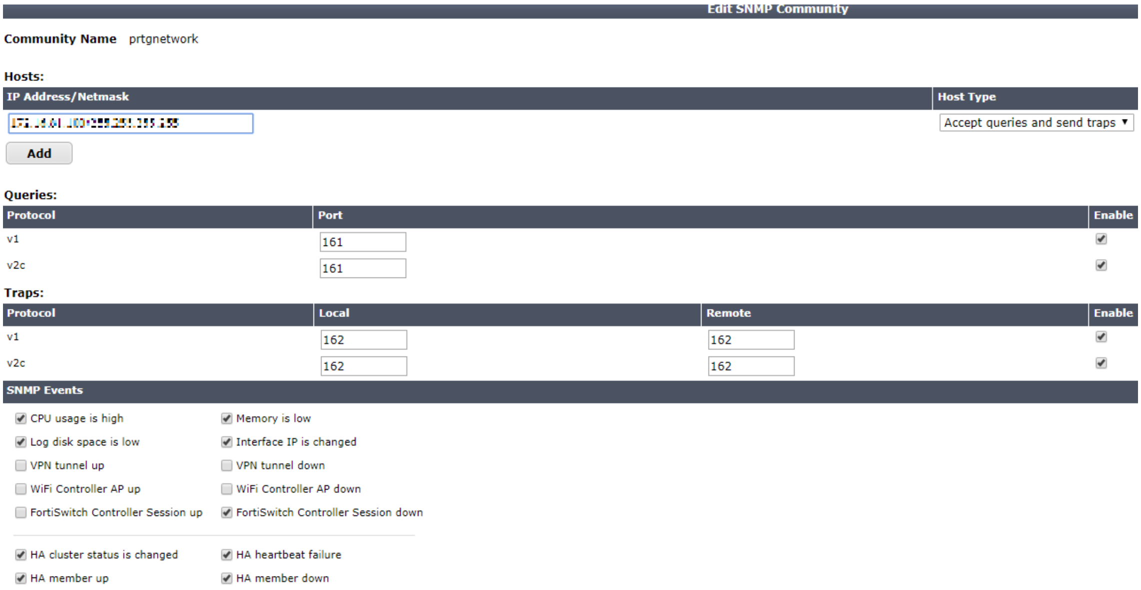


Figure 18. The principle of a firewall policy.

The new firewall rules created for the monitoring network can be found from “Thesis firewall rule list - Redundant_server.xlsx” in appendix 1.

4.2.6 Fortigate SNMP, NetFlow and Syslog Configuration

Aside from firewall policies, in order to enable SNMP, the SNMP v2c community must be configured in Fortigate. The settings used are displayed in Figure 19.



Edit SNMP Community

Community Name prtgnetwork

Hosts:

IP Address/Netmask	Host Type
[redacted]	Accept queries and send traps ▼

Queries:

Protocol	Port	Enable
v1	161	☑
v2c	161	☑

Traps:

Protocol	Local	Remote	Enable
v1	162	162	☑
v2c	162	162	☑

SNMP Events

☑ CPU usage is high
☑ Log disk space is low
☐ VPN tunnel up
☐ WiFi Controller AP up
☐ FortiSwitch Controller Session up
☑ Memory is low
☑ Interface IP is changed
☐ VPN tunnel down
☐ WiFi Controller AP down
☑ FortiSwitch Controller Session down

☑ HA cluster status is changed
☑ HA member up
☑ HA heartbeat failure
☑ HA member down

Figure 19. Fortigate SNMP community settings.

To allow communication in the network between devices, the following settings are applied:

- IP Address/Netmask
  - This is the IP of the PRTG core server
- Protocol port
  - Port 161 is used in all the network devices to communicate using SNMP
- SNMP Events
  - Miscellaneous events from Fortigate are sent to PRTG

NetFlow is a feature that provides the ability to collect IP network traffic as it enters or exits an interface /23/. In PRTG this traffic can be visualized to determine the source and destination of traffic, type of service and the causes of congestion. To enable this feature in Fortigate, the configuration must be done for each interface individually using the CLI. NetFlow information is exported from the source device using User Datagram Protocol (UDP) and collected using a collector (in this case PRTG). The sending device is the

Fortigate firewall, which uses the standard NetFlow UDP port 2055. The CLI commands used to enable NetFlow feature in Fortigate are listed below.

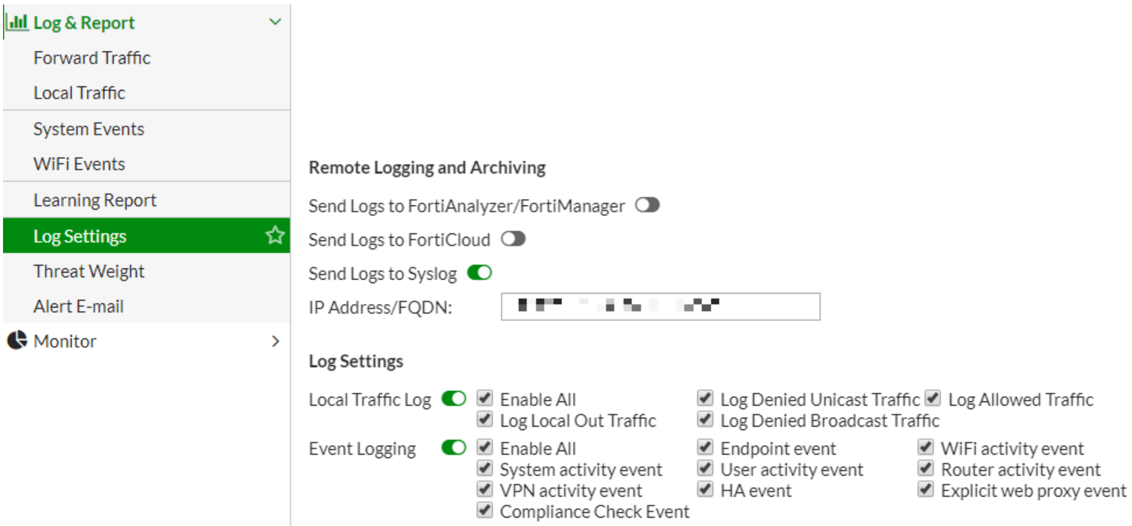
Configuring the NetFlow collector IP:

```
config system netflow
set collector-ip <ipv4_addr>
set collector-port <port_int>
end
```

Enabling NetFlow on the Interface

```
config system interface
edit <interface name>
set netflow-sampler both
end
```

Syslog was added to this project to receive event messages in PRTG. Syslog itself is a protocol used by network devices to send information to a syslog server (in this case PRTG). To allow Fortigate to forward these messages, the following update was configured in the logging options of the firewall (Figure 20):



Log & Report
Forward Traffic
Local Traffic
System Events
WiFi Events
Learning Report
Log Settings
Threat Weight
Alert E-mail
Monitor

Remote Logging and Archiving

Send Logs to FortiAnalyzer/FortiManager ○
Send Logs to FortiCloud ○
Send Logs to Syslog ●
IP Address/FQDN: [redacted]

Log Settings

Local Traffic Log ● ☑ Enable All ☑ Log Denied Unicast Traffic ☑ Log Allowed Traffic
☑ Log Local Out Traffic ☑ Log Denied Broadcast Traffic

Event Logging ● ☑ Enable All ☑ Endpoint event ☑ WiFi activity event
☑ System activity event ☑ User activity event ☑ Router activity event
☑ VPN activity event ☑ HA event ☑ Explicit web proxy event
☑ Compliance Check Event

Figure 20. Send logs to PRTG syslog server from Fortigate.

The IP address of the syslog server is the PRTG core server’s address.

4.2.7 Fortiswitch 124D

Figure 21. Fortiswitch 124D.

Fortiswitches are used in this setup to add more physical ports for connected devices. In a larger production facility, the amount of needed network ports can be over 50, depending on the number of engines and auxiliary systems.

Aside from the physical installation of the Fortiswitch, all management and configuration are done in the Fortigate GUI. Fortiswitches have their own GUI and CLI available, but it is not recommended to use these features while they are under the Fortilink remote control

Figure 22 displays all active ports in Fortiswitches in green. Ports 17 and 18 are the interconnected ISL ports.

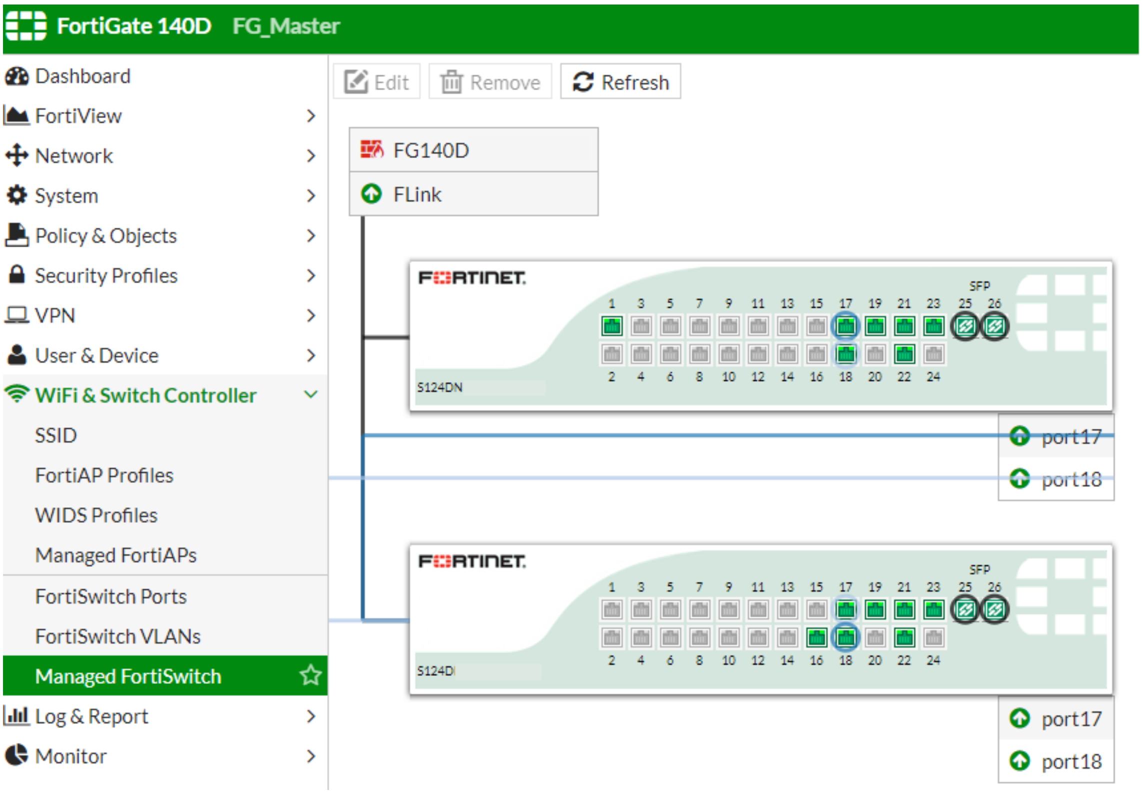


Figure 22. Managing Fortiswitches from Fortigate GUI.

4.2.8 Dell PowerEdge Servers

This project uses Dell’s PowerEdge servers as hardware for virtual machines. Table 6 displays the specifications for the devices.

Table 6. Dell PowerEdge servers.

Model	CPU	RAM	Hard drive
R430	2 CPUs x Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz	64GB	1.09TB
R430	2 CPUs x Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz	64GB	1.09TB
R420xr	Intel(R) Xeon(R) CPU E5-2430 v2 @ 2.50GHz	16GB	745GB
T630	2 CPUs x Intel(R) Xeon(R) CPU E5-2623 v3 @ 3.00GHz	32GB	1.09TB

4.2.9 Configuration of the PRTG Core Server

The PRTG software was installed to a Dell PowerEdge T630 server running a Windows Server 2012 R2 64-bit operating system. The Windows installer is available on the PRTG website and does not require any additional configuration prior or during the installation procedure. During the installation, PRTG configures all the software components needed to run the software, including webserver for web GUI access, database for storage and the Enterprise Console to be used as a Windows native application.

After the installation has been completed, PRTG can be accessed using a browser (Google Chrome 61 or later, Mozilla Firefox 56 or later or Microsoft Internet Explorer 11) from the localhost address 127.0.0.1, port 8080 as shown in Figure 23.

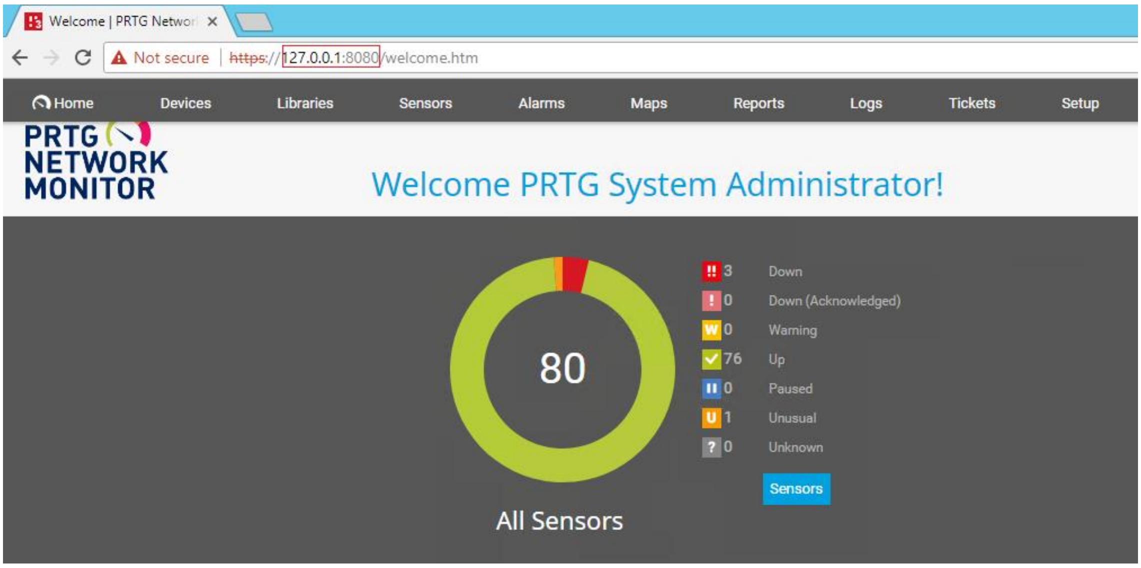


Figure 23. Accessing the web GUI of PRTG.

Upon installation, PRTG core server creates a local probe, which is used to monitor the local network. Probes in PRTG are the components that do the actual monitoring. In this instance, as the network is not open to the Internet, only a local probe is used. It is also possible to monitor different locations and networks using a single core server and multiple remote probes that report and send data to the core server. The local probe has its own built-in sensors that are created on the first installation (Figure 24). These sensors, as any other sensors in PRTG, can be modified or deleted.

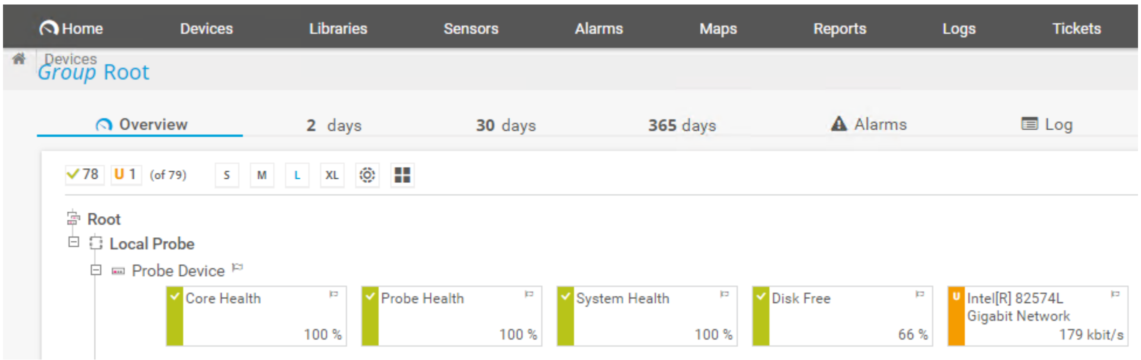
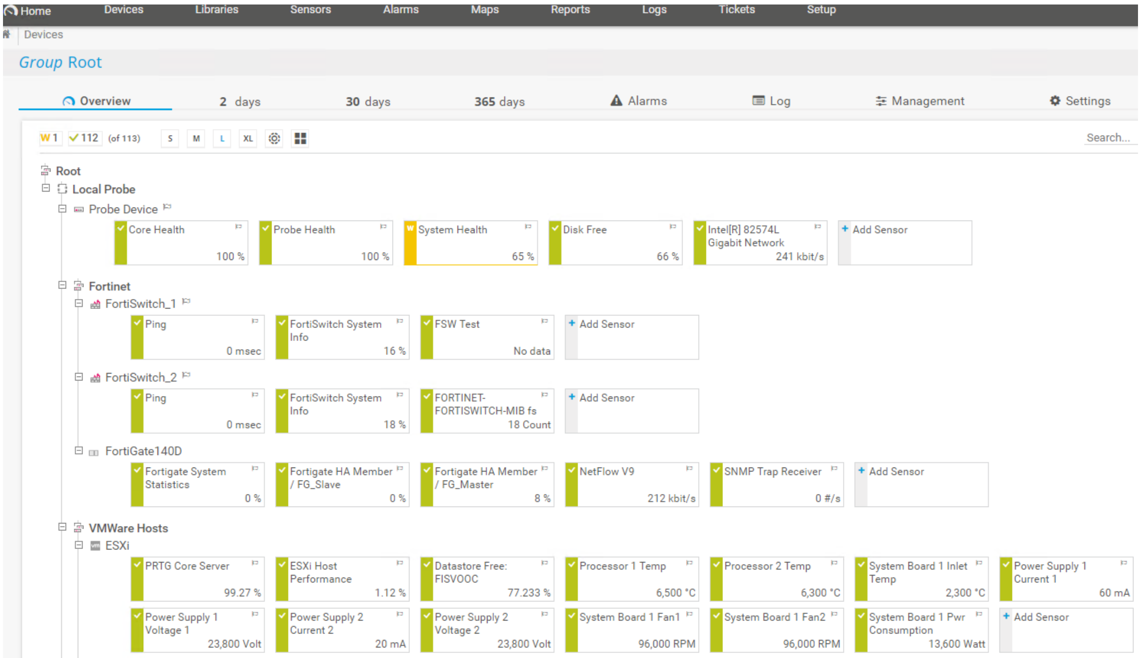


Figure 24. Local probe sensors created automatically.

During the first login, system administrators are also prompted to change the default login credentials. This becomes more important if the core server is exposed to the Internet to prevent any unauthorized login attempts.

4.2.10 Configuration of Devices PRTG

The majority of configuration was done in PRTG’s “Devices” section displayed in Figure 25.



Root
Local Probe
Probe Device
Core Health 100 %
Probe Health 100 %
System Health 65 %
Disk Free 66 %
Intel[R] 82574L Gigabit Network 241 kbit/s
Add Sensor

Fortinet
FortiSwitch_1
Ping 0 msec
FortiSwitch System Info 16 %
FSW Test No data
Add Sensor

FortiSwitch_2
Ping 0 msec
FortiSwitch System Info 18 %
FORTINET-FORTISWITCH-MIB fs 18 Count
Add Sensor

FortiGate140D
Fortigate System Statistics 0 %
Fortigate HA Member / FG_Slave 0 %
Fortigate HA Member / FG_Master 8 %
NetFlow V9 212 kbit/s
SNMP Trap Receiver 0 #/s
Add Sensor

VMWare Hosts
ESXi
PRTG Core Server 99.27 %
ESXi Host Performance 1.12 %
Datastore Free: FISVOOC 77.233 %
Processor 1 Temp 6,500 °C
Processor 2 Temp 6,300 °C
System Board 1 Inlet Temp 2,300 °C
Power Supply 1 Current 1 60 mA
Power Supply 1 Voltage 1 23,800 Volt
Power Supply 2 Current 2 20 mA
Power Supply 2 Voltage 2 23,800 Volt
System Board 1 Fan1 96,000 RPM
System Board 1 Fan2 96,000 RPM
System Board 1 Pwr Consumption 13,600 Watt
Add Sensor

Figure 25. Devices-menu of PRTG web GUI.

The software has an auto discovery feature that allows users to add network devices automatically to PRTG if they are connected and there are no firewall rules blocking the access. This feature, nor the auto discovery for device sensors was not used during this project as it proved to be inaccurate for the purposes of the thesis. All the devices and sensors were added manually.

The devices in PRTG are displayed in a tree hierarchy. Administrators are able to move devices to different branches if required and new branches can be created when needed. This thesis uses the hierarchy shown in Figure 26.

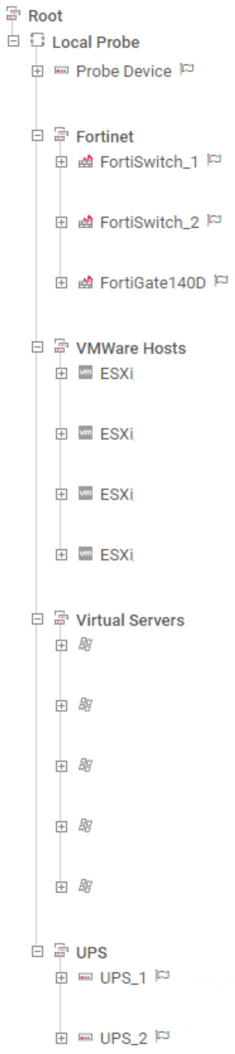


Figure 26. Tree hierarchy of PRTG.

Each physical and virtual device is added separately, and their respective sensors are displayed under the device. The benefit of using a tree hierarchy is inheritance. When similar devices are added under a branch in PRTG, they can be set to inherit SNMP, WMI, VMware or WBEM credentials from their parent device or branch, which in return reduces the number of repetitive administrator tasks needed during the configuration.

To add a new device in PRTG, system administrators can right-click on the desired branch on the Devices-view and select the option “Add Device” (figure 27). This opens the menu where the device information is defined, as shown in Figure 28.

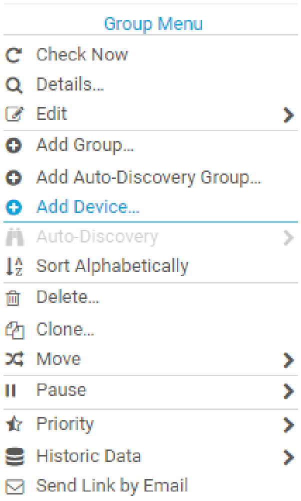
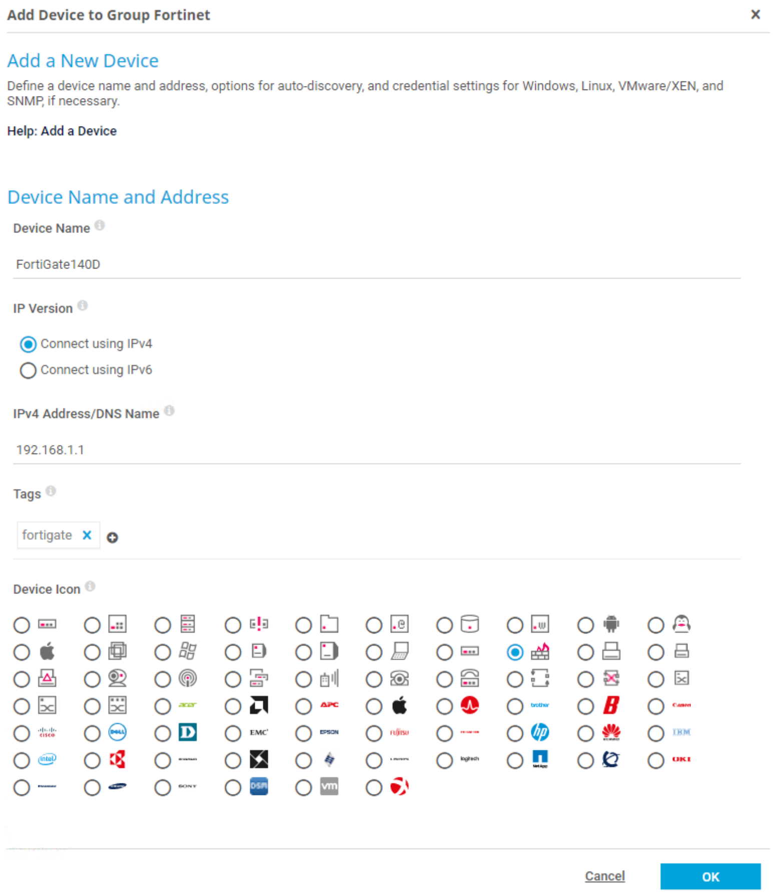


Figure 27. Group Menu for adding a new device to PRTG.


Add Device to Group Fortinet

Add a New Device

Define a device name and address, options for auto-discovery, and credential settings for Windows, Linux, VMware/XEN, and SNMP, if necessary.

Help: Add a Device

Device Name and Address

Device Name: FortiGate140D

IP Version:
● Connect using IPv4
○ Connect using IPv6

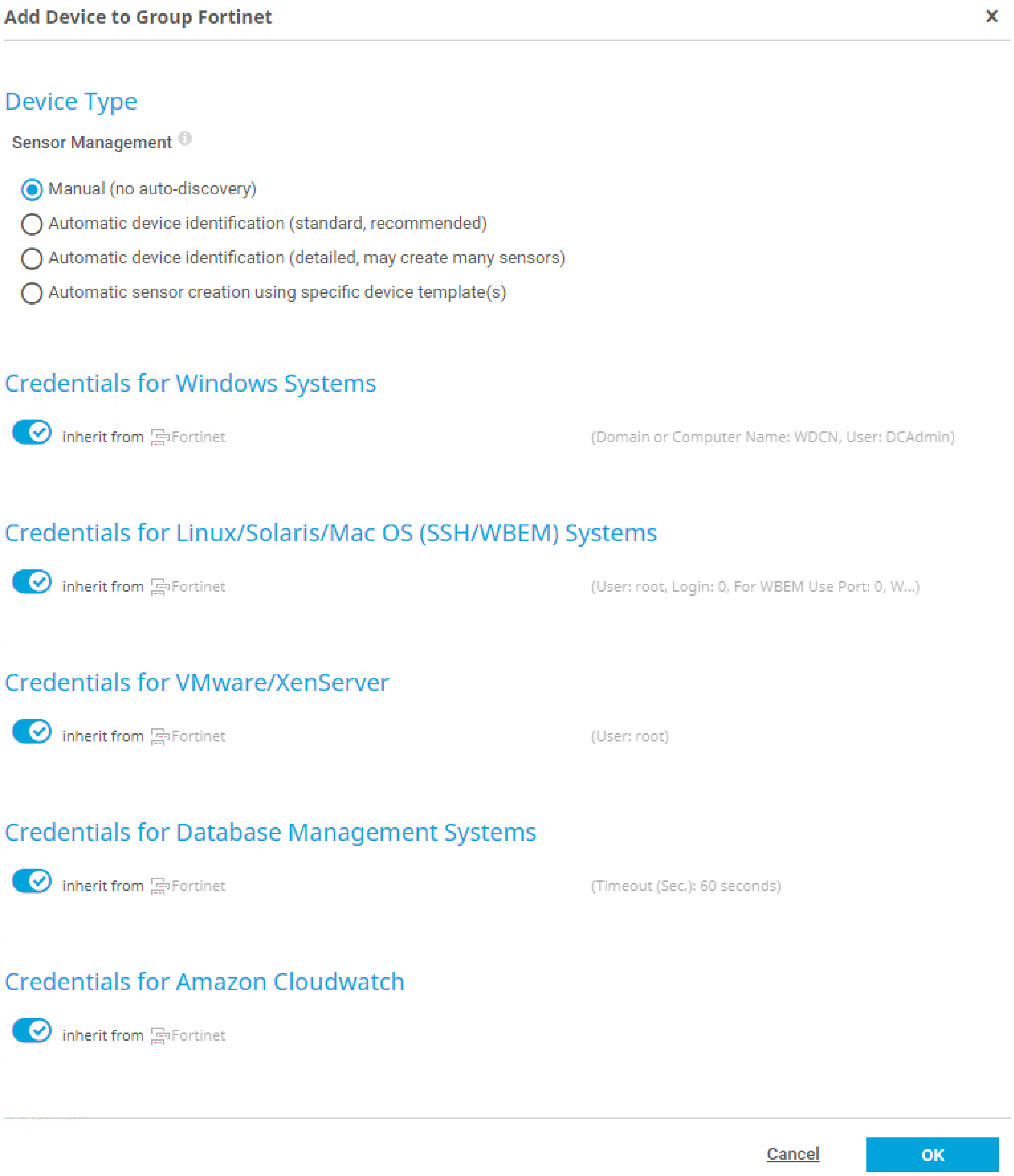
IPv4 Address/DNS Name: 192.168.1.1

Tags: fortigate

Device Icon

Figure 28. Adding of the FortiGate140D firewall to PRTG.

PRTG users must define the IP address and a device name, device icon and tags are optional but allow a better visual interpretation of the device view when similar icons are used for similar devices. Tags can be used to group objects (devices) and to assist in search features or when creating reports. Users must also select the Sensor Management method under the "Device Type" (Figure 29).



Add Device to Group Fortinet ×

Device Type

Sensor Management

● Manual (no auto-discovery)
○ Automatic device identification (standard, recommended)
○ Automatic device identification (detailed, may create many sensors)
○ Automatic sensor creation using specific device template(s)

Credentials for Windows Systems

✓ inherit from Fortinet (Domain or Computer Name: WDCN, User: DCAdmin)

Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems

✓ inherit from Fortinet (User: root, Login: 0, For WBEM Use Port: 0, W...)

Credentials for VMware/XenServer

✓ inherit from Fortinet (User: root)

Credentials for Database Management Systems

✓ inherit from Fortinet (Timeout (Sec.): 60 seconds)

Credentials for Amazon Cloudwatch

✓ inherit from Fortinet

Figure 29. Device Type and Credentials options for a new device.

PRTG has predefined sensor settings that can be used by the automatic sensor creation in the program for different devices under Sensor Management shown in the figure above. In this project, the option "Manual (no auto-discovery)" option was used to add only the required sensors to each device. Figure 28 displays also the inherited credentials that were discussed in the tree hierarchy. This device addition process was done to all the devices used in this project. Although PRTG has its network discovery feature that creates the devices automatically, after a small test, it was apparent that it did not create all the required devices and thus it was easier to add them one by one manually.

4.2.11 Creating the Sensors in PRTG

As sensors are the main component of the monitoring process of PRTG, this section of the project was the most time consuming and demanding as well as the core part of the thesis. The number of sensors per device used in the project varies between 3 (UPS) and 20 (servers) depending on the purpose of the device. In the hardware servers, it was mandatory to monitor the hardware itself, ESXi and the virtual machines running on the ESXi, which resulted in a higher number of sensors.

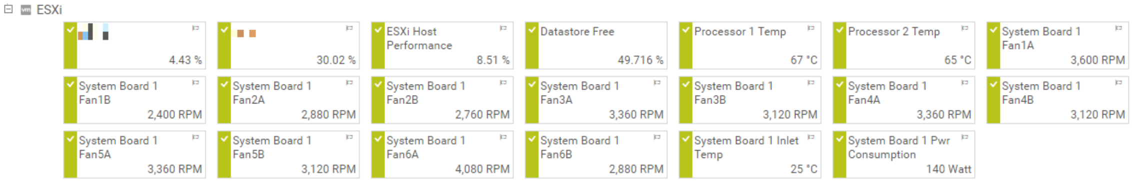
The start of the sensor adding process is similar to adding a new device, with the exception that PRTG user right-clicks on the device listed in the web GUI instead of the parent branch in the tree. Instead of using PRTG's auto-discovery feature for adding new sensors, all the sensors were added manually to optimize the measured values. When new sensors are added, they are displayed in the Devices-overview with a particular color to indicate its state (Table 7).

Table 7. PRTG Sensor States /21/.

Sensor	Color	Status	Meaning
!!	Red	Down	PRTG is unable to reach the device
!!	Green/Red	Down (Partial)	At least one node in a cluster is down

!	Bright-Red	Down (Acknowledged)	Sensor is down, acknowledged by PRTG user
W	Yellow	Warning	Error reading, but PRTG will try again
U	Orange	Unusual	Unusual values for this weekday and the time of day
✓	Green	Up	The last scan was okay, and the sensor is currently receiving data
⏸	Blue	Paused	Sensor is currently paused (for a certain time, indefinitely, triggered by a dependency)
?	Black	Unknown	No data received yet or an error in network communication

PRTG has a feature to add multiple sensors to a device using either vendor or protocol specific options. Figure 30 displays one of the hardware servers used in sWOIS with sensors added.



ESXi

✓ 4.43 %

✓ 30.02 %

✓ ESXi Host Performance 8.51 %

✓ Datastore Free 49.716 %

✓ Processor 1 Temp 67 °C

✓ Processor 2 Temp 65 °C

✓ System Board 1 Fan1A 3,600 RPM

✓ System Board 1 Fan1B 2,400 RPM

✓ System Board 1 Fan2A 2,880 RPM

✓ System Board 1 Fan2B 2,760 RPM

✓ System Board 1 Fan3A 3,360 RPM

✓ System Board 1 Fan3B 3,120 RPM

✓ System Board 1 Fan4A 3,360 RPM

✓ System Board 1 Fan4B 3,120 RPM

✓ System Board 1 Fan5A 3,360 RPM

✓ System Board 1 Fan5B 3,120 RPM

✓ System Board 1 Fan6A 4,080 RPM

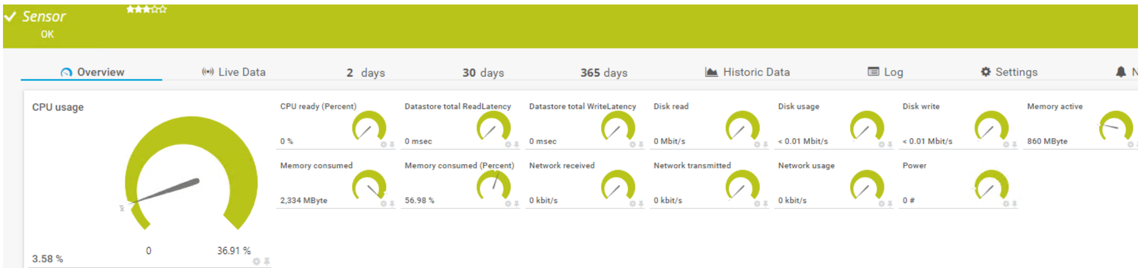
✓ System Board 1 Fan6B 2,880 RPM

✓ System Board 1 Inlet Temp 25 °C

✓ System Board 1 Pwr Consumption 140 Watt

Figure 30. Hardware server sensors.

In this server, the sensors vary from ESXi Host Performance to processor temperature and all the physical fan speeds. The status of the virtual machines installed to this ESXi are displayed in the first two sensors on the top left of the image. When the sensor is clicked in the web GUI, a more detailed information is available (Figure 31).



CPU usage 3.58 %

0

36.91 %

CPU ready (Percent) 0 %

Datastore total ReadLatency 0 msec

Datastore total WriteLatency 0 msec

Disk read 0 Mbit/s

Disk usage < 0.01 Mbit/s

Disk write < 0.01 Mbit/s

Memory active 860 MByte

Memory consumed 2,334 MByte

Memory consumed (Percent) 56.98 %

Network received 0 kbit/s

Network transmitted 0 kbit/s

Network usage 0 kbit/s

Power 0 #

Figure 31. Virtual machine status sensor.

This sensor is one of the SOAP sensors available in PRTG, it creates multiple channels ranging from CPU usage to network activity, but it still is counted only as one sensor. If all the measurements were added manually, this would consume 14 sensors total, which would become an issue when the PRTG cost is concerned. As the price of PRTG is based solely on the number of sensors used, more sensors equal more cost. Sensor types used per device are listed in Table 8.

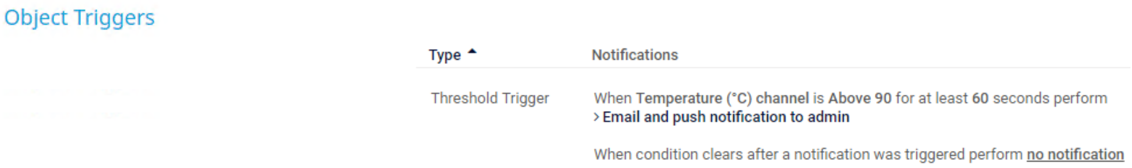
Table 8. List of sensor types used in this project.

Device	Sensor Types	Total Number of Sensors
Core Server	PRTG native sensors, syslog	6
Fortiswitch_1	SNMP	27

Fortiswitch_2	SNMP	27
Fortigate140D	SNMP, syslog, NetFlow	43
ESXi_1	SOAP, WBEM	25
ESXi_2	SOAP, WBEM	25
ESXi_3	SOAP, WBEM	21
ESXi_4	SOAP, WBEM	14
VirtualServer_1	SNMP, WMI	9
VirtualServer_2	SNMP, WMI	9
VirtualServer_3	SNMP, WMI	3
VirtualServer_4	SNMP, WMI	3
VirtualServer_5	SNMP, WMI	2

4.2.12 Defining Sensor Threshold Values and Alarms

To get the maximum value of using a network monitoring tool, threshold values and alarms are added to PRTG to be able to react to malfunctions even before they occur. These values are added to individual sensors and their channels manually to get a notification when a sensor is transmitting values outside of its predefined safe limits. When the values are over or under its limit for a specified period of time, email notifications are sent to PRTG administrators. A time buffer is added to the threshold to prevent false alarms. For example, a device is rebooting and is using higher CPU and RAM than when it is in idle state. If no time buffer is added, this would result in an alarm in PRTG. In Figure 32, the threshold trigger for a processor temperature is defined. If the temperature is over 90°C for 60 seconds, PRTG administrators will receive an email alarm.



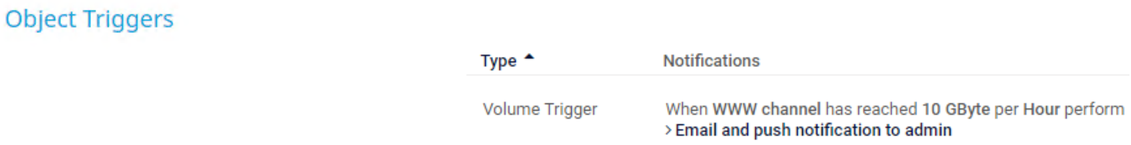
Object Triggers

[redacted]

Type ▲	Notifications
Threshold Trigger	When Temperature (°C) channel is Above 90 for at least 60 seconds perform › Email and push notification to admin When condition clears after a notification was triggered perform no notification

Figure 32. Trigger threshold for a processor's temperature.

Similar triggers are also added for RAM usage, fan speed, hard disk usage and RAID health. Other sensors, such as the interface sensors in Fortigate use an up or down type alarm. If the sensor is not responding to PRTG, it triggers an alarm if the next scan is also unsuccessful. Triggers are also added to NetFlow sensors. If a specific protocol is using an unexpected amount of bandwidth for an extended period, this might be a result of a failure or congestion in the network, which acquires the attention of an administrator.



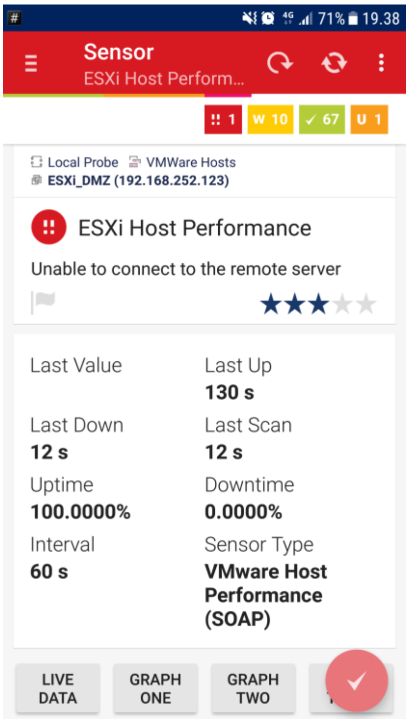
Object Triggers

Type ▲	Notifications
Volume Trigger	When WWW channel has reached 10 GByte per Hour perform › Email and push notification to admin

Figure 33. Trigger added to WWW-protocol.

4.3 Testing

The testing phase was started simultaneously with the implementation phase. The testing took place as the adding of sensors progressed and new sensors were created in PRTG. Sensors, such as interface up-down were easily tested by removing the device from the network (either by unplugging the network cable or changing the device’s IP address) but other sensors required different test methods, which are listed in Table 9. During the testing the PRTG mobile application for Android was used to receive the push notifications instantly.



Local Probe VMWare Hosts
ESXi_DMZ (192.168.252.123)

ESXi Host Performance

Unable to connect to the remote server

Last Value

Last Up
130 s

Last Down
12 s

Last Scan
12 s

Uptime
100.0000%

Downtime
0.0000%

Interval
60 s

Sensor Type
VMware Host Performance (SOAP)

Figure 34. Sensor information in PRTG Android application.

There was also a group of sensors which were not tested with very extreme values as it could have resulted in severe hardware failure (processor temperatures, fan speeds, hard disk usage, RAID health). These values were monitored, and the alarms tested with safe values. Table 9 displays the results of the testing phase and the methods used.

Table 9. Test phase results for sensors.

Sensor	Test Method	Alarm Triggered	Test Successful
CPU usage	Adjust threshold	Email, push notification	✓
RAM Usage	Adjust threshold	Email, push notification	✓
Health sensors	Power off device	Email, push notification	✓

Hard disk free	Adjust threshold	Email, push notification	✓
Bandwidth	Large file transfer between devices	Email, push notification	✓
Interface monitor	Disconnect Ethernet cable	Email, push notification	✓
NetFlow	Large file transfer between devices	Email, push notification	✓
Temperature sensors	Adjust threshold	Email, push notification	✓
Fan speeds	Adjust threshold	Email, push notification	✓
Power consumption	Adjust threshold	Email, push notification	✓
Current sensors	Adjust threshold	Email, push notification	✓
Voltage sensors	Adjust threshold	Email, push notification	✓
IIS sensor	Stop IIS in host OS	Email, push notification	✓
InTouch sensor	Exit program	Email, push notification	✓
Active Directory sensor	Stop Windows service	Email, push notification	✓

RAID sensor	Power off device	Email, push notification	✓

4.4 Review

After the initial planning phase of the project was concluded with Wärtsilä, the implementation and testing phases have been ongoing continuously. The majority of the work was done in the implementation phase as the sensor amount in PRTG was higher than anticipated beforehand.

At the beginning of the implementation phase it was required to configure the PRTG core server, update the firewall configuration to match the new network segmentation and add all the sensors to the monitoring software before the testing could be done successfully. The sensor implementation to sWOIS environment had some difficulties, which required the assistance of PRTG's support team to update the core server software version.

The testing phase was started after the firewall configuration was completed and the first sensors added to PRTG. This was mainly done on a trial and error basis by reading the sensor measurements and by knowing somewhat on what to expect of the sensor results. All the sensor types installed to PRTG have been tested and the results documented in Table 9. The alarm system as it is now (email and push notification) will be reviewed with Wärtsilä and PRTG support. The future development for the alarm is to implement a notification to the operator view in the InTouch software and reduce the amount of email notifications needed from the monitoring system.

5 CONCLUSIONS

The objective of the thesis was to design, implement and test a working network monitoring solution to sWOIS. Based on the requirement specifications from Wärtsilä, the selected monitoring software was implemented and tested in the sWOIS network environment. Table 10 displays the main focus points of the requirements and how they were completed in the thesis.

Table 10. Project summary.

Description	Result
Detect hardware failures	Sensors added and tested successfully
Read virtual machine system status (ESXi)	Sensors added and tested successfully
Collect hardware system status (On/Off)	Sensors added and tested successfully
Network traffic monitoring	Sensors added and tested successfully
Alert WOIS operator on HW/SW/Network failures	InTouch implementation required
Fortinet monitoring / syslog / SNMP	Sensors added and tested successfully
Hardware monitoring (CPU, RAM, temp)	Sensors added and tested successfully
UPS monitoring	Hardware not available for testing, will be tested in future development
iDRAC port monitoring	Sensors added and tested successfully
Option to extend monitoring to customer's network	To be investigated in future development

Based on the Table 10 results, there are some areas that require future development, but the current result of the project can be considered as a success. The PRTG monitoring software has been successfully implemented to the sWOIS automation system environment.

REFERENCES

/1/ This is Wärtsilä. Wärtsilä Web Pages. Accessed 13.12.2017.
https://www.wartsila.com/about

/2/ Environmental Excellence. Wärtsilä Web Pages. Accessed 13.12.2017.
https://www.wartsila.com/marine/why-us/environmental-excellence

/3/ Wärtsilä Marine Applications. Wärtsilä Web Pages. Accessed 13.12.2017.
https://www.wartsila.com/marine/applications

/4/ Wärtsilä Energy. Wärtsilä Web Pages. Accessed 6.1.2018.
https://www.wartsila.com/energy

/5/ Wärtsilä Services. Wärtsilä Web Pages. Accessed 6.1.2018.
https://www.wartsila.com/services

/6/ sWOIS user manual.doc. Wärtsilä Sharepoint. Accessed 6.1.2018.

/7/ High Availability with two Fortigates. Accessed 20.1.2018.
http://cookbook.fortinet.com/high-availability-two-Fortigates-54/

/8/ Inter-Switch Link and IEEE 802.1Q Frame Format. Accessed 20.1.2018.
https://www.cisco.com/c/en/us/support/docs/lan-switching/8021q/17056-741-4.html#intro

/9/ FGCO HA with 802.3ad aggregated interfaces. Accessed 20.1.2018.
http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_config_802.htm

/10/ PRTG Network Monitor. Accessed 29.10.2017.
https://www.paessler.com/prtg

/11/ PRTG Quick Overview. Accessed 29.10.2017.
https://www.paessler.com/learn/videos/prtg-basics/quick-overview

/12/ PRTG – What Is A Sensor? Accessed 5.2.2018.
https://www.paessler.com/learn/videos/prtg-basics/what-is-a-sensor

/13/ VMware ESXi. Accessed 3.3.2018.
https://www.vmware.com/products/esxi-and-esx.html

/14/ What is InTouch? Accessed 3.3.2018.
https://www.wonderware.com/hmi-scada/intouch/features/

/15/ A Simple Network Management Protocol (SNMP). Accessed 7.4.2018.
https://tools.ietf.org/html/rfc1157

/16/ The SNMP Protocol. Accessed 7.4.2018.
http://www.snmp.com/protocol/

/17/ PRTG Manual: Monitoring via SNMP. Accessed 7.4.2018.
https://www.paessler.com/manuals/prtg/snmp_monitoring

/18/ Introducing SNMP. Accessed 7.4.2018.
https://www.paessler.com/learn/whitepapers/introducing_snmp/part-1

/19/ iDRAC with Lifecycle Controller. Accessed 7.4.2018.
http://www.dell.com/learn/us/en/15/solutions/integrated-dell-remote-access-controller-idrac

/20/ PRTG Sensor States. Accessed 14.4.2017.
https://www.paessler.com/manuals/prtg/sensor_states

/21/ Web-Based Enterprise Management. Accessed 21.4.2018.
https://www.dmtf.org/standards/wbem

/22/ Simple Object Access Protocol Overview. Accessed. 21.4.2018.
https://docs.oracle.com/cd/A97335_02/integrate.102/a90297/overview.htm

/23/ How to Configure NetFlow on a Fortigate. Accessed 21.4.2018.
http://kb.fortinet.com/kb/documentLink.do?externalID=FD36460

/24/ Network Monitoring via SNMP. Accessed 14.4.2017
https://hlassets.paessler.com/common/files/infographics/network-monitoring-via-snmp-lightbox.png

APPENDIX 1

FIREWALL RULES - THESIS FIREWALL CONFIGURATION

		INTERFACE		SOURCE	DESTINATION		SERVICE
INDEX	NAME	FROM	TO	SOURCE IP	DESTINATION IP	DESTINATION PORT	
32	Monitor-ESXi	Monitoring Network	ESXi Management Zone	192.168.100.100	192.168.114.1, 192.168.113.1, 192.168.112.1, 192.168.111.1	135, 161, 162, 5989, 80, 443	RPC, SNMP, WBEM, HTTP, HTTPS
33	Monitor-Test NWs	Monitoring Network	Test NW 1 & 2	192.168.100.100	192.168.105.1/24, 192.168.106.1/24	135, 161, 162, 5989	RPC, SNMP, WBEM
34	Monitor-FortiSwitch	Monitoring Network	FortiLink	192.168.100.100	192.168.50.1/24	161, 162	SNMP
35	Monitor-DMZ	Monitoring Network	DMZ	192.168.100.100	192.168.102.1/24	135, 161, 162, 5989	RPC, SNMP, WBEM
36	Monitor-iDRAC	Monitoring Network	iDRAC	192.168.100.100	192.168.60.1/24	161, 162	SNMP