

Touko Uhrman

Design of a modern wide area network in a power distribution environment

Helsinki Metropolia University of Applied Sciences

Bachelor of Engineering

Information Technology and Communications

Bachelor's Thesis

30.4.2018

Author Title	Uhrman Touko Design of a modern information network in a power distribution environment
Number of Pages Date	38 pages 30 April 2018
Degree	Bachelor's Degree
Degree Programme	Bachelor of Engineering
Specialisation option	Information Technology and Communications
Instructor	Louhelainen Jukka, Senior lecturer
<p>This thesis shows the steps of designing and implementing new and more secure modern wide area network to customer.</p> <p>The customer had an old and securely vulnerable network at their power distribution environment. Since security and blocking threats comes more relevant every day, it is necessary to have up to date technology and security.</p> <p>Solution for the new customer's network was Checkpoint's high-availability cluster, which brings more redundancy to the environment. Mobile routers are used to detect the state of the power distribution network, and the state of the network is monitored with open source program called Zabbix.</p> <p>All the connections had to be encrypted with site-to-site VPN, for maximum security.</p> <p>At the end of the project, customer will have new and secure wide area network with real time monitoring.</p>	
Keywords	Mobile Network, Firewall Cluster, Network designing

Tekijä Otsikko	Uhrman Touko Modernin WAN-verkon toteutus sähköverkkoympäristöön
Sivumäärä Aika	38 sivua 30.4.2018
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot ja tietoliikenne
Ohjaaja	Lehtori Jukka Louhelainen
<p>Insinööriyön tarkoituksena oli suunnitella ja toteuttaa uusi sekä turvallisempi moderni WAN-verkko asiakkaalle.</p> <p>Asiakkaalla oli vanha ja tietoturvallisesti haavoittuva verkko ympäristössään. Koska tietoturva ja uhkien torjuminen käy yhä tärkeämmäksi, on tärkeää, että sähköverkkoyrityksillä on tietoturvallisesti ajan tasalla olevaa teknologiaa.</p> <p>Ratkaisuksi asiakkaan uuteen verkkoon valittiin Checkpointin korkean käytettävyyden palomuuriklusteri. Asiakkaan sähkö- ja erotinasemiin kytketään mobiilireitittimiä, joiden avulla valvotaan sähköverkon tilaa. Verkon monitorointiin käytetään avoimen lähdekoodin ohjelmaa nimeltä Zabbix.</p> <p>Kaikkien yhteyksien tulee olla salattuja site-to-site VPN:illä maksimaalisen tietoturvallisuuden takaamiseksi.</p> <p>Insinööriyön tuloksena asiakkaalle valmistui uusi ja tietoturvallinen WAN-verkko, jossa on reaaliaikainen monitorointi.</p>	
Avainsanat	mobiiliverkko, palomuuriklusteri, verkkosuunnittelu

Table of Contents

Abbreviations

1	Introduction	1
2	Network Topology	2
2.1	Old Network Topology	2
2.2	Cisco ASA	3
2.3	New Network Topology	4
2.4	IP Addressing	5
2.5	High-Availability Cluster Firewall	6
2.6	Mobile Routers	8
2.7	APN	10
2.7.1	Public APN	10
2.7.2	Private APN	11
2.8	Network monitoring	12
3	Preconfiguration	13
3.1	Building the Cluster	13
3.2	Configuring the Cluster	17
3.3	Testing HA functionality	20
3.4	Mobile Routers	20
4	On-Site Configuration	22
4.1	Zabbix	24
4.2	Finishing Cluster Policies	31
4.3	Mobile Routers IPSec VPN	32
4.4	Operator's APN	35
4.5	Site-to-Site connection	35
5	Conclusions	37
	References	38

Abbreviations

WAN	Wide Area Network
LAN	Local Area Network
DHCP	Dynamic Host Configuration Protocol
VPN	Virtual Private Network
GW	Gateway
MHz	Megahertz
Cluster	Two or more devices working in failover
PoE	Power over Ethernet
ACL	Access list
NFE	Sub- or recloser station
ETH	Ethernet
GPS	Global Positioning System
LTE	4G Mobile connection
DHCP	Dynamic Host Configuration Protocol
NAT	Network Address Translation
DNS	Domain Name System
NTP	Network Time Protocol

VRRP Virtual Router Redundancy Protocol

APN Access Point Name

VLAN Virtual Local Area Network

DMZ Demilitarized zone

1 Introduction

NDC Networks Oy got a new customer and they needed designing and implementing a secure” no-single-point-of-failure” mobile network, which was designed for power distribution environment.

Their old network consists of NFE stations, which are connected via serial cable to radio modems. This means there is no secure connections besides physical security.

The growth of the security threats means, that the customer needs modern network solution with point-to-point encrypted traffic.

This means all the connections must be secure and every network device must be working in failover. That is why VPN connections and firewall cluster are the main points of this thesis.

In the first chapters the old network topology with its devices are studied. The new network topology is also introduced, and which devices are chosen for it.

At the end of the project the customer must have working High-Availability firewall connected to mobile network, and monitoring tool which offers real-time vision to our and customer’s maintenance control room.

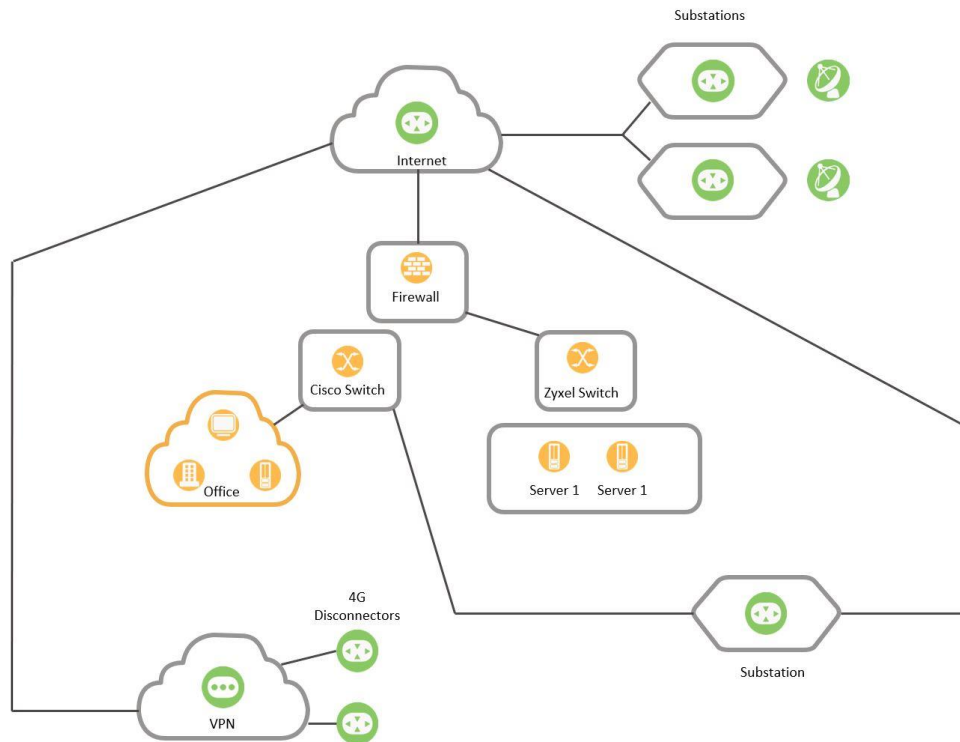
The project was challenging but also very educational. I learned a lot about mobile networks, Checkpoint products and managing medium sized infrastructure project.

Public IP addresses and the customer’s name are changed for security reasons.

2 Network Topology

2.1 Old Network Topology

Investigation of the old network topology started with a meeting with customers where they provided a simplified image of their current network.



Picture 1. Simplified picture of old network topology

The old network topology consists of electrical substations and electrical recloser stations. Most of the substations are connected with fiber and have satellite modem as back up, and all of the recloser stations are connected with radio modems.

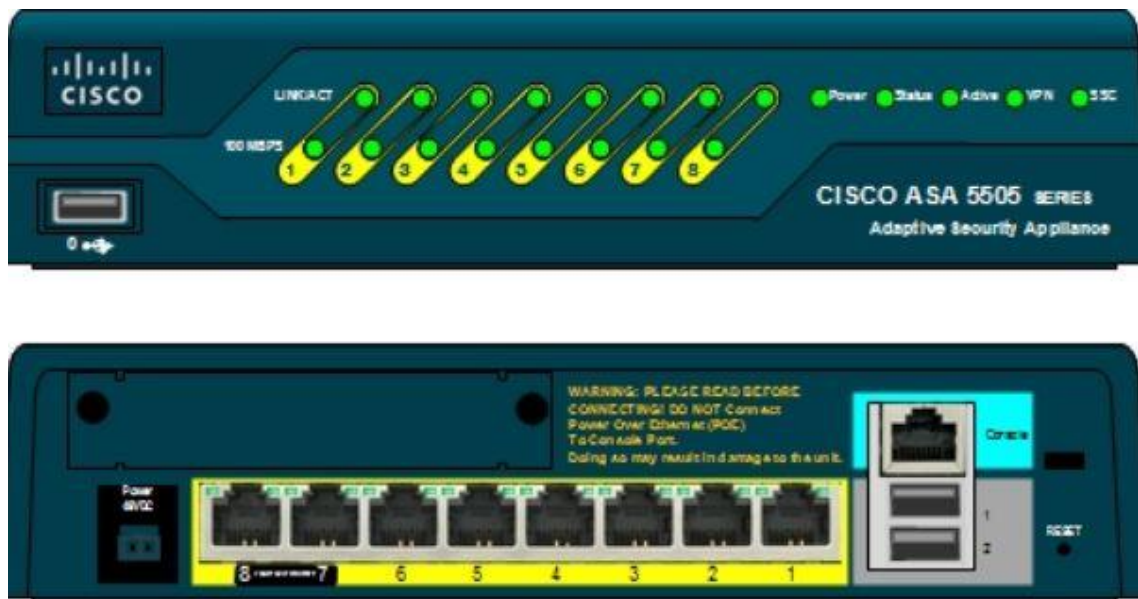
Behind firewall, there is Zyxel switch and in its domain are two servers.

The office network is behind Cisco switch, which is connected to their Cisco ASA firewall.

In the end, most of these network components are getting replaced with new devices, meaning that the most important part of looking the old topology was to figure out firewall rules and which firewall rules were relevant regarding to the new network topology.

2.2 Cisco ASA firewall

Firewall used for the old network topology is Cisco ASA 5505 model.



Picture 2. Cisco ASA 5505 [2]

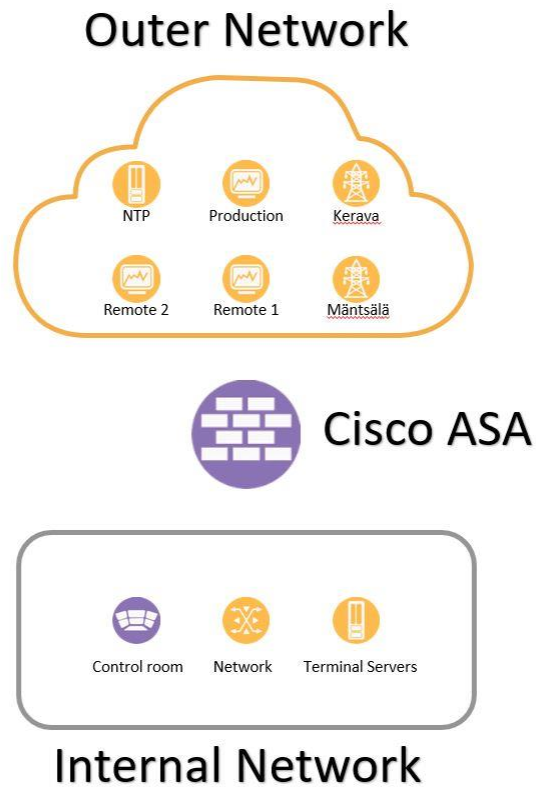
There is routes and firewall rules which need to be integrated to a new High-Availability firewall cluster. VPN rules were not so important since the purpose was to build new VPN certificates with the new firewall. The necessity of the existing VPN connections would be discussed with client.

For ASA, Cisco has its own VPN Client that must be used for connection.

However, the customer could not provide working VPN client, but they did provide Cisco ASA's configuration file. This was not ideal solution since the configuration file could have been changed after exporting the configuration file from the firewall, meaning that was not the real time vision of the ASA's configuration. Solution for this was that the customer would establish real time connection to ASA and recover the current configuration from the firewall.

Cisco ASA's configuration would result in a decision, that would it be more practical to migrate ASA's configuration to Checkpoint firewall, or just to build that configuration to new firewall from scratch.

Inspection of the configuration started with figuring out the ACL's and after those moving to NAT rules. Below picture is drawn after a quick look of the ASA's configuration.



Picture 2 Simplified picture of the firewall's point of view

ASA's configuration had under 10 networks and 33 ACL rules, so it would be more easier and more fail proof to do the configuration from scratch than migrating the configuration to Checkpoint firewall.

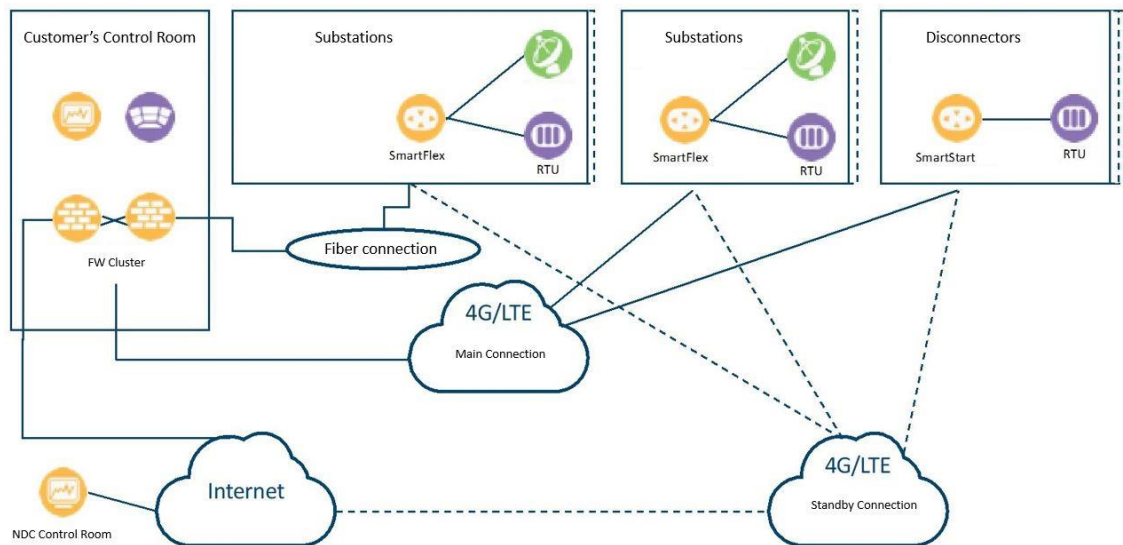
2.3 New Network Topology

The offered system solution combines the commercial 3G / 4G mobile operator's networks, the existing telecommunications network and the new elements are high-availability firewall, network and mobile routing equipment and software.

Encrypted traffic will be used between routers, firewalls and monitoring server. This is implemented with Site-to-Site VPN.

The network solution is based on four each other supportive systems:

1. The customer's main connectivity is existing fiber network which connects the main substations. The first back up connection for the fiber connected stations is mobile routers
2. Mobile network built with mobile routers, in which recloser stations main- and backup connections are construct
3. Some of the substations use satellites as back up connection.
4. VPN IPsec tunnels are configured for the real-time vision maintenance control.



Picture 3. Simplified New Network Topology

2.4 IP Addressing

The new topology started with designing new private IP-Addressing for the network.

The idea was to have six addresses reserved for each substation and recloser station so most reasonable decision was to use /29 mask.

Real-time plan is to have addresses for 40 electrical recloser stations and 9 substations. For future growth, allocated addresses were 10.110.10.x to 10.110.11.x with a /29 mask to recloser stations, which means there are addresses allocated for 96 recloser stations in total.

For substations, allocated addresses were 10.110.13.x with a /29 mask, which means there are addresses for 32 stations in total.

Cluster IP's and APN IP's are introduced later in this thesis.

2.5 High-Availability Firewall Cluster

For the firewall cluster we chose 2x Checkpoint 3100 Next Generation Threat Prevention Appliance, because of they were familiar from the previous projects. Next Generation firewall is the smallest of Checkpoint's firewalls. It's designed for small to medium sized infrastructure projects.

4x Aruba 2930F 24G 4SFP was chosen for the building of the cluster for the same reasons as the Checkpoint firewalls.

Two Aruba 2930F 24G 4SFP would be placed on the public side of the firewall and two would be placed on the internal side. Internal side Aruba switches would replace the Cisco office switch and the Zyxel switch for the two servers in DMZ.

The cluster would be built in our office premises and tested in the premises before moving to customer's environment. That was because of change of misconfiguration and it would be easier to troubleshoot.

The Checkpoint order includes:

- Checkpoint Rack shelf for dual 3000 gateways 1U 19" in which the firewall cluster is built.

- Checkpoint Smart-1 405 Next Generation Security Management Appliance. This is Checkpoints hardware, there is GUI inside where you can maintenance cluster's policies, gather and index logs of the firewalls and you have visibility of integrated threats. With this comes 19" rack connectors for the installation on the firewall cluster rack.
- Checkpoint Standard Collaborative Enterprise Support, which is Checkpoint's own technical support.

Below pictures shows useful statistics of the Firewall.

Base Configuration
<ul style="list-style-type: none"> • 6 on-board 10/100/1000Base-T RJ-45 ports • 1x CPUs, 4x physical cores, 4x virtual cores (total) • 8 GB memory • 1 power supply • 1x 320GB (HDD) or 1x 240GB (SSD) drive
Power Requirements
<ul style="list-style-type: none"> • Single Power Supply rating: 40W • AC power input: 110-240V, (47-63Hz) • Power consumption maximum: 29.5W • Maximum thermal output: 100.7 BTU/hr.
Dimensions
<ul style="list-style-type: none"> • Enclosure: Desktop • Dimensions(W x D x H): 8.3x8.3x1.65 in. (210x210x41.9mm) • Weight: 2.9 lbs. (1.3 kg)
Environmental Conditions
<ul style="list-style-type: none"> • Operating: 0° to 40°C, humidity 5% to 95% • Storage: -20° to 70°C, humidity 5% to 95% at 60°C
Certifications
<ul style="list-style-type: none"> • Safety: UL, CB, CE, TUV GS • Emissions: FCC, CE, VCCI, RCM/C-Tick • Environmental: RoHS, REACH¹, ISO14001¹

Picture 4. Hardware information [3]

Network Connectivity
<ul style="list-style-type: none"> • Total physical and virtual (VLAN) interfaces per gateway: 1024/4096 (single gateway/with virtual systems) • 802.3ad passive and active link aggregation • Layer 2 (transparent) and Layer 3 (routing) mode
High Availability
<ul style="list-style-type: none"> • Active/Active and Active/Passive - L3 mode • Session failover for routing change, device and link failure • ClusterXL or VRRP

Picture 5. Network information [3]

2.6 Mobile routers

B+B SmartWorx mobile routers were chosen for this project. They were chosen because familiarity from previous projects and their potentiality in developing with software extensions.

40x B+B SmartStart Mobile routers would be used in recloser stations.



Picture 6. SmartStart mobile router. [1]

The internal memory provides ample storage for custom scripts, software applications and a wide variety of protocols. In addition to its Ethernet and RS-232 ports, SmartStart has built-in digital I/O connectivity. Competing routers in the same price range generally provide only Ethernet or RS-232. SmartStart provides all three. [1]

The router supports VPN tunnel creation using various protocols to ensure safe communications. The router provides diagnostic functions which include automatic monitor-

ing of the wireless and wired connections, automatic restart in case of connection losses, and a hardware watchdog that monitors the router status. [1]

SmartStart's provides fall back to 3G/2G technologies to ensure that connectivity is reliable in areas where LTE is still under development. [1]

9x B+B SmartFlex mobile routers would be used in substations.



Picture 7. SmartFlex mobile router [1]

Specifications include wide operating temperature ranges from -40 to +75 °C (-20 to +60 °C LTE450 module). It accepts input voltage ranges from 10 V DC to 60 V DC and is equipped with sleep mode for reducing electrical consumption. [1]

The standard configuration includes 2 Ethernet ports with 2 independent LANs/IP addresses. The standard configuration also includes 1 USB host port, 1 microSD card holder, 2 SIM card holders for automatic failover to an alternate service provider, 2 binary inputs(I/O), 1 binary output (I/O) and onboard GPS. An optional built-in WiFi module is also available, with industrial grade operating temperature ranges from -40 to +75 °C (-20 to +60 °C LTE450 module). Further optional boards available: 3x ETH (the router can be configured with up to 5 total Ethernet ports and 3 independent LANs/IP addresses) or ETH – RS232 – RS485 (isolation strength up to 2.5kV) or RS232 – RS485 (isolation strength up to 2.5kV) or RS232. [1]

The SmartFlex supports real time data encryption and the creation of VPN tunnels using IPsec, OpenVPN and L2TP. It supports DHCP, NAT, NAT-T, DynDNS, NTP,

VRRP, control by SMS, and numerous other functions, as well as additional software like SmartCluster VPN Server and R-SeeNet. [1]

The router provides diagnostic functions which includes automatic monitoring of the wireless and wired connections, automatic restart in case of connection losses, and a hardware watchdog that monitors the router status. [1]

2.7 APN

An Access Point Name is the name of gateway between mobile network and another computer network meaning that the pathways between mobile devices, the mobile data networks and the internet are defined by Access Point Names.

Customer had two choices to choose from: Public APN or Private APN.

2.7.1 Public APN

Public APNs are designed to provide basic internet access for the most commonly used apps and websites. It basically utilizes common carrier APNs (the same as you would see on a phone or tablet SIM) to give a device access to the public Internet to send and receive data. The IP address of the SIM is hidden behind the networks fire-wall, so the device can't be addressed directly across the public internet, which means all devices with this setup need to initiate a communication session with the host service/client.

Public APN is more cheaper and easier to set up, but since the data is sent across the public internet the information security question comes in hand.

There would also be option to select dynamic APN but that is not a viable option since the IP's of the device's must be static.

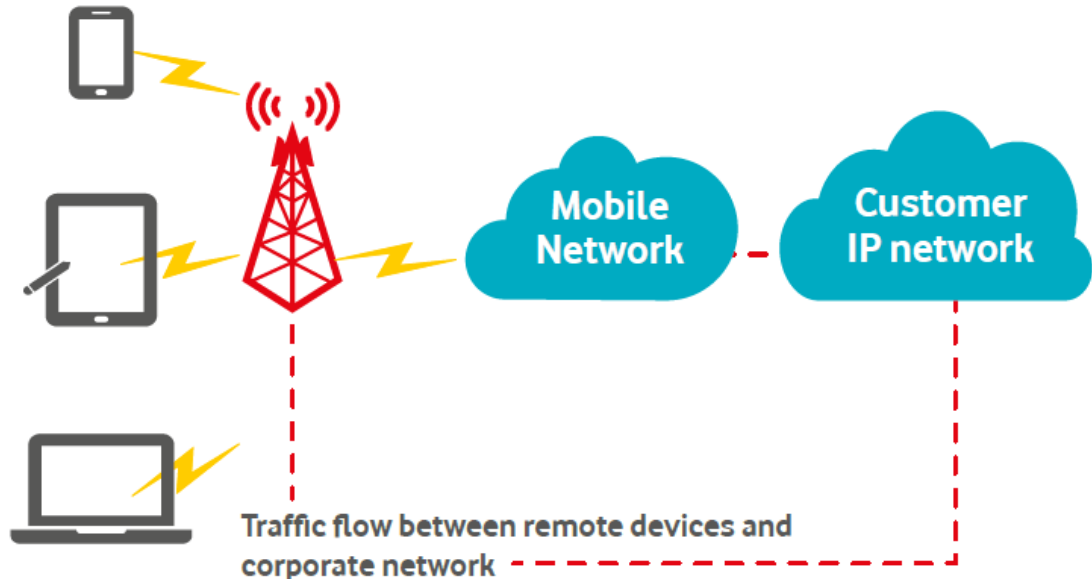
2.7.2 Private APN

Private APN's route mobile data traffic from mobile devices directly into organisation's network. This means these devices do not share public data pathways and are more secure than Public APNs.

Getting information from mobile devices to back-end systems is more stable, improving the end user experience. Particularly when using real time applications.

Specific IP addresses can be assigned to SIM cards, so devices can be uniquely identified. Very useful to account for certain assets, machines, applications, or people.

The problem is that these IP addresses exist in a private space meaning they cannot be accessed from the "outside world" this makes them extremely secure but means that you need a method of getting in to the private IP space. This is typically achieved through a VPN tunnel but can also be done on a peer-to-peer level by using a centrally allocated router configured on that IP space to talk to all other devices in the field. [7]



Picture 8. Private APN [4]

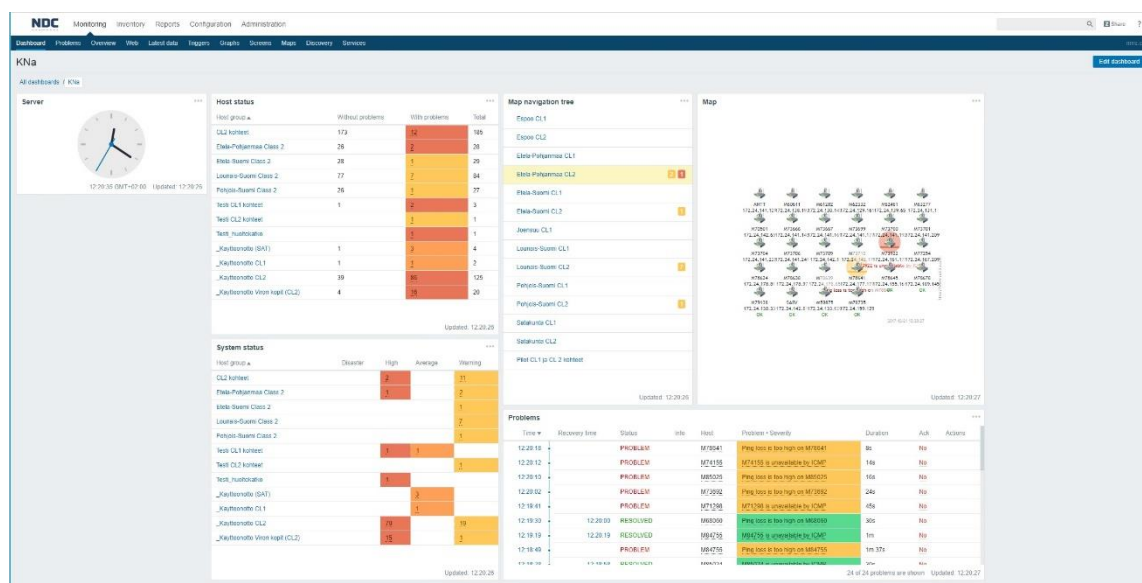
At the end of the APN discussions, the customer decided to go with the Public APN. That was because it was more cost effective, and more easier and cheaper to set up for their size of network infrastructure.

If the security comes more of a concern to customer, it is possible to change from public APN to private one. However, the project continued by ordering APN from operator provider. This would take couple weeks to set up and receive the SIM cards.

2.8 Network Monitoring

The Network Monitoring is handled with open source monitoring software called Zabbix.

Zabbix monitors devices connected to network and saves information of monitored hardware to its database and shows real-time information via SNMP.



Picture 9. Example vision of Zabbix

The server communicates to the native software agents that are available for many operating systems, including Linux, UNIX and Windows. [8]

Zabbix is software that monitors numerous parameters of a network and the health and integrity of servers. Zabbix uses a flexible notification mechanism that allows users to configure e-mail-based alerts for virtually any event. This allows a fast reaction to serv-

er problems. Zabbix offers excellent reporting and data visualisation features based on the stored data. This makes Zabbix ideal for capacity planning. [8]

Zabbix supports both polling and trapping. All Zabbix reports and statistics, as well as configuration parameters, are accessed through a web-based frontend. A web-based frontend ensures that the status of your network and the health of your servers can be assessed from any location. Properly configured, Zabbix can play an important role in monitoring IT infrastructure. This is equally true for small organisations with a few servers and for large companies with a multitude of servers. [8]

Zabbix is free of cost. Zabbix is written and distributed under the GPL General Public License version 2. It means that its source code is freely distributed and available for the general public. [8]

3 Configuration

3.1 Building the Cluster

The idea was to build firewall cluster to test environment, before building it in customer's environment. There are two firewalls that are connected to each other and to all four switches. The switches are placed on internal side and public side of the network. Public side switches are connected to each other with trunk link. Trunk link would also be used with internal side switches.

The management server would be connected to firewall and it had to be working as a cluster link.

This chapter shows the steps of building the cluster, which includes putting the hardware together and connecting them with RJ45 cables.



Picture 10. Arrived packages

Packages arrived in office at the same time, which made it easy to start putting the pieces together.

Four HP Aruba 24 port switches. Two would be connected to the public side of the firewall and two would be connected to the internal network. There would also be trunk link between public and internal network switches.



Picture 11. 24-port HP Aruba switch

Two Checkpoint firewalls. They would be connected to each other and to the four Aruba Switches.



Picture 12. Checkpoint firewall

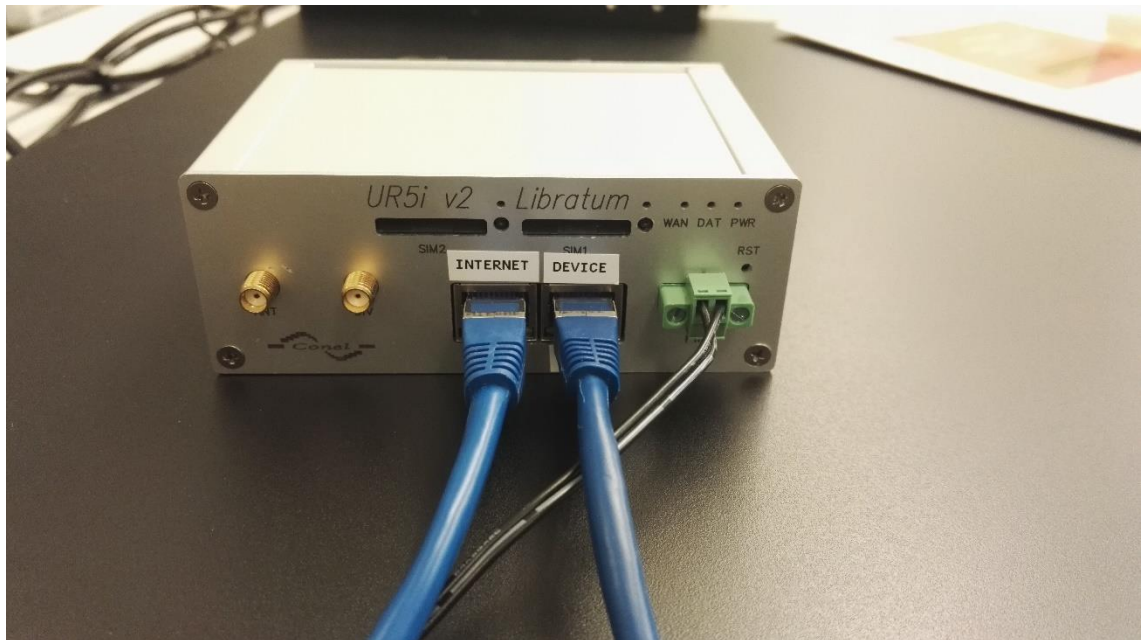
The Checkpoint management appliance would be connected to switches and from switches to firewalls. These links are used for managing and monitoring cluster's security and policies



Picture 13. Checkpoint Management System

The customer's network would be simulated in test environment with Conel's UR5i v2L router.

One of the ethernet ports would be working with the same IP as customer's internet gateway. The other port would be working as a DHCP client and be connected to our office's router for internet access. The internet gateway port was connected to one of the public side switches. Static route from the cluster's internal network to the internet gateway address had to be configured for internet access. Internet access for test environment would also be used to download critical updates to Firewalls.



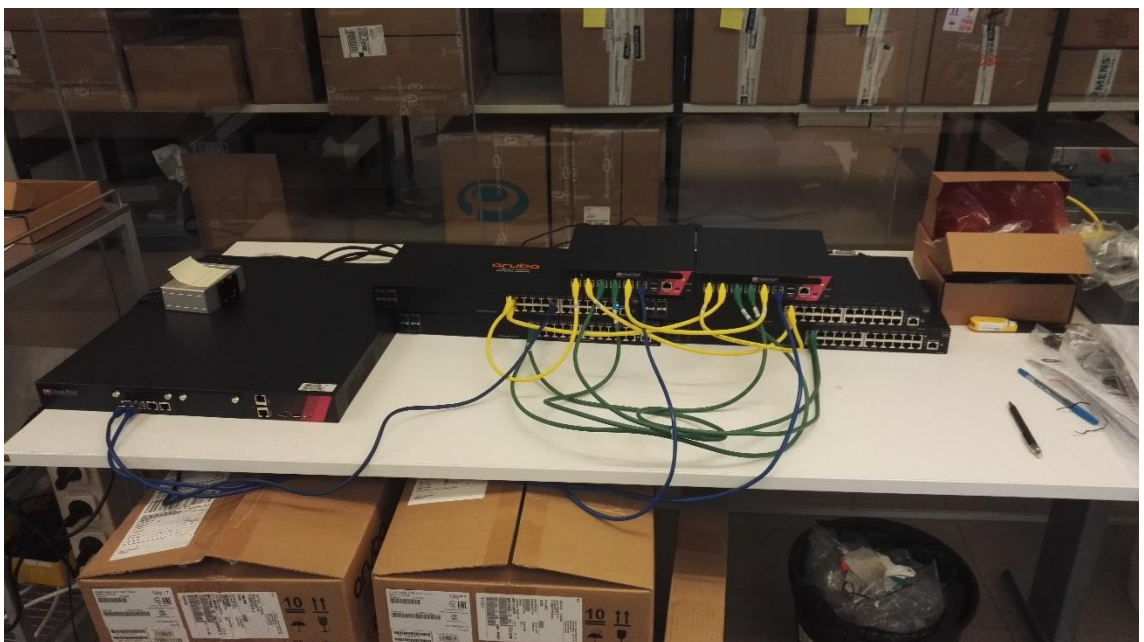
Picture 14. UR5i V2L router

Firewalls were placed on top. The internal switches are below the public internet switches. The management server appliance is placed on the left.



Picture 13. Setting up hardware

The devices are connected with Cat6 cable. Green cables represent internal network and yellow ones the public network.



Picture 15. Connected Firewall Cluster

3.2 Configuring the Cluster

The configuration started with configuring each device individually.

The Firewalls and Management Appliance Server configuration had a configuration Wizard where you input all the basic information. In the wizard you chose SIC key for the device. The devices were securely connected to Management server with this key. After the basic configuration in wizard, including admin user name and password, were configured, the device's IP's and ports were configured.

Secure Internal Communication (SIC)

Activation Key: !

Confirm Activation Key:

▼ [Learn more about SIC](#)

SIC - Secure Internal Communication, provides secure communication between Check Point distributed components that belong to a single management domain, or to a Multi-Domain Security Management system. For example, between a Gateway and its management server (Security Management Server or Multi-Domain Management Server). In order to have Secure Internal Communication between two Check Point distributed components, you must enter an Activation Key.

NOTE: You must initialize or re-initialized SIC on the two Check Point distributed components. This can be done via SmartConsole or SmartProvisioning, by editing the object of the component with which you are setting up SIC, and entering the Activation Key that you specified on this page.

Picture 16. Secure Internal Communications

The firewalls would have different IP Addresses but otherwise they must be identical.

Address 192.168.2.11 was chosen for the management port in the firewall 1, 192.168.2.12 for the firewall 2 and 192.168.2.1 for the management appliance server.

Ports 1-2 would be bonded together and named as bond1 meaning that they are tied as one port. In Cisco systems this setting is called EtherChannel. Address for the

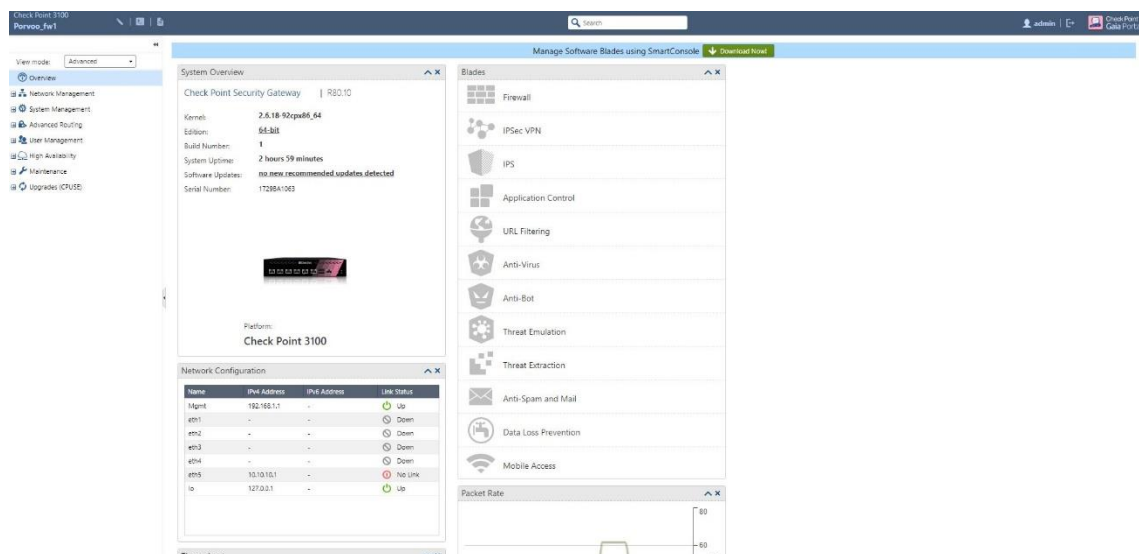
bond1 in the firewall 1 was 200.100.100.1 and 200.100.100.2 for firewall 2. They would be connected to the public side switches.

Ports 3-4 would be configured as bond2. Selected address for the firewall 1 was 10.104.1.2 and 10.104.1.3 for the firewall 2. The bond2 interfaces were connected to internal side switches.

The last ports of the firewalls were connected to each other as cluster sync link and the addresses for these were 10.10.10.1 for the firewall 1 and 10.10.10.2 for the firewall 2.

Ports 1 and 2 were configured in the management appliance server as bond and address 192.168.2.1 was chosen for it.

After configuring the devices individually, they would be connected to the management appliance server. The purpose of the management server was to manage both firewalls, meaning that the cluster itself would be configured in management server. Policies and NAT rules would also be distributed from the management server.



Picture 17. Firewall Interface

The setup from management server started by adding the firewalls one by one to the server. The adding was easy and was done with wizard. Trusted connection between firewalls and the server was established with previously configured SIC key.

When both firewalls were connected to the server with trusted connection, policy rule had to be configured to accept traffic from management server to the firewalls. Otherwise the connection would be lost when configuring cluster and installing other policies.

Before creating the cluster, the Aruba switches had to be configured with basic settings. The Default Vlan had to be configured with an IP Address, meaning that the switches could be accessed via GUI. First connection to switches was made with console cable using Putty.

On public side switches, VLAN 10 was used as public access VLAN and VLAN 20 was used as management VLAN. Internal side switches used the same VLANS except VLAN 10 was used as internal Access VLAN. Public switches were connected to each other at port 24 and that was configured as tagged port. The same tagged configuration was done in internal side switches.

On public switch 1, port 1 was connected to Internet GW and ports 2 and 3 was connected to firewalls. Ports 13 and 14 were used as management ports. Port 13 was connected to management server and port 14 was connected to firewall 1.

The same connections would be used on public switch 2, except different destination ports.

The idea after all the basic configuration was done, was to create VPN tunnel between the cluster and client. This was done because when the cluster is installed on the premises with the basic configuration, it could be managed with VPN connection and the rest of the configuration would be added remotely.

There were two VPN protocol options to choose from: Web client, working with SSL and IPSec protocol, in which you needed Checkpoint VPN Client to connect.


The VPN connection was created with SSL first, but after configuring and establishing connection with the Web Client there was only options to use applications which were added and configured in the management server. This was not useful, since you needed a local connection to devices, and web client did not offer that.

After the SSL VPN was dropped from use, the IPSec tunnel was created. In the IPSec configuration you had to give the VPN a DHCP Pool, in which the addresses to clients was decided and distributed. Address 192.168.3.0/24 was chosen for this use.

Making the VPN connection was successful after initial configuration but accessing the Management network failed. With a tight schedule, there was no time to finish this configuration and it had to be done later at the on-site installation.

3.3 Testing HA functionality

After the firewalls were added to management server and joint together as cluster, HA functionality had to be tested. This means if the cluster was working properly, shutting down the active firewall would change the standby firewall as active without too many ping losses. Before starting the test, the firewall 1 was working as active firewall.



_FW1




IP Address: 192.168.2.11

Version: R80.10

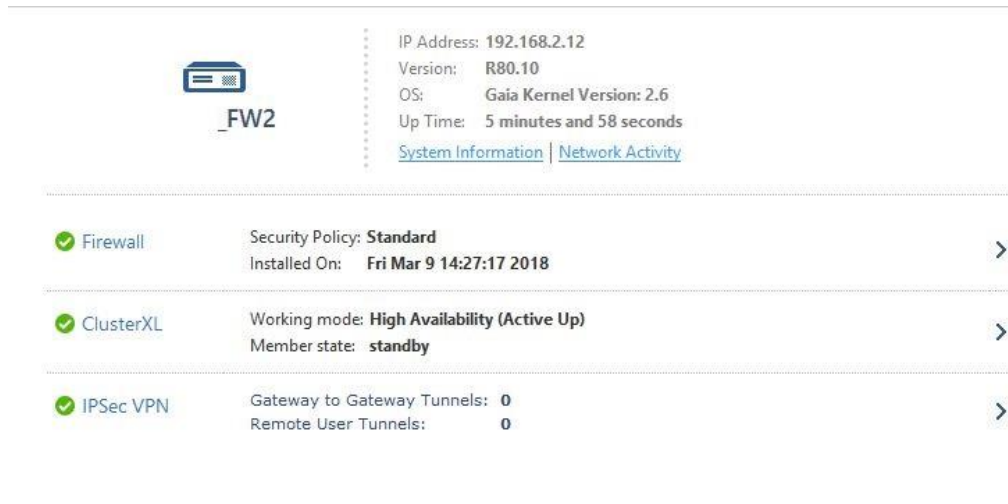
OS: Gaia Kernel Version: 2.6

Up Time: 9 minutes and 46 seconds

[System Information](#) | [Network Activity](#)

 Firewall	Security Policy: Standard Installed On: Fri Mar 9 14:23:13 2018	>
 ClusterXL	Working mode: High Availability (Active Up) Member state: active	>
 IPSec VPN	Gateway to Gateway Tunnels: 0 Remote User Tunnels: 0	>

Picture 18. Active Firewall



Picture 19. Standby Firewall

The firewall 2 was working as a standby firewall.

For the testing purposes, laptop was configured to the same network as the cluster's internal network, which was 10.104.1.0/24. The laptop was then connected to internal switches port. To test the internet connection, ping to Google's DNS server was established. After everything was set up, the active firewall was turned off.

The test was successful, because there was only one ping loss and the firewall 2 was chosen as active cluster member.

```

Command Prompt
Reply from 8.8.8.8: bytes=32 time=41ms TTL=53
Reply from 8.8.8.8: bytes=32 time=44ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=40ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=41ms TTL=53
Reply from 8.8.8.8: bytes=32 time=43ms TTL=53
Reply from 8.8.8.8: bytes=32 time=47ms TTL=53
Reply from 8.8.8.8: bytes=32 time=42ms TTL=53
Reply from 8.8.8.8: bytes=32 time=44ms TTL=53
Reply from 8.8.8.8: bytes=32 time=41ms TTL=53
Reply from 8.8.8.8: bytes=32 time=42ms TTL=53
Reply from 8.8.8.8: bytes=32 time=45ms TTL=53
Reply from 8.8.8.8: bytes=32 time=40ms TTL=53
Reply from 8.8.8.8: bytes=32 time=41ms TTL=53
Reply from 8.8.8.8: bytes=32 time=44ms TTL=53
Reply from 8.8.8.8: bytes=32 time=43ms TTL=53
Reply from 8.8.8.8: bytes=32 time=44ms TTL=53
Reply from 8.8.8.8: bytes=32 time=43ms TTL=53
Reply from 8.8.8.8: bytes=32 time=44ms TTL=53
Reply from 8.8.8.8: bytes=32 time=31ms TTL=53
Reply from 8.8.8.8: bytes=32 time=41ms TTL=53
Reply from 8.8.8.8: bytes=32 time=42ms TTL=53
Request timed out.
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=44ms TTL=53
Reply from 8.8.8.8: bytes=32 time=45ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=41ms TTL=53
Reply from 8.8.8.8: bytes=32 time=41ms TTL=53
Reply from 8.8.8.8: bytes=32 time=46ms TTL=53
Reply from 8.8.8.8: bytes=32 time=45ms TTL=53

```

Picture 20. Ping test

The test was repeated successfully, with connecting the laptop to a port in the second Internal Switch and turning off the firewall 2 after the firewall 1 had returned the connectivity.

More crucial and real time scenario tests would be implemented at the commissioning tests.

3.4 Mobile Routers

The configuration file of the mobile routers would contain changing values of IP addresses and IPSec settings, but otherwise the parameters would remain same on all the routers. The configuration itself started with exporting the .cfg file from router, that would be used as a template file.

The configurations were configured with python script that had two variables configured in the script: IP address and network address.

The script uses the template configuration file that is saved in .txt form. It performs simple find and replace function and saves the new values in a new configuration file.

```
#!/usr/bin/env python3

def replace_words(testi, device_values):
    for key, val in device_values.items():
        testi = testi.replace(key, val)
    return testi

# Create empty dictionary and input the values

device = {}

device["$hostname"] = input("\nHostname: ")
device["$network"] = input("\nIP Address: ")

# Open the text file and read the lines
```

```
t = open('config_file.txt', 'r')
tempstr = t.read()
t.close()

# Replacing the values

output = replace_words(tempstr, device)

# Making new config file

fout = open('newcfg.cfg', 'w')
fout.write(output)
fout.close()
```

The original idea was to create script, that would create the config file and input the certificates. However, the lack of coding knowledge resulted in two separate scripts, one that would create the configuration file and one that would input the certificates to the created configuration file.

The certification script will be introduced later in this thesis.

4 On-Site Configuration

On-Site configuration was done in a customer's data center. The installation started with connecting the 19" rack connectors to the devices and attaching the devices to data center's rack.

After the devices were attached to the rack, RJ45 cables were connected the same way that they were in test environment. There were few adjustments in Aruba Switches regarding Default VLAN. One of the switches had two Default VLAN addresses and neither of them was working properly.

The solution for this was to connect to switch with serial cable and clearing the Default VLAN and configuring it with proper IP Address.

After the configuration changes in the Switch, the Cluster was working properly, and it had a connection to internet. The connection to internet was established by connecting the public switch to the operators switch, which was already set up and running at the data center.



Picture 21. Finished Cluster installation.

However, issues appeared when finishing up the VPN configuration. Like in the test environment, the remote network did not reach the management network, which was a issue since remote configuration would not be possible this way.

The problem could not be solved at the site, so TeamViewer session would be hosted at data center for remote access, to troubleshoot the VPN connection.

The problem was solved later by forcing all the VPN traffic through security gateway, which was the cluster in this case, and adding NAT with translation method of hiding remote traffic behind a gateway.

Security Gateway acts as a VPN router for the Remote Access client. All connections opened by the client, either to the internal network or to the Internet, pass through the Security Gateway. The packets are encrypted between the client and the Security Gateway and are then forwarded to the destination. If the destination is external, the traffic between the Security Gateway and the destination will be forwarded in clear. The feature also allows for forwarding VPN traffic to destinations in other VPN Sites, or to other clients currently connected to this Security Gateway. [5]

4.1 Zabbix

The idea was to create Zabbix working in a Linux server. The solution for this was to create Debian operating system on an Amazon cloud hosting service.

After the Debian was set up, pem key had to be created at Amazon for ssh connection. This was done simply by creating the key pair, naming it, and downloading it from Amazon. After downloading it, the permissions of the .pem file had to be changed to read mode only by basic chmod command.

```
chmod 400 my-key-pair.pem
```

Putty was used to connect to the Zabbix server with the newly created. pem key. The idea was to install and create Zabbix server with working database and frontend, after successful ssh connection.

```
# wget http://repo.zabbix.com/zabbix/3.4/debian/pool/main/z/zabbix-  
release/zabbix-release_3.4-1+stretch_all.deb  
# dpkg -i zabbix-release_3.4-1+stretch_all.deb  
# apt-get update
```

After the Zabbix service install, MySQL had to be installed, and database with PHP frontend had to be configured.

Installing MySQL server and PHP frontend.

```
# apt-get install zabbix-server-mysql
```



```
# apt-get install zabbix-frontend-php
```

Importing initial schema and data for the server.

```
# zcat /usr/share/doc/zabbix-server-mysql/create.sql.gz | mysql -uzabbix -  
p Zabbix
```

Editing the Zabbix database file.

```
# vi /etc/zabbix/zabbix_server.conf  
DBHost=localhost  
DBName=zabbix  
DBUser=zabbix  
DBPassword=<password>
```

After the Zabbix installation and database configuration server had to be started for the frontend and Zabbix agent installation.

```
# service zabbix-server start  
# update-rc.d zabbix-server enable
```

Starting web server and configuring Apache settings for Zabbix frontend.

```
# service apache2 restart  
  
php_value max_execution_time 300  
php_value memory_limit 128M  
php_value post_max_size 16M  
php_value upload_max_filesize 2M  
php_value max_input_time 300  
php_value always_populate_raw_post_data -1  
# php_value date.timezone Europe/Helsinki
```

Installing and starting Zabbix agent.

```
# apt-get install zabbix-agent
```

```
# service zabbix-agent start
```

IPSec VPN tunnel between Zabbix and firewall cluster had to be done next. It was implemented with strongSwan. StrongSwan is an open-source IPSec solution for Linux.

Installing the strongSwan on Zabbix server.

```
# apt-get install strongswan
```

Editing the ipsec. conf file with the right encryption suite. Also, outside address and addresses behind strongSwan had to be configured.

```
# vim ipsec. conf
```

```
conn %default
ikelifetime=480m
keylife=60m
rekeymargin=3m
keyingtries=1
keyexchange=ikev1
authby=secret

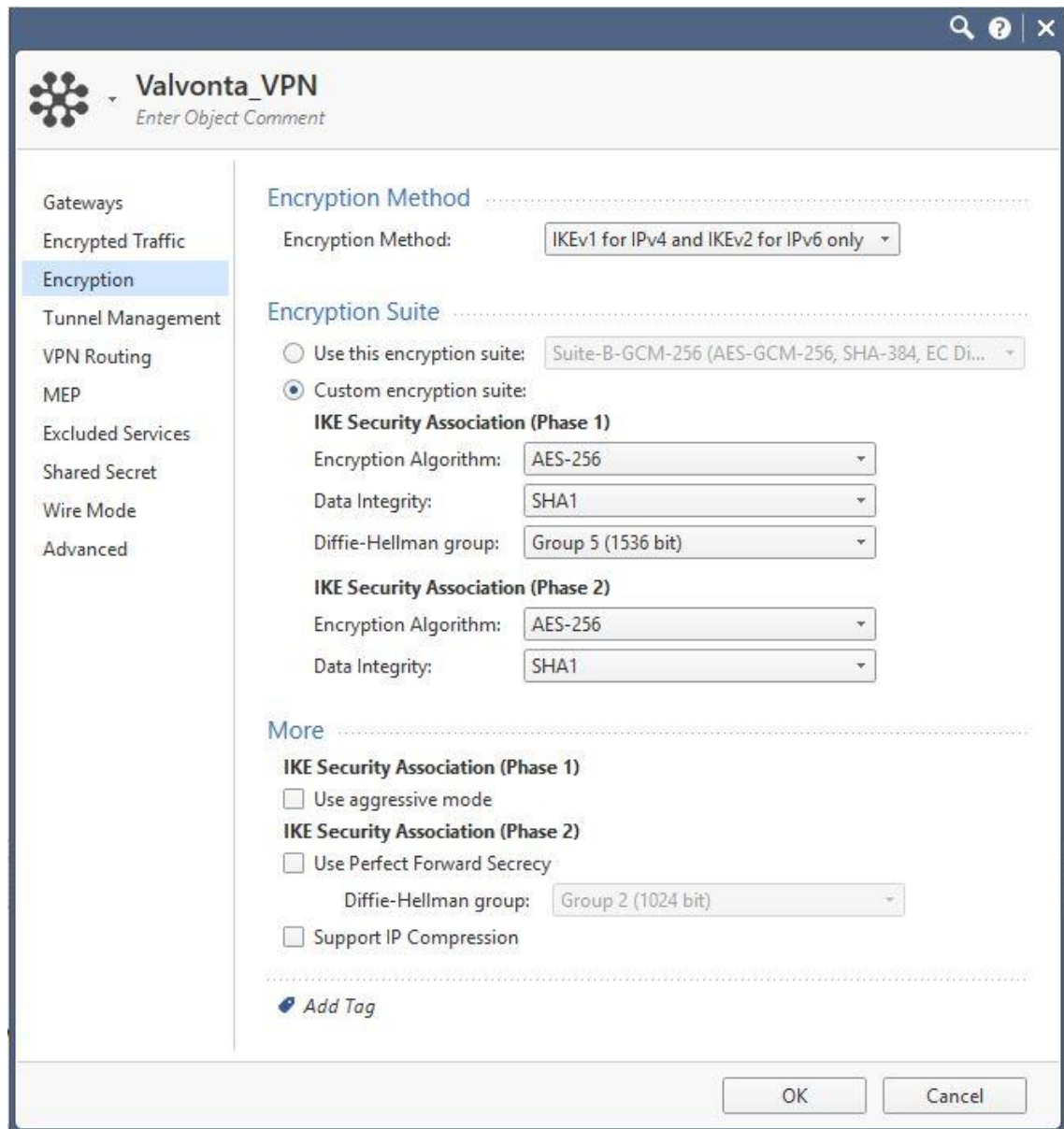
conn psv-vpn
lef=%any
#strongswan outside address
leftsubnet=172.31.24.220/32

#network behind strongswan
leftid=100.10.10.1
leftfirewall=yes
right=200.10.10.1
rightsubnet=192.168.2.0/24rightid=200.10.10.1
auto=start
ike=aes256-sha1-modp1536      #P1: modp1536 = DH group 5
esp=aes256-sha1             #P2
installpolicy=yes

include /var/lib/strongswan/ipsec.conf.inc
include /etc/ipsec.d/*.conf
```

After the strongswan IPSec configuration, the same encryption suite would be configured on cluster firewall's VPN community.

The community was configured as start topology and the Zabbix side would be chosen as satellite gateway and firewall cluster as center gateway.



Picture 22. Monitoring Encryption Suite

When the VPN configuration was done on both ends, the tunnel's status was checked in Zabbix server.

```
root@ip-172-31-14-220:/etc# ipsec status
```

```
Security Associations (1 up, 0 connecting):
psv-vpn[1]:      ESTABLISHED    6      seconds      ago,
172.31.14.220[100.10.10.1]...200.10.10.1[200.10.10.1]
```

```
psv-vpn{1}:  INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs:
c8d151e3_i eed57c3c_o
psv-vpn{1}:  172.31.24.220/32 ==> 192.168.2.0/24
```

4.2 Finishing Cluster Policies

The initial policies were already installed for the firewall cluster. However, before the commissioning tests, all the policies had to be configured for full functionality and security.

There were 35 policy rules total, but some of them were most likely unnecessary. Removing the unnecessary rules had to be done with customer, meaning that the policies would be explained to them one by one, and the decision if the rule would be used in the new topology or not, was decided together in agreement.

The rules were organized in layers. For example, one for system rules and one for VPN rules. The first three layers were disabled before the discussion with customer, since they were not necessary for the cluster's functionality.

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
Outside_access_in (1-5)								
1		Interface_outside	* Any	* Any	* Any	Accept	Log	* Policy Targets
2		* Any	Interface_outside_address	* Any	UDP_6781	Accept	Log	* Policy Targets
3		* Any	udp-server	* Any	UDP_6781	Accept	Log	* Policy Targets
4		Empower_prod_servers	DomainControllers	* Any	echo-request https UDP_4767	Accept	Log	* Policy Targets
5		Sub-policy cleanup rule	* Any	* Any	* Any	Drop	Log	* Policy Targets
Inside_access_in (6-18)								
6		Interface_inside	* Any	* Any	* Any	Accept	Log	* Policy Targets
7		DomainControllers	xpowerServers	* Any	echo-request TCP_6997	Accept	Log	* Policy Targets
8		DomainControllers	Empower_prod_servers	* Any	TCP_6997 echo-request TCP_6997	Accept	Log	* Policy Targets
9		network_10.104.1.0_24	NetconRemote-net	* Any	* Any	Accept	Log	* Policy Targets
10		network_10.104.1.0_24	* Any	* Any	* Any	Accept	Log	* Policy Targets
11		TerminalServers	PSVRemote-net	* Any	Remote_Desktop_P	Accept	Log	* Policy Targets
12		iOS	NetControl-ScreenHost	* Any	echo-request http https	Accept	Log	* Policy Targets
13		DomainControllers	time.nist.gov	* Any	ntp-udp	Accept	Log	* Policy Targets
14		DomainControllers	* Any	* Any	domain-udp	Accept	Log	* Policy Targets
15		network_10.104.1.0_24	host_192.194.255.68	* Any	https	Accept	Log	* Policy Targets
16		host_10.104.1.6	host_192.194.255.67	* Any	UDP_4767	Accept	Log	* Policy Targets
17		network_10.104.1.0_24	* Any	* Any	* Any	Drop	Log	* Policy Targets
18		Sub-policy cleanup rule	* Any	* Any	* Any	Drop	None	* Policy Targets
xpower servers (19-22)								
19		Interface_xpower	* Any	* Any	* Any	Accept	Log	* Policy Targets
20		xpowerServers	DomainControllers	* Any	echo-request TCP_6997	Accept	Log	* Policy Targets
21		network_192.168.200.0_24	* Any	* Any	* Any	Drop	Log	* Policy Targets
22		Sub-policy cleanup rule	* Any	* Any	* Any	Drop	None	* Policy Targets
System Rules (23-30)								
VPN Rules (31-34)								
31	Zabbix VPN	* Any	* Any	NDC_valonta_VPN	* Any	Accept	Log	* Policy Targets
32	Router VPN	Internal Network	PSV_10.110.10.192	PSV_Routers_VPN	iee_104_tcp_2404	Accept	Log	* Policy Targets
33	Router VPN	Internal Network	PSV_10.110.10.192	PSV_Routers_VPN	icmp-proto	Accept	Log	* Policy Targets
34		* Any	* Any	RemoteAccess	* Any	Accept	Log	* Policy Targets
Cleanup Rule (35)								
35	Cleanup rule	* Any	* Any	* Any	* Any	Drop	Log	* Policy Targets

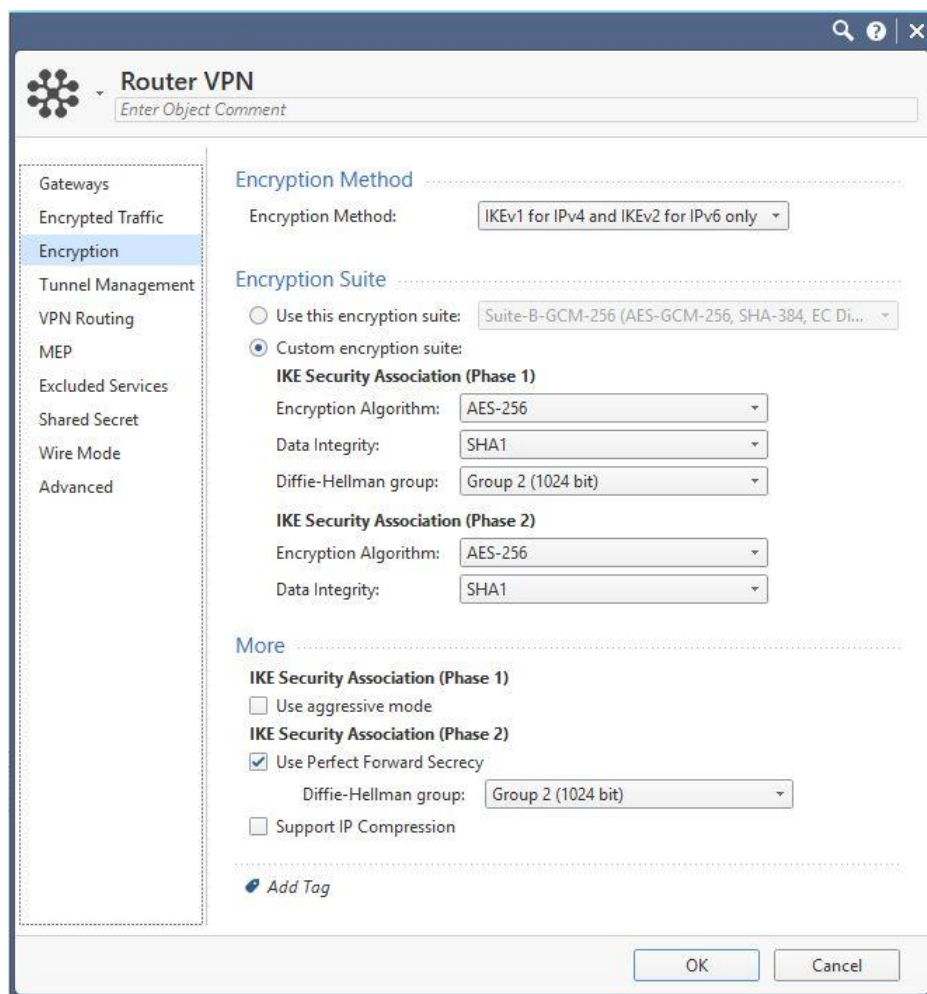
Picture 23. Policy Rules

4.3 Mobile Routers IPsec VPN

Configuring the VPN connection between mobile routers and firewall cluster was important for secure mobile traffic. Without the VPN, the data would be decrypted, which means it would be easier to eavesdrop and used for malicious intentions.

The protocol for the VPN connection was IPsec because of the Checkpoints easy ability to create and manage VPN communities and connections.

Following encryption suite was used for connection between firewall and routers.



Picture 24. Encryption Suite

The Mobile Routers would be created in the Management server as interoperable devices and added to the VPN Community. They would be working with dynamic addresses.

After creating the VPN community and the first router on the firewall, the certificates had to be created. This was done with management server's CLI with following script:

```
#!/bin/bash
#Script for making .p12 file

echo Write devices serial number:
read serial
cpca_client create_cert -n $serial -f $serial.p12 -k IKE -w password
echo Certification done!
```

The idea was to create .p12 file with the router's serial number. After that, the file would be transferred to the Zabbix server with SCP, where the public key and private key file would be exported with shell script:

```
#!/bin/bash

Read -p "Insert Router's Serial : " serial

openssl pkcs12 -in $serial.p12 -nokeys -password pass:password >$serial.crt
openssl pkcs12 -in $serial.p12 -nocerts -nodes -password pass:password
| openssl rsa >$serial.key

csplit -f tempcert- $serial.crt '/-----BEGIN CERTIFICATE-----/' '{*}'
cat tempcert-01|awk 'split_after==1{n++;split_after=0} /-----END CERTIFICATE-----/ {split_after=1} {print > "tempcert" n ".pem"}'

mv tempcert.pem $serial.crt
rm -f tempcert*
```

The script first asks router's serial number and after that it creates the .crt file and .key file. It then splits the certificate itself from .crt file by creating a new file called tempcert.pem and moving it back to .crt file.

The certificates could not be imported to the configuration file on their original form. The solution for this was to convert the original files to base64 form with a simple shell script:

```
#!/bin/bash
#Changes cert and key file to b64

echo Give Serial Number
read serial

base64 $serial.crt >$serial.b64.crt
base64 $serial.key >$serial.b64.key
```

Establishing VPN connection will not work without CA, meaning it would have to be imported from the management server. The certificate was imported from the server with Checkpoint's ICA management tool.

The management tool was not accessible by default, so it had to be enabled first from the CLI:

```
[Expert@HostName]# cpa_client [-d] set_mgmt_tool on [-a "administrator DN" | -u "user DN"]
```

Checking if the tool is using SSL for safety reasons:

```
[Expert@HostName]# cpa_client set_mgmt_tool print
Using SSL
```

Certificates would then be created and imported to browser for encrypted connection.

After importing the certificate to the browser, the ICA management tool was accessed over https using port 18265:

```
https://192.168.2.1:18265
```

The CA certificate would then be downloaded from the website. It would also be changed to base64 form, but it had only be done once, since it would remain the same on all router configurations.

4.4 Operator's APN

The Operator delivered their own APN router to the data center. The APN would be connected to the internal side switch by the client. It would be configured working as a HA in commissioning tests.

The APN router had interface to the firewall's side configured with IP 192.168.4.1/29. Firewall's end had to be configured with new VLAN with address 192.168.4.2/29. The VLAN would also be configured in all Aruba switches.

The APN network was 10.100.100.0/24. In firewall, route to the mobile routers had to be configured with this network for working connection.

The purpose was to have the existing VPN connection between mobile routers and firewall cluster travel through APN network. This would be established by changing the IPSec configuration on mobile routers end to travel through APN router. This means that the IPSec destination address would be changed to 192.168.4.2.

Also, the firewall's end had to be modified with minor changes to previously mentioned interoperable device. This means slight changes to the device's topology.

4.5 Site-to-Site connections

Establishing Site-to-Site connection from Zabbix to mobile routers was the last step to validate the functionality of the network. This means all the traffic from mobile router would travel to firewall and Zabbix through operator's APN.

SNMP templates were imported to Zabbix to monitor different values of the mobile routers.

Zabbix would trigger an alarm if the router does not respond to ping, has high ping response time or high ping loss. More templates would be added later when needed.

Also, basic SNMP templates would be added to monitor the state of Zabbix server and the state of the firewall cluster.

<input type="checkbox"/>	Severity	Name ▲
<input type="checkbox"/>	Warning	High ICMP ping loss
<input type="checkbox"/>	Warning	High ICMP ping response time Depends on: Template Mobiilireititin ICMP Ping: High ICMP ping loss
<input type="checkbox"/>	High	Unavailable by ICMP Ping (mobiilireititin)

Picture 25. First SNMP templates

The mobile router's IPsec was configured with 0.0.0.0/0 network, so it would be easier to set up in the firewall's end.

Only two policies would be needed in the firewall: ICMP protocol and IEC 104 protocol, which is used in the customer's Scada monitoring. Traffic would be enabled from APN network and routers interfaces to firewall's inside interface. Internal network, in which SCADA resides, was configured with ICMP and IEC 104 traffic to the routers.

After the policies were added on the firewall cluster, the connection would be tested with simple ping test.

```
PING 10.11 (10.11) 56(84) bytes of data:
64 bytes from 10.11: icmp_seq=1 ttl=63 time=420 ms
64 bytes from 10.11: icmp_seq=2 ttl=63 time=105 ms
64 bytes from 10.11: icmp_seq=3 ttl=63 time=112 ms
64 bytes from 10.11: icmp_seq=4 ttl=63 time=95.1 ms
64 bytes from 10.11: icmp_seq=5 ttl=63 time=93.0 ms
64 bytes from 10.11: icmp_seq=6 ttl=63 time=104 ms

--- 10.11 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5002ms
rtt min/avg/max/mdev = 93.079/154.989/420.230/118.790 ms
```

Picture 26. Ping test

After successful ping test from the firewall cluster to the mobile router, state of the VPN tunnel was checked in the Checkpoint's VPN monitoring tool.

Tunnel details		
Previous Next Copy		
Tunnel	🔒 Device_PSV_10.1...	↔️ Cluster
State	✅ Up	
Community	🔗 _Routers_VPN	
Type	Regular	
	First direction	Second direction
From	🔒 Cluster	
To	🖨 Device_PSV_10.1...	
State	✅ Up	
Peer IP	10.	

Picture 27. State of the VPN tunnel

Tunnel details offered simplified details of the tunnel. However, it showed that the state of the tunnel was up, and detailed info could be viewed from the CLI if needed.

Confirming that the connection was established and secure, means that the router could be added to the Zabbix for SNMP monitoring.

The screenshot shows the Zabbix monitoring dashboard. The top navigation bar includes 'Monitoring', 'Inventory', 'Reports', 'Configuration', and 'Administration'. The main dashboard area is divided into several sections:

- Dashboard:** Contains 'Favourite graphs', 'Favourite screens', and 'Favourite maps' sections, all showing 'No graphs added', 'No screens added', and 'No maps added' respectively.
- Problems:** A table listing recent issues:

Time	Recovery time	Status	Info	Host	Problem - Severity	Duration	Ack	Actions
16:53:05	16:54:04	Testhost	Unavailable by ICMP Ping (probeinterval)	Testhost	99s	No		
2018-04-19 10:46:26		PROBLEM	Operational (ELISA / TELIA)	Testhost	9d 6h 7m	No		
2018-04-18 16:18:07		PROBLEM	Lack of free swap space on Zabbix server	Zabbix server	10d 36m	No		
- Host status:** A table showing the status of hosts:

Host group	Without problems	With problems	Total
Palomusurilaiset	2		2
Templates/Network Devices		1	1
Zabbix servers		1	1
- System status:** A table showing the overall system health:

Host group	Disaster	High	Average	Warning	Information	Not classified
Palomusurilaiset						
Templates/Network Devices						1
Zabbix servers				1		
- Status of Zabbix:** A table showing the status of Zabbix parameters.

Picture 28. Zabbix SNMP monitoring

The green filling shows that the connection to the router is established and SNMP monitoring is working. This means that the initial state of the project was completed, and the rest of the routers could be added to Zabbix and delivered to the customer.

5 Conclusions

The new network infrastructure offers encrypted connections, with real-time vision of the network's health, to the customer.

The project proceeded on time, and it will continue with commissioning tests and transferring from ASA to Checkpoint's firewall cluster.

The Checkpoint products were hard to learn and differed from other manufacturers products. However, after learning and configuring them, Checkpoint's products seem stable and are heavily focused on the security, which in present-day is very important.

Thanks to NDC Networks, for giving me the opportunity to learn about power distribution networks and network security.

References

1. Advantech B+B Routers <http://advantech-bb.com/product-technology/> Accessed 1.3.2018
2. Cisco ASA 5505 <http://www.mustbegeek.com/reset-password-in-cisco-asa-firewall/> Accessed 1.3.2018
3. Checkpoint Appliances Documentation <https://www.checkpoint.com/downloads/product-related/datasheets/ds-3200-appliance.pdf> Accessed 9.3.2018
4. Vodafone Private APN <http://www.vodafone.qa/en/internet/mobile/dedicated-apn> Accessed 10.3.2018 Accessed 11.3.2018
5. Checkpoint Documentation sk101239 https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk101239 Accessed 1.4.2018
6. Checkpoint Documentation sk39915 https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk39915 Accessed 1.4.2018
7. Public vs Private APN <https://www.linkedin.com/pulse/m2m-tips-public-ip-vs-private-addressing-m2miot-devices-james-mack/> Accessed 2.4.2018
8. Zabbix Documentation 3.2 <https://www.zabbix.com/documentation/3.2/manual/introduction/about> Accessed 17.4.2018 Accessed 4.4.2018