Juuso Martin

Secure Mobile Office Solution over LTE Network

Helsinki Metropolia University of Applied Sciences

Bachelor of Engineering

Information Technology

Bachelor’s Thesis

29 September 2017

Author(s) Title Number of Pages Date	Juuso Martin Secure Mobile Office Solution over LTE Network 51 pages + 5 appendices 29 September 2017
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor(s)	Jani Ripatti, Senior Systems Engineer Marko Uusitalo, Senior Lecturer

The goal of this project was to create a proof of concept of a working, secure and agile mobile office solution by using SRX 320 with LTE mini-PIM and L3 VPN over LTE. In addition, another goal was to improve the author’s knowledge of MPLS and VPN technology.

A configuration for the solution was built from the start because no previous versions existed. A test environment was created to mimic possible usage of the concept. The test environment consisted of a laptop behind SRX 320 with LTE mini-PIM as mobile office and SRX 1500 was deployed at the lab with a Linux server behind to act as a corporate server.

The initial bandwidth of LTE was first measured by using speedtest.net to get estimate how fast the connection was. Then the measurements of L3 VPN between sites were made by using iPerf3 bandwidth program. The first measurements gave bad results but after optimizing packet sizes the desired results were got, they were almost good as the initial measurements.

It can be safely stated that all the goals were met and the testing results show great promise for the solution to be implemented in the future.

Keywords	LTE IPSEC VPN SRX MPLS JUNIPER

Contents

Appendices

List of Abbreviations

AS	Autonomous System. A collection of IP networks and routers under the control of one entity
BGP	Border Gateway Protocol. Exchanges routing and reachability information between Autonomous Systems.
cSRX	Container technology version of the SRX gateway device.
DHCP	Dynamic Host Configuration Protocol. Assigns IP addresses to the hosts.
DOS	Denial of Service. Method used to attack computer networks.
DSL	Digital Subscriber Line. Family of technologies used to transmit data over telephone lines.
ESXi	Type-1 hypervisor developed by VMware.
GRE	Generic Routing Encapsulation. Tunnelling protocol developed by Cisco.
IGP	Internal Gateway Protocol. Protocol used to exchange routing information between routers within AS.
IKE	Internet Key Exchange. Protocol used to set up a IPsec VPN tunnel
IPSec	Internet Protocol Security. Protocol suite that authenticates and encrypts the packets of data sent over network.
ISP	Internet Service Provider. Organization that provides internet to subscribers.
KVM	Kernel-based Virtual Machine. Virtualization support in Linux kernel.
LDP	Label Distribution Protocol. Protocol that MPLS capable routers exchange label mapping information.

LIB Label Information Base. Table that stores MPLS labels and forwarding information on MPLS capable routers.

LSP Label Switched Path. Unidirectional path through MPLS network

LSR Label Switching Router. MPLS enabled router in MPLS network.

LTE Mobile network that works on specific frequency, also referred as 4G mobile network.

MIMO Multiple-Input and Multiple-Output. Implementation of multiple antenna receiving and transmitting traffic at the same time.

MSS Maximum Segment Size. Maximum amount of data in TCP segment.

MTU Maximum Transmit Unit. Maximum size of packet transiting through network before fragmentation.

NAT Network Address Translation. Remapping of IP addresses on routers.

OSPF Open Shortest Path First. IGP protocol used to route packets within single routing domain.

PIM Physical Interface Module. Network interface card for SRX developed by Juniper Networks.

POE Power Over Ethernet. Enables transmission of power over ethernet cable, e.g. used to power wireless LAN access points.

SNR Signal-to-Noise Ratio. Used to measure the quality and strength of LTE/4G signal.

TCP Transmission Control Protocol. Used to crate connections between computers.

UTM Unified Thread Management. Security suite for SRX devices developed by Juniper Networks

VPN Virtual Private Network. Extends private network over public or shared network. Enables users to send and receive data as if they were part of a private network.

VRF virtual routing and forwarding. Technology that enables multiple routing tables to co-exist at the same time.

vSRX Virtualized version of SRX gateway.

WAN Wide Area Network. Computer network that extends over a large geographical distance.

1 Introduction

Juniper Networks has a customer that needed to have a remote site wirelessly and securely connected to the corporate network. Currently Juniper Networks has no solution ready for the wireless and secure deployment of the branch office. The goal was to create a secure mobile office solution that is very easy and agile to deploy anywhere in the nation by using LTE mini-PIM on SRX 320. The solution needed to have a high level of security and redundant connectivity for nonstop performance. Configuration for the fresh solution needed to be made from the start and needed to be done using MPLS based technologies to separate multiple connections to fulfil the requirements of the customer.

A test environment was built to benchmark the solution and to test the maximum performance of the newly released LTE mini-PIM. The performance of the remote connection was measured by running tests on the iPerf network testing program and Speedtest.net network connection speed test website. A setup including SRX 320 with LTE card was made to mimic remote site and a setup using SRX 1500 was made to mimic corporate network. Both setups had a server connected for traffic testing. All test results were analysed and the performance of the solution tested.

Juniper Networks

Juniper Networks was founded by Pradeep Sindhu on February 6, 1996, in California. Instead of starting small like many start-ups at the time Juniper Networks decided that they would start big and tackle the toughest problems in the field and solve it once and for all.

In September 1998 Juniper Networks launched their first product M40 router and it was revolutionary. The M40 was a way better router than anything on the market at the time and showed that a new serious player had entered the networking business and market.

Fast forwarding to present Juniper Networks (Figure 1) is one of the biggest network hardware companies in the world among Cisco and Huawei. Juniper employs more than 9000 people around the globe and the annual revenue is above 5 billion US dollars (Juniper Networks, 2017). The product portfolio has increased from one router to many switches, firewalls, routers and to their respective management platforms as well as software solutions. During the years, many records have been set by Juniper Networks regarding the speed of the connection or performance of the hardware together with high reliability valued by the most demanding carriers and service providers. Today Juniper is a well respected company and customers are rather pleased.

Figure 1. Juniper Networks logo as of 2009

Structure of paper

This thesis focuses to give reader a good explanation on today’s problems on remote offices and aims to solve these problems with fresh solution using LTE and MPLS technologies to achieve agile deployment and secure connection.

After describing the rough solution, this paper will focus on SRX product family and to two specific products from that family which were used in testing environment. Along the introduction of two SRX devices, a LTE card for SRX 320 is also introduced.

Next this paper will focus on configuration used in testing environment. All-important configuration lines are explained and why certain parameter is used. Also protocols and other technical aspects of configuration are opened as much as possible to the reader for broader understanding of configuration. After configuration part comes verification section to ensure everything works as intended before tests.

Next chapter is about how testing environment was built, how tests were done and the results of the tests. The last chapter sums up the thesis and the results.

2 Pain of Remote Office Sites

Today internet is used literary everywhere, from the coldest of the north to the warmth of the south seas, but with internet also comes security risks. Remote offices and any remote sites such as popup shops rely on internet and on a connection to corporate network services. Usually security and connectivity from a remote site network to the corporate network is done by using the Virtual Private Network (VPN) service which links these two networks into one and enables the use of corporate services. A VPN service requires internet or a similar shared medium to be able to function.

Remote sites may have easy access to internet via cable and have suitable equipment to do VPN which is secure enough for traffic to transit. But not every site has an easy connection or cabling at all. It would not be cost effective to install the required cabling. A wireless connection to internet is needed on remote sites. By using wireless connectivity not only costs are lowered but new remote sites become possible because there is no need for physical cabling.

The problem is that there is no easy way to accomplish such connection required. For a remote office to be truly mobile it needs be easy to open it and close it as needed. A worksite barrack is a good example of a temporary office that needs to have connectivity to various IT systems and needs to be agile and has to be able to be deployd anywhere. One could argue here that doing proper cabling for connection is not a big deal, but it is really not cost effective and decreases the mobility and agility of the solution.

Another good deployment example is a group of isolated rapidly deployed temporary research facilities. This could be a group of scientists who need connectivity to very north of Finland to wilderness with secure connectivity to the different parts of educational and research networks.

Both examples require a simple, scalable and secure solution to provide fast and reliable connectivity to other parts of the organizations’ networks.

Any device today that does this connection wirelessly is ether just not capable to connect to all necessary services at the same time or is not secure enough. Every system which passes the qualification of the services needed and security is expensive.

3 Secure Mobile Office Solution over LTE

The target solution aims to tackle all previously mentioned problems. There is no need to do cabling for every remote site because of the high performance mobile network (LTE). There is neither need for complicated configuration because only a couple of the key configuration lines are needed to be changed to get any network up and a couple of more lines to multiply lines for more traffic as any customer desires. Separation to different parts of the network in the solution will be handled by Multiprotocol Label Switching (MPLS) based technologies such as MPLS L3 VPN and Virtual Private LAN Service(VPLS).

As the solution will use the same nationwide mobile service provider it can be easily deployed by only configuring it once and then it can be moved or shipped wherever needed without any extra configuration.

Extreme simplicity is achieved by using only one device in the solution which can cover multiple different use cases and provides an adequate number of ports for end device connectivity on the mobile sites. There is also an option to provide Power over Ethernet (POE) for the end devices such as surveillance cameras, Wireless LAN access points and Voice over IP phones.

The platform used in the solution is Juniper SRX320 firewall used as a secure router. The selected platform is often used as a “Swiss Army knife” to build various different solutions such as next generation application firewalling, routing, content security or VPN termination point. The selected platform together with LTE connectivity can offer all the required features in a single device which makes the solution easily manageable, small form factor and agile.

4 SRX Gateway

This chapter describes the SRX product family and covers the important areas regarding the study. To accomplish a good understanding of SRX functionality and security functions deployment examples of SRX are looked into and both SRX 320 and SRX 1500 that are used in the solution are introduced. The study alsol provides information on the new LTE mini-PIM slot card functionality and specs.

4.1 SRX Product Family

The SRX product family consists of a variety of different size service gateways (Table 1), scaling from small business and branch offices to the needs of data centers and service providers. Usually people talk about SRX firewalls or SRX routers but all SRX family devices are service gateways. This means that it can do both firewall and routing and also switching, Wide Area Network (WAN) connectivity and security solutions such as Unified Threat Management (UTM). More information on security is provided in Chapter 5.2. All SRX devices have the same JunOS operating system and functionalities which makes it easy to configure.

Table 1. SRX Product family listing and common use cases

Scale	**Products**	**Use case**
Virtual	cSRX vSRX	Private cloud, hybrid cloud and public cloud
Small	SRX110, SRX220, SRX300 and SRX550	Small Enterprise and branch office
Medium	SRX 1400, SRX 1500, SRX 3400, SRX 3600 and SRX 4000	Mid-size enterprise and data center
Large	SRX 5400, SRX 5600 and SRX 5800	Large data center and service providers

Virtual scale

The virtualized versions of SRX are just like the physical ones as of features and functions. The only real lack is that there is no dedicated hardware for features such as routing engine and storage because virtual appliance is running on top normal computer among other software. All virtual appliances get their compute and storage resources from the computer which it is run on. The performance is heavily depended on how much resources they have available for use.

vSRX is the ‘classic’ virtualized appliance, meaning it can run on any virtual machine platform (hypervisor) the most common ones are ESXi from VMWare and KVM which is built-in in Linux operating systems. One can use vSRX as a lab test equipment or as a real production solution.

cSRX is a lightweight and agile version of virtual SRX. The letter C stands for container. Using Docker containers significantly reduces overhead, because the container shares the host’s OS. As shown in Figure 2, cSRX differs from vSRX in many important ways. Its spin-up time is measured in milliseconds, it has a notably smaller footprint and it uses far less memory. cSRX is a relatively new solution from Juniper Networks but there is a lot of potential. A potential use case might be to use this as firewall on demand or the only firewall for connection, because connections usually last for a short period time. Spinning-up a firewall only for the period of connection reduces maintenance costs and saves performance for other tasks. To better understand this , when one does a Google search a Docker container is spin-up and down just for the search. (Juniper Networks, 2017.)

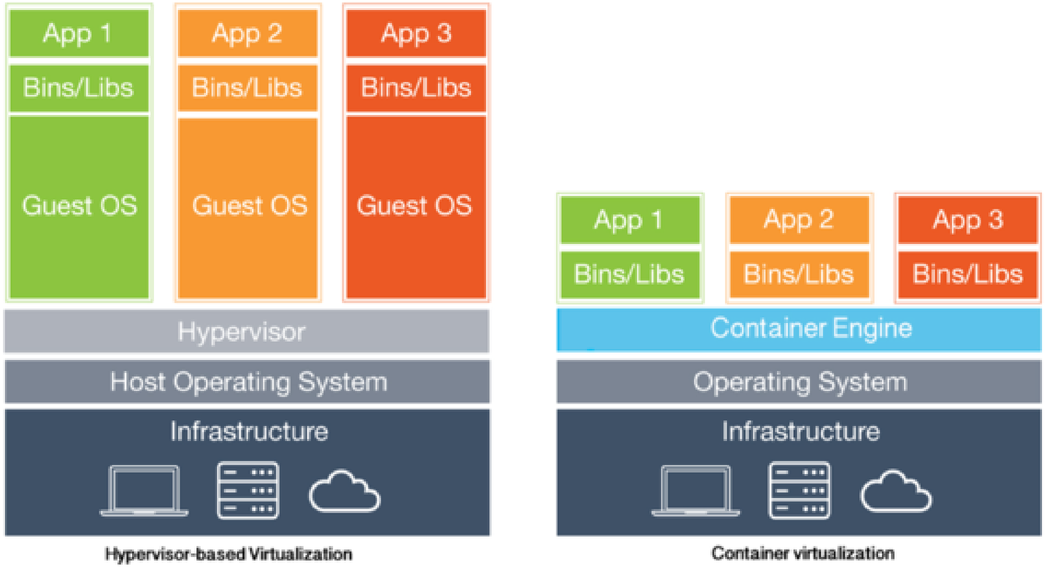


Figure 2. Differences between hypervisor-based and container based virtualization (Chenxi Wang, 2016)

Small scale

Small scale does not mean that the devices as such are tiny, but the network is relatively small. Small scale or small branch network is a network that is considered to have under dozen connected computers or other devices. There is only one branch firewall device in this network and it has to be very versatile to accomplish all the tasks that it needs to handle. Typically, a network like this is a branch network of a larger corporate office network and needs to have connectivity to it via internet. So, this one device is required not only to connect to internet but to corporate network as well. Also, branch firewall must provide connectivity to all of the devices in the network, switching and in some cases wireless connectivity to network.

Figure 3. shows an example of a small branch location. Here Juniper Networks SRX 210 connects four hosts to internet. SRX 210 also needs to act as a firewall, switch and Digital Subscriber Line (DSL) modem. It is important to notice that all hosts are directly connected to SRX 210. If an upstream device were to fail, there is no redundancy in place or any other way to keep the connection up. However, replacing one device and configuring with back-up configuration is not a huge task. This solution has the lowest cost overall.

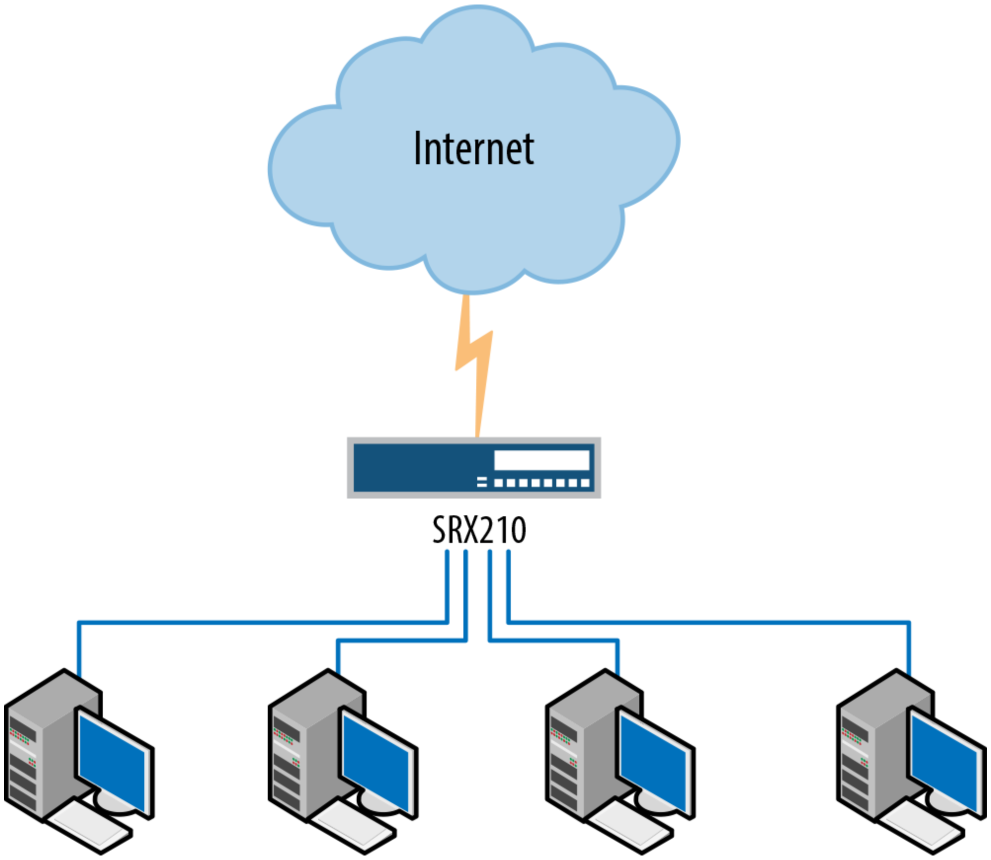


Figure 3. An example of small branch network (Rob Cameron, 2013).

Medium scale

On a Medium scale branch, high availability and redundancy is important. Important services such as email and web servers need to be connected at all time with no exceptions. If any problems should emerge with important services it would mean no business for some time and loss of income for company.

Here the importance of a right networking device is critical for business. Figure 4 illustrates how a medium branch is deployed and SRX 240 is placed at the interned edge. Email and web-server are connected directly to the SRX 240 for maximum performance and security. Because services are directly connected to internet the gateway device has to provide security as well. SRX devices not only provide firewall services but offer also Intrusion Protection Service for email and web services.

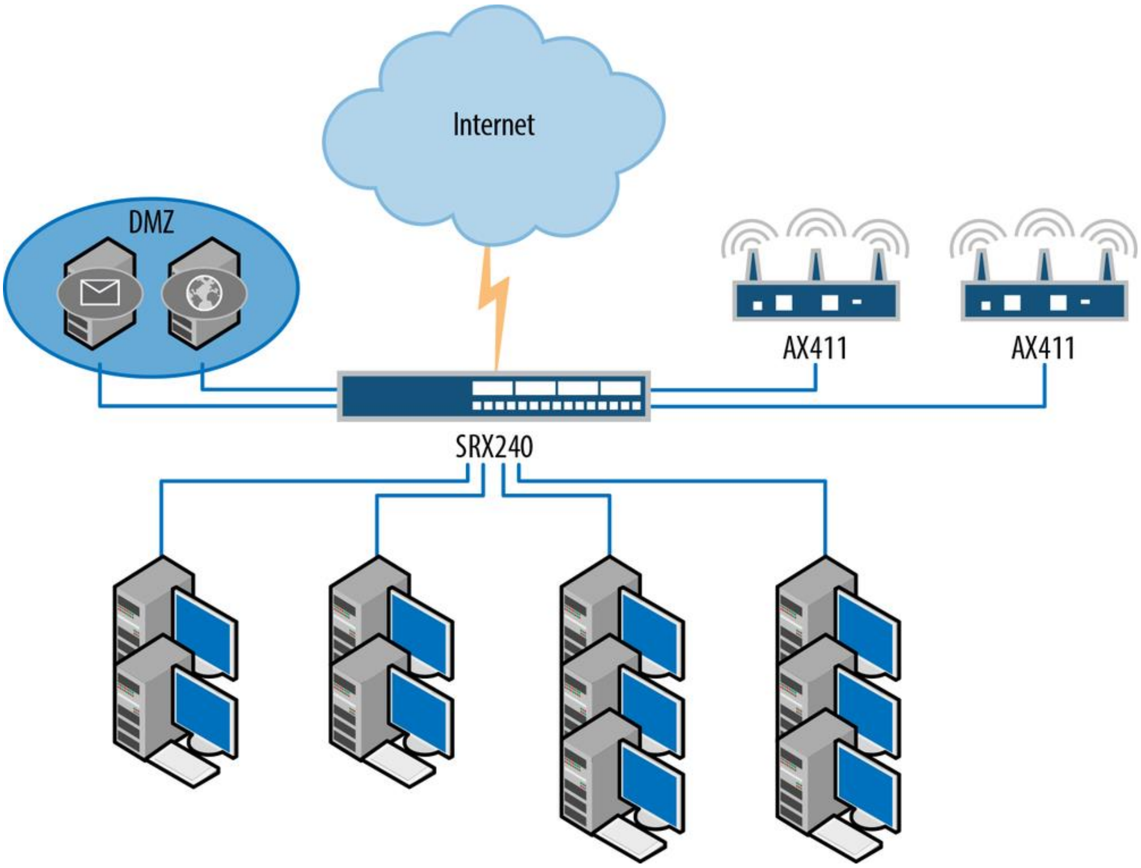


Figure 4. An example of medium branch network (Rob Cameron, 2013).

SRX 240 is a little older model and today Juniper recommends the use of SRX 1500 or similar products for medium branch. SRX 1500 outperforms SRX 240 roughly 10 to 1. SRX 1500 is chosen for this solution to act as the medium branch network edge device, connecting the test lab to internet.

Large Scale

Even when scaling services to a large branch, SRX devices are capable of providing enough performance, speed and security to deploy services. In Figure 5 it can be seen that two SRX 650 are used along with two connections to internet. This is for two reasons:

- Better connection speed and more bandwidth
- Improved redundancy and high availability

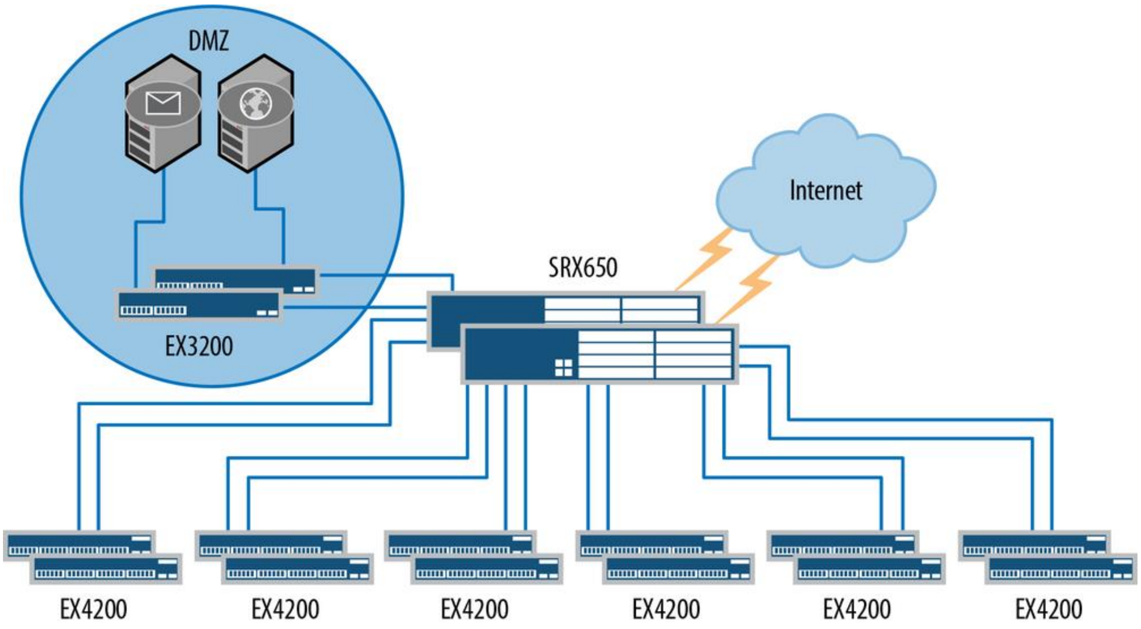


Figure 5. An example of large branch network (Rob Cameron, 2013).

There is no limit on scaling networks when using SRXs devices, SRX is truly well manufactured product series which serve multiple purposes on any corporate network.

4.2 SRX 320

The SRX 320 is suitable for small enterprises and branch offices. It combines security, routing, switching and WAN interfaces with a next-generation firewall and advanced threat mitigation capabilities (Juniper Netwoks, 2014). There is also an option to provide Power over Ethernet (POE) for the end devices such as surveillance cameras, Wireless LAN access points and Voice over IP phones.

The platform used in the solution is Juniper SRX 320 (Figure 6) firewall used as a secure router. The selected platform is often used as a “Swiss Army knife” to build various different solutions such as next generation application firewalling, routing, content security or VPN termination point.

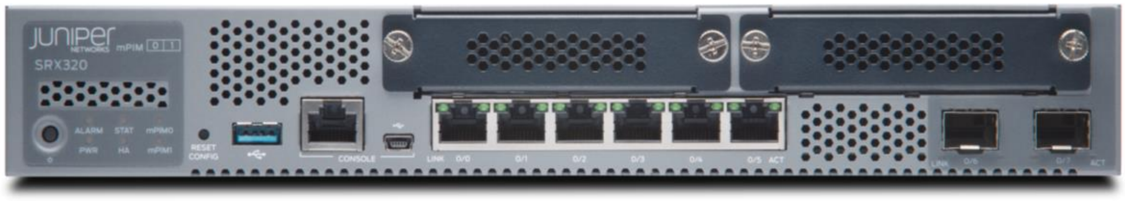


Figure 6. SRX320 front in real life.

The SRX 320 can be used in many different ways to build or support solutions, while some other devices lack portability or customization options has SRX 320 all of these features. As seen in Figure 7 and Table 2, SRX 320 packs lots of different ways to connect devices and various media types. For this solution, the SRX 320 is used along LTE mini-Physical Interface Module (PIM) on slot 3 (Figure 7, number 3).

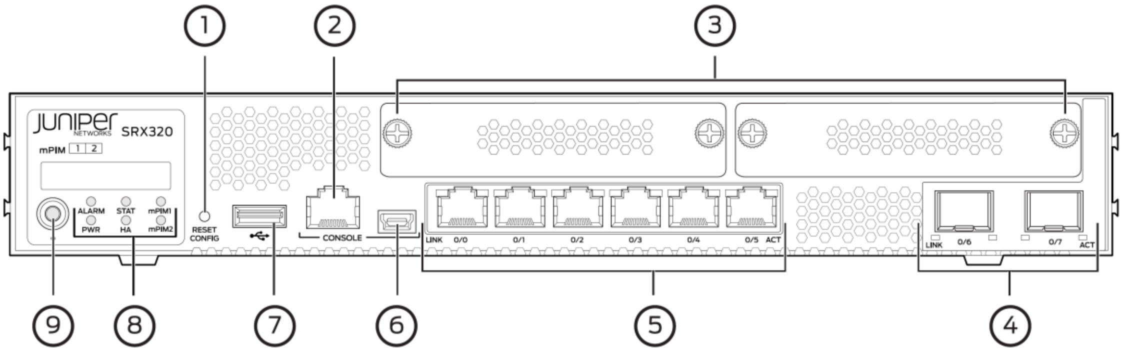


Figure 7. SRX320 Front sketch image with numbered spots, refer to table 2.

Below, in Table 2 explanation for numbered spots in Figure 7 can be found.

Table 2. SRX320 Front Panel Components

Number	Component	Description

1	Reset Button	Return configuration to rescue configuration or the factory default configuration
2,6	Console Port	Serial - Used for CLI management. The port uses RJ-45 serial connection and supports RS-323 standard USB – Port uses Mini-B type USB connector. To use CLI thru USB you must download a USB driver.
3	Mini-PIM Slots	The Mini-PIM slots can be used to provide LAN and WAN functionality along with connectivity to various media types. LTE Card used in this thesis is connected in this kind of slot.
4	1G SFP Ports	Two 1G Small Form-factor Pluggable (SFP) ports for network traffic
5	1G Ethernet Ports	Six Gigabit Ethernet LAN ports. Uses RJ-45 Connector. These ports can be used to: • Function as front-end network ports

		• Provide LAN and WAN connectivity to hubs, switches, local servers, and workstations • Forward incoming data packets to the services gateway • Receive outgoing data packets from the services gateway
7	USB port	One normal type USB3.0 port. Used to connect storage devices.
8	LEDs	Indicate component and system status. Also, good information for troubleshooting.
9	Power Button	Used to power up and shutdown the device

LTE mini-PIM

LTE mini-Physical Interface Module (PIM) is a physical interface card which goes into mini-PIM slot (Figure 7, number 3). By using LTE mini-PIM module it is possible to connect wireless WAN networks to SRX devices. For example, SRX can be connected to the internet via LTE mini-PIM as the primary or backup interface or also to private mobile networks over LTE. Basically, mobile network connectivity for SRX devices.

In Figure 8 there is a LTE mini-PIM card. It has two connectors for the antennas. The purpose of using two antennas is not to have backup for another antenna, but to increase performance and speed by using Multiple-Input and Multiple-Output (MIMO) method. MIMO is method that uses multiple antennas to send and receive signals at the same time thus increasing volume of data sent and received.

The card also has indication LEDs which are seen green in the figure almost at the center of the front panel of the card. The left side indication led stack is for the signal strength, the more LEDs are lit from bottom to top the better the signal strength is. The right side indication led stack has 2 different functions, the top two LEDs shows which one of mobile networks are used, LTE(4G) or 3G. The bottom two LEDs indicate which SIM card is in use. There are handy lines drawn on the panel to ease the understanding of LEDs. The front also includes a mini USB connector for the debugging purposes. The card is secured with two thumbscrews on either side when plugged in to SRX. When plugged into SRX the card is connected via an edge connector at the far side of the card.

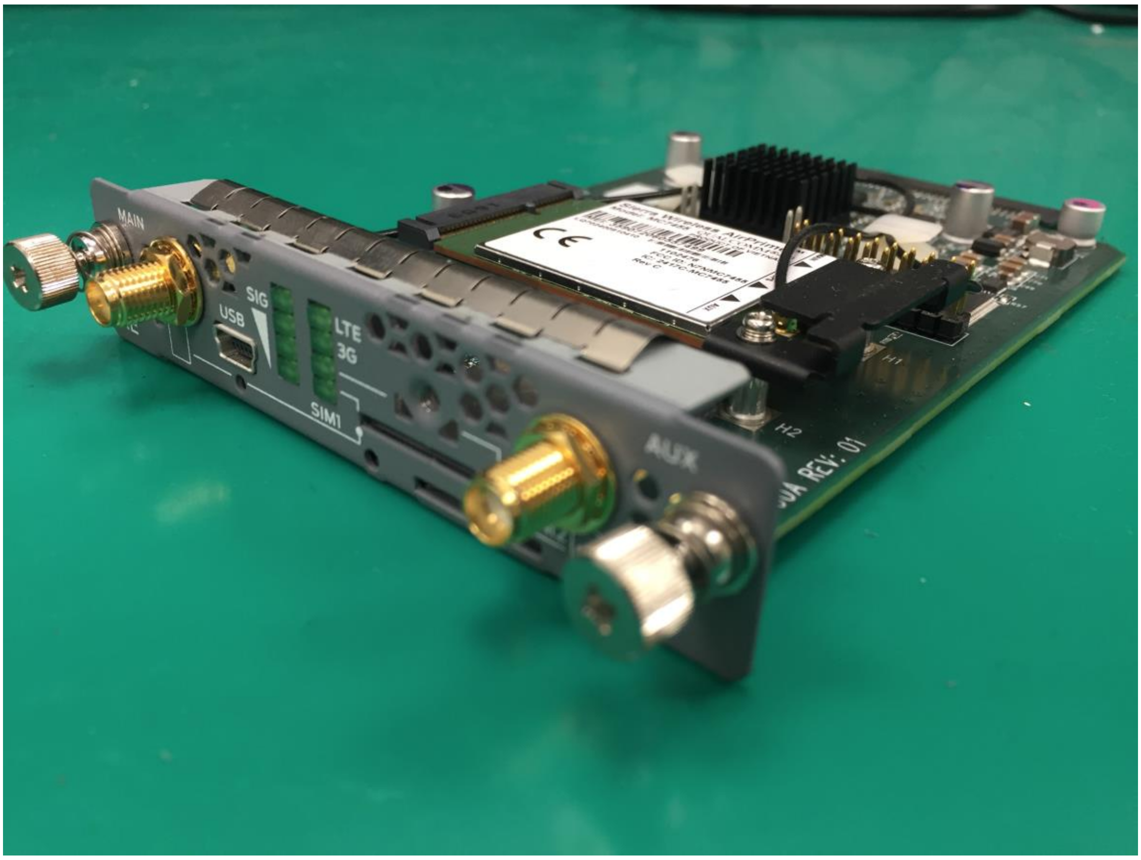
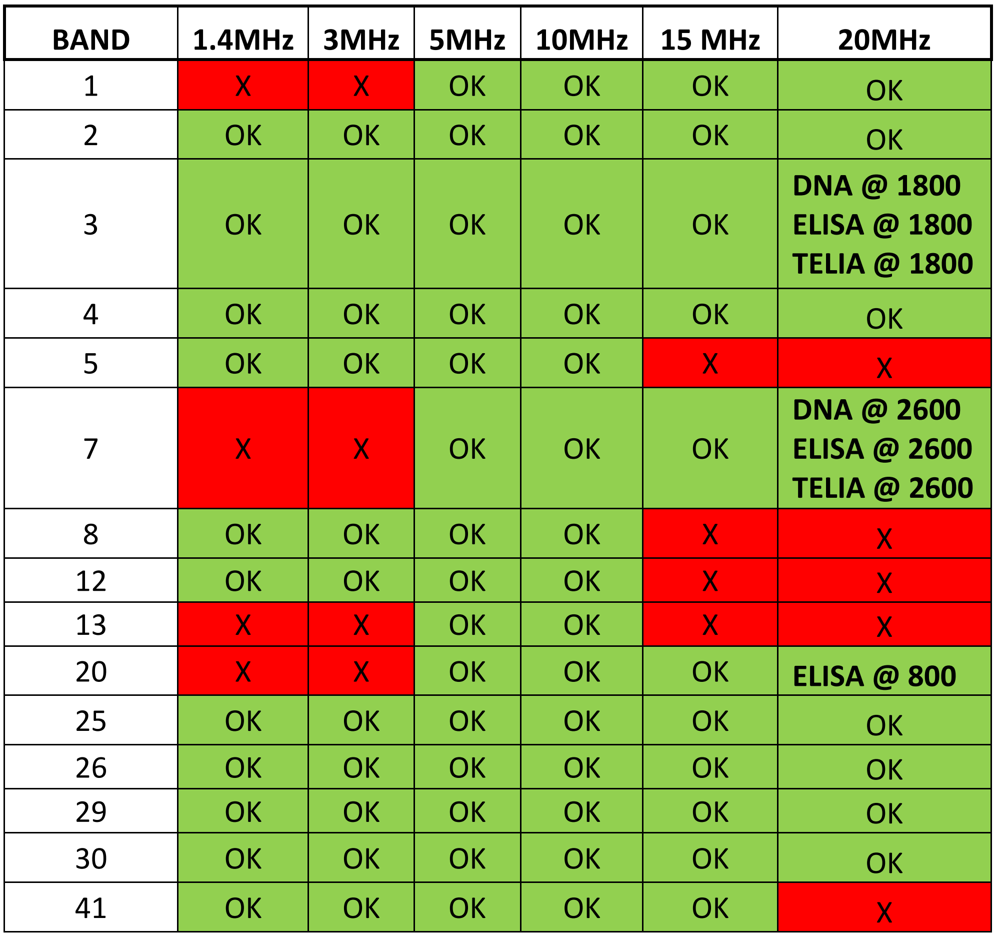


Figure 8. Picture 1. LTE Mini-PIM card and all front panel connections

LTE mini-PIM uses the Sierra Wireless MC7455 LTE card in its core. The MC7455 is rated to have 300Mbit/s max download speed and 50Mbits/s max upload speed. These informed maximum speeds are almost as fast as any carriers max speed in Finland, so this adapts well to the needs of the solution. The MC7455 card also supports a wide range of different mobile bands as seen in Table 3. Green and red backgrounds represent support for channel bandwidth on a specific band. All Finnish mobile carriers are marked on their supported bands with the frequency in Mhz. Elisa is supported on three different bands and is ideal for the final solution and testing connectivity in various places.

Table 3. Support for LTE networks in Finland.



BAND	1.4MHz	3MHz	5MHz	10MHz	15 MHz	20MHz
1	X	X	OK	OK	OK	OK
2	OK	OK	OK	OK	OK	OK
3	OK	OK	OK	OK	OK	**DNA @ 1800** **ELISA @ 1800** **TELIA @ 1800**
4	OK	OK	OK	OK	OK	OK
5	OK	OK	OK	OK	X	X
7	X	X	OK	OK	OK	**DNA @ 2600** **ELISA @ 2600** **TELIA @ 2600**
8	OK	OK	OK	OK	X	X
12	OK	OK	OK	OK	X	X
13	X	X	OK	OK	X	X
20	X	X	OK	OK	OK	**ELISA @ 800**
25	OK	OK	OK	OK	OK	OK
26	OK	OK	OK	OK	OK	OK
29	OK	OK	OK	OK	OK	OK
30	OK	OK	OK	OK	OK	OK
41	OK	OK	OK	OK	OK	X

The reason for having two SIM card slots in the LTE mini-PIM is to minimize connectivity loss in situations where a network (LTE or 3G) cannot be reached. If connection is dropped and mobile network service cannot be reached, there is a high chance it is only one carrier that is having issues. With a connection to a different mobile carrier network with another SIM card connection can be usually re-established.

By using the LTE mini-PIM in solution truly enables the concept mobile office. The only requirement to connect a remote office to the rest of the world is to have power to SRX and have mobile internet ready.

4.3 SRX 1500

SRX 1500 is quite similar to any other SRX device but it has considerably more raw performance power than the small 300 to 500 series devices. On its own weight class, it is not so impressive among other devices but for small companies it has the ideal price and performance.

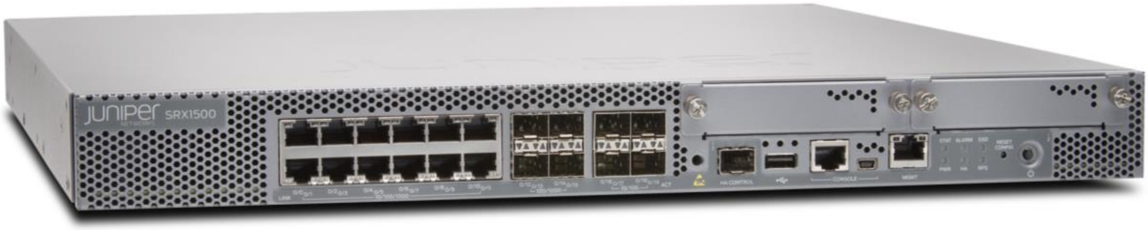


Figure 9. Picture 2. SRX 1500

In Figure 9 there is SRX 1500, it has 20 ports capable of 1GB Ethernet and among those 20 are 4 10GB Ethernet SPF+ ports. SRX 1500 also has 2 Physical Interface Module (PIM) ports for any future upgrades to scalability or security. The device fits into one U slot on rack.

SRX 1500 was chosen to represent a small company network in the lab for the present setup. Before this device the lab had MX80 which was tried to be replicated to be the small company network and have IPSec VPN but it was changed to the SRX device for simplicity, ease of management and configuration.

5 Configuration

This chapter looks into the configuration of the final solution. Major areas such as Security, Interfaces, Protocols and Routing used in configuration are covered. Each sub-area in the configuration, for example IPSec, is explained thoroughly and explained why certain configuration parameters are used. Most of the configuration parameters are identical in both ends of the final setup with their own natural specification e.g. IP addresses and inbound and outbound interfaces. All key differences in SRX320 and SRX1500 configurations are brought up.

5.1 General

When data traverses from end to end in a network it goes through multiple encapsulations, header swaps and even fragmentation. After a while data still manages get to where it was needed and in one piece.

There is a configuration example seen in Figure 10, which very much resembles the final configuration used in the present study. The aim is to avoid fragmentation which happens when the packet size goes over the limit of certain connection types. To increase performance over connection that requires multiple steps of encapsulation the maximum transmission unit (MTU) value in main transmission interface is limited.

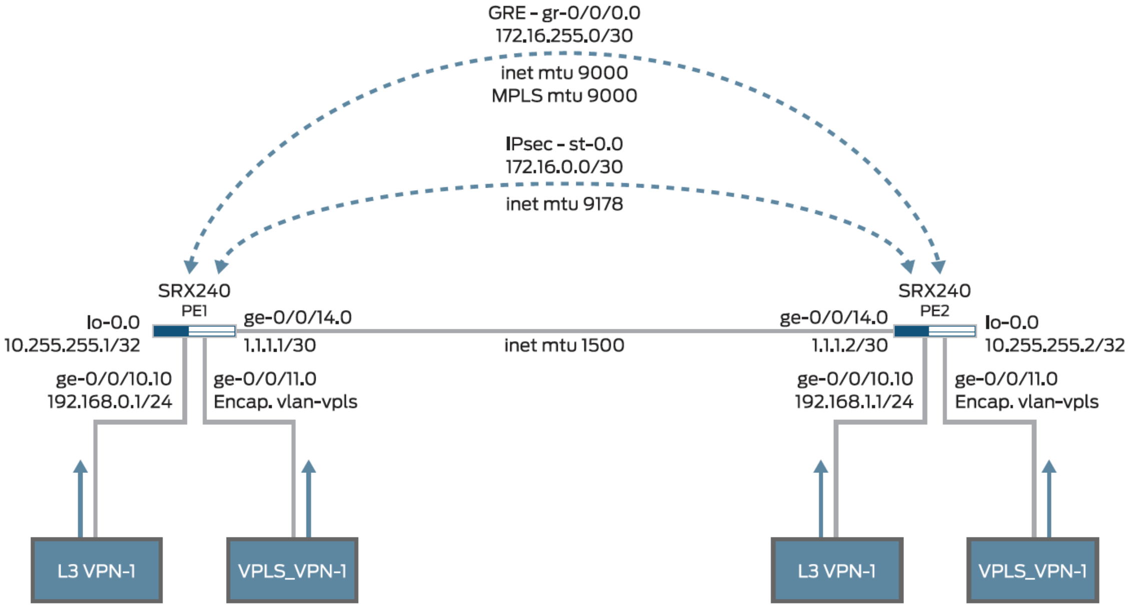


Figure 10. Example configuration with key points

Juniper SRX devices can be configured to work either in pure router mode (Packet mode) or as a stateful firewall (Flow mode) with a simple configuration and by rebooting the device into the new mode. The factory default mode is the Flow mode which is also used here. The Packet mode is used when no flow mode services such as IPSEC VPN, NAT or application based firewalling is not needed but the device is used as a plain router with or without MPLS based services. (Marschke & Reynolds, 2008, p. 362.)

For the separation of the different networks within the organization's network MPLS L3 VPN is used together with the secure connectivity over IPSec. This means that features from both Packet and Flow mode are needed simultaneously. This can be achieved by running the device in Flow mode but using a selective filtering for traffic which has to support Packet based services and MPLS in this case. Selective Packet mode filtering is explained later in the text.

5.2 Security

In JunOS which is the operating system used on all the SRX gateways all traffic is blocked by default. That is the most efficient way to control which traffic goes through and which does not. By pocking holes to firewall only for traffic that is required to pass, a high level of security is accomplished.

The final configuration uses multiple types of security to accomplish the most secure connection between test environment end points. It is most important that only a certain connection is allowed to connect to a certain network and communicate with systems in that network.

IPSec VPN

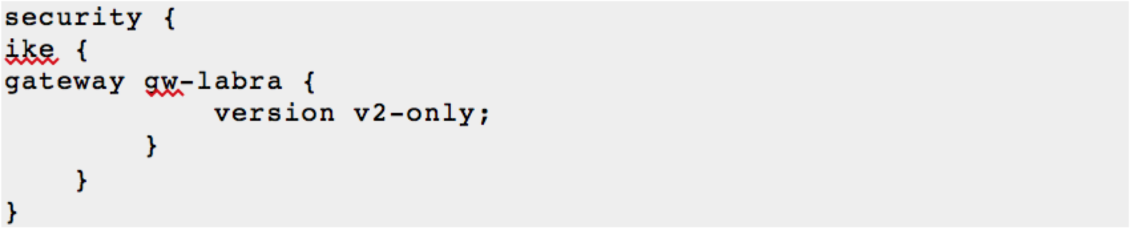
The term IPSec VPN comes from two different security adding features. VPN stands for Virtual Private Network which means connecting two Local Area Networks (LANs) into one. These two LANs can reside anywhere in the world but a shared medium to communicate is required to create VPN. Having connection from one LAN to another across the world might be great but it still needs to be a highly secure and reliable connection.

And to secure VPN communication while passing through internet IP Security Architecture (IPSec) can be used. IPSec is a collection of protocols for securing connection at the IP packer layer (OSI Layer 3).

At the core of IPSec VPN is tunnelling. Tunnels in the networking world behave in the same way as tunnels in real world. They provide passage from one point to another not caring what is between them. Basically, this is true for IPSec tunnels also but high security is also needed, so one creates their own private tunnel and encrypt the traffic when sending it to travel across the world in a tunnel and when the packet emerges on the other side it gets decrypted. In this final configuration (Appendix 1 and 2) a satellite office is connected to the corporate core using IPSec tunnelling. Packets traversing from the satellite office to the corporate core through network are not skipping the whole internet. Packets still travel as normal through multiple devices in internet but all the transit routers between do not care about the contents of the traffic. If anyone or anything would try to read the contents of the traffic that would be impossible because of the encryption used.

Setting up IPSec is relative simple in this solution regardless of the fact that SRX 320 LTE mini-PIM has a dynamic address assigned by ISP. Setting up IPSec VPN is done via the Internet Key Exchange (IKE) protocol. IKEv1 is done in two phases known as phase 1 and phase 2. In phase 1 both identities are authenticated and secure communication between is established for further negotiations. In phase 2 the rest of the negotiation process is completed and the encryption keys are exchanged and later used to secure data that traverses the VPN. (Marschke & Reynolds, 2008, p. 406.) (Juniper Networks, 2016-03-30.)

The final solution uses Internet Key Exchange version 2 (Figure 11) at both ends.



```
security {
ike {
gateway gw-labra {
            version v2-only;
        }
    }
}
```

Figure 11. Configuration snippet from SRX 320

IKE v2 is used because it has several advantages over IKEv1:

- Replaces eight initial exchanges with a single four-message exchange.
- Reduces the latency for the IPsec SA setup and increases connection establishment speed.
- Increases robustness against DOS attacks.
- Improves reliability through the use of sequence numbers, acknowledgements, and error correction.
- Improves reliability, as all messages are requests or responses. The initiator is responsible for retransmitting if it does not receive a response.

IKEv2 also has support for important features such as dynamic endpoint VPN which is critical for this solution because other end has dynamic IP. (Juniper Networks, 2017)

IKEv2 authentication process or message exchange can be thought of as a two phase process also like IKEv1 for making it easier to understand, as seen in Figure 12.

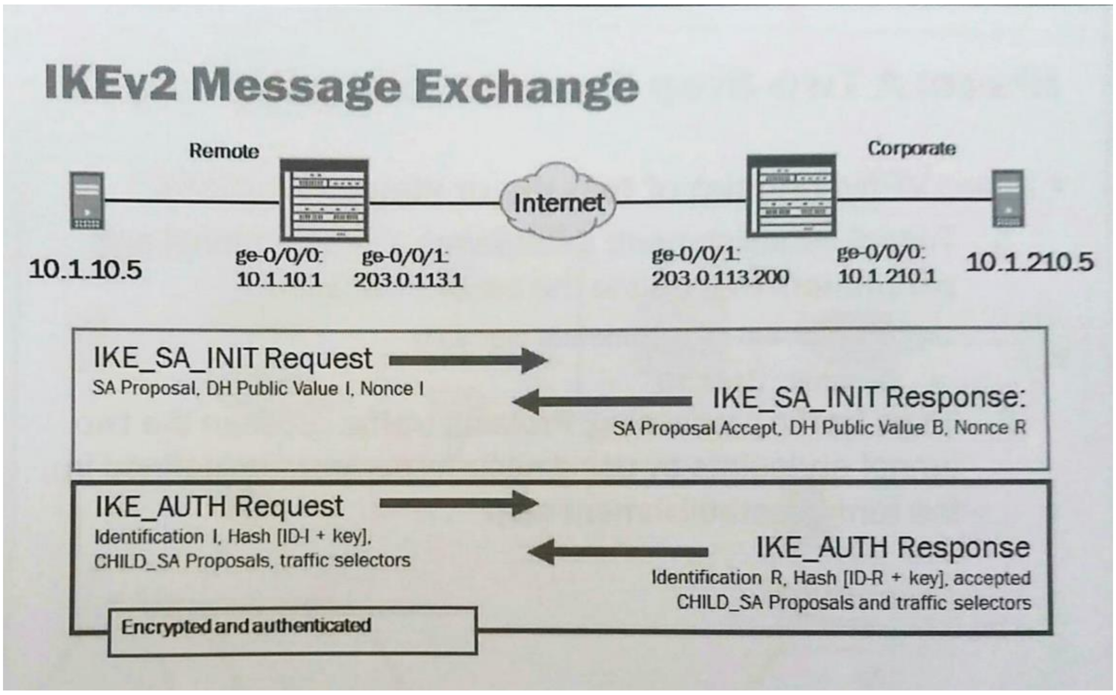
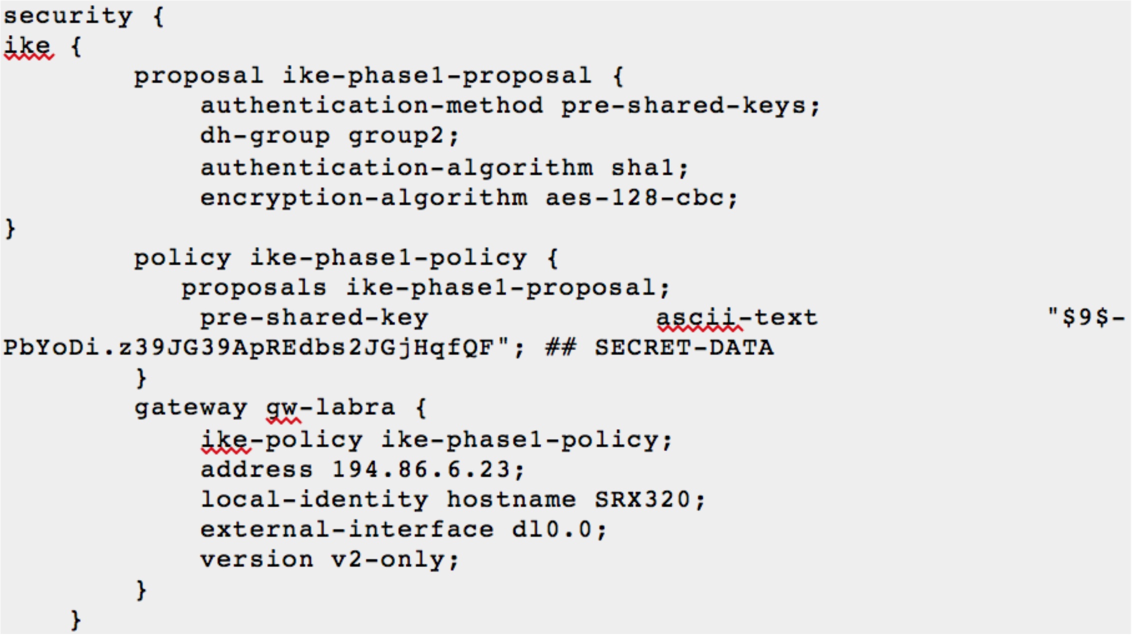

IKEv2 Message Exchange
Remote
Corporate
Internet
10.1.10.5
ge-0/0/0:
10.1.10.1
ge-0/0/1:
203.0.113.1
ge-0/0/1:
203.0.113.200
ge-0/0/0:
10.1.210.1
10.1.210.5
IKE_SA_INIT Request
SA Proposal, DH Public Value I, Nonce I
IKE_SA_INIT Response:
SA Proposal Accept, DH Public Value B, Nonce R
IKE_AUTH Request
Identification I, Hash [ID-I + key],
CHILD_SA Proposals, traffic selectors
IKE_AUTH Response
Identification R, Hash [ID-R + key], accepted
CHILD_SA Proposals and traffic selectors
Encrypted and authenticated

Figure 12. "Two phases" of IKE authentication

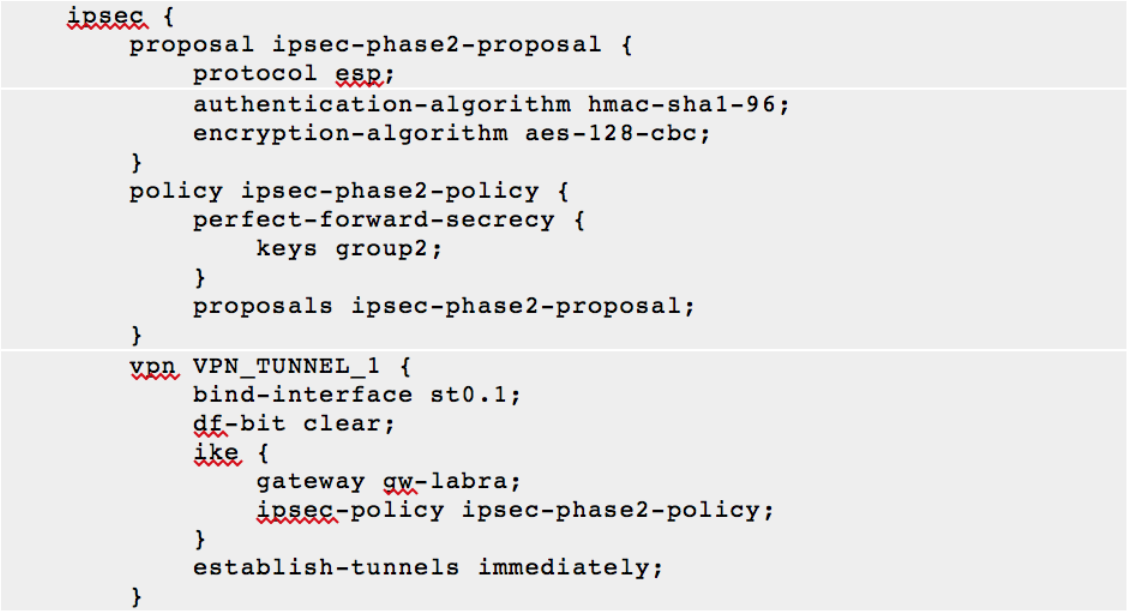
First the IKE_SA_INIT Request is sent from SRX 320 to the public of SRX 1500. The IKE_SA_INIT request contains important information (see Figure 13) for SRX 1500 on how to establish a secure channel for future message exchange.



```
security {
ike {
        proposal ike-phase1-proposal {
            authentication-method pre-shared-keys;
            dh-group group2;
            authentication-algorithm sha1;
            encryption-algorithm aes-128-cbc;
}
        policy ike-phase1-policy {
           proposals ike-phase1-proposal;
            pre-shared-key              ascii-text              "$9$-
PbYoDi.z39JG39ApREdbs2JGjHqfQF"; ## SECRET-DATA
        }
        gateway gw-labra {
            ike-policy ike-phase1-policy;
            address 194.86.6.23;
            local-identity hostname SRX320;
            external-interface dl0.0;
            version v2-only;
        }
    }
```

Figure 13. Important configuration lines for IKE_SA_INT request for SRX 1500

SRX 1500 sends IKE_SA_INIT response to SRX 320 with information on how it would like to communicate in the future. After this SRX 320 and SRX 1500 both independently compare the information they received and if pre-shared keys (in this case) match a secure communication channel is established for next phase. In the imaginary phase 2 an IKE_AUTH request is sent by SRX 320 to SRX 1500 via newly created secure channel containing information of security association (SA) negotiation shown in Figure 14. SRX 1500 sends back again same kind of information and if both sides agree that the authentication and encryption look identical a peer has been validated. Once the identity of the peer had been validated the first CHILD_SA is created, which is equivalent to the IKEv1 phase2. (Internet Engineering Task Force, 2010.)



```
    ipsec {
        proposal ipsec-phase2-proposal {
            protocol esp;
            authentication-algorithm hmac-sha1-96;
            encryption-algorithm aes-128-cbc;
        }
        policy ipsec-phase2-policy {
            perfect-forward-secrecy {
                keys group2;
            }
            proposals ipsec-phase2-proposal;
        }
        vpn VPN_TUNNEL_1 {
            bind-interface st0.1;
            df-bit clear;
            ike {
                gateway gw-labra;
                ipsec-policy ipsec-phase2-policy;
            }
            establish-tunnels immediately;
        }
```

Figure 14. Important configuration lines for IKE_AUTH request

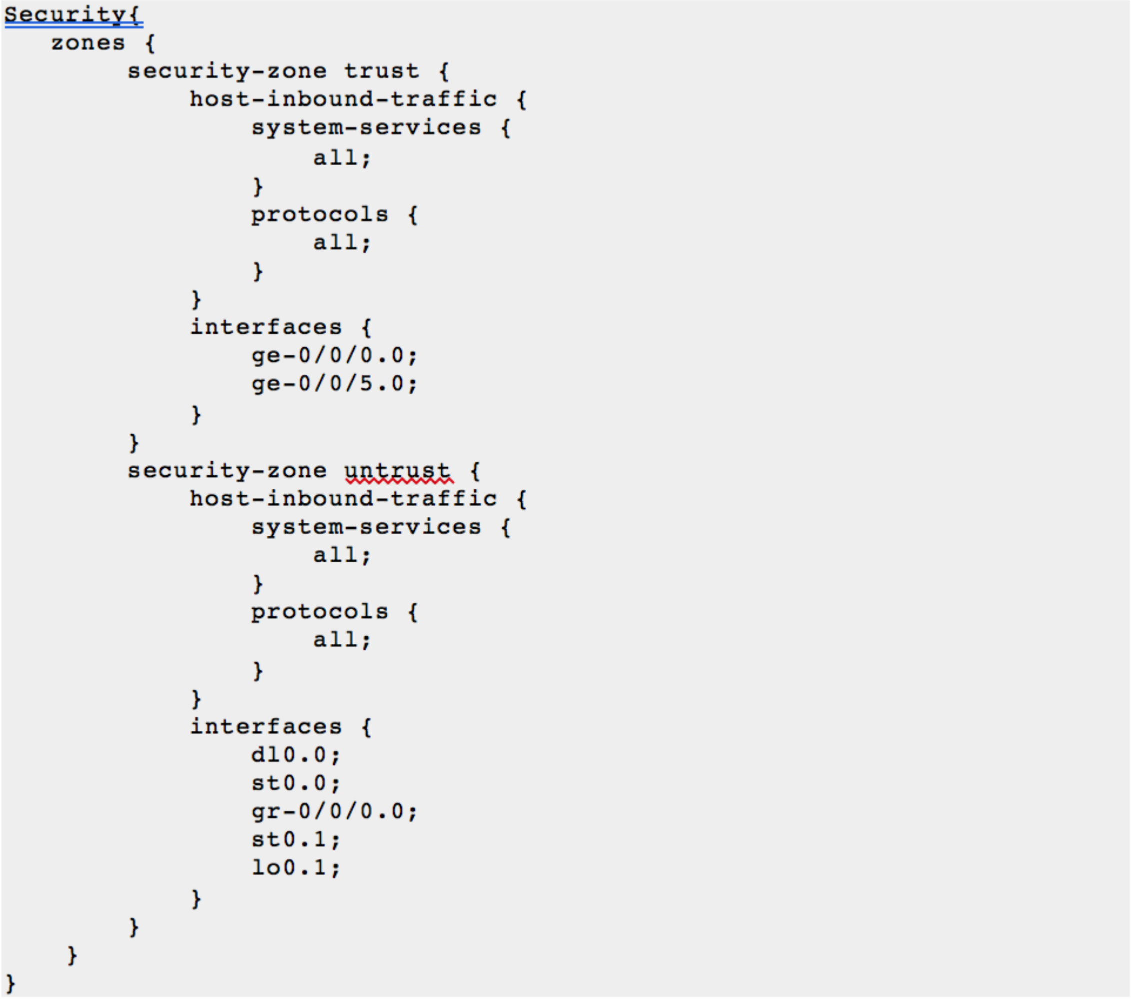
After this point, all communication between these two peers is sent through IPsec VPN tunnel and encrypted very securely from end- to- end.

Zones

A zone is a collection of one or more network segments sharing identical security requirements. Logical interfaces must be assigned to zones in order to accept and pass traffic. In one device, there can be multiple zones but a logical interface can be only assigned to one zone at the time. For each zone, different restrictions can be assigned as desired to accomplish needed security. For example, traffic can be rejected if it does not match the expected protocol. (Juniper Networks, 2016.)

In Figure 15 it can be seen that interfaces ge-0/0/0.0 and ge-0/0/5.0 are assigned to zone trust and all system services and protocols are allowed. This is because ge-0/0/0.0 is needed to transport all kind of traffic in the test situation and ge-0/0/5 is a trusted configuration interface. Interfaces assigned to security zone untrust on the other hand need to have strict guidelines which kind of traffic can pass if this solution were to be implemented. This can be defined because it is known exactly which kind of traffic to expect. For testing proposes all traffic in the untrust zone is allowed.

In the selective packet mode, the interface still needs to be placed in the zone even if it later on bypasses the Flow engine. The filter to select the packet mode processing needs to be applied in all customer facing IP interfaces as well as in the Generic Routing Encapsulation (GRE) tunnel interface.



```
Security{
   zones {
        security-zone trust {
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
                    all;
                }
            }
            interfaces {
                ge-0/0/0.0;
                ge-0/0/5.0;
            }
        }
        security-zone untrust {
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
                    all;
                }
            }
            interfaces {
                dl0.0;
                st0.0;
                gr-0/0/0.0;
                st0.1;
                lo0.1;
            }
        }
    }
}
```

Figure 15. Zones and traffic selectors in SRX 320 configuration

Zones used in SRX 1500 site are almost identical with its own interface names.

Policy

Traffic always enters one zone and exits from another or the same zone. A security policy is needed to enable the traverse and restrict traffic that is not allowed to use that route.

With policies traffic can be matched to strict criteria and accepted to pass or even rejected for good. For example, creating specific policy harmful traffic can be rejected.

As Figure 16 indicates, a broadly defined policy can allow all kinds of traffic from any source from a zone to any destination in another zone. Policies can also be very precise and strict as right side of Figure 16 indicates. A policy with exact timeframe only allowing certain type of traffic from specific source to specific destination. This allows a very high level of security.

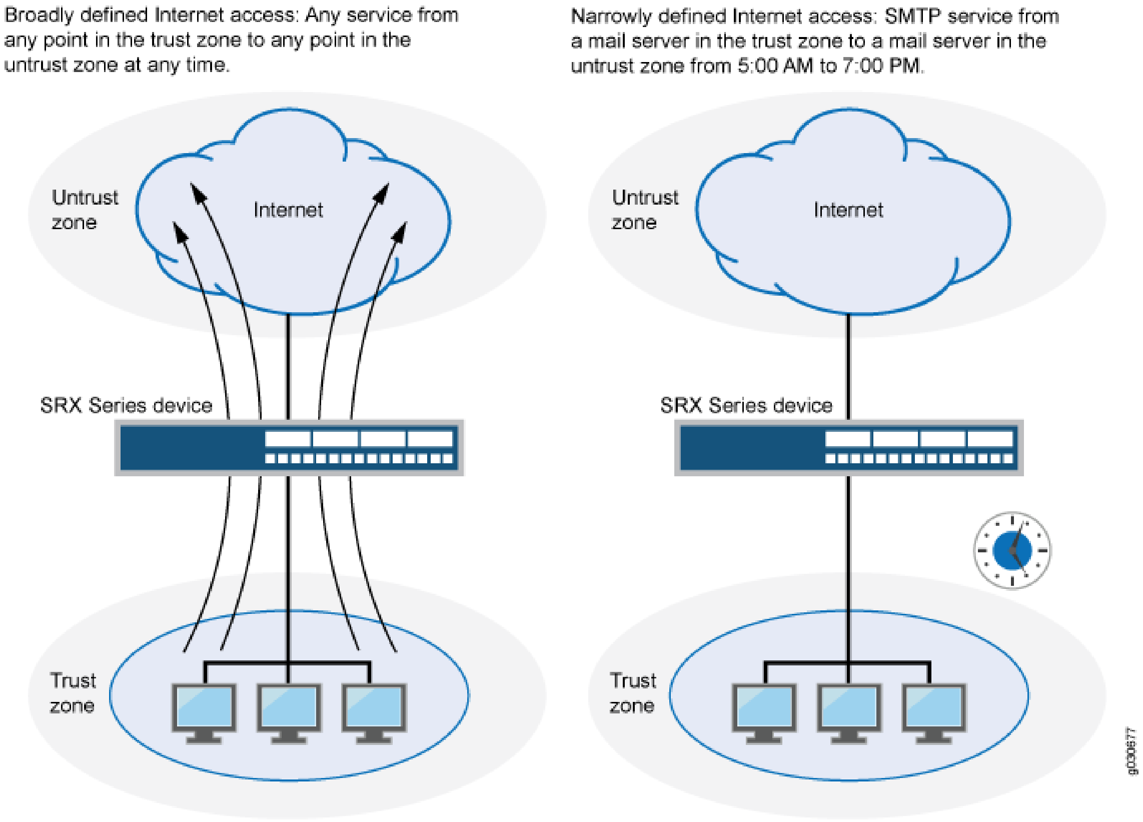
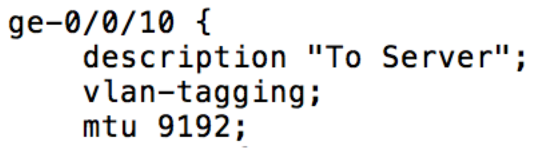

Broadly defined Internet access: Any service from any point in the trust zone to any point in the untrust zone at any time.
Narrowly defined Internet access: SMTP service from a mail server in the trust zone to a mail server in the untrust zone from 5:00 AM to 7:00 PM.
Untrust zone
Internet
SRX Series device
Trust zone
Untrust zone
Internet
SRX Series device
Trust zone
g030677

Figure 16. Policy can be very strict or broad (Juniper Networks, 2017).

In the final configuration, it was decided that all kind of traffic is okay to be allowed across all zones for the sake of testing a wide range of traffic. If a customer should adopt this solution all traffic should be restricted as much as it can be to achieve a high level of security. As seen in Appendix 1 and Appendix 2 both devices have all traffic allowed between or inter zone in policies section of configuration.

5.3 Interfaces

All SRX devices have two major categories of interfaces: permanent transient. Users cannot remove permanent interfaces, but can remove, change and move transient interfaces. A permanent interface is any interface that is always present on the device such as Ethernet interfaces. Transient interfaces are any interfaces that can be moved, removed or replaced by a user on the device, such interface would be LTE mini-PIM on this solution. All interfaces have a short name descripting its characteristics and are numbered by their position in the device. In Figure 3 and table 2, SRX 320 has 5 Ethernet interfaces on the front and they are named Gigabit Ethernet and a number. When configuring the device this can be seen as ge-0/0/0, ge-0/0/1 and so on, this can be seen in Figure 17. The part "ge" stands for Gigabit Ethernet and "0/0/0" stand for where it is located on the device. (Marschke & Reynolds, 2008, pp. 30-33.)



```
ge-0/0/10 {
    description "To Server";
    vlan-tagging;
    mtu 9192;
```

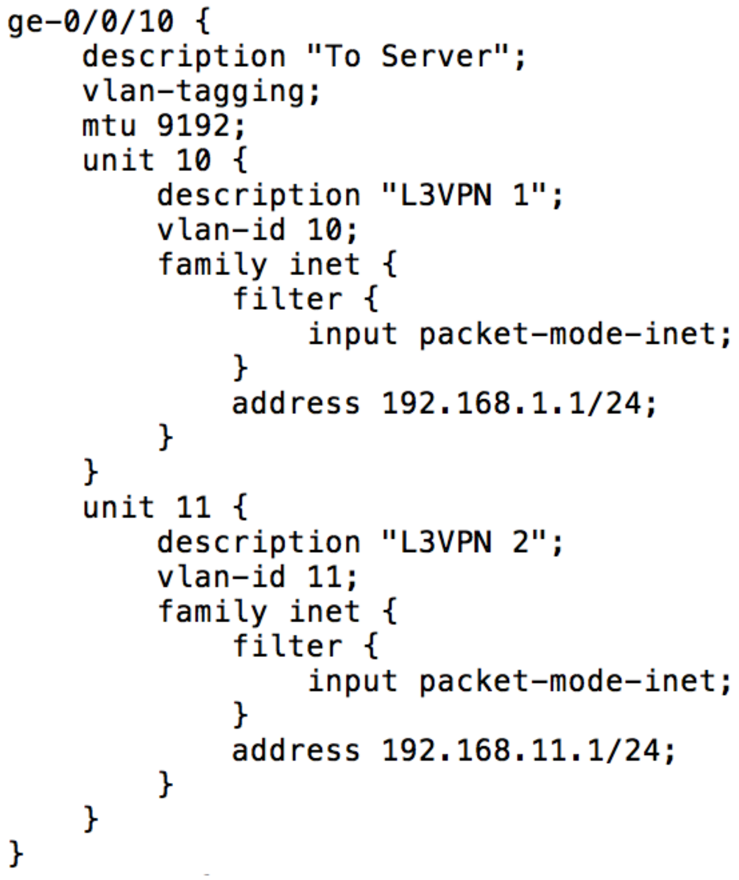
Figure 17. Permanent interface ge-0/0/10

All interfaces have two types of properties: physical and logical properties. Physical properties are tied to the entire port were as logical properties are only tied to certain logical portion represented by the unit number of logical interface.

Physical property on an interface is any property that should affect to the entire physical interface, such properties include:

- MTU values, Maximum Transmission Unit Limits the maximum size of frame that can be transmitted from the interface
- Encapsulation,
- Clocking, aligning bits as they are transmitted out of the interface

All interfaces that send or receive traffic require a logical unit configured as seen in Figure 18. The logical unit sort of splits the physical interface into many parts and allows multiple different configurations under the main physical one. For example, an Ethernet interface which is physical can be subdivided into multiple Virtual LANs (VLANs). All logical interfaces are separated by a period after the main interface. All IP addresses and configurations that are logical are added under sub-interface.



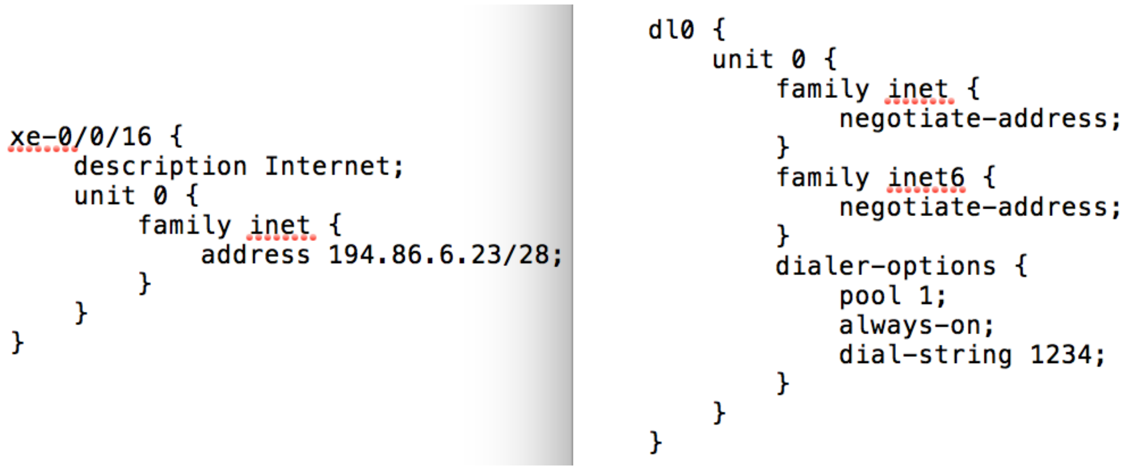
```
ge-0/0/10 {
    description "To Server";
    vlan-tagging;
    mtu 9192;
    unit 10 {
        description "L3VPN 1";
        vlan-id 10;
        family inet {
            filter {
                input packet-mode-inet;
            }
            address 192.168.1.1/24;
        }
    }
    unit 11 {
        description "L3VPN 2";
        vlan-id 11;
        family inet {
            filter {
                input packet-mode-inet;
            }
            address 192.168.11.1/24;
        }
    }
}
```

Figure 18. Logical units configured in final configuration.

Outside connection interfaces

This configuration has many important interfaces which use various protocols and functions. For everything to work there has to be internet access that is handled by the LTE card on the SRX 320 site and by Ethernet port on the SRX 1500 site. The LTE card is shown in configuration as cl-0/0/2 which has physical properties e.g. radio access and the logical interface of the LTE card is dl0 which has address negotiation options.

On the SRX 1500 there is xe-0/0/16 which stands for 10 Gigabit Ethernet interface connecting to internet with public IP assigned by Internet Service Provider (ISP). Both outside connecting interfaces can be seen in Figure 19.



```
xe-0/0/16 {
    description Internet;
    unit 0 {
        family inet {
            address 194.86.6.23/28;
        }
    }
}
```

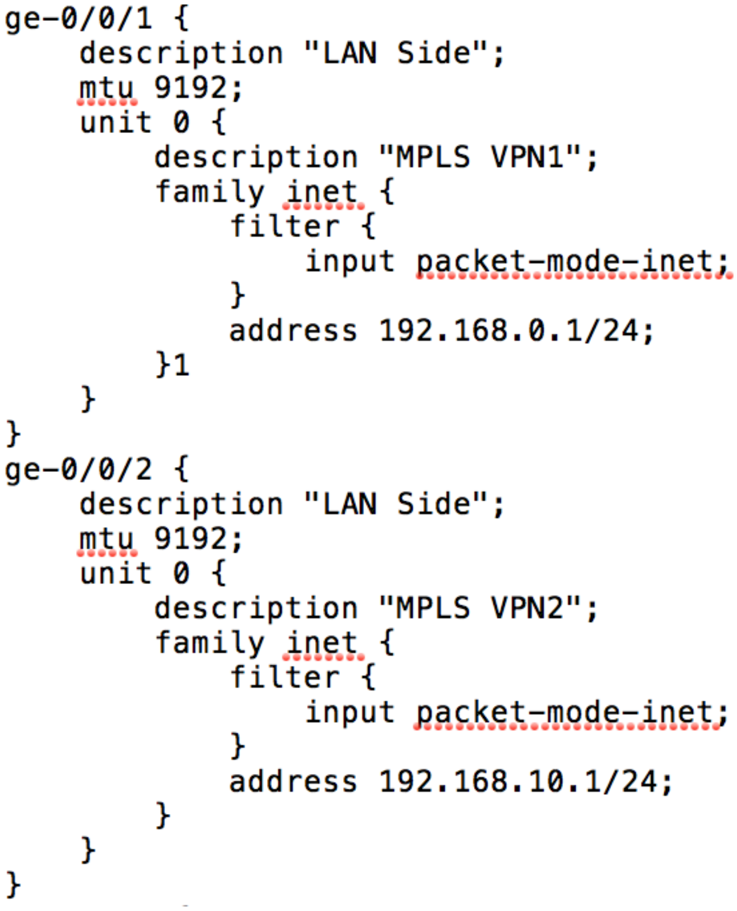
```
dl0 {
    unit 0 {
        family inet {
            negotiate-address;
        }
        family inet6 {
            negotiate-address;
        }
        dialer-options {
            pool 1;
            always-on;
            dial-string 1234;
        }
    }
}
```

Figure 19. SRX 1500 (left) and SRX 320(right) connection to internet.

Client interfaces

Then there are the client side interface on both sides. The client interface is an interface where a customer physically attaches a computer or any device. Currently these client interfaces do not hand out IP addresses but Dynamic Host Configuration Protocol (DHCP) service would be easy to set up for any customer that desires so in the future. Now handling of IP addresses is done manually by setting a fixed IP on the router and client device.

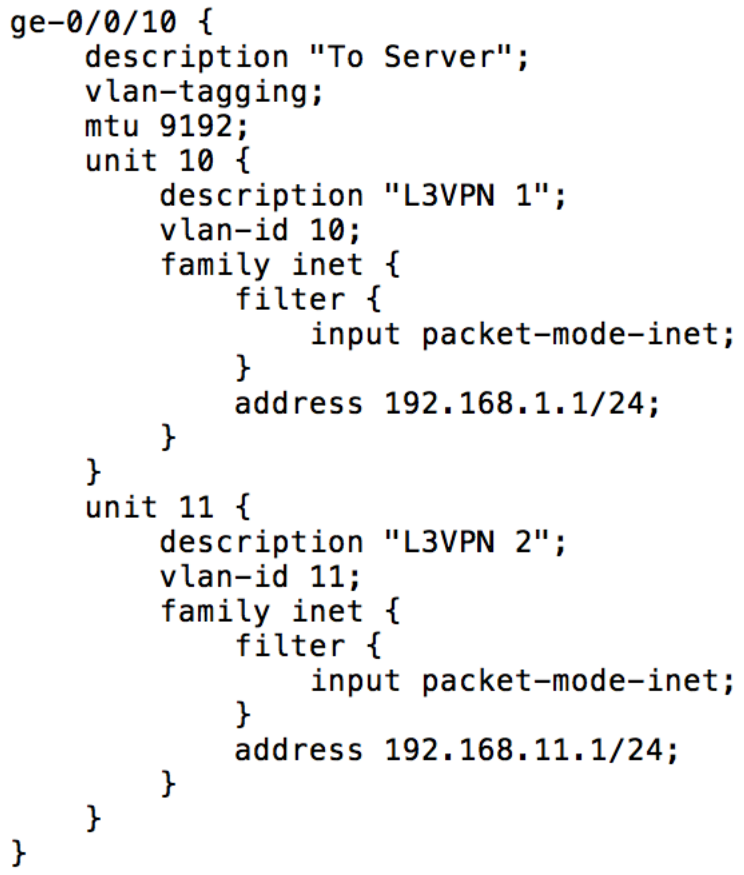
SRX 320 site has two ports that are configured for customer use, ge-0/0/1 and ge-0/0/2 (Figure 20). Both ports have their own IP address and are part of different routing instances. This is done so that it can be tested and verified if multiple networks can be transferred over this solution. Both interfaces have been configured to use firewall filter to assign traffic to the packet mode.



```
ge-0/0/1 {
    description "LAN Side";
    mtu 9192;
    unit 0 {
        description "MPLS VPN1";
        family inet {
            filter {
                input packet-mode-inet;
            }
            address 192.168.0.1/24;
        }1
    }
}
ge-0/0/2 {
    description "LAN Side";
    mtu 9192;
    unit 0 {
        description "MPLS VPN2";
        family inet {
            filter {
                input packet-mode-inet;
            }
            address 192.168.10.1/24;
        }
    }
}
```

Figure 20. Client interface configuration on SRX 320

SRX 1500 site has only one interface configured for client, ge-0/0/10. This is done because it was necessary to test how well traffic can transfer from two networks to one end point. This client port still has two IP addresses, they are configured under logical units 10 and 11 as seen in Figure 21. Two IP addresses are used because these logical units still belong to different networks. As SRX 320 has two client interfaces so does SRX 1500, but they are both tied to same physical interface instead of two separate interfaces as with SRX 320.

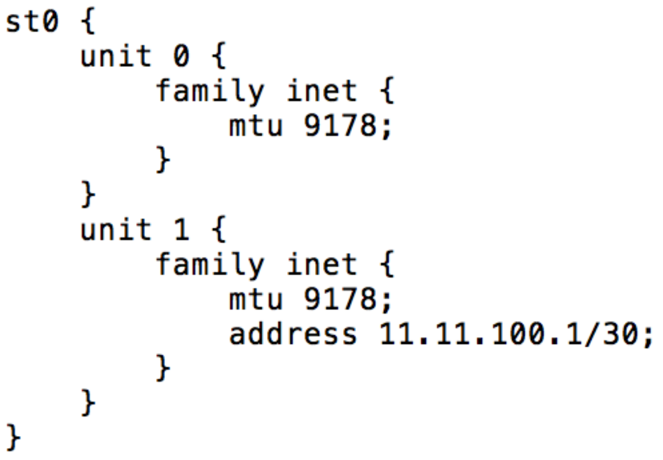


```
ge-0/0/10 {
    description "To Server";
    vlan-tagging;
    mtu 9192;
    unit 10 {
        description "L3VPN 1";
        vlan-id 10;
        family inet {
            filter {
                input packet-mode-inet;
            }
            address 192.168.1.1/24;
        }
    }
    unit 11 {
        description "L3VPN 2";
        vlan-id 11;
        family inet {
            filter {
                input packet-mode-inet;
            }
            address 192.168.11.1/24;
        }
    }
}
```

Figure 21. SRX 1500 client network configuration

Tunnel interfaces

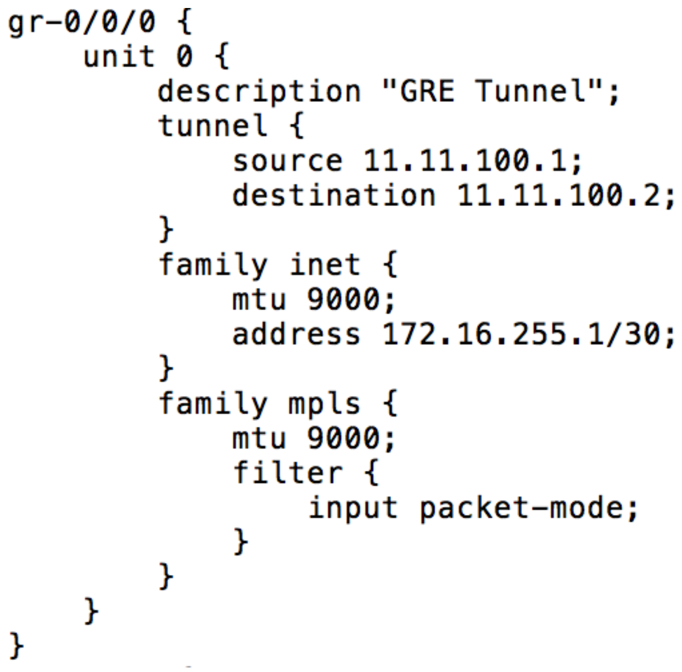
IPSec VNP is bound to the virtual interface st0.0 (Figure 22) on both SRXs. St0 stands for secure tunnel interface and all traffic routed into the interface will be sent to VPN. Both st0.1 interfaces have IP addresses that belong to the same subnet.



```
st0 {
    unit 0 {
        family inet {
            mtu 9178;
        }
    }
    unit 1 {
        family inet {
            mtu 9178;
            address 11.11.100.1/30;
        }
    }
}
```

Figure 22. St0 configuration on SRX 320

GRE tunnel requires a special gr-0/0/0 pseudo interface. This specific interface is used for GRE protocol which creates a tunnel and enables the transports of a variety of Layer 3 protocols. Gr interface is always configured with the source IP address for GRE packets, destination address of the tunnel and the families of protocols that will be transported in the protocol. The GRE tunnel configuration in this case carries IP traffic and MPLS traffic over the network. The tunnel is configured with the source IP address of 11.11.100.1 and a destination address of 11.11.100.2, both IP addresses belong to IPSec because the aim was to do IPSec over GRE tunnel (Figure 23). It is worth noticing that on SRX 1500 source and destination IP addresses on GRE tunnel are flipped because the source address for GRE packets is backwards.



```
gr-0/0/0 {
    unit 0 {
        description "GRE Tunnel";
        tunnel {
            source 11.11.100.1;
            destination 11.11.100.2;
        }
        family inet {
            mtu 9000;
            address 172.16.255.1/30;
        }
        family mpls {
            mtu 9000;
            filter {
                input packet-mode;
            }
        }
    }
}
```

Figure 23. GRE tunnel configuration on SRX 320

Loopback interfaces

The loopback interface in the JunOS device has a special role. It is a logical interface which never goes down and because of this it is usually configured for routing protocols. There is no real transit traffic going through the device via the loopback interface. For example, Open Shortest Path First (OSPF) uses the loopback address as its router ID in case it is configured on the device. Another common example for using the loopback interface is using it as a peering interface which is used to form a BGP neighbour adjency. When a BGP session uses the loopback interface as a peering address it relies on the underlying OSPF routing protocol to manage connectivity between the loopback addresses with an optimal route through the network. This way the underlying OSPF topology can preserve the logical BGP connectivity in the case of connectivity failure or equipment failure.

In JunOS the loopback interface also has a special role for the control plane protection to prevent access for unwanted management access, protocol usage or denial of service (DOS). Control plane protection with loopback filtering is not covered in this thesis.

There can be only one loopback interface per routing instance on JunOS device for simplicity. Adding multiple loopback interface units will result in failed commit of the configuration. A loopback interface was configured on all routing instances to enable simple end-to-end ping testing between the simulated customer networks.

Other used interfaces

On SRX 320 other interfaces can be seen in use as well. These interfaces serve various purposes such as:

- Ge-0/0/0, Is used for testing normal internet connectivity and performance for LTE. (port1)
- Ge-0/0/3 is used for VPLS which is might be implement to solution in the future, all configuration to make up work is already in place (port 3)
- Ge-0/0/5 is used to configure SRX 320 with SSH from inside network.

SRX 1500 also has one “extra” interface for use, fxp0 it is the dedicated out of band management port for it.

5.4 Routing Protocols

Routing Protocols are about making network functional and they allow sending traffic across the network. Some protocols even allow controlling how traffic is sent from network.

MPLS Technology

Multi-Protocol Label Switching (MPLS) is about using some old technologies and some new technologies. The power of MPLS really comes from using the best of both worlds. MPLS network works differently from normal Internet Protocol (IP) networks, by far. Normal IP Networks operate by looking up address information on received packets and looking up the next hop for that address in a routing table. After this it sends the packet to the next hop router based on the final destination address. (Bushong, et al., 2008, p. 268.)

In a label-switched network routing operations are similar but are not forwarded by the hop-by-hop basis. Each packet is assigned a label and is forwarded by Label Switching

Router (LSR). LSR looks up where the packet is coming from on the label and where is it going, assigns it to same path as everything else coming from the same source and going to the same destination by the label. By doing this the router needs to only keep track of what routers have been established through it and never need to do forwarding lookup. (Bushong, et al., 2008, pp. 268-270.)

MPLS might sound complicated and confusing but it is really simple in its core. Here is a quick look on how label-switching network works.

- MPLS enabled router attaches a label to each outgoing packet.
- MPLS enabled router then uses this label to look up where to forward the packet (instead of destination IP address).
    - Labels must be unique to any specific physical link. To perform lookup MPLS enabled router uses both port and label information.
- By repeating this forwarding process packet traverses along path that has been set up in the network.

MPLS also enables the creation of fully separated and independent Virtual Private Network (MPLS VPN) within one physical network. This feature enables the required criteria of multiple networks within one connection over LTE to our remote office solution. This feature of MPLS is called Virtualization and it has more perks to it than previously mentioned capability including:

- Fast adding of new networks, which may result from business integrations or acquisitions.
- Security zones between networks, enabling access management.
- Quick provisioning of new services over the connection without involvement of your service provider

It is important to note that MPLS only works in packet based forwarding. All packets that come from client interfaces (ge-0/0/1-2 on SRX 320) all inspected when they arrive and dropped to packet mode so MPLS can do its magic. After this change to the packet mode and MPLS fuctions, IPsec and GRE are applied to encrypt and forward the packet. (Juniper Networks, 2017)

LDP

Label Distribution Protocol (LDP) is an MPLS-specific protocol that Label Switching Routers (LSR) can use to exchange information about labels for each packet so they can assign correct labels to each of their forwarding paths and form label-switched paths (LSP). LDP shares information to other MPLS routers show they can establish Label Information Base (LIB).

LDP requires existing Internal Gateway Protocol (IGP) configuration to work which means one has to get OSPF or Intermediate System-to-Intermediate System (IS-IS) running first. LDP is configured on same interfaces as IGP. When LDP and IGP are configured on interface successfully, the interface_begins to transmit and receive LDP messages. LDP starts of by sending LDP discovery message to all the LDP enabled interfaces. When an adjacent router receives the discovery message, it starts a simple 3-way Transmission Control Protocol (TCP) handshake and establishes a TCP session with the source router.

Once the TCP session for LDP is established, the routers begin sharing label mapping information which contains IPv4 prefixes for MPLS labels and they form Label Information Databases (LIB) on every router. And when the topology changes, an LDP message is generated that allows the generation of alternative path. (Bushong, et al., 2008, p. 274.)

BGP

Border Gateway Protocol (BGP) is a protocol that connects different autonomous systems (AS) to each other on top of other protocols such as OSPF or IS-IS. BGP is used as External or Internal meaning that, external (eBGP) is used to connect two different AS. Internal (iBGP) is used to create paths inside AS from one PE to another PE, ultimately creating full mesh. BGP is usually used on loopback interfaces of routers because it stays up as long as router is up. If iBPG is mapped inside ISP core and a link would go down a new route would be established using OSPF or IS-IS but BGP session stays up and unaffected. (TechTarget, 2017.)

BGP is used in this solution to carry routing information for multiple network layers between two routers used in solution. BGP adjacency is formed on loopback addresses of the routers, because as long as the device is up the loopback interface is also up. As the routers belong to the same AS is iBGP used here. BGP's main task is to carry information about routing instances and OSPF areas over this network so connections can be made across.

BGP is used in this solution to carry information about customer networks across VPN tunnel. iBGP adjacency is formed on loopback interfaces of edge routers because as long as the device is up, the loopback address is also up. Internal BGP's task is to carry routing tables of the customers' network across the VPN tunnel. (Juniper Networks, 2016.)

5.5 Routing Instances

Routing Instances are collections of routing tables, interfaces and routing protocol parameters. Routing instances are often pictured as virtual routers inside a router. Each Routing instance has to have unique name because IP table is formed after that name. For example, if a routing instance is configured with the name “routing-instance1”, the corresponding IP table is formed “routing-instance1.inet.0”. (Juniper Networks, 2014.)

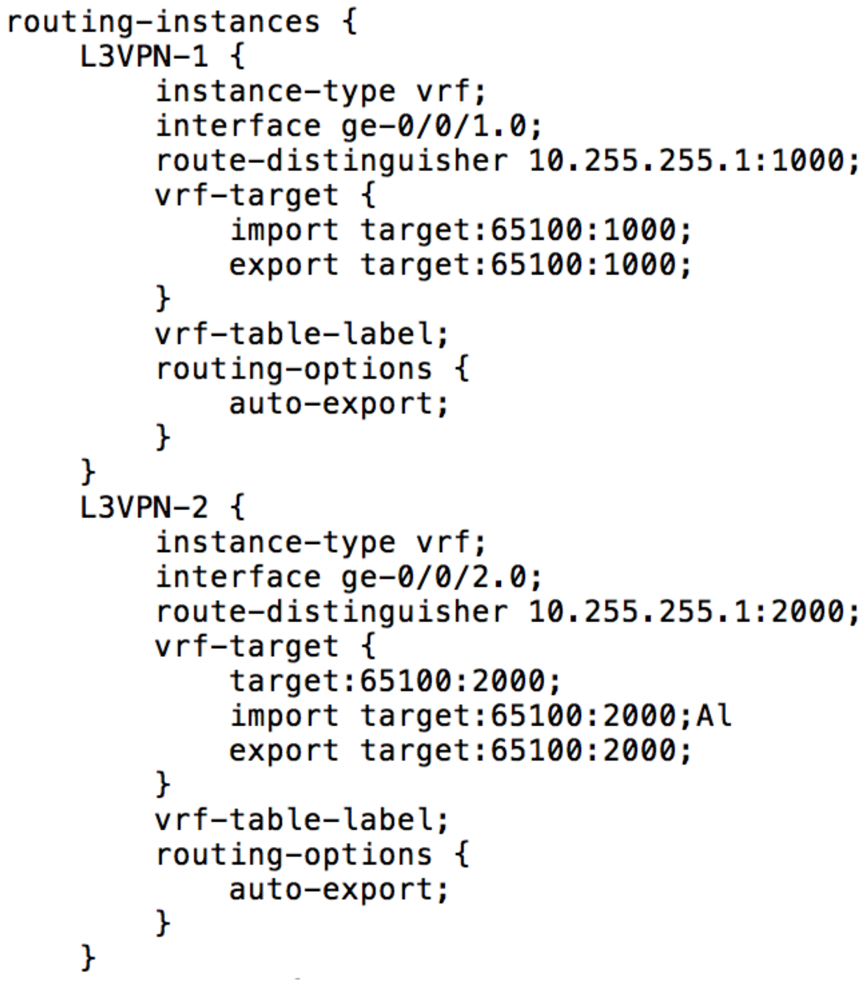
Routing instances come in 12 different types. Here are some types that are often used:

- Virtual router, is used for non-VPN related applications, basic traffic forwarding.
- VPLS, is Used to create point-to-multipoint LAN implementations between a set of sites in a VPN.
- Virtual Routing and Forwarding (VRF), is used for Layer 3 VPN implementations. This routing instance has VPN routing table as well as VPN forwarding table.

This solution uses two VRF routing instances for customer networks and one VPLS is configured for future implementations. For now, the focus is on the VRF type routing instance and covering why certain parameters are configured.

VRF requires route-distinguisher and route-target parameters to be configured or else applying configuration using commit command will not go through. VRF is used to overcome the problem of overlapping networks. For example, in this configuration both sides use 192.168.0.0/24 as their local network. Each customer can be assigned its very own VRF so that overlapping networks are kept isolated from each other in their own routing instances L3VPN-1 and L3VPN-2.

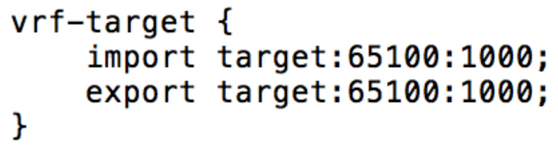
This is really usefull but a way to keep track of which 192.168.0.0/24 route belong to which VRF is needed. This is where the route-disguiser (RD) parameter is used. As the name RD implies, RD is used to recognise which route belong to which VRF. As seen in Figure 24, on both VRF routing instances a parameter “route-distinguisher” is configured with IP address and distinguisher number to keep track of which local network belong to which VRF.



```
routing-instances {
    L3VPN-1 {
        instance-type vrf;
        interface ge-0/0/1.0;
        route-distinguisher 10.255.255.1:1000;
        vrf-target {
            import target:65100:1000;
            export target:65100:1000;
        }
        vrf-table-label;
        routing-options {
            auto-export;
        }
    }
    L3VPN-2 {
        instance-type vrf;
        interface ge-0/0/2.0;
        route-distinguisher 10.255.255.1:2000;
        vrf-target {
            target:65100:2000;
            import target:65100:2000;Al
            export target:65100:2000;
        }
        vrf-table-label;
        routing-options {
            auto-export;
        }
    }
```

Figure 24. Routing instances used in configuration and their parameters.

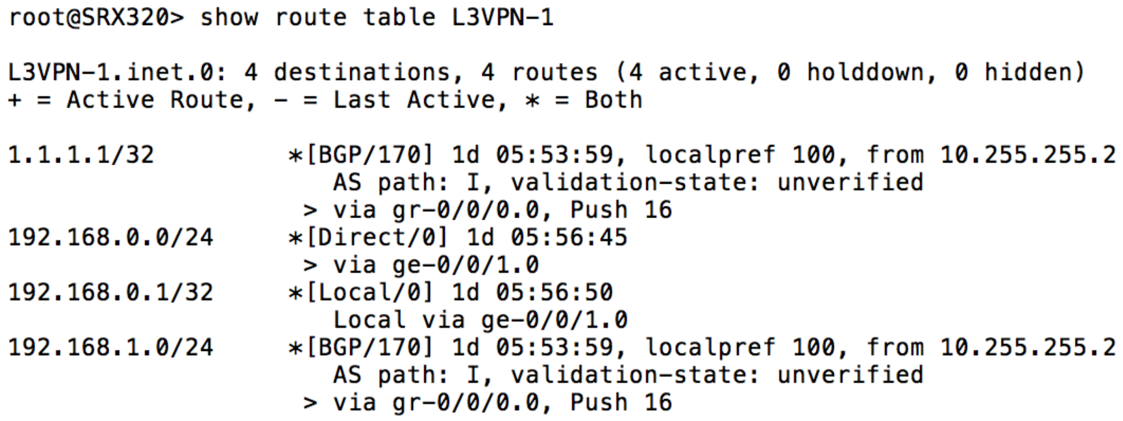
VRF route-target is used to share routes among different VRFs. The route target has a local AS number and a route target value. Import target means which routes are sent and export target means which routes can be learned from other VRFs. In this configuration export and import parameters are the same because the aim is to keep these networks separate as they mimic two different clients (figure 25). (Packetlife.net, 2013.)



```
vrf-target {
    import target:65100:1000;
    export target:65100:1000;
}
```

Figure 25. Import and Export targets on vrf-target configuration under routing instances.

If it is necessary to check if VRF instances really work as they should the show table command can be issued on SRX 320 for L3VPN-1 to see if any routes have been learned from SRX 1500 (Figure 26).



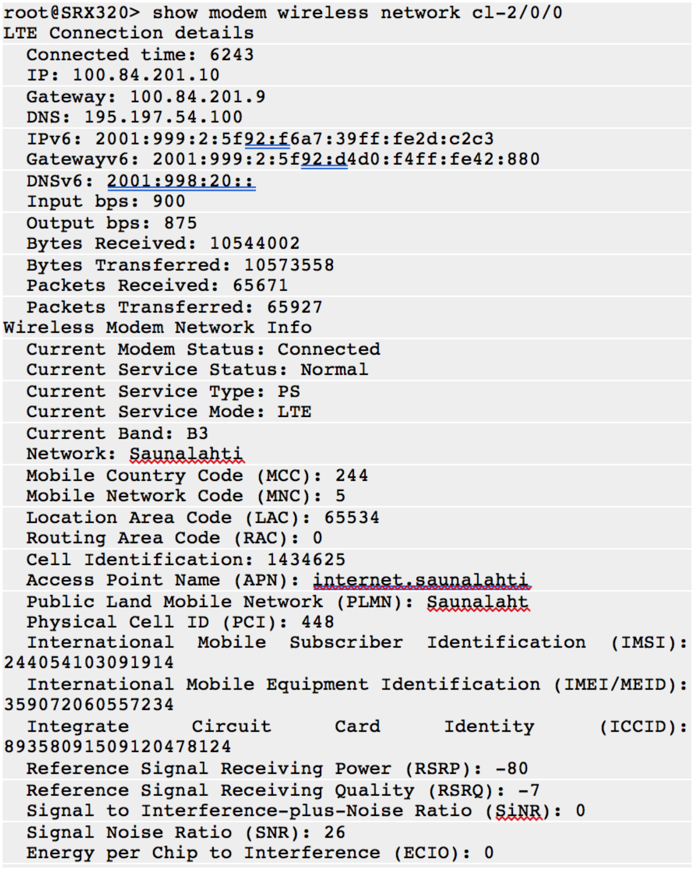
```
root@SRX320> show route table L3VPN-1

L3VPN-1.inet.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

1.1.1.1/32         *[BGP/170] 1d 05:53:59, localpref 100, from 10.255.255.2
                      AS path: I, validation-state: unverified
                    > via gr-0/0/0.0, Push 16
192.168.0.0/24     *[Direct/0] 1d 05:56:45
                    > via ge-0/0/1.0
192.168.0.1/32     *[Local/0] 1d 05:56:50
                      Local via ge-0/0/1.0
192.168.1.0/24     *[BGP/170] 1d 05:53:59, localpref 100, from 10.255.255.2
                      AS path: I, validation-state: unverified
                    > via gr-0/0/0.0, Push 16
```

Figure 26. L3VPN-1 routing table on SRX 320

As can be seen in the routing table of L3VPN-1, a new route is learned through BGP, 192.168.1.0/24 network and 1.1.1.1 the loopback address on lo0.0 on SRX 1500.

5.6 Checking Configuration

As of now everything is configured and needs to be checked that the connection indeed has been established and the system works as intended. First and foremost, one has to check if all wires are connected, LTE card is connected and has lights. It is important to notice that all show commands are issued on SRX 320 here, issuing commands on 1500 is irrelevant because if the configuration works it can be proven on one device. The next step is to verify the LTE mini-PIM signal and if it has connectivity to internet. By issuing the command "show modem wireless network cl-2/0/0" as seen in Figure 27 the LTE mini-PIM has received an IP address 100.84.201.10 from ISP. LTE mini-PIM has also received lots of other information including gateway, DNS and IPv6 address.



```
root@SRX320> show modem wireless network cl-2/0/0
LTE Connection details
  Connected time: 6243
  IP: 100.84.201.10
  Gateway: 100.84.201.9
  DNS: 195.197.54.100
  IPv6: 2001:999:2:5f92:f6a7:39ff:fe2d:c2c3
  Gatewayv6: 2001:999:2:5f92:d4d0:f4ff:fe42:880
  DNSv6: 2001:998:20::
  Input bps: 900
  Output bps: 875
  Bytes Received: 10544002
  Bytes Transferred: 10573558
  Packets Received: 65671
  Packets Transferred: 65927
Wireless Modem Network Info
  Current Modem Status: Connected
  Current Service Status: Normal
  Current Service Type: PS
  Current Service Mode: LTE
  Current Band: B3
  Network: Saunalahti
  Mobile Country Code (MCC): 244
  Mobile Network Code (MNC): 5
  Location Area Code (LAC): 65534
  Routing Area Code (RAC): 0
  Cell Identification: 1434625
  Access Point Name (APN): internet.saunalahti
  Public Land Mobile Network (PLMN): Saunalaht
  Physical Cell ID (PCI): 448
  International  Mobile  Subscriber  Identification  (IMSI):
244054103091914
  International Mobile Equipment Identification (IMEI/MEID):
359072060557234
  Integrate     Circuit     Card     Identity     (ICCID):
89358091509120478124
  Reference Signal Receiving Power (RSRP): -80
  Reference Signal Receiving Quality (RSRQ): -7
  Signal to Interference-plus-Noise Ratio (SiNR): 0
  Signal Noise Ratio (SNR): 26
  Energy per Chip to Interference (ECIO): 0
```

Figure 27. LTE mini-PIM connection info

As seen in Figure 27 is also "Wireless Modem Network Info". Under this section there is a lot of important information:

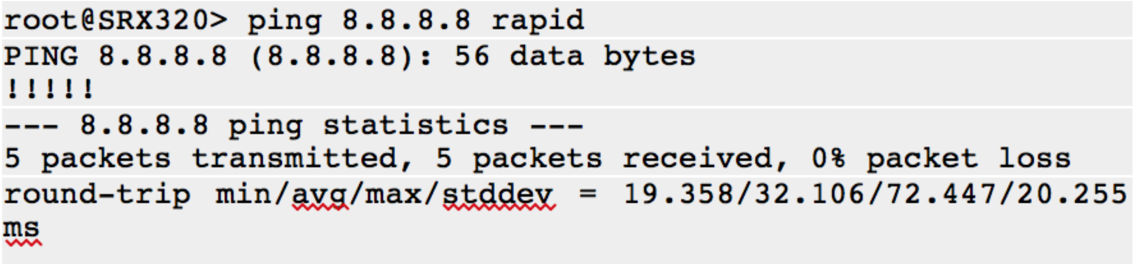
- Current Band: B3, refer to Table 3.
- Current network: Saunalahti
- Access Point Name (APN): internet.saunalahti

And near bottom of the output as seen in Figure 27 there is Signal to Noise Ratio (SNR) which tells signal quality and strength. Alone this number which SNR presents tells nothing to but paired with the information provided in Table 4 a solid verdict can be formed to judge if signal is enough.

Table 4. Chart to determinate if signal is any good

SNR VALUE	VERDICT
> 20 dB	High Signal
13 to 20 dB	Medium Signal
0 to 13 dB	Low Signal
< 0 dB	Poor Signal

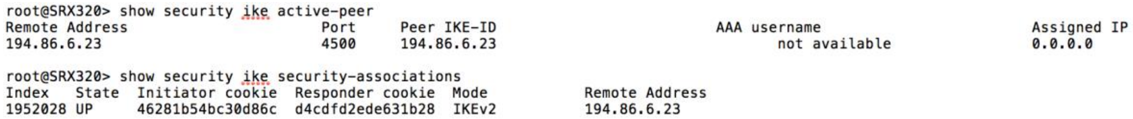
Next it is good to test the connection by pinging to some IP on internet so connection to internet can be determined. For this test, one would ping Google's DNS service 8.8.8.8 by issuing the command "ping 8.8.8.8 rapid". As seen in Figure 28 the ping has successfully done 5 tests and the packet loss was 0%.



```
root@SRX320> ping 8.8.8.8 rapid
PING 8.8.8.8 (8.8.8.8): 56 data bytes
!!!!!
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 19.358/32.106/72.447/20.255
ms
```

Figure 28. Ping test run on SRX 320 to 8.8.8.8 (Google DNS)

Now that connectivity to outside world has been firmly established the next up in the hierarchy is IKE. By issuing the command "show security ike active-peer" As seen in Figure 29 the IKE is up and a peer has been established.

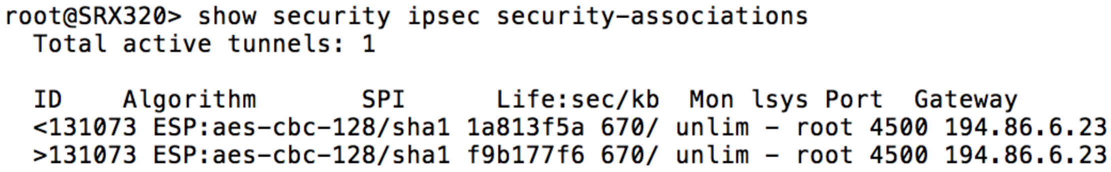


```
root@SRX320> show security ike active-peer
Remote Address                        Port     Peer IKE-ID                         AAA username                   Assigned IP
194.86.6.23                           4500     194.86.6.23                                 not available          0.0.0.0

root@SRX320> show security ike security-associations
Index    State  Initiator cookie  Responder cookie  Mode           Remote Address
1952028 UP      46281b54bc30d86c  d4cdfd2ede631b28  IKEv2          194.86.6.23
```

Figure 29. Checking if IKE is active and working.

As seen in Figure 29 there is also the “show security ike security-associations” command which shows cookies and mode used.

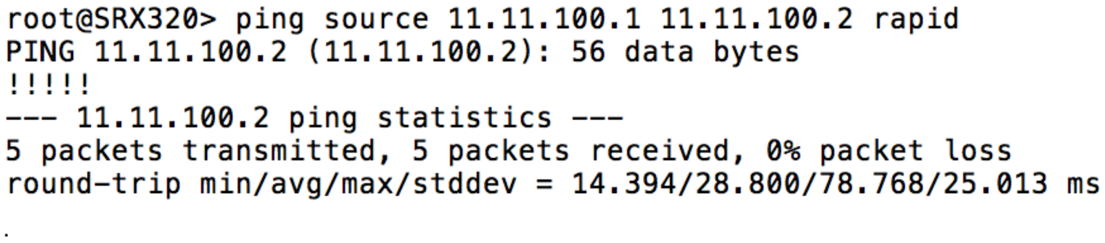
When the IKE peer has been established so has IPSEC as well. As seen in Figure 30 one tunnel is active between the peers.



```
root@SRX320> show security ipsec security-associations
  Total active tunnels: 1

  ID     Algorithm       SPI      Life:sec/kb  Mon lsys Port  Gateway
  <131073 ESP:aes-cbc-128/sha1 1a813f5a 670/ unlim - root 4500 194.86.6.23
  >131073 ESP:aes-cbc-128/sha1 f9b177f6 670/ unlim - root 4500 194.86.6.23
```

Figure 30. Checking that IPSec tunnel is established

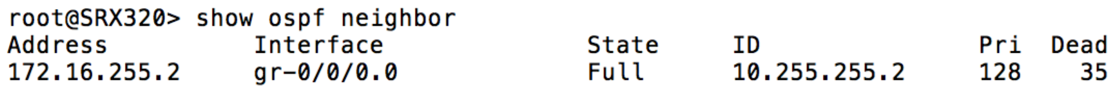
Now that **a** working IPSEC tunnel has been established, a ping test can be run over it to confirm that it works. The ping test is run from the origin of tunnel (st0.1) to the end of tunnel (st0.1 on SRX 1500). As seen in Figure 31 there is connectivity from one end to another.



```
root@SRX320> ping source 11.11.100.1 11.11.100.2 rapid
PING 11.11.100.2 (11.11.100.2): 56 data bytes
!!!!!
--- 11.11.100.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 14.394/28.800/78.768/25.013 ms
.
```

Figure 31. Ping test through IPSec tunnel

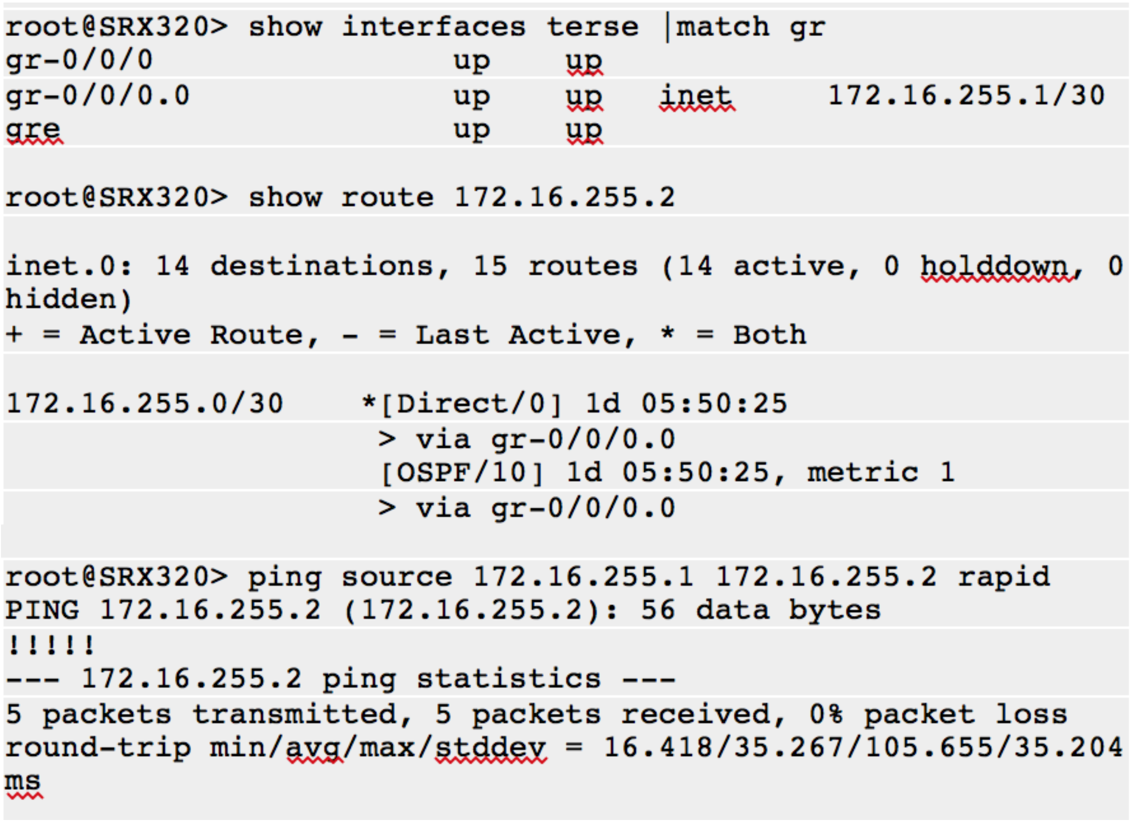
Now that the tunnel is open it can be expected to have a new OSPF neighbour also. This can be figured out by issuing the command “show ospf neighbour” as seen in Figure 32.



```
root@SRX320> show ospf neighbor
Address          Interface              State     ID               Pri  Dead
172.16.255.2     gr-0/0/0.0             Full      10.255.255.2     128    35
```

Figure 32. Checking for OSPF neighbor

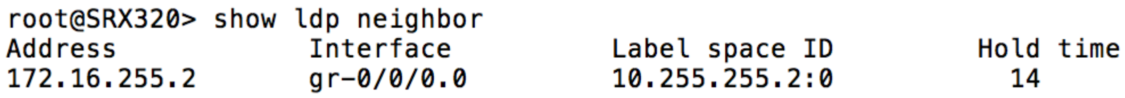
The next step is the GRE tunnel, as for that the first thing is to verify if the gr interface is up by issuing the command “show interfaces terse |match gr”, as can be seen in Figure 33 gr-0/0/0 is up. Also in Figure 33 it can be seen that the ping test from the tunnel interface to the other side was completed successfully.



```
root@SRX320> show interfaces terse |match gr
gr-0/0/0                up    up
gr-0/0/0.0              up    up   inet     172.16.255.1/30
gre                     up    up

root@SRX320> show route 172.16.255.2

inet.0: 14 destinations, 15 routes (14 active, 0 holddown, 0
hidden)
+ = Active Route, - = Last Active, * = Both

172.16.255.0/30    *[Direct/0] 1d 05:50:25
                    > via gr-0/0/0.0
                    [OSPF/10] 1d 05:50:25, metric 1
                    > via gr-0/0/0.0

root@SRX320> ping source 172.16.255.1 172.16.255.2 rapid
PING 172.16.255.2 (172.16.255.2): 56 data bytes
!!!!!
--- 172.16.255.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 16.418/35.267/105.655/35.204
ms
```

Figure 33. GRE tunnel state and ping test to test tunnel

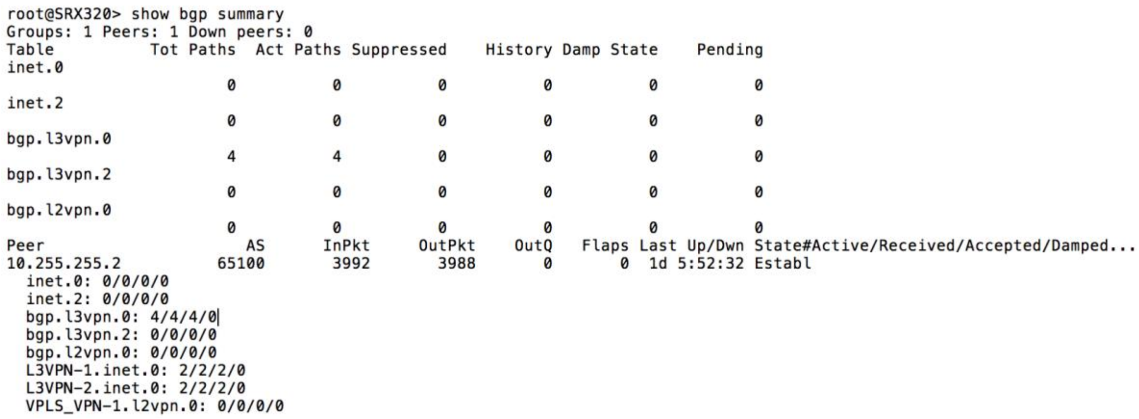
Next is the LDP neighbour, the LDP neighbour is found out by issuing the command “show ldp neighbour” as shown in Figure 34



```
root@SRX320> show ldp neighbor
Address            Interface          Label space ID         Hold time
172.16.255.2       gr-0/0/0.0         10.255.255.2:0           14
```

Figure 34. Checking for LDP neighbor

Next is the BGP summary, this is the most exciting of all of the verify connectivity tests. If everything is well in here, an assumption can be made to say almost for sure the solution is connected as intended. The BGP summary is done by issuing the command “show BGP summary” as seen in Figure 35. From the “show bgp summary” command output it can be seen that there are no other than the total L3 VPN routes learned in the network. By looking at the peer 10.255.255.2 in more detail summary state it can be seen for this specific BGP neighbour. Two L3 VPN instances that have been configured in the device L3VPN-1 and L3VPN-2 are seen on the list with both VRF instances having two active/received/accepted prefixes. This means that routing information is correctly passed between the neighbours and these two routes should also be visible on the corresponding individual routing table.



```
root@SRX320> show bgp summary
Groups: 1 Peers: 1 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
inet.0
                       0          0          0          0          0          0
inet.2
                       0          0          0          0          0          0
bgp.l3vpn.0
                       4          4          0          0          0          0
bgp.l3vpn.2
                       0          0          0          0          0          0
bgp.l2vpn.0
                       0          0          0          0          0          0
Peer                     AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn State#Active/Received/Accepted/Damped...
10.255.255.2          65100       3992       3988       0       0  1d 5:52:32 Establ
  inet.0: 0/0/0/0
  inet.2: 0/0/0/0
  bgp.l3vpn.0: 4/4/4/0
  bgp.l3vpn.2: 0/0/0/0
  bgp.l2vpn.0: 0/0/0/0
  L3VPN-1.inet.0: 2/2/2/0
  L3VPN-2.inet.0: 2/2/2/0
  VPLS_VPN-1.l2vpn.0: 0/0/0/0
```

Figure 35. BGP summary seen on SRX 320

Also for more detailed information about the customer networks merging the command “show route table L3VPN-1” can be used to see if the IPSEC VPN has learned any routes to and from the network that was desired to merge. By issuing the command “show route table L3VPN-2” information about other routing table as well can be seen.

6 Performance Testing

Performance testing aims to improve performance and throughput compared to normal throughput straight to internet speed testing services, in other words speed without IPSec VPN. All testing was done by using iPerf3 and speedtest.net service. iPerf3 is a tool for actively measuring the maximum achievable bandwidth on an IP Network. And speedtest.net is an internet service to quickly test the maximum bandwidth on internet connection. Some loss in bandwidth in tests is expected on the IPSEC VPN connection due to heavy headers which increase the size of packets.

6.1 Setup

This section describes the testing environment, programs used and the initial measurements of connection. The testing environment was mostly controlled but the only thing that could not be affected was the local mobile internet connectivity and speed. During some parts of the day mobile networks can be crowded and speeds are decreased heavily. In Appendix 3 the topology used on the testing can be seen, here are some important notes about the topology:

- SRX 1500 has 1Gigabit link, which means 1000Mbits/sec of download and 1000Mbits/sec uplink, so it is not bottleneck for testing.
- Ge-0/0/1 is connected to testing laptop and ge-0/0/10 is connected to server.
- VPLS VPN performance is not tested but if IPSEC VPN works so does VPLS.

ON SRX 320 a laptop was connected to ge-0/0/1 as seen in Figure 36 and on ge-0/0/5 was connected to a local network so SRX 320 could be configured using SSH.

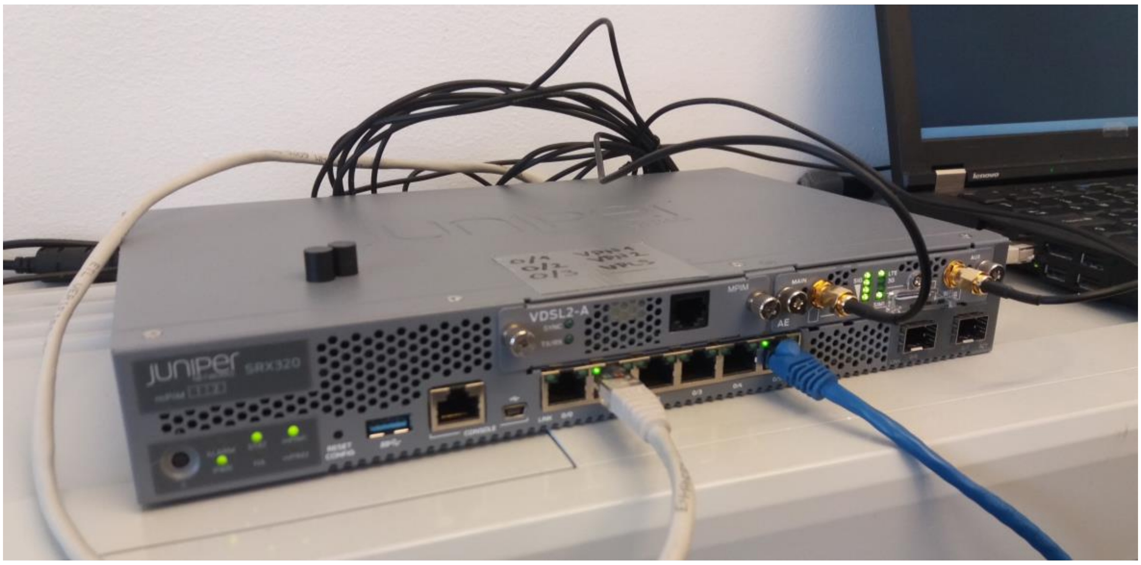


Figure 36. SRX 320 with LTE mini-PIM connected to laptop and local area network.

Internet connection on SRX 320 was done by using a 150Mbits/50Mbits Elisa mobile internet subscription. Elisa was chosen to be the testing carrier, because of their broad coverage and good signal quality.

The signal-to-noise ratio during the testing was 20-26 which translates to high signal strength and quality as seen in Table 4.

Antennae were separated from each other by at least one meter because achieving maximum performance was critical. The reason for separating antennae from each other was to optimize the receiving of LTE signal. The distance between antennae was calculated by measuring the wavelength of the LTE signal used. By figuring out which band is used (seen in Figure 27) the frequency can be determined by referring to Table 3 and then calculate the distance. In Table 3 Elisa is marked at 1800 MHz if Band 3 (B3) is used and on 800 MHz if Band (20) is used. And referring to Table 5 the appropriate “at least” distance can be determined.

Table 5. Preferred distance chart (Fourie, 2015).

Frequency	*Preferred “at least “distance of antennas.*
800 MHz	100 cm
1800MHz	0.50cm

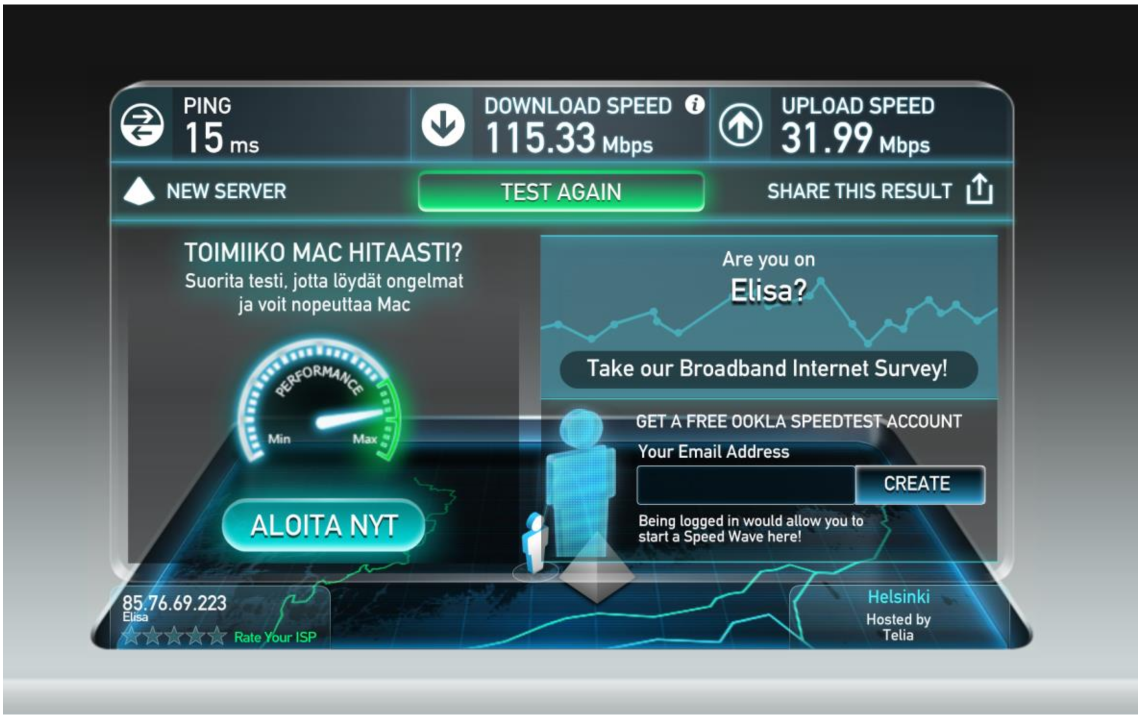
The programs and services used to test were speedtest.net and iPerf3. Speedtest.net is an internet site which measures the maximum bandwidth on internet connection and also shows latency in milliseconds. This was used to measure the reference speed for testing. iPerf3 were also used, which is a program that can be run on any computer. iPerf3 requires that the other device on the other end must be a computer (i.e. server in this case) running iPerf3 in server mode and the other in client mode. In these tests iPerf3 server was running on Linux server behind SRX 1500 and client was running on the laptop behind SRX 320. All commands issued to run iPerf3 were done on the laptop client.

All used hardware and their software versions can be found in Appendix 4 and pictures of the set up can be found in Appendix 5.

6.2 Reference and Expectations

First, a reference speed was determined for the solution. The reference speed was determined by measuring the current LTE maximum bandwidth to internet. The test does not involve methods used IPSec VPN to achieve connection between customer networks or the security used to encrypt traffic. In other words, this test was just plain test of the internet speed by using LTE mini-PIM. This test can be compared to testing the internet speed on a laptop when using a mobile phone hotspot to connect to internet.

Speedtest.net service was used to the measure current maximum bandwidth. There were no special criteria for this test, only that nothing else was using a significant amount of the bandwidth at the time of testing. As seen in Figure 37 a maximum download speed of 115.33 Mbit/s and maximum upload speed of almost 32 Mbit/s was achieved. These results can be considered as top of the line speed on the 4G mobile network currently deployed in the Helsinki metropolitan area. It is important to notice that as one cell of the network gets more crowded the connection speed does decrease.



PING 15 ms

DOWNLOAD SPEED 115.33 Mbps

UPLOAD SPEED 31.99 Mbps

TOIMIIKO MAC HITAASTI?
Suorita testi, jotta löydät ongelmat
ja voit nopeuttaa Mac

Are you on
Elisa?

Take our Broadband Internet Survey!

GET A FREE OOKLA SPEEDTEST ACCOUNT

Your Email Address

Being logged in would allow you to start a Speed Wave here!

85.76.69.223
Elisa

Helsinki
Hosted by
Telia

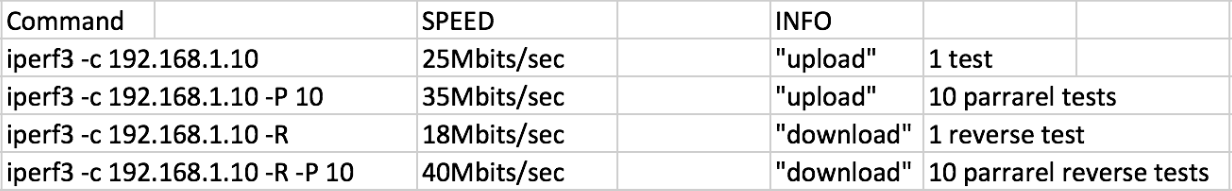
Figure 37. Speedtest.net test results

Expectations for IPSec VPN throughput and performance were high after this test. A 10 to 15 Mbit/s decrease was expected in maximum speeds due to increased packet size and packet amount.

6.3 IPSec VPN Performance tests

All tests were run by using only iPerf3, because the test setup was not connected to the internet in such a manner that speedtest.net could also have be used.

In Figure 38 testing the commands used, speeds and additional info can be seen. Four tests were run, two default tests and two test with parameter that does 10 default tests at the same time. As seen in Figure 38, the average download and upload speed are not up to the expectations, but more interesting was the slight trend of increasing speeds while running multiple tests at the same time.

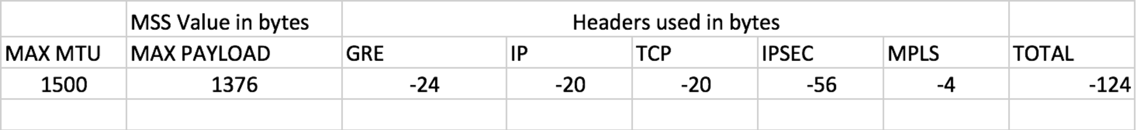


Command		SPEED		INFO		
iperf3 -c 192.168.1.10		25Mbits/sec		"upload"	1 test	
iperf3 -c 192.168.1.10 -P 10		35Mbits/sec		"upload"	10 parrarel tests	
iperf3 -c 192.168.1.10 -R		18Mbits/sec		"download"	1 reverse test	
iperf3 -c 192.168.1.10 -R -P 10		40Mbits/sec		"download"	10 parrarel reverse tests	

Figure 38. Command and first test results when running iPerf3.

The slight change in speed was due to Maximum Transmission Unit (MTU) limit. While doing only one test at the time packets were bigger than when doing 10 tests at the time. Too big packets mean fragmentation, which is chopping one packet into smaller ones before sending. While doing 10 tests at the same time, packets used to test are smaller than the ones used in a single test. Smaller packets mean less fragmentation, which was seen in increased transfer speeds. In short, smaller packets mean more optimized traffic.

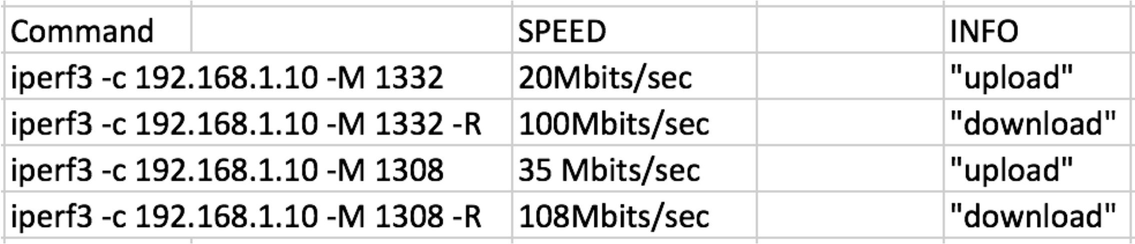
To achieve the maximum bandwidth, the maximum MTU on LTE network it was necessary to calculate the Maximum Segment Size (MSS). MMS is the maximum amount of data that a computer can handle in a single packet, often referred to as “payload”. As seen in Figure 39, the maximum MTU size is 1500 bytes in ISP end of LTE network, so MSS was needed to be calculated by that value. As seen in Figure 39, after subtracting the header sizes from the original MTU the maximum of MSS was 1376 bytes. (USAT Corporation , 2016.)



	MSS Value in bytes	Headers used in bytes					
MAX MTU	MAX PAYLOAD	GRE	IP	TCP	IPSEC	MPLS	TOTAL
1500	1376	-24	-20	-20	-56	-4	-124

Figure 39. Maximum payload/MSS calculation.

After determining the max MSS, tests were run again but this time using the parameter “-M” to set a fixed payload size to all packet used in the test. As seen in Figure 40, the test results have increased dramatically and they exceeded the set expectations by little. The packet size was successfully optimized for this solution. In Figure 40 it can be seen that the tests were run using MSS of 1332 bytes to count for any missing headers in calculations or any other mistakes. And afterwards tested with the reduced size of 1308 bytes, increasing the results.



Command		SPEED		INFO
iperf3 -c 192.168.1.10 -M 1332		20Mbits/sec		"upload"
iperf3 -c 192.168.1.10 -M 1332 -R		100Mbits/sec		"download"
iperf3 -c 192.168.1.10 -M 1308		35 Mbits/sec		"upload"
iperf3 -c 192.168.1.10 -M 1308 -R		108Mbits/sec		"download"

Figure 40. Second test results after using smaller MSS and commands how tests were done in iPerf3.

It is important to notice that all the tests were run to test the performance of one customer network over the internet using IPSEC VPN. But can be trustworthy assumed that when one connection works others will also work because they use the same configuration and the same uplink to connect via internet. If both customer networks L3VPN-1 and L3VPN-2 were used at the same time at maximum speed, the connection would be impacted with roughly halving of the maximum bandwidth.

To sum all the tests up everything exceeded the criteria of initial expectations and the performance requirements were matched. The only things – all beyond the scope of the present study - that might bottleneck the implementation and are outside of area of thesis:

- Packets per second (Pps) performance of routers.
- Configuring fixed MSS for end devices.
- Low mobile network performance.

7 Discussion and Conclusion

The thesis pursued a mobile office solution that is easy and agile to deploy anywhere in the nation by using the recently released LTE mini-PIM for SRX 320. The goal was to create working configuration for SRX 320 with LTE mini-PIM to test L3 VPN performance over internet and if possible improve the performance. As any VPN service this also needed to be terminated to some other device. SRX 1500 in Juniper Networks lab was chosen to be the termination point of the VPN.

The configuration was built from the start to the testing environment. The testing environment had to be built in a way that only the LTE uplink on SRX 320 would affect testing results. A high performance laptop and server were allocated to be client machines on the VPN. Tests were run by using speedtest.net to measure the initial bandwidth of the LTE connection and iPerf3 was used to measure the bandwidth of the L3 VPN solution.

The configuration was checked with show commands to ensure that everything was working as expected before the testing of the solution.

As mentioned in Chapter 6.2, the expectations for bandwidth were set high after testing the initial speed of mobile network (Figure 37). The first testing results on the L3 VPN were low as seen in Figure 38 due to an unknown reason at the time. After researching why this might had been, it was figured out that headers increase packet size so much that the packet gets fragmented and lowers the overall performance greatly. To address this problem, smaller MSS was used and the results turned out to be as expected. The results can be seen in Figure 40.

All the performance expectations and requirements were met. The security requirements for this solution were met while designing the solution, L3 VPN and MPLS technologies were chosen to address these requirements. As for the agility and the mobility, this solution is packed in a device (SRX 320) not much bigger than a lunchbox and requires only electricity and mobile network from the ISP, so it is safe to say the goals were met.

Policies and traffic filtering in the configuration were more like proof of concept, because basically all traffic was allowed through SRX 320 which is not the case on real implementation of this solution. If Juniper Networks were to implement this solution to a customer, strict firewall rules would be needed to guarantee the top of the line security.

I hope in the future bits of this thesis will be implemented on real deployment of secure mobile office solution.

References

Bushong, M., Gadecki, C. & Garret, A., 2008. *Junos for dummies.* 1st edition ed. s.l.:Wiley publishing inc..

Chenxi Wang, I., 2016. Containers 101: Linux containers and Docker explained. s.l.:infoworld.com.

Fourie, A., 2015. *How far apart must LTE antennas be spaced?.* [Online]
Available at: https://www.linkedin.com/pulse/how-far-apart-must-lte-antennas-spaced-andre-fourie [Accessed 27 08 2017].

Internet Engineering Task Force, 2010. *Protocol Standards.* [Online]
Available at: Internet Engineering Task Force [Accessed 23 08 2017].

Juniper Netwoks, 2014. *SRX product page.* [Online]
Available at: http://www.juniper.net/assets/us/en/local/pdf/brochures/1500024-en.pdf
[Accessed 22 05 2017].

Juniper Networks, 2014. *Routing Instances Overview.* [Online]
Available at:
https://www.juniper.net/documentation/en_US/junos/topics/concept/routing-instances-overview.html
[Accessed 15 08 2017].

Juniper Networks, 2016-03-30. *VPN Overview.* [Online]
Available at:
https://www.juniper.net/documentation/en_US/junos12.1x46/topics/concept/vpn-security-overview.html
[Accessed 23 08 2017].

Juniper Networks, 2016. *Security Zones and Interfaces Overview.* [Online]
Available at: https://www.juniper.net/documentation/en_US/junos/topics/concept/zone-and-interface-overview.html
[Accessed 15 08 2017].

Juniper Networks, 2016. *Understanding Internal BGP Peering Sessions.* [Online]
Available at: https://www.juniper.net/documentation/en_US/junos/topics/concept/bgp-ibgp-understanding.html
[Accessed 10 08 2017].

Juniper Networks, 2017. *Company Profile.* [Online]
Available at: https://www.juniper.net/uk/en/company/profile/
[Accessed 25 08 2017].

Juniper Networks, 2017. *Juniper cSRX Container Firewall.* [Online]
Available at: https://www.juniper.net/uk/en/products-services/security/srx-series/csrx/
[Accessed 16 06 2017].

Juniper Networks, 2017. *Security Policies Overview.* [Online]
Available at: https://www.juniper.net/documentation/en_US/junos/topics/concept/policy-overview.html#broad-policy
[Accessed 22 08 2017].

Juniper Networks, 2017. *Understanding Internet Key Exchange Version 2.* [Online]
Available at: https://www.juniper.net/documentation/en_US/junos/topics/concept/vpn-security-ikev2-understanding.html
[Accessed 14 08 2017].

Juniper Networks, 2017. *Understanding Selective Stateless Packet-Based Services.* [Online]
Available at:
https://www.juniper.net/documentation/en_US/junos/topics/concept/security-selective-stateless-packet-based-service-understanding.html
[Accessed 26 08 2017].

Marschke, D. & Reynolds, H., 2008. *Junos Enterprise Routing.* 1st edition ed. s.l.:O'Reilly.

Packetlife.net, 2013. *Route Distinguishers and Route Targets.* [Online]
Available at: http://packetlife.net/blog/2013/jun/10/route-distinguishers-and-route-targets/
[Accessed 20 08 2017].

Rob Cameron, B. W., 2013. *Juniper SRX Series, 1st Edition.* s.l.:O'Reilly Media, Inc..

TechTarget, 2017. *BGP tutorial: The routing protocol that makes the Internet work.* [Online]
Available at: http://searchtelecom.techtarget.com/feature/BGP-essentials-The-protocol-that-makes-the-Internet-work
[Accessed 02 08 2017].

USAT Corporation , 2016. *What are the main MTU and MSS design considerations?.* [Online]
Available at: http://usatcorp.com/faqs/main-mtumss-design-considerations/
[Accessed 27 08 2017].

SRX 320 Configuration

root@SRX320> show configuration

```
## Last commit: 2017-07-06 18:31:25 UTC by root
version "15.1I20170527_1007_lchen [lchen]";
system {
    host-name SRX320;
    domain-name SRX_LTE;
    root-authentication {
        encrypted-password                "$5$j4ApvRk3$ElqmkTREEAMDp7Wblant7kzb-
JoP5IRbC65iXQa1nVs7"; ## SECRET-DATA
    }
    name-server {
        8.8.8.8;
        8.8.4.4;
    }
    login {
        user admin {
            uid 2001;
            class super-user;
            authentication {
                encrypted-password                                        "$5$fRY-
plZ5Y$UzO/Uqr1LBnOXyDEO/MlyK91py3ns/.CtGgrU4woJE7"; ## SECRET-DATA
            }
        }
    }
    services {
        ssh;
        telnet;
        xnm-clear-text;
        netconf {
            ssh;
        }
        web-management {
            http {
                interface ge-0/0/0.0;
            }
        }
        dhcp {
            pool 192.168.1.0/24 {
                address-range low 192.168.1.2 high 192.168.1.10;
                router {
                    192.168.1.1;
                }
            }
        }
    }
    syslog {
        archive size 100k files 3;
        user * {
            any emergency;
        }
        file messages {
            any notice;
            authorization info;
        }
        file interactive-commands {
            interactive-commands any;
        }
    }
    max-configurations-on-flash 5;
    max-configuration-rollbacks 5;
    license {
        autoupdate {
            url https://ae1.juniper.net/junos/key_retrieval;
        }
    }
}
security {
    log {
        mode event;
    }
    ike {
        proposal ike-phase1-proposal {
            authentication-method pre-shared-keys;
            dh-group group2;
            authentication-algorithm sha1;
            encryption-algorithm aes-128-cbc;
        }
        policy ike-phase1-policy {
            mode aggressive;
            proposals ike-phase1-proposal;
            pre-shared-key ascii-text "$9$-PbYoDi.z39JG39ApREdbs2JGjHqfQF"; ## SECRET-DATA
        }
        gateway gw-labra {
            ike-policy ike-phase1-policy;
            address 194.86.6.23;
            local-identity hostname SRX320;
            external-interface dl0.0;
            version v2-only;
        }
    }
    ipsec {
        proposal ipsec-phase2-proposal {
            protocol esp;
            authentication-algorithm hmac-sha1-96;
            encryption-algorithm aes-128-cbc;
        }
        policy ipsec-phase2-policy {
            perfect-forward-secrecy {
                keys group2;
            }
            proposals ipsec-phase2-proposal;
        }
        vpn VPN_TUNNEL_1 {
            bind-interface st0.1;
            df-bit clear;
            ike {
                gateway gw-labra;
                ipsec-policy ipsec-phase2-policy;
            }
            establish-tunnels immediately;
        }
    }
    nat {
        source {
            rule-set trust-to-untrust {
                from zone trust;
                to zone untrust;
                rule source-nat-rule {
                    match {
                        source-address 0.0.0.0/0;
                    }
                    then {
                        source-nat {
                            interface;
                        }
                    }
                }
            }
        }
    }
    policies {
        from-zone trust to-zone trust {
            policy trust-to-trust {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
        from-zone trust to-zone untrust {
            policy trust-to-untrust {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
        from-zone untrust to-zone trust {
            policy untrust-to-trust {
                description ulos;
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
        from-zone untrust to-zone untrust {
            policy untrust-to-untrust {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
    }
    zones {
        security-zone trust {
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
                    all;
                }
            }
            interfaces {
                ge-0/0/0.0;
                ge-0/0/5.0;
            }
        }
        security-zone untrust {
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
                    all;
                }
            }
            interfaces {
                dl0.0;
                st0.0;
                gr-0/0/0.0;
                st0.1;
                lo0.1;
            }
        }
    }
}
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 192.168.1.1/24;
            }
        }
    }
    gr-0/0/0 {
        unit 0 {
            description "GRE Tunnel";
            tunnel {
                source 11.11.100.1;
                destination 11.11.100.2;
            }
            family inet {
                mtu 9000;
                address 172.16.255.1/30;
            }
            family mpls {
                mtu 9000;
                filter {
                    input packet-mode;
                }
            }
        }
    }
    ge-0/0/1 {
        description "LAN Side";
        mtu 9192;
        unit 0 {
            description "MPLS VPN1";
            family inet {
                filter {
```

```
                input packet-mode-inet;
            }
            address 192.168.0.1/24;
        }
    }
}
ge-0/0/2 {
    description "LAN Side";
    mtu 9192;
    unit 0 {
        description "MPLS VPN2";
        family inet {
            filter {
                input packet-mode-inet;
            }
            address 192.168.10.1/24;
        }
    }
}
ge-0/0/3 {
    description "VPLS VPN LAN";
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation vlan-vpls;
    unit 0 {
        description VPLS_VPN-1;
        encapsulation vlan-vpls;
        vlan-id 512;
    }
}
ge-0/0/4 {
    unit 0;
}
ge-0/0/5 {
    unit 0 {
        family inet {
            address 192.168.69.25/24;
        }
    }
}
ge-0/0/6 {
    unit 0;
}
ge-0/0/7 {
    unit 0 {
        family inet;
    }
}
cl-2/0/0 {
    dialer-options {
        pool 1 priority 100;
```

```
            }
            act-sim 2;
            cellular-options {
                sim 1 {
                    radio-access lte-only;
                }
                sim 2 {
                    radio-access automatic;
                }
            }
        }
        dl0 {
            unit 0 {
                family inet {
                    negotiate-address;
                }
                family inet6 {
                    negotiate-address;
                }
                dialer-options {
                    pool 1;
                    always-on;
                    dial-string 1234;
                }
            }
        }
        lo0 {
            unit 1 {
                family inet {
                    address 10.255.255.1/32;
                }
            }
        }
        st0 {
            unit 0 {
                family inet {
                    mtu 9178;
                }
            }
            unit 1 {
                family inet {
                    mtu 9178;
                    address 11.11.100.1/30;
                }
            }
            unit 3 {
                family inet;
            }
        }
    }
    routing-options {
```

```
    autonomous-system 65100;
}
protocols {
    mpls {
        interface gr-0/0/0.0;
    }
    bgp {
        tcp-mss 1200;
        group IBGP {
            type internal;
            local-address 10.255.255.1;
            local-as 65100;
            neighbor 10.255.255.2 {
                family inet {
                    any;
                }
                family inet-vpn {
                    any;
                }
                family l2vpn {
                    signaling;
                }
            }
        }
    }
    ospf {
        traffic-engineering;
        area 0.0.0.0 {
            interface lo0.1 {
                passive;
            }
            interface gr-0/0/0.0;
        }
    }
    ldp {
        interface gr-0/0/0.0;
        interface lo0.1;
    }
    l2-learning {
        global-mode switching;
    }
}
firewall {
    family inet {
        filter packet-mode-inet {
            term all-traffic {
                then {
                    packet-mode;
                    accept;
                }
            }
        }
    }
    family mpls {
        filter packet-mode {
            term all-traffic {
                then {
                    packet-mode;
                    accept;
                }
            }
        }
    }
}
routing-instances {
    L3VPN-1 {
        instance-type vrf;
        interface ge-0/0/1.0;
        route-distinguisher 10.255.255.1:1000;
        vrf-target {
            import target:65100:1000;
            export target:65100:1000;
        }
        vrf-table-label;
        routing-options {
            auto-export;
        }
    }
    L3VPN-2 {
        instance-type vrf;
        interface ge-0/0/2.0;
        route-distinguisher 10.255.255.1:2000;
        vrf-target {
            target:65100:2000;
            import target:65100:2000;
            export target:65100:2000;
        }
        vrf-table-label;
        routing-options {
            auto-export;
        }
    }
    VPLS_VPN-1 {
        instance-type vpls;
        interface ge-0/0/3.0;
        route-distinguisher 10.255.255.1:3000;
        vrf-target target:65100:3000;
        protocols {
            vpls {
                no-tunnel-services;
                site 1 {
                    site-identifier 1;
                    interface ge-0/0/3.0;
                }
                mac-tlv-receive;
                mac-tlv-send;
            }
        }
    }
}
```

SRX 1500 Configuration

```
admin@srx1500-2> show configuration
## Last commit: 2017-07-06 09:49:21 UTC by admin
version 15.1X49-D90.7;
system {
    host-name srx1500-2;
    root-authentication {
        encrypted-password "$5$rsQOQ4l6$toH/zddXN1jr8Vb.TI-
TIsk84Nq2Yka0fQmPhWnmRyT."; ## SECRET-DATA
    }
    login {
        user admin {
            uid 2000;
            class super-user;
            authentication {
                encrypted-password "$5$vK6waEUj$omO00YVPRmJF5Pj3qkrqti3bi-
ZUQTrP11igqGnwTyi3"; ## SECRET-DATA
            }
        }
    }
    services {
        ssh {
            root-login deny;
        }
    }
}
security {
    ike {
        proposal ike-phase1-proposal {
            authentication-method pre-shared-keys;
            dh-group group2;
            authentication-algorithm sha1;
            encryption-algorithm aes-128-cbc;
        }
        policy ike-phase1-policy {
proposals ike-phase1-proposal;
pre-shared-key ascii-text "$9$c1brK8-VYZUHX7UHqmF3SrevX7dbs4JG"; ## SECRET-
DATA
        }
        gateway gw-srx1500-labra {
            ike-policy ike-phase1-policy;
            dynamic hostname SRX320;
            external-interface xe-0/0/16;
            version v2-only;
        }
}
    ipsec {
        proposal ipsec-phase2-proposal {
            protocol esp;
        authentication-algorithm hmac-sha1-96;
        encryption-algorithm aes-128-cbc;
    }
    policy ipsec-phase2-policy {
        perfect-forward-secrecy {
            keys group2;
        }
        proposals ipsec-phase2-proposal;
    }
    vpn TUNNEL1 {
        bind-interface st0.1;
        df-bit clear;
        ike {
            gateway gw-srx1500-labra;
            ipsec-policy ipsec-phase2-policy;
        }
        establish-tunnels immediately;
    }
}
policies {
    from-zone internet to-zone internet {
        policy internet_to_internet {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
}
zones {
    security-zone internet {
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            xe-0/0/16.0;
            gr-0/0/0.0 {
                host-inbound-traffic {
                    system-services {
                        all;
                    }
                    protocols {
                            all;
                        }
                    }
                }
                st0.1;
                lo0.1;
            }
        }
    }
}
interfaces {
    gr-0/0/0 {
        unit 0 {
            description "GRE Tunnel";
            tunnel {
                source 11.11.100.2;
                destination 11.11.100.1;
            }
            family inet {
                mtu 9000;
                address 172.16.255.2/30;
            }
            family mpls {
                mtu 9000;
                filter {
                    input packet-mode;
                }
            }
        }
    }
    ge-0/0/3 {
        description "VPLS VPN LAN";
        flexible-vlan-tagging;
        mtu 1522;
        encapsulation vlan-vpls;
        unit 0 {
            description VPLS_VPN-1;
            encapsulation vlan-vpls;
            vlan-id 512;
        }
    }
    ge-0/0/10 {
        description "To Server";
        vlan-tagging;
        mtu 9192;
        unit 10 {
            description "L3VPN 1";
            vlan-id 10;
            family inet {
                filter {
                    input packet-mode-inet;
            }
            address 192.168.1.1/24;
        }
    }
    unit 11 {
        description "L3VPN 2";
        vlan-id 11;
        family inet {
            filter {
                input packet-mode-inet;
            }
            address 192.168.11.1/24;
        }
    }
}
xe-0/0/16 {
    description Internet;
    unit 0 {
        family inet {
            address 194.86.6.23/28;
        }
    }
}
ge-0/0/19 {
    description foo;
}
fxp0 {
    unit 0 {
        family inet {
            address 192.168.250.145/24;
        }
    }
}
lo0 {
    unit 1 {
        family inet {
            address 10.255.255.2/32;
        }
    }
    unit 2 {
        family inet {
            filter {
                input packet-mode-inet;
                output packet-mode-inet;
            }
            address 1.1.1.1/32;
        }
    }
    unit 3 {
        family inet {
            filter {
                    input packet-mode-inet;
                    output packet-mode-inet;
                }
                address 2.2.2.2/32;
            }
        }
    }
    st0 {
        unit 0 {
            family inet;
        }
        unit 1 {
            family inet {
                mtu 9178;
                address 11.11.100.2/30;
            }
        }
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 194.86.6.17;
    }
    autonomous-system 65100;
}
protocols {
    mpls {
        interface gr-0/0/0.0;
    }
    bgp {
        tcp-mss 1200;
        group IBGP {
            type internal;
            local-address 10.255.255.2;
            local-as 65100;
            neighbor 10.255.255.1 {
                family inet {
                    any;
                }
                family inet-vpn {
                    any;
                }
                family l2vpn {
                    signaling;
                }
            }
        }
    }
    ospf {
        traffic-engineering;
        area 0.0.0.0 {
            interface lo0.1 {
                passive;
            }
            interface gr-0/0/0.0;
        }
    }
    ldp {
        interface gr-0/0/0.0;
        interface lo0.1;
    }
    lldp {
        interface all;
    }
}
firewall {
    family inet {
        filter packet-mode-inet {
            term all-traffic {
                then {
                    packet-mode;
                    accept;
                }
            }
        }
    }
    family mpls {
        filter packet-mode {
            term all-traffic {
                then {
                    packet-mode;
                    accept;
                }
            }
        }
    }
}
routing-instances {
    L3VPN-1 {
        instance-type vrf;
        interface ge-0/0/10.10;
        interface lo0.2;
        route-distinguisher 10.255.255.1:1000;
        vrf-target {
            import target:65100:1000;
            export target:65100:1000;
        }
        vrf-table-label;
        routing-options {
            auto-export;
        }
    }
    L3VPN-2 {
        instance-type vrf;
        interface ge-0/0/10.11;
        interface lo0.3;
        route-distinguisher 10.255.255.1:2000;
        vrf-target {
            target:65100:2000;
            import target:65100:2000;
            export target:65100:2000;
        }
        vrf-table-label;
        routing-options {
            auto-export;
        }
    }
    VPLS_VPN-1 {
        instance-type vpls;
        interface ge-0/0/3.0;
        route-distinguisher 10.255.255.1:3000;
        vrf-target target:65100:3000;
        protocols {
            vpls {
                no-tunnel-services;
                site 1 {
                    site-identifier 1;
                    interface ge-0/0/3.0;
                }
                mac-tlv-receive;
                mac-tlv-send;
            }
        }
    }
}
```

TOPOLOGY

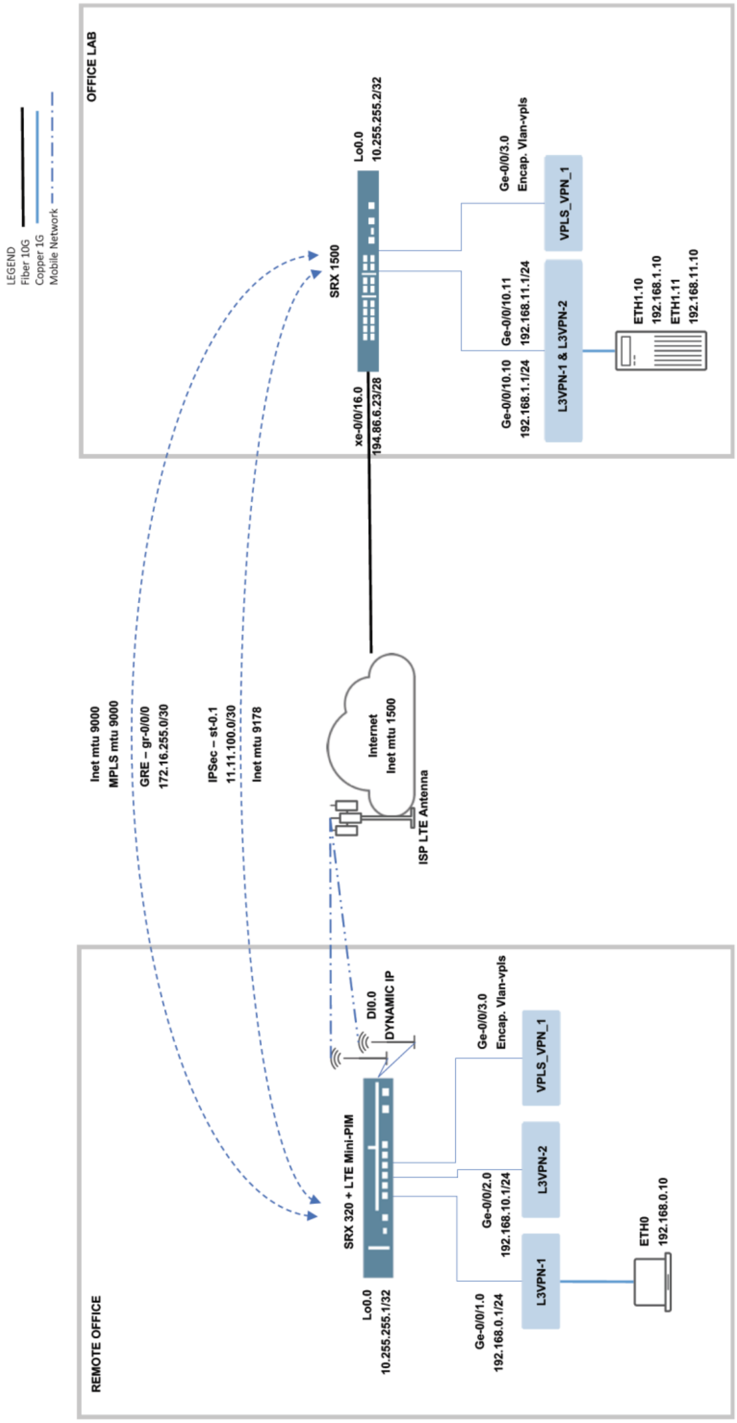


Figure 1. Topology of testing environment

List of used hardware

Laptop
Model: Lenovo T410
OS: CentOS 6.4
CPU: Intel Core i5 520M / 2.4 GHz
RAM: 6GB @ 1066MHz
LAN: Gigabit Ethernet

Server
Model:
OS: Red Hat 4.4
CPU: Intel(R) Pentium(R) D CPU 3.40GHz
RAM: 2GB
LAN: 1 Gigabit Ethernet

Router1
Model: SRX 320
Software version: 15.1X49-D100.6

LTE Mini-PIM
Firmware: 17.1.80
Mobile Subscription (SIM): Elisa
LTE chip: Sierra Wireless MC7455

Router2
Model: SRX 1500
Software version: 15.1X49-D100.6

Pictures of setup

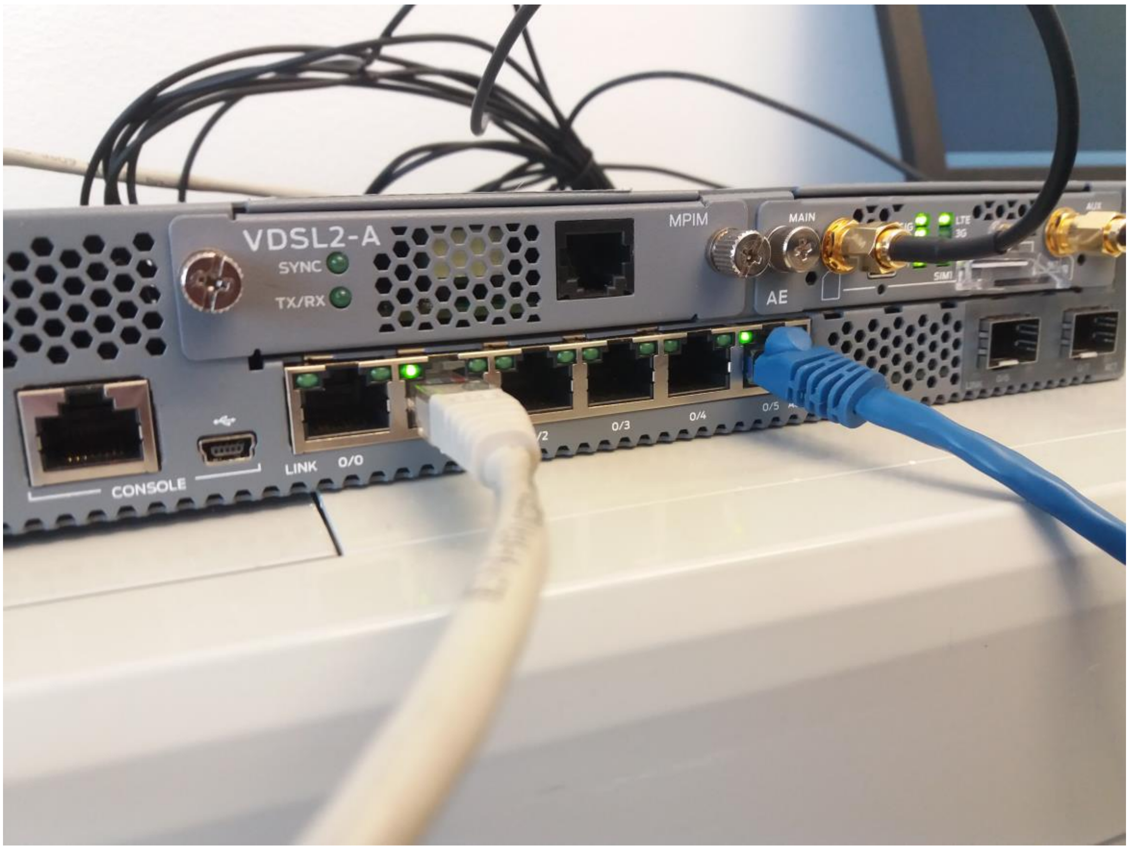


Figure 1. SRX 320. Connection to laptop (left) and local area network connection (right) to configure SRX 320

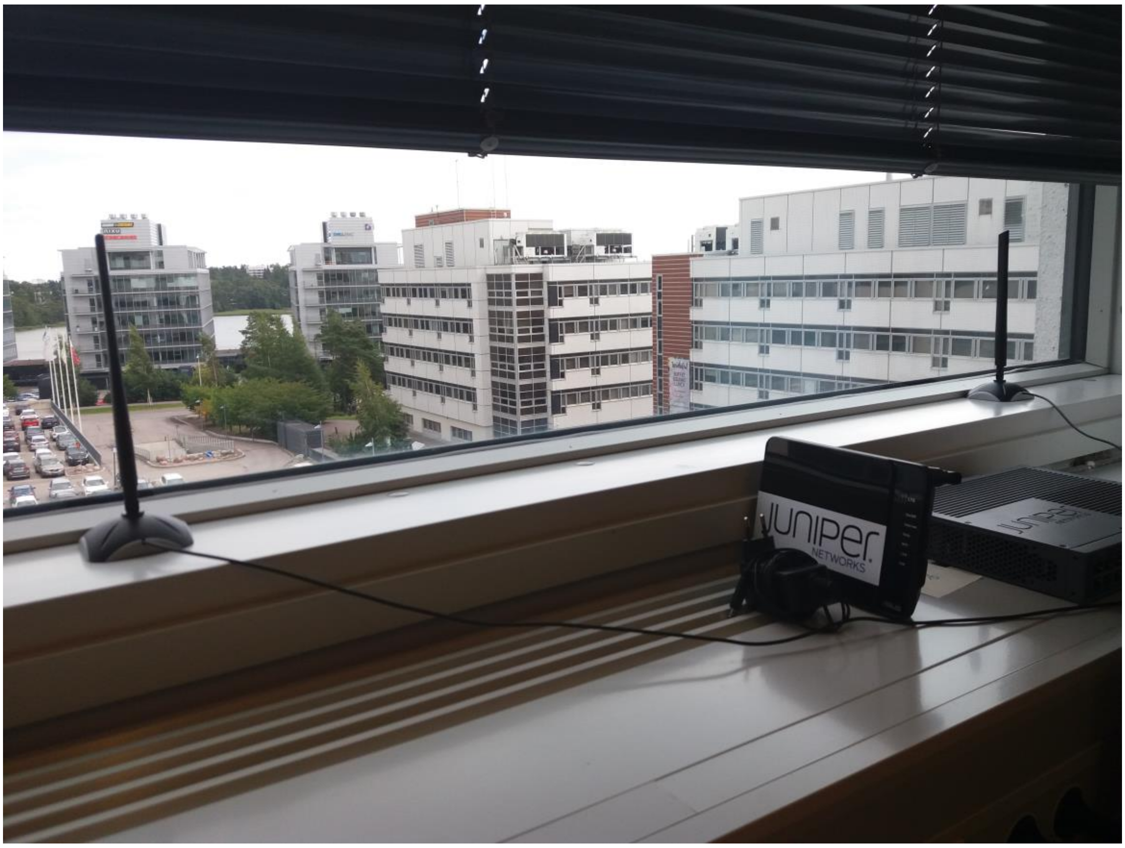


Figure 2. Antenna set up at testing site. Antennas are separated at least by a meter.

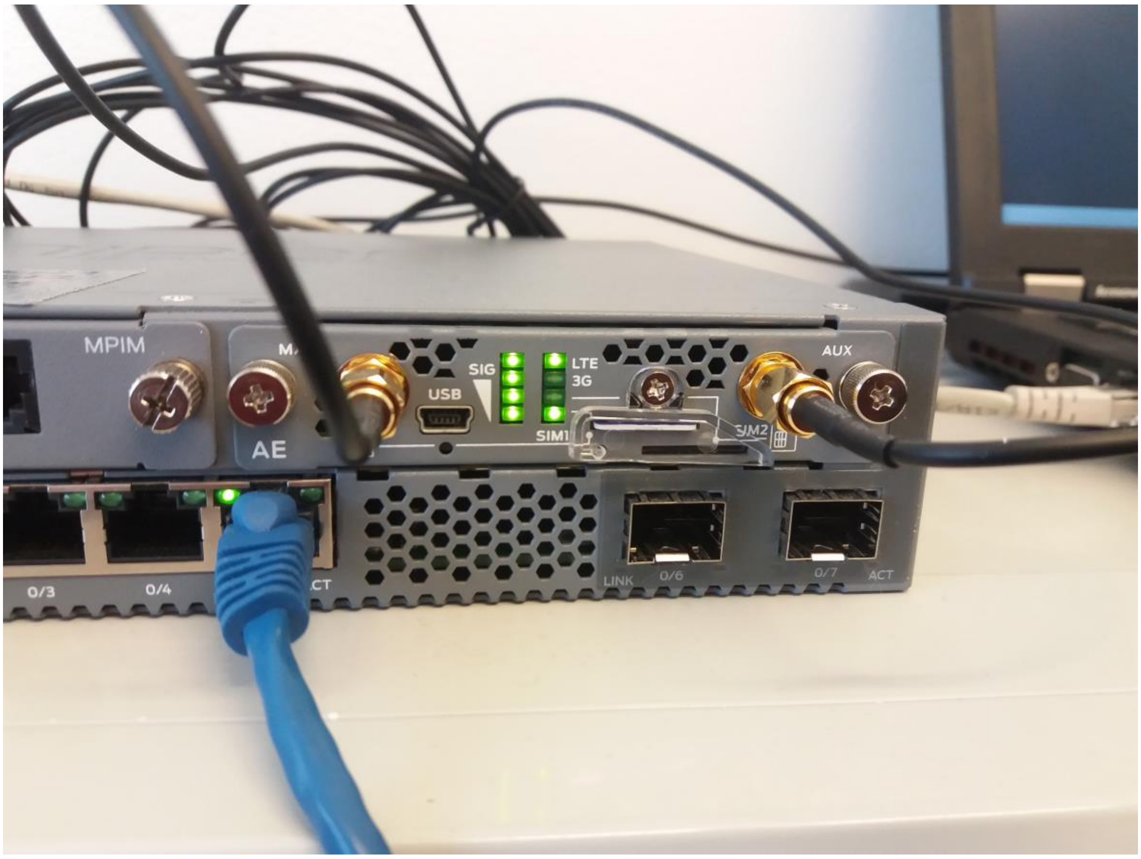


Figure 3. LTE mini-PIM powered on and connected to internet. Both antennas attached.

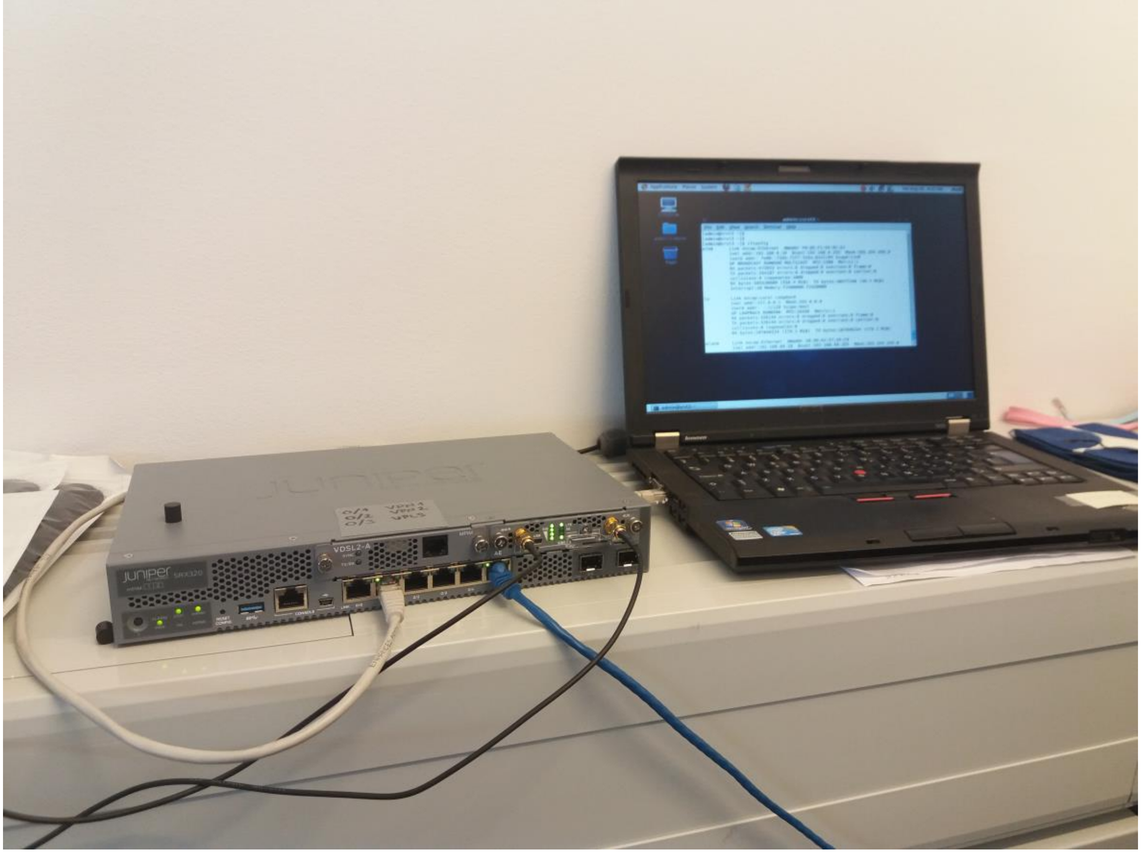


Figure 4. Remote office set up. Testing laptop connected to SRX 320.