jamk.fi

Technical specification for federation of cyber ranges

Juha Piispanen

Master's thesis
December 2018
Technology, communication and transport
Master's Degree Programme in Information Technology
Cyber Security

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Description

Author(s)	Type of publication	Date
Piispanen, Juha	Master's thesis	December 2018
		Language of publication: English
	Number of pages 50	Permission for web publication: x

Title of publication
Technical specification for federation of cyber ranges

Degree programme
Master's Degree Programme in Information Technology,Cyber Security

Supervisor(s)
Rantonen, Mika
Huotari, Jouni

Assigned by
JYVSECTEC, JAMK University of Applied Sciences

Abstract

The cybersecurity strategy of the European Union states that one of the tools to make a cyber-domain safer and achieve cyber resilience is reached with cyber security exercises. Cyber security exercises use cyber ranges such as JYVSECTEC's RGCE. There are several different kinds of cyber ranges in Europe, the capabilities of which vary. By connecting these cyber ranges together, it might be possible to design more versatile cyber security exercises.

The main goal of this master's thesis was to define the technical requirements for the cyber range federation and the overlay network that connects the cyber ranges. Other research questions were to research technical solutions for the overlay network and define use cases for the federation. The researched literature was gathered from academic, vendor publications and standards.

The master's thesis resulted in use cases, a list of requirements and a checklist. The list of requirements includes 17 different requirements for the interconnection of cyber ranges. After the initial technical connection, there are many different aspects to consider before the federation is usable. The purpose of the checklist meaning is to take these aspects or problems into account and thus help to connect the functions of different cyber ranges together.

Keywords/tags (subjects)
Cyber Security, Cyber security exercise, cyber range, SD-WAN,

Miscellaneous (Confidential information)

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Date
Piispanen, Juha	Opinnäytetyö, ylempi AMK	Joulukuu 2018
		Julkaisun kieli: Englanti
	Sivumäärä 50	Verkkojulkaisulupa myönnetty: x

Työn nimi
Technical specification for federation of cyber ranges

Tutkinto-ohjelma
Master's Degree Programme in Information Technology, Cyber Security

Työn ohjaaja(t)
Mika Rantonen
Jouni Huotari

Toimeksiantaja(t)
JYVSECTEC, JAMK University of Applied Sciences

Tiivistelmä

Euroopan Unionin kyberturvallisuusstrategia määrittää kyberturvallisuusharjoitukset yhdeksi työkaluksi, jolla voidaan lisätä kyberresilienssiä. Kyberturvallisuusharjoitusten alustana käytetään usein kyberympäristöä, kuten JYVSECTECin RGCE:tä. Euroopassa on useita kyberympäristöjä, joiden ominaisuudet eroavat toisistaan. Kyberympäristöjen yhteenliittämisellä mahdollistettaisiin laajempia ja monipuolisempia kyberturvallisuusharjoituksia

Opinnäytetyön tärkeimpänä tavoitteena oli tehdä vaatimusmäärittely verkolle, jolla eri kyberympäristöt voitaisiin liittää toisiinsa. Muina tutkimuskysymyksinä oli tutkia eri tekniikoita, joilla tämä verkko voitaisiin toteuttaa sekä määrittää käyttötapauskuvaukset yhteenliittämiseen. Tutkimusmateriaalina käytettiin tieteellisiä julkaisuja, yleisiä standardeja sekä valmistajien julkaisuja

Opinnäytetyön tuloksena oli 17 vaatimuksen lista yhteenliittämiseen tarkoitetulle verkolle. Tämän lisäksi opinnäytetyössä laadittiin tarkastuslista, jota voidaan käyttää kyberympäristöjen välillä yhteenliittämisen jälkeen, jotta liittymisen jälkeen muodostunutta kyberympäristöä voidaan käyttää kyberturvallisuusharjoituksessa.

Avainsanat (asiasanat)
Kyberturvallisuus, kyberturvallisuusharjoitus, kyberympäristö, SD-WAN

Muut tiedot (Salassa pidettävät liitteet)

CONTENTS

FIGURES

ACRONYMS

CR	Cyber Range
DSL	Digital Subscriber Line
JYVSECTEC	Jyväskylä Security Technology
MPLS	Multiprotocol Label Switching
NAT	Network Address Translation
PKI	Public Key Infrastructure
QoS	Quality of Service
RGCE	Realistic Global Cyber Environment
SD-WAN	Software-defined Wide Area Network
UDP	User Datagram Protocol
VPN	Virtual Private Network
VXLAN	Virtual Extensible Local Area Network
WAN	Wide Area Network

1 Introduction

1.1 Background

> *"Ensuring the security of society is a key task of the government authorities and the vital functions of our society must be secured in all situations. As an information society Finland relies on information networks and systems and, consequently, is extremely vulnerable to disturbances which affect their functioning. An international term for this interdependent, multipurpose electronic data processing environment is the cyber domain." (*Secretariat of the Security Committee 2013)

Safe cyber domain is a possibility and resource for both individuals and companies. Both Finland's and European Union's cybersecurity strategy states that one of the tools to make cyber domain safer and achieve cyber resilience is cyber security exercises. Without EU level cyber security exercises, it is not possible to simulate cooperation among the private sector and EU's members. There has been five EU level table top cyber security exercises since 2010. (Secretariat of the Security Committee 2013, European Commission 2013)

There is a need to make these EU level cyber security exercises but now they have been organized by one organization and most of these exercises has been table top exercises. Live exercises need cyber range and connecting different cyber ranges are difficult and normally takes many person-hours because it has been done manually. The purpose of this master's thesis is to define use cases for the cyber range federation and define the requirements for the network that connects the cyber ranges together.

This thesis was assigned by JYVSECTEC (Jyväskylä Security Technology). JYVSECTEC is an independent cyber security research, training and development center. JYVSECTEC is a part of the Institute of Information Technology of JAMK University of Applied Sciences. JYVSECTEC started as an EU funded development project in 2011. Nowadays JYVSECTEC produce cyber exercises, consulting, research, testing and training services to its customers. These services are held in Finland's national cyber range RGCE that is developed and operated by JYVSECTEC. (JYVSECTEC 2018)

1.2 Research objectives

There are several different kinds of cyber ranges in Europe. These cyber ranges are mostly isolated and do not have any interconnection capabilities. Interconnection between these cyber ranges might be beneficial to their actors because capabilities varies between cyber ranges, and it is not cost effective that everyone builds the same capabilities.

The main research questions for this thesis are listed below:

- What are the use cases for cyber range federation?
- What are the technical requirements for the cyber range federation?
- Research technical solutions for the overlay network

This research objective is not to build the cyber range federation, but to define the use cases and requirements for the cyber range federation. Also, research techniques and protocols that may be used in cyber range federation. The last object of this research is to make example technical scenario that can be used to test cyber range federation and evaluate different kind of solutions of cyber range federation.

1.3 Research methods

For the research method, qualitative research method was selected. Qualitative research gathers previous made researches and publications and researchers own thinking and reasoning. There are many different methods for how to analyze data from qualitative research. One of those methods is inductive analysis and this was selected to this master's thesis. David R. Thomas (2006) describes the inductive approach as "inductive analysis refers to approaches that primarily use detailed readings of raw data to derive concepts, themes, or a model through interpretations made from the raw data by an evaluator or researcher"

The research starts with describing the use cases for cyber range federation. After the use cases are describe, technical requirements for the network that connects the cyber ranges are defined based on the use cases. When the requirements are defined, potentials techniques and protocols are selected and researched. Because

cyber range federation is more than just connecting two or more networks together, checklist is made for different kind of exercise scenarios.

1.4 Related research

There are hardly any published researches or technical examples of cyber range federation. Often cyber ranges are owned by government or military, which is why if there are some researches, they are not public. Those few researches that exist focus more on connecting datacenters and not on how to connect the cyber ranges and services inside the cyber ranges. One example of this kind of research is Vallaot's Master's thesis (2017) from the University of Tartu. In this Master's thesis, the cyber range federation is researched focusing on Estonian's and Czech Republic's cyber range. This thesis focus is more on the datacenter interconnection and does not bring any general specification for the requirements of cyber range federation.

2 Theoretical backround

2.1 Cyber ranges

Cyber ranges provide a safe and legal environment to practice hands-on cyber skills. The first cyber ranges were designed and owned by military and government, however, nowadays many public companies offer cyber range services to their customers. Cyber ranges also offer a secure environment for security testing and product development. Cyber range is generally an isolated environment with Internet like capabilities. The ranges often use both virtual and physical infrastructures to offer services to their end users. Cyber ranges are built to offer a safe and realistic environment to train and test cyber skills. When cyber range offers realistic and internet like environment, real life scenarios and threats can be used inside of the cyber range without the fear of damaging any real production systems. (NIST. 2018)

Australian Defence Science and Technology Group categorize cyber ranges to three types: simulation, overlay and emulation. Most of the cyber ranges are simulated or emulated. Simulation type cyber range uses software models of real word object that is run by a small number of servers. Simulated cyber ranges are somewhat cheap and easy to deploy. On the other hand, simulated cyber ranges do not necessarily offer results that reflect reality. Overlay cyber ranges do not have their own environment and they share the same hardware than production networks. Emulated cyber ranges have dedicated hardware for cyber ranges and use real computers and applications. Of the three, emulated cyber range is closest to a realistic environment. When a cyber range is realistic, the results of tests and exercises are more likely to be correct when compared to real world environments. Emulated cyber ranges are the most expensive because they need dedicated hardware; however, nowadays costs can be reduced with virtualization. (Davis, Magrath, 3)

Realistic Global Cyber Environment (RGCE) is JYVSECTEC's cyber range. RGCE can be categorized to be an emulated cyber range. RGCE combines physical devices and virtualized technologies to isolated sandbox like cyber environment. RGCE mimics the

real Internet, which is done by using real life protocols and structures of the Internet. Because RGCE has all the same counterparts as the real Internet, real life scenarios and threats can be tested in RGCE. JYVSECTEC examples of RGCE's Internet services and features are (JYVSECTEC – Jyväskylä Security Technology 2018b):

- Tier I, II and III Internet Service providers with fully functional BGP routing and realistic structure with public IP addresses
- Realistic name service architecture including root DNS servers
- Global PKI Infrastructure for certificates
- Global Time services
- Controlled update and software repositories for various operating systems
- TOR Onion network

RGCE also offers industry specific systems. These environments are comprehensive and offer business functions to a certain field of business. JYVSECTEC currently has environments for financial sector, Internet service providers, cloud providers and two critical infrastructure environments. For example, critical infrastructure environments consist of a separated automation environment and a normal office environment. These environments are built with industry standards and represent best practice design. Furthermore, these environments are connected, hence, the cooperation in exercises can be trained and tested between the exercise participants. (JYVSECTEC – Jyväskylä Security Technology 2018b)

2.2 Cyber security exercises

In 2015 The European Union Agency for Network and Information Security (ENISA) reported that there has been an exponential growth in the number of cyber security exercises over past decade. In the same report ENISA reported that over 40 % of exercises were held in Europe. Preparedness exercises have been used in various security sectors for a long time and now as it can be seen, this kind of exercises are also used in cyber security sector. Cyber security exercises are useful to train organizations to be prepared for cyber threats and attacks and ensure business continuity. With cyber security exercises organizations can reveal weaknesses in their procedures and improve them. Most exercises are provided to one organization. However, nowadays more and more incidents affect more than one company at once; therefore, exercises are provided to multiple organizations at once. When an exercise is

targeted to multiple organizations at once, organizations can train their processes together. (ENISA 2015, 14)

Exercises should be designed with Threat-Driven approach. With this kind of approach, the exercise scenario including attack vectors and threat actors is designed for the client organization. In that case, the exercise events pose realistic risks to an organization and when the risks are realistic, the training audience gets a proper understanding of the scenario. This also immerses the training audience in the scenario. The exercise should always have its objectives, and the Threat-Driven approach should always acknowledge these objectives. For example, if the objective of the exercise is to learn how to mitigate distributed denial of service (DDOS) attack, the attack vectors should include the DDOS. (JYVSECTEC – Jyväskylä Security Technology 2018b)

2.2.1 Key elements of cyber security exercise

The definitions of the key elements of cyber security exercise:

White team is responsible for command and control of the exercise. The members of the white team are responsible for specifying the objectives of the exercise and the creation of the exercise scenario and events. White team also monitors the event compliance and assesses the performance of the blue team's responses to the events. During the exercise, the white team often makes modifications to exercise events or injects so that the exercise would meet its objectives.

Blue team is a group of people responsible for defending an information system and is the target audience of the cyber security exercise. The exercise can have multiple blue teams from a same company or from different companies. Blue team members can represent multiple divisions inside the organization.

Red team is the threat actor in cyber security exercise. Depending on the nature of the exercise red team can be also the exercise's target audience. Normally red team is a part of cyber range organization's staff that carry out the injects that the white team has designed.

Green team is the support team of the exercise. Green team's task is to operate the exercise environment's (cyber range's) infrastructure and support other teams in technical matters.

Event/inject is a specific activity that the white team has planned during the planning phase of the exercise, e.g., Red Team NMAP scan, target blue team network 31.32.34.0/24.

2.2.2 Types of cyber security exercises

Cyber security exercises can be categorized to three different types. These are table top, full live and hybrid.

Table top

Table top exercises do not have technical events, and they are the simplest exercises from a technical perspective. In most cases in table top exercises the events are run at one table where the table top exercise gets its name. Table top exercises should be targeted to a small group of training audience. Table top exercises are good for opening the communication between the training audience and to a test business process on a higher level. These exercises focus on the communication and interactions between exercise participants. (Kick 2014, 9)

Full live

In full live exercise the events are executed, as the name suggests, in real time. The events are based on real life events and are executed by the red team. Full live exercises need a technical platform, a cyber range, where the technical events can be executed. In live exercises it is important that the white team understands what kind of threats the training audience is facing in their day to day life, and that the planned events correlate with these threats. In full live exercises the red team adapts to the blue team's technical environment and dynamically adds events based on their findings. For example, when the red team finds a new vulnerability, the red team makes a new event corresponding to the findings and exploits the vulnerability. (Kick 2014, 11)

Hybrid

Hybrid exercises take parts from both table top exercise and full live exercise. In a hybrid exercise, the red team executes the events against predefined targets under the white team's control. Technical events executed by red teams trigger the responses from the blue teams, and these responses are played in table top manner. As in table top exercises, the focus of hybrid exercises is on improving the communication and interaction between target audience. (Kick 2014, 10)

2.3 SD-WAN

2.3.1 Introduction

Software-defined Wide-Area Network (SD-WAN) applies software defined networking to WAN connections. These WAN connections are used to connect enterprise networks over large geographical distances. With WAN connections, an enterprise can connect its branch offices to datacenters or to headquarters. SD-WAN provides a policy-based and dynamic path selection across multiple WAN connections. It also supports service chaining for additional services such as WAN optimization. All these functions are controlled by network control that is moved from the network devices into the cloud. (SDxCentral; Gartner 2018)

SD-WAN is one of the solutions to solve the issues in traditional WAN services. Multi-Protocol Label Switching (MPLS) and Carrier Ethernet have been used to deliver business grade WAN services to enterprises. However, with these technologies the delivery time has become an issue. Nowadays, it can take months to interconnect new sites to network and even service changes, e.g. bandwidth changes can take a few weeks. (MEF 2017, 3)

Even though there are plenty of different SD-WAN solutions and many vendors, there is no definition to SD-WAN terminology, deployment scenarios, standardized APIs or architectures. (MEF 2017, 3)

2.3.2 Characteristics of SD-WAN

Metro Ethernet Forum (MEF) defines seven fundamental characters for managed SD-WAN services. SD-WAN could also have more services that add value to SD-WAN-service; however, MEF only defines one of these value-added services.

Secure, IP-based Virtual Overlay Network

Secure, IP-based virtual overlay network is provided by SD-WAN. Normally this is done by using IPsec tunnels over public network or using MPLS-network. VXLANs are also used to provide a secure virtual overlay network. SD-WAN supports mesh and hub and spoke topologies and there is no need to modify the underlay networks since SD-WAN is a virtual overlay network. (MEF 2017, 5)

Transport-independence of Underlay Network

SD-WAN supports any kind of underline networks. It can be a wired or wireless network. Each of the SD-WAN's WAN connections may use a different technology, e.g. DSL or LTE connections, which makes SD-WAN very agile and simplifies the deployments of new virtual networks. (MEF 2017,5)

Service Assurance of each SD-WAN Tunnel

SD-WAN measures QoS performance over each SD-WAN tunnel in real-time. These QoS-measurements can include for example packet loss and latency. SD-WAN uses these measurements to determine if the particular WAN connection meets its requirements. For example, a real-time application can need very low latency and only MPLS-VPN based WAN connection meets this requirement; hence, SD-WAN uses only that connection to forward real-time application data. (MEF 2017,5)

Application-Driven Packet Forwarding

At the customer premises or the start point of the SD-WAN tunnel, SD-WAN performs application-level classification. With this classification, SD-WAN can specify the

applications, which are forwarded of different WAN-connections that are used to create SD-WAN tunnels. It also enables the capability to make QOS, security and business policies based on application. (MEF 2017,6)

High Availability through Multiple WAN

High Availability through Multiple WAN means that SD-WAN supports Hybrid WAN. Hybrid-WAN means that a site has two or more WAN connections that use different WAN technologies and the site can use these connections for packet forwarding. With SD-WAN, tunnels can be created over different underlay network technologies. (MEF 2017,6)

Policy-based Packet Forwarding

MEF describes the policy-based packet forwarding as “SD-WANs use policies to make application forwarding (or blocking) decisions for SD-WANs tunnels over each WAN”. These policies are defined at application level. Policies are created for QoS, Security and Business priorities. For example, SD-WAN can send payment card transactions prior to a normal communication application. In this case, the company sees that payment card transactions are more important to business than phone calls. (MEF 2017,6)

Service Automation via Centralized Management, Control and Orchestration

SD-WAN moves the control from network devices to the cloud. With centralized management, control and orchestration of SD-WAN-tunnels the service automation is achieved. With service automation a subscriber can self-install the customer premises equipment (CPE) and with zero touch provisioning (ZTP) all configurations and policies are installed from the Internet. With ZTP there is no need to send service provider installer or network administrator to customer premises. All service modifications can be carried out from the cloud via web portal. (MEF 2017,7)

WAN Optimization

Many of the SD-WAN vendors have started from WAN optimization services, which is why many of the SD-WAN services support WAN optimization. The main function of WAN optimization is to increase WAN bandwidth and QoS performance. This is accomplished with data deduplication, compression and caching. In addition, forward error correction and protocol spoofing can be used. WAN optimization is defined as a value-added service because SD-WAN does not require it. (MEF 2017,7)

2.3.3 SD-WAN service components

SD-WAN vendors divide their solutions normally into three layers. The layers are management/orchestration plane, control plane and data plane. On the management plane there is the SD-WAN policy manager. SDN Controller is on the control plane and the data plane contains the CPE device. Figure 1 (Cisco 2018a) contains Cisco system's SD-WAN fabric. Cisco uses the described architecture with three layers. (Cisco 2018a; Nuage 2016)

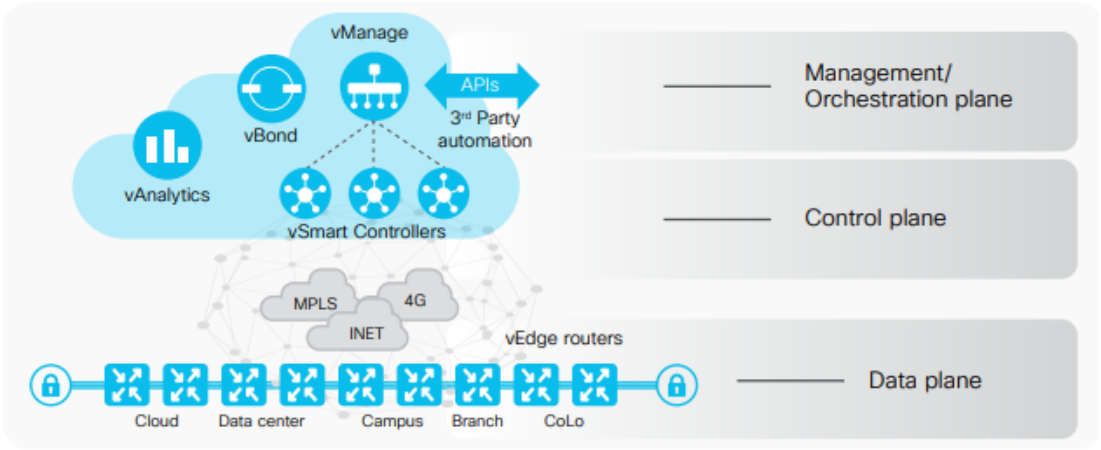

Figure 1 Cisco's SD-WAN architecture (Cisco 2018a)

Management plane

Management plane layer provides visibility and control to the network. The management plane contains the SD-WAN orchestrator and a service portal. These components can be deployed in either a hosted cloud or on-premises. The service portal is the most visible part of the SD-WAN, because from there users make all the configuration to SD-WAN and sees the current state of the SD-WAN. The state includes in-

formation such as the operational state of SD-WAN-tunnels and QoS-metrics. This information is from SD-WAN-controller and the orchestrator uses this data to change the dataflows based on QoS-metrics. The orchestrator is also responsible for connecting different components together. When the new CPE-device is connected to network, the orchestrator notifies the CPE where and how to connect to the SD-WAN controller. (MEF 2017, 9; Nuage 2016, 4)

Control plane

Control plane is responsible for the all normal control plane functions such as routing. In SD-WAN all control plane functions are managed by an SD-WAN-controller. The SD-WAN-controller also provides the device management to SD-WAN-domain. The device management includes configuration, IP address management and policies for SD-WAN-edges and gateways. Depending of the SD-WAN architecture, the SD-WAN-controller can also be a hub that notifies the CPE devices of the direct path between CPE-devices. (MEF 2017, 8; Nuage 2016, 4)

Data plane

Data plane functions are distributed to SD-WAN CPE devices. Most of the vendors offer these devices either as virtual or physical service. These edge devices connect different locations to underlays networks, such as DSL, Cable or MPLS network. Edge devices use these underlay networks to create and terminate secure tunnels. These tunnels use some tunneling protocol, such as IPsec, GRE or VXLAN. All decisions that the edge devices make are controlled by the SD-WAN-controller. (MEF 2017, 7; Nuage 2016, 4)

2.4 IPsec

2.4.1 Introduction

Internet Protocol Security (IPsec) secures communications at the IP layer. It is mostly used in VPN-connections between network devices or between remote users and an

enterprise network. IP itself do not have any means to provide confidentiality, integrity and authentication. IPsec is a collection of standards that provide these three functions. (RFC 6071, 4) (RFC 5406, 2)

2.4.2 Encapsulation Security Payload

IPsec uses the authentication header (AH) or encapsulating security payload (ESP) protocols to secure over-the-wire transmission. ESP provides confidentiality, integrity and authentication. AH also provides integrity and authentication. ESP can be used without confidentiality therefore nowadays typical IPsec implementation uses ESP and AH is obsoleted. (RFC 5406, 3)

ESP header is used after the IP header. The IP header can be original IP header, or it can be new depending on which IPsec mode is used.

2.4.2.1 Transport and tunnel mode

IPsec can be used either transport or tunnel mode. Transport mode can be used in point-to-point connections. As Figure 2 shows, transport mode inserts ESP header between IP and Layer-4 headers and does not encrypt the original IP header. (Fall et al. 2012)

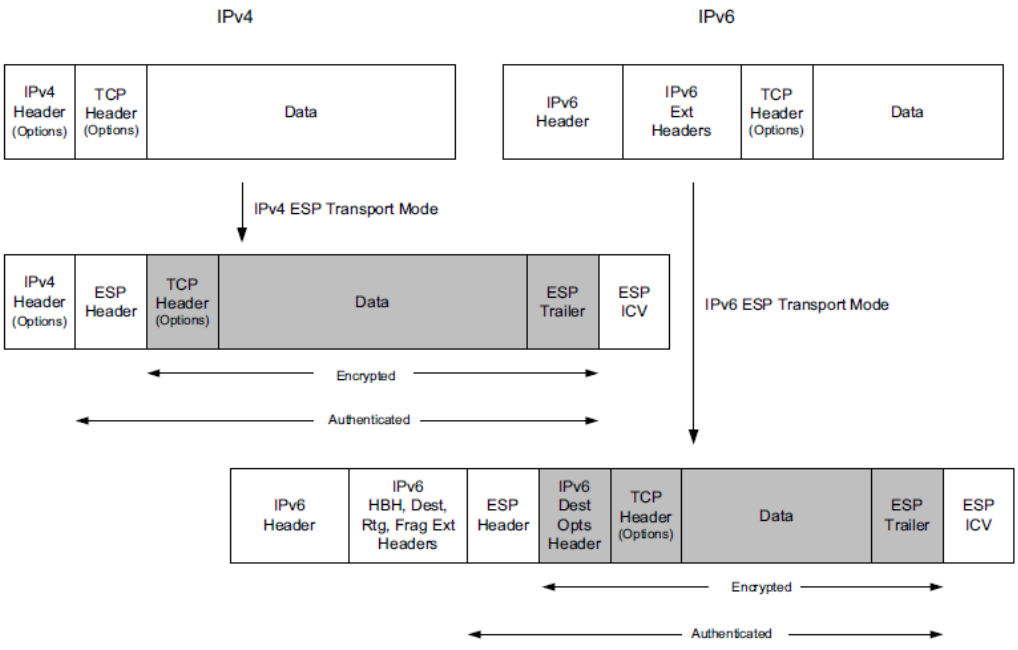

Figure 2 ESP Transport mode (Fall et al. 2012.)

In the tunnel mode, ESP encapsulates and protects the entire IP datagram. The tunnel mode is normally used in Virtual Private Networks (VPN) and is needs to be used when the two IPsec tunnel ends are not directly connected. Figure 3 shows the ESP datagram in tunnel mode where it can be seed that there is a new IP header that contains addresses of the IPsec peers. The originals IP addresses are protected and encrypted inside the IPsec packet. (Fall et al., R. W, Richard, Stevens 2012.)

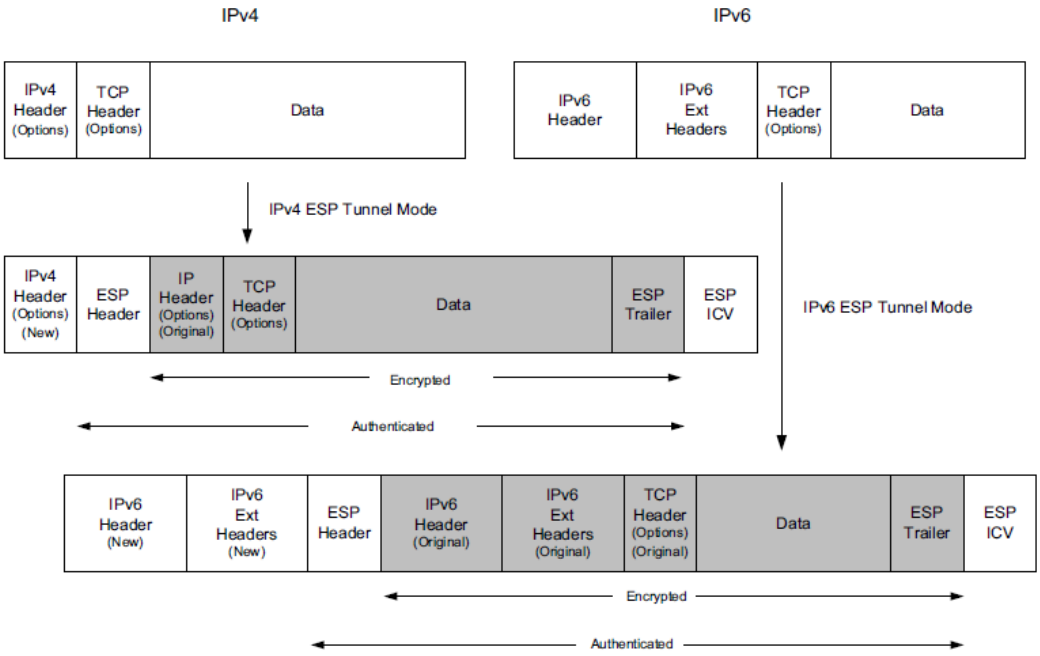

Figure 3 ESP Tunnel mode (Fall et al., R. W, Richard, Stevens 2012.)

2.5 GRE

2.5.1 Introduction

Generic Routing Encapsulation (GRE) provides tunneling methods to send packets through public network. GRE creates virtual point-to-point links that can be used with wide variety of network protocols. GRE is just an encapsulation protocol and does not offer encryption and all GRE packets leave in clear text. Therefore, GRE is often used with IPsec. (Teare 2010, 649)

2.5.2 Encapsulation

GRE adds two headers to the original packet that is called a payload packet. GRE encapsulation structure can be seen in Figure 4.

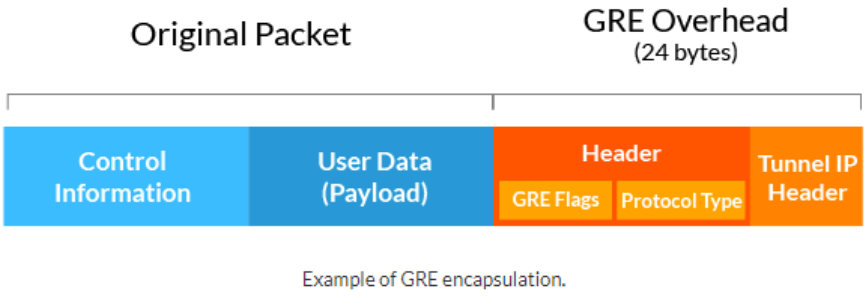

Figure 4 GRE encapsulation (Imperva 2018)

The payload packet is encapsulated inside of GRE Header, and the then the GRE packet is encapsulated in a delivery protocol. Inside the GRE Header there is a protocol type field that is used to indicate the payload's protocol. The field uses values that are specified in RFC 1700. For example, if Internet Control Message Protocol (ICMP) packet is encapsulated inside the GRE, the value of protocol type field is 1. The delivery protocol is often IP. When IP is used, the GRE packet is encapsulated inside of IP header. The IP header contains IP addresses of the GRE tunnels endpoints. Figure 5 shows the encapsulation structure when GRE is used inside of IP sec. With IPsec, GRE packets are encrypted. (RFC 2784, 2)

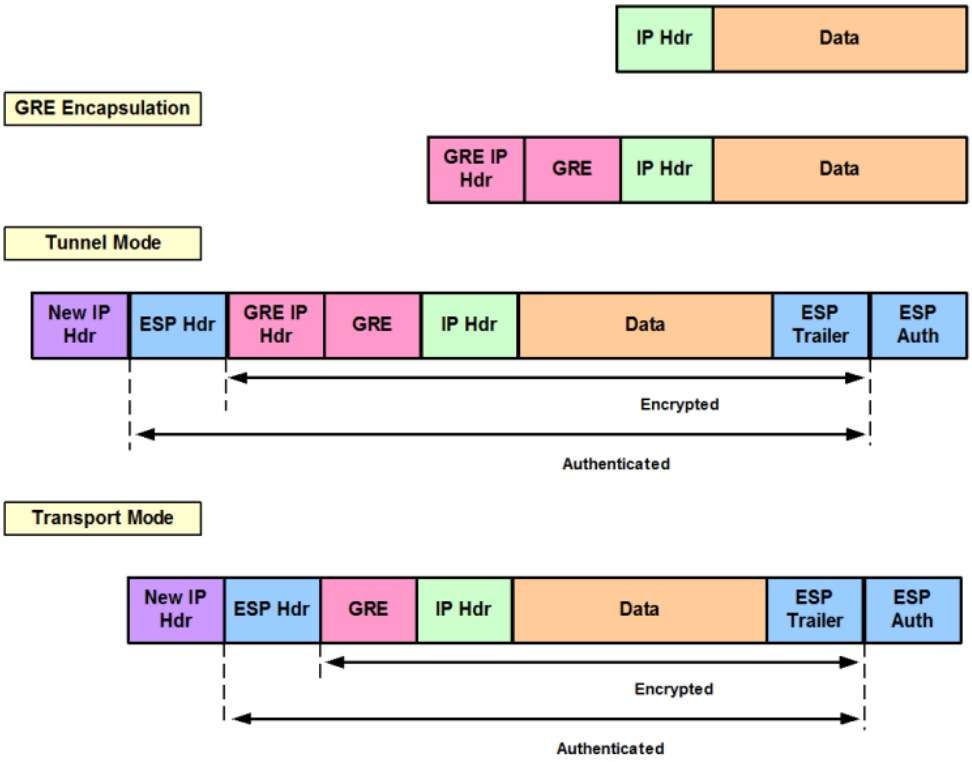

Figure 5 GRE over IPsec (duConet 2017)

IPsec does not support IP broadcast or multicast. Without these, IPsec prevents use of protocols like routing protocols. When GRE is used over the IPsec, all these limitations are fixed because GRE encapsulates the original packet inside of GRE header and only after that IPSEC encapsulation is used. (Cisco 2018b)

2.6 VXLAN

2.6.1 Introduction

Virtual Extensible Local area network (VXLAN) is a technology that allows networks to support more virtual local area networks (VLAN). IEEE's 802.1Q standard defines VLAN-ID to be 12-bits long, which limits the number of the VLANs to 4094. VXLAN protocol uses a longer logical network identifier and allows for more VLANs and therefore more logical networks. (Juniper)

The demand for an increased number of logical networks comes from datacenters. Nowadays datacenters use virtualization, and one physical server has now multiple virtual machines with each of these machines having its own layer-two address. This

requires large layer-two address tables and very big broadcast domains. To solve this problem, administrators have used VLAN; however, because of the increased number of virtual machines and tenants 4094 VLAN is not enough anymore. Normally datacenter administrators use one shared physical network for all tenants and implement isolation to this shared network. (RFC 2018b, 2.)

VXLAN runs over the existing networking infrastructure and creates a layer-two overlay network on an existing layer-three network. One VXLAN overlay network is termed a VXLAN segment. Each VXLAN segment is an isolated network and only machines in the same VXLAN segment can communicate with each other. VXLAN segments are identified by a 24-bit segment ID that is called a VXLAN Network Identifier (VNI). 24-bit VNI allows over 16 million VXLAN-segments to coexist within the same administrative domain. (RFC 2018b, 7.)

VNI identifies the scope of the Inner MAC and because each VXLAN segment is isolated from each other, there could be overlapping MAC-addresses across segments. The VNI is in an outer header that encapsulates the original MAC frame that are originated from the endpoint. RFC describes the VXLAN as “Due to this encapsulation, VXLAN could also be called a tunneling scheme to overlay Layer 2 networks on top of Layer 3 networks”. VXLAN tunnels are stateless and each frame going to VXLAN tunnel is encapsulated according to a set of rules. The end point of VLAN tunnel is called VXLAN Tunnel End Point (VTEP) and it could be implemented in both physical or virtual device. The VXLAN encapsulation is taken place in VTEP; thus, the VXLAN end point does not have to support the VXLAN. It only sees the normal Ethernet network. (RFC 2018b, 7.)

2.6.2 VXLAN Frame

VXLAN defines MAC Address-in-User Datagram Protocol (MAC-in-UDP) encapsulation scheme. MAC-in-UDP means that the original Layer 2 frame has added a VXLAN header and then placed in a UDP packet. VXLAN tunnels layer 2 networks over layer 3 network with this MAC-in-UDP encapsulation. (Cisco 2013)

Figure 6 shows the VXLAN packet format. The original layer two frame that is called the inner MAC frame is encapsulated with four headers.

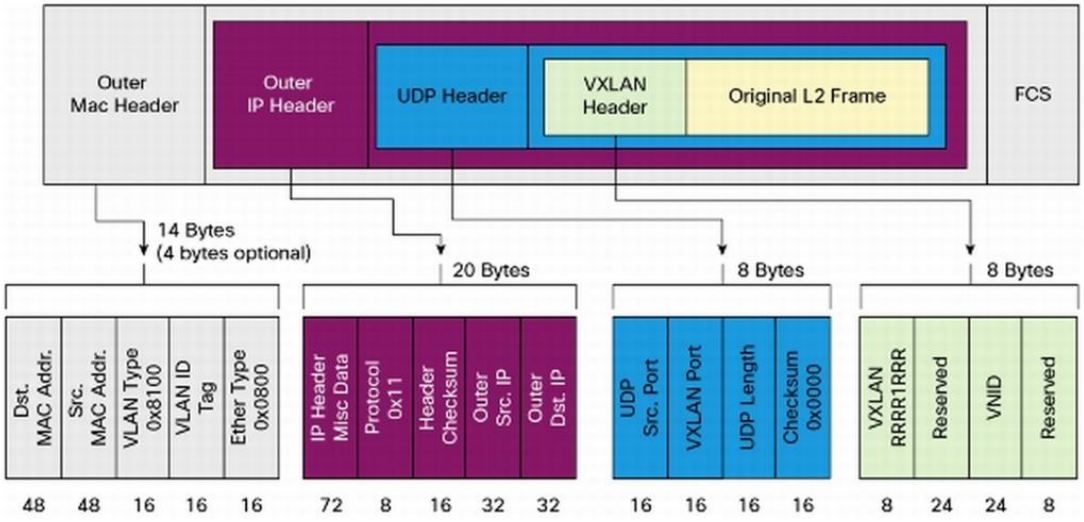

Figure 6 VXLAN header (Cisco 2013)

VXLAN Header

VXLAN header is an 8-byte field. It contains 8-bit flags field, 24-bit VXLAN segment ID / VXLAN Network Identifier (VNI) field and two reserved fields (24 bits and 8 bits). The fifth bit of Flags Field is I-flag and it must be set to 1 for valid VNI. VNI field defines the individual VXLAN overlay network, in which the communicating endpoints are situated. The reserved fields must always be set to zero on transmission.

Outer UDP Header

Outer UDP Header contains the destination port, source port and UDP checksum fields. For the destination port, VXLAN uses value 4789 that is assigned by IANA. This port should always be the default destination port on VXLAN implementation. The source port is provided by the VTEP and RFC recommends that the source port is calculated using a hash of fields from the inner packet. This is to enable a level of entropy for the load-balancing of traffic across the VXLAN overlay. With VXLAN, the UDP Checksum field should be transmitted as zero. In UDP packet that is received with a UDP, the checksum of zero must be accepted for decapsulation.

Outer IP and Ethernet Header

Outer IP header is created by the VTEP. It contains the source IP address of the VTEP that the original end point (Source of the inner source MAC) uses for communication. Destination IP address can be a unicast or multicast address. When using a unicast address, it represents the destination VTEP (Inner destination MAC's VTEP). The multicast address is needed when the original endpoint is sending broadcast traffic to the VXLAN, e.g. the address resolution protocol (ARP) broadcast frame. The Outer Ethernet header is the new MAC frame that is generated by the VTEP

2.6.3 VXLAN architecture

VXLAN creates the VXLAN overlay network on top of the Layer 3 IP network. In the edge of the underlay Layer 3 network are the VTEP devices. VTEPs are the VXLAN tunnel endpoints responsible for routing the VXLAN encapsulated frames over the Layer 3 network. (Cisco 2013)

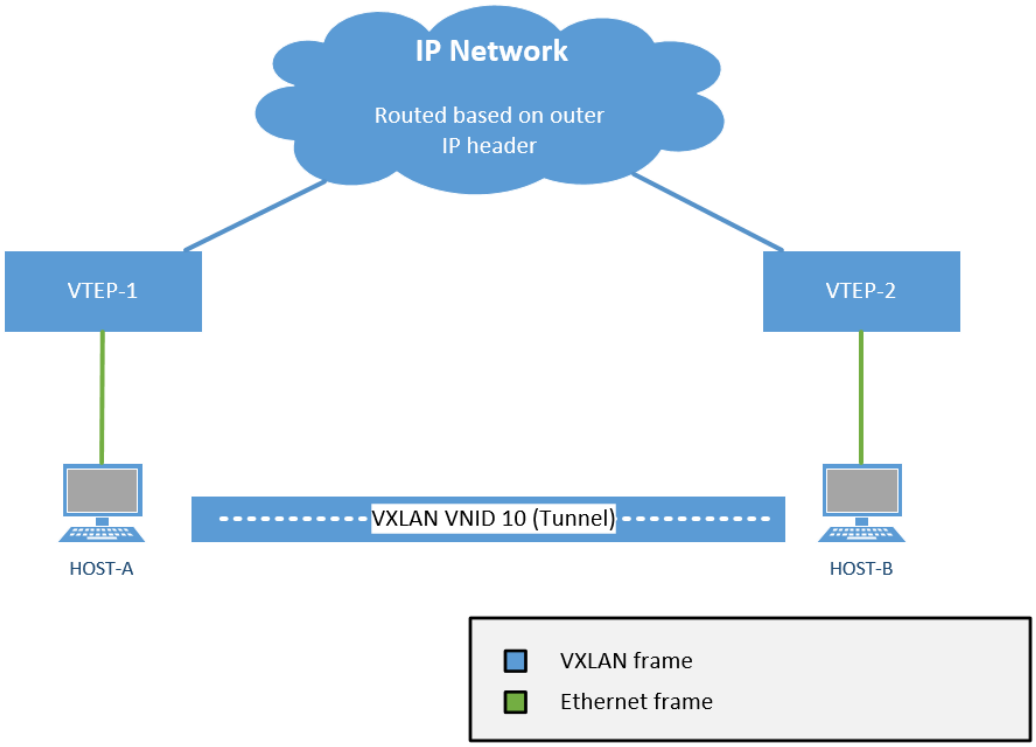

Figure 7 VXLAN packet forwarding (Cisco 2013)

Figure 7 shows the VXLAN packet forwarding flow. Host-A and Host-B are in the same VXLAN that has VNID 10. When Host-A sends a packet to Host-B, the packet is first forwarded to VTEP-1. VTEP-1 adds VXLAN header to the packet and outer IP header. The outer header has the destination IP address of the VTEP-2. The encapsulated packet is then routed through the Layer 3 IP network to the VTEP-2. VTEP-2 then deletes the outer header and VXLAN header and forwards the normal Ethernet frame to Host-B that is in the same VXLAN than the Host-A. (Cisco 2013)

2.7 Summary

SD-WAN brings flexibility to VPN connections. With SD-WAN, companies can use different kinds of connections and protocols. Generally, SD-WAN does not bring new protocols but it uses old protocols for SD-WAN tunnels such as VXLAN or IPsec. Some SD-WAN vendors use propriety protocols to create SD-WAN tunnels. The key element with SD-WAN is the centralized management and zero touch provisioning. With these functions, SD-WAN reduces the management overhead and speeds up the configuration process. SD-WAN often also reduces the cost of the VPN architecture because it can use different kinds of connections and is not limited to expensive Internet services such as MPLS-VPN.

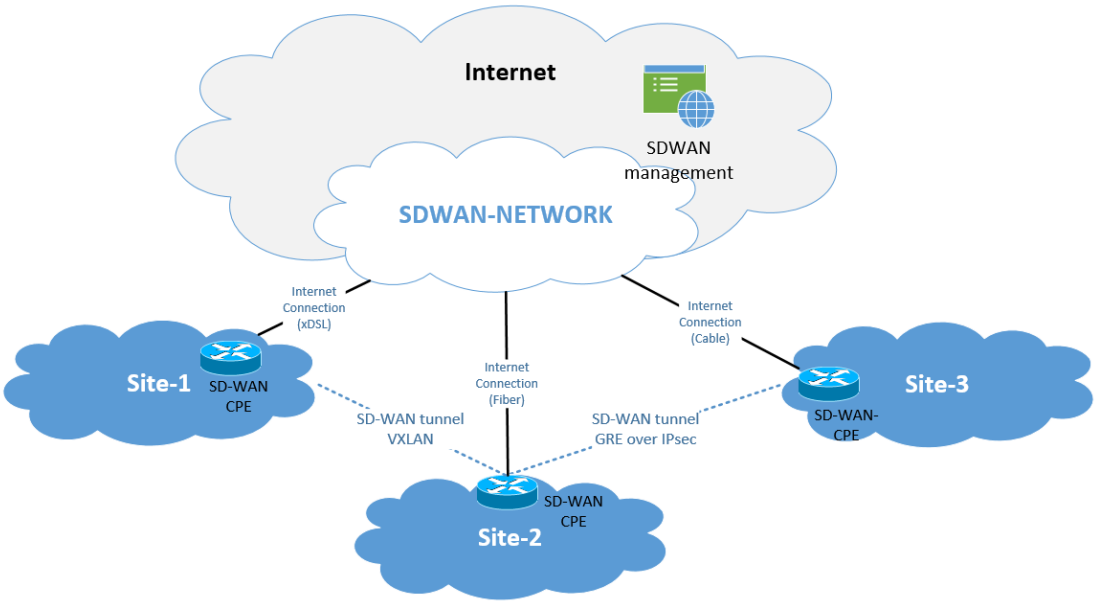

Figure 8 SD-WAN architecture

Figure 8 shows an example of a topology of the SD-WAN. In this case, SD-WAN connects three different sites together. SD-WAN uses different connection types in every site and also the tunneling protocol differs between SD-WAN tunnels. Even though Site-3 and Site-1 use different kinds of protocols and Internet connections, they are able to connect through Site-2. All configuration and management is implemented in SD-WAN management portal.

3 Requirements for federation of cyber ranges

3.1 Use cases

3.1.1 Networked cyber ranges

In the networked cyber range scenario, two or more cyber ranges can be connected to each other (Figure 9) in a point-to-point, point-to-multipoint, or mesh-like manner. The need for various connections arises due to different types of exercises and differences in cyber range structure

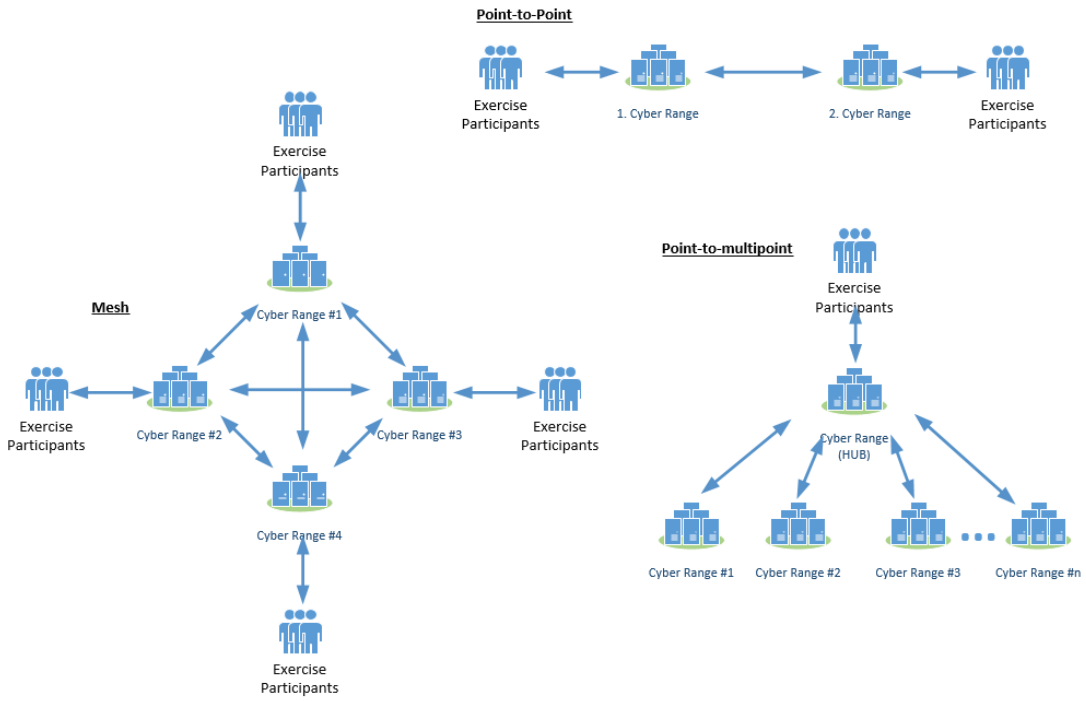

Figure 9 Networked cyber ranges

The need for various connections arises due to the different types of exercises and differences in cyber range structures. Some of the cyber ranges are capable of providing large-scale exercises independently while smaller ranges are capable of providing more dedicated smaller-scale exercises. By connecting smaller ranges together, it becomes possible to enhance the capacity to provide larger-scale exercises.

This use case can include extending the capacity of one cyber range by adding resources or other environments from another range. Additionally, the capabilities of

an exercise can be enhanced by connecting multiple cyber ranges together to create one logical cyber range for the exercise. Logical cyber range is a designated set of interoperable assets and capabilities within one or more ranges interconnected through a secure connection. With this approach, the participants in the exercise can connect to the exercise through all participating cyber ranges.

One range can also offer additional features or capabilities to the other ranges that can provide more versatile or larger-scale exercises. For example, one range can offer an exercise-planning service (i.e. the exercise's control plane) for the use by another range which has blue teams and red teams; with no capabilities to provide injects, scoring, or other control functionalities. This kind of setup, of course, depends on how the exercise scenario is written, and on the goals that will be set for the exercise.

The connectivity between ranges can be point-to-point, point-to-multipoint, or mesh-like depending on the setup and needs of the exercise.

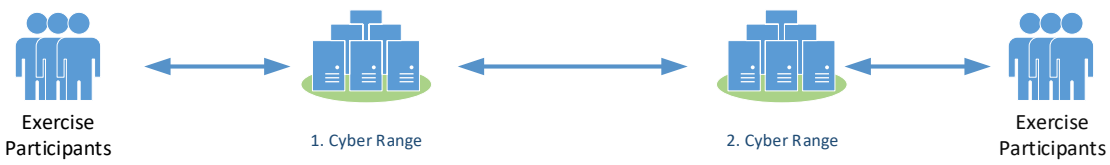

Figure 10 Point-to-Point

Figure 10 shows the connectivity between just two cyber ranges, both of which have participants in the exercise who are connected to the ranges.

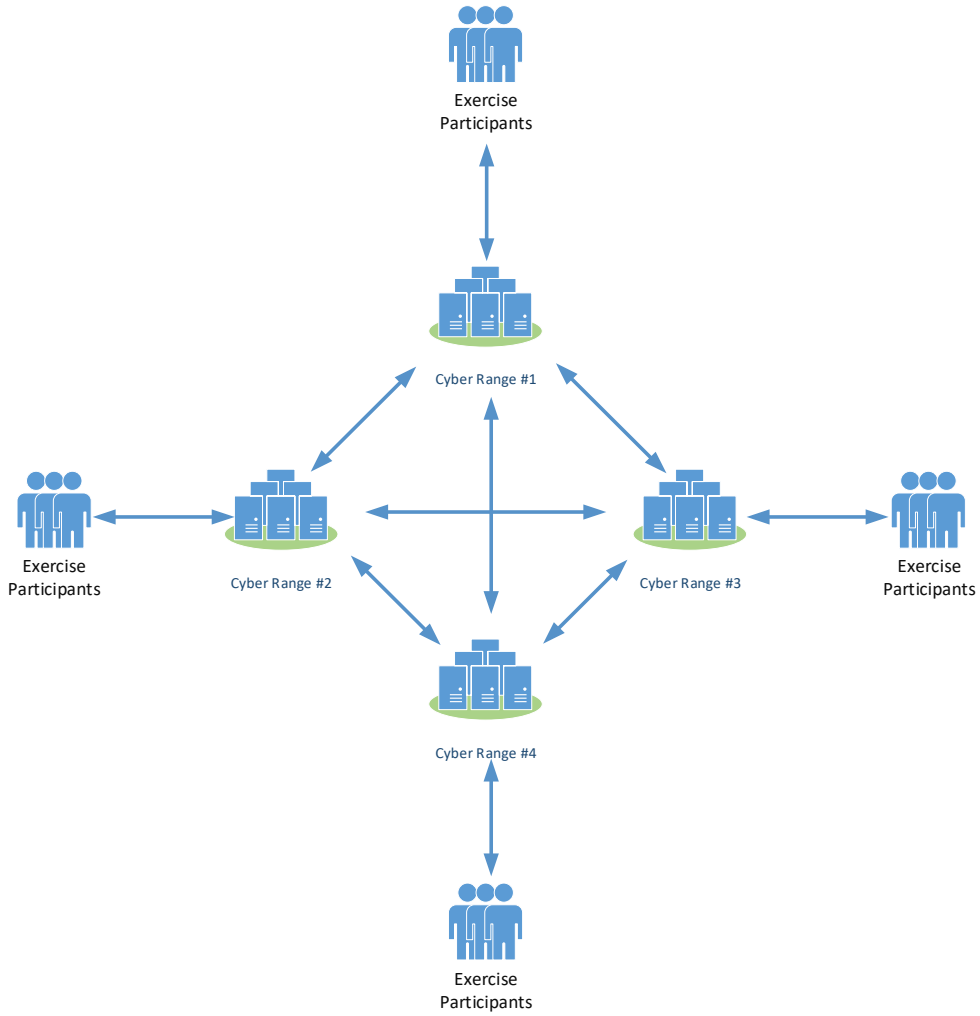

Figure 11 Mesh

Figure 11 shows a scenario for connecting three or more cyber ranges to each other in a mesh-like or full-mesh manner. This type of connectivity allows for many connections in a full-mesh topology. The formula $n*(n-1)^2$ represents the number of links between n ranges. Depending on the form of the exercise, it might be worthwhile to evaluate critically the need for full-mesh topology.

3.1.2 Extension of the cyber range's functionalities

In use case 2 one cyber range serves as an exercise provider (a hub) for the exercise. The hub offers connectivity to other cyber ranges that are used to provide additional functionalities to the hub for the exercise. The logical topology for this type of interconnection is point-to-multipoint where all the ranges are connected to one specific cyber range (Figure 12).

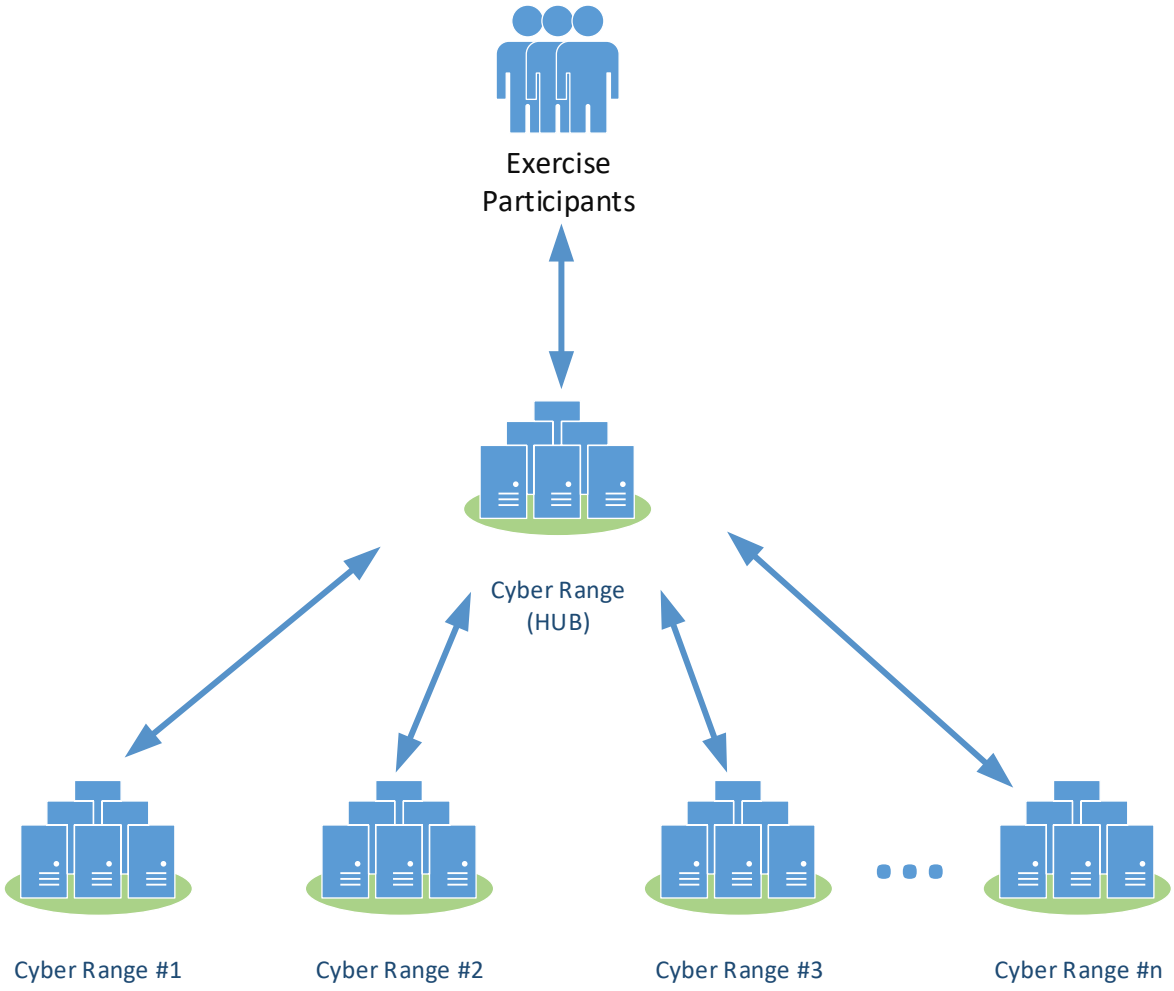

Figure 12 Hub and Spoke

The hub provides exercises to participants, and it adds or enhances the exercises with capabilities from other cyber ranges. In a cyber exercise, all participants use the hub range and if they have a need for capabilities from other cyber ranges or labs, they use those capabilities through the hub range.

3.1.3 Testbeds

Use case 3 offers the use of domain-specific features such as testbeds or labs to provide additional features that are not otherwise available. Testbeds are considered technology-specific testing and experimental environments that do not provide cyber exercises. Testbeds can include technologies such as IoT, ICS, robotics, smart grids, cyber-physical devices, AI, VR/AR, Big Data and healthcare. These kinds of testbed environments are rarely designed for a use in cyber exercises; however, they can be

used as a part of cyber exercises when connected to an appropriate cyber range (Figure 13).

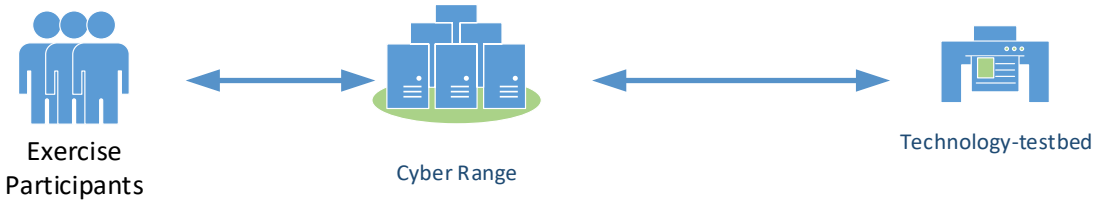

Figure 13 Testbeds

The connecting of testbeds to a cyber range usually takes place in a point-to-point manner; this means that use case 3, from a technical perspective, is close to use case one with two cyber ranges.

3.2 Requirement for physical Network connection

Specifications and checklists in this chapters uses key words that are specified in RFC 2119 to indicate requirements levels. RFC 2119 specify following words:

1. MUST This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
2. MUST NOT This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.
3. SHOULD This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
4. SHOULD NOT This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
5. MAY This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does

include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

3.2.1 Leased-line connectivity

Cyber ranges can be interconnected using dedicated lines; either physical cables or leasing dedicated connections (leased-line) from Internet Service Providers. Leased-line suitability for interconnecting a cyber range non-stop depends on the usage and must be agreed on between the cyber ranges. The connection's properties heavily depend on the exercise and must be agreed between the participating cyber ranges.

3.2.2 Internet connectivity

Cyber range needs an access to Internet to able to be connected to one or many cyber ranges. Using the dedicated physical links between cyber ranges is not necessarily plausible; therefore, a cyber range must have connection to the Internet. Using a dedicated Internet connection for cyber range interconnection provides a separation from production networks, and it is more predictable in terms of bandwidth usage.

Specification 1.1: Cyber Range MUST have a dedicated Internet connection for cyber range

Considering modern cyber ranges, many services and activities during the exercise need quite a large amount of throughput, which creates the need for an Internet connection to have reasonable amount of bandwidth available for cyber range interconnection. This results the following specifications:

Specification 1.2: The minimum bandwidth for the dedicated Internet connection MUST be greater than 100Mbit/s

Depending on how the scenarios and activities planned for exercises are developed, the need for even more bandwidth between cyber ranges can increase, which results in the following specification:

Specification 1.3: Bandwidth of the dedicated Internet connection SHOULD be able to be increased to 1000Mbit/s

To be able to have a reasonable quality connection to interconnect the cyber ranges, the latency to overlay network, providing the secure and routed connection between cyber ranges, needs to be as low as possible.-Vallaots (Vallaots 2017, 39) has defined that good latency for console use of the virtual machines is under 200 milliseconds. The overlay network itself creates some latency and the connections of other cyber ranges to overlay networks interface generate latency, which results in the following specification:

Specification 1.4: Round-Trip-Time (RTT) to Internet access MUST be less than 25ms

The Cyber range should be able to decide itself what IP protocol to use for the Internet connection. Therefore, the Internet connection can be either IPv4 or IPv6 (or both), which results in the following specification:

Specification 1.5: Internet connectivity MUST support either IPv4 or IPv6 protocols

3.2.3 Overlay network

Interconnecting multiple cyber ranges for usage examples described in chapter 2.1 requires scalable and easily set-up overlay network covering all the participating nations. Overlay network's function is to create "virtual" WAN-network for cyber ranges to join which is encrypted and provides appropriate tunneling functionalities. The overlay network should be implemented as SD-WAN solution from commercial ISP or creating own managed SD-WAN (SD-WAN manager) setup. Using ISP specific overlay solution can provide more predictable SLAs and Quality of Service (QoS), the

need for these must be considered during planning the exercise. Simplified structure of cyber ranges connection to overlay network is represented in Figure 14.

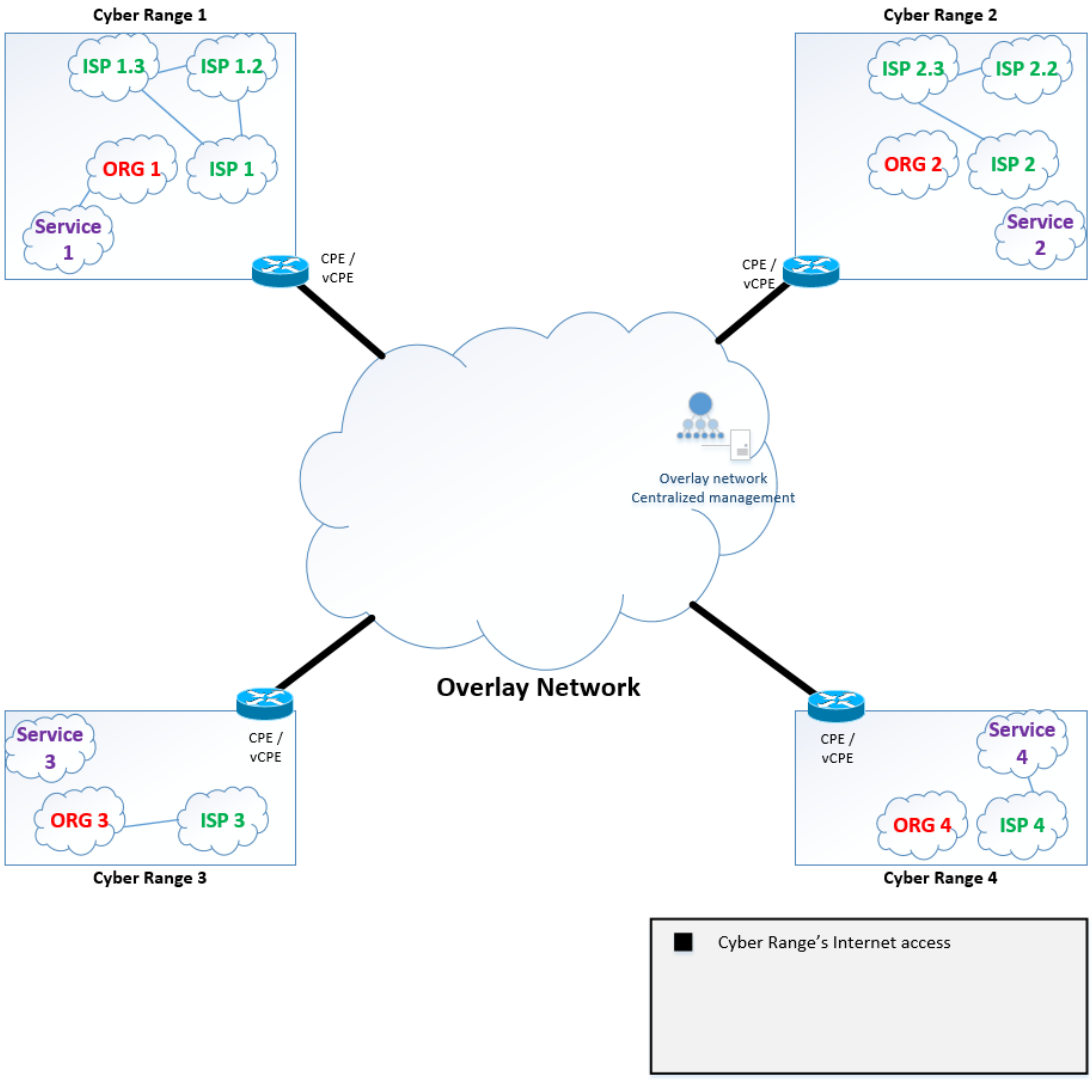

Figure 14 Overlay network

As shown in Figure 14, each cyber range has its own organizations (org1-4, there can be more than just one per cyber range), ISPs (usually multiple ISPs per cyber range), and services (multiple per cyber range). These organizations, ISPs and services are inside of cyber ranges and are normally isolated from the internet. These are connected through the overlay network to a different cyber range. When different kind of services and organizations are connected together, they may need layer two or layer three connections. For example, if two ISPs are peering with border gateway protocol together, they need a layer two tunnel between the cyber ranges. On the

other hand, layer three connection is best for some web-service when the client does not have to be in a same layer two network.

Specification 2.1: Overlay network MUST support L3 connectivity into cyber range (i.e. routed connectivity between cyber ranges)

Specification 2.2: Overlay network SHOULD support L2 connectivity into cyber range (i.e. extending L2 network between cyber ranges)

Cyber ranges are built to mimic the real Internet; therefore the overlay network must support both IPv4 and IPv6 protocols. If one of these is not supported, the realism and available scenarios are reduced.

Specification 2.3: Overlay interface MUST support IPv4 and IPv6 connections in dual-stack

Specification 2.4: Overlay network MUST support IPv4 and IPv6 (Cyber Range internet connectivity does not need to be dual-stack)

Previous in this chapter three different use cases were defined for the federation of cyber ranges. Those use cases defined three different network topologies that the overlay network must support. Three topologies were point-to-point, hub-and-spoke and mesh-like topologies. Mesh-topology can be divided to two different topologies partial-mesh and full-mesh. Depending on the overlay network the full-mesh can be costlier and take more resources than partial-mesh. However, in the case of SD-WAN, both of these uses same kind of physical topology, only the logical topology is defined from SD-WAN portal.

Specification 2.5: Overlay network MUST support the following topologies: point-to-point, hub-and-spoke, partial-mesh and full-mesh

In addition to exercise environments in Cyber range, there must be Internet access using some kind of customer premises equipment (CPE) that should be either physical or virtualized. With the CPE device cyber ranges connect to the overlay network.

Some cyber ranges or testbeds can be behind some firewall or router that is using network address translation (NAT). Those firewalls and router can be owned by a different owner than the owner of the cyber range. In that case, the cyber ranges may not be able to make changes to NAT or disable it, so the CPE device and the overlay network should support connectivity behind NAT. Usually, this is done by SD-WAN Orchestrator. The definition of the Internet connection defines that Internet connection's round-trip-time should be less than 25ms. SD-WAN will bring some delay also to the network, however, since SD-WAN can constantly monitor available paths and choose the least congested to route data, SD-WAN can keep the latency low. The maximum end-to-end round-trip-time depends on what kind of data is used in cyber ranges. If all the communications between cyber ranges are done via the overlay network with some real time application, the RRT should be less than 100ms. However, for normal data usage and to console or remote desktop usage less than 200ms is good. These result in the following specifications for the overlay network:

Specification 2.6: Overlay network SHOULD support connectivity behind NAT/FW

Specification 2.7: Overlay network endpoint SHOULD be implemented either in hardware or in virtual appliance

Specification 2.8: End-to-End Round-Trip-Time (RTT) MUST be less than 200ms

Overlay network topologies and connections should be managed with centralized management software that can be externally purchased or hosted by some other Cyber Range. Centralized management software should be available to all cyber ranges that are part of the overlay network.

Specification 2.9: Overlay network must have centralized management to control interconnections between cyber ranges

Specification 2.10: Centralized management should be available to all cyber ranges

When the federation is implemented with multiple cyber ranges, there can be more than one concurrent exercise to different customers. It is important that the different customer data is kept separated and the possibility of leakages of information is kept minimal. The operators should be able to make different topologies and networks inside of the overlay network that segregates the concurrent exercises.

Specification 2.11: Overlay network MUST support segregation of concurrent exercises

Because SD-WAN can use the public Internet, it is important that the overlay network is secured and encrypted. When SD-WAN tunnels are encrypted, no one can see the real data even they eavesdrop the traffic. These result in the following specifications for the overlay network:

Specification 2.12: Overlay network MUST be encrypted using industry standard protocols

4 Cyber range interconnection

Once Cyber ranges have the interconnection implemented using overlay network or leased-lines, the different logical connections between cyber ranges' exercise environments must be agreed upon between the cyber range owners. Figure 15 represents different scenarios that might be relevant when creating a joint-exercise between cyber ranges.

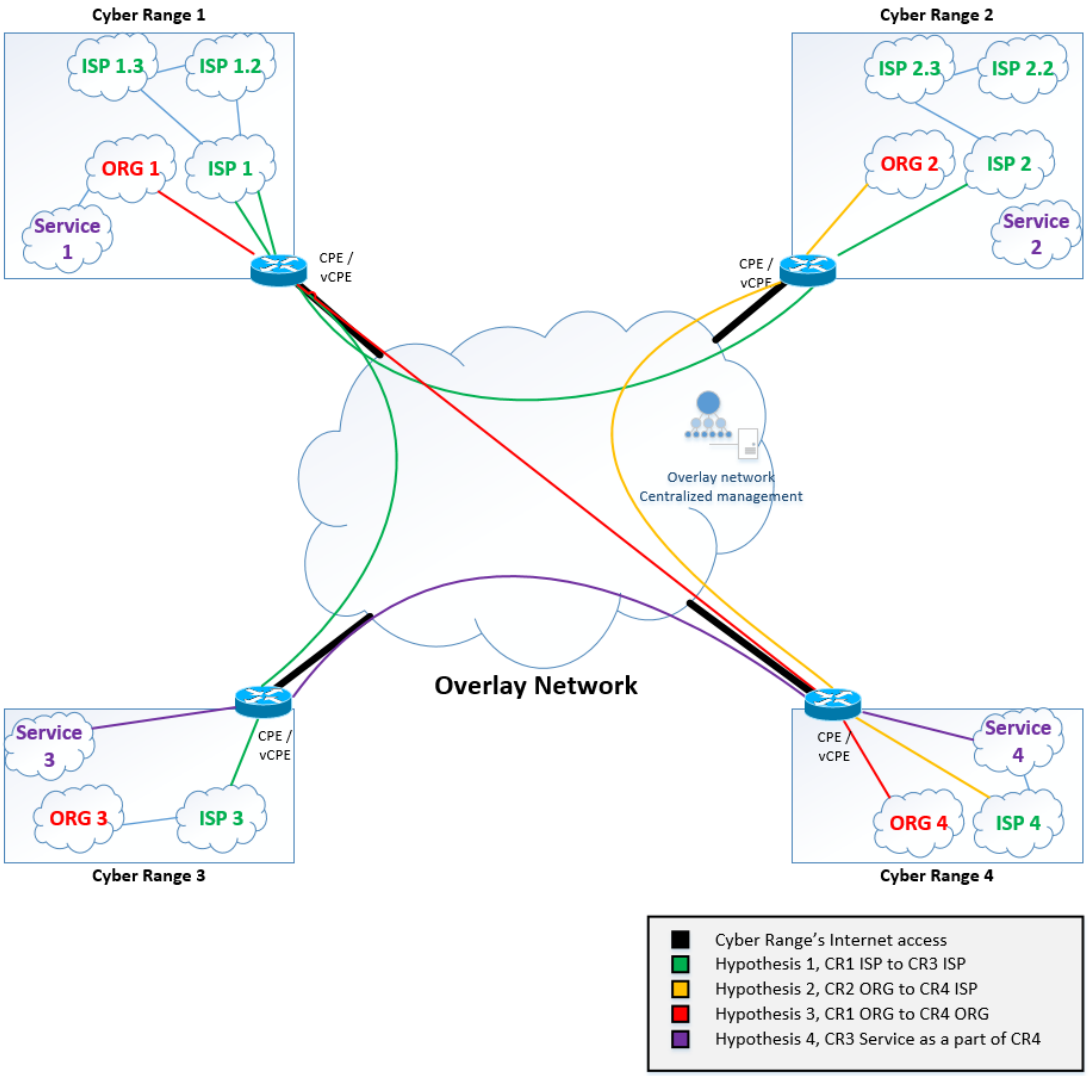

Figure 15 Logical connections

Cyber range's exercise environments mean fictional or simulated Internet Service Providers (ISP) or organizations that are inside or a part of the Cyber Range. In this chapter, the term Internet Service Provider (or exercise Internet Service Provider,

ISP) or organization (or exercise organization) mean networks that are inside the Cyber Range.

As shown in Figure 15, there might an exercise where cyber range (CR) 1's Internet Service Provider will be connected to CR2's Internet Service Provider and to CR3's Internet Service Provider (scenario 1, green lines). Another possibility is to connect CR2's organization environment as part Cyber range 4's Internet Service Provider (scenario 2, orange line).

In addition, it is possible to connect CR1's organization environment as a part of another organization that is in Cyber Range 4 (scenario 3, red line). Another option is also connect single device/service as a part of Cyber range, this is scenario 4 (purple line). In the following chapters, more detailed checklists are presented per scenario.

4.1 Scenario 1

Connecting multiple exercise Internet Service Providers from different cyber ranges

Connecting two exercise ISPs together between cyber ranges requires routing. Routing protocols and details should be agreed upon depending on the architecture of the cyber ranges. For example, for BGP connectivity between exercises, ISPs need many configurations to be specified so that the two ISPs can exchange routing information and transmit data.

Checklist 1.1: Routing protocols that are used to connect exercise ISPs SHOULD be agreed upon

An interconnection between two or more exercise ISP connected on Layer3 level and using Border Gateway Protocol (BGP) routing protocol creates needs to have certain configuration details exchanged between the participating Cyber Ranges. In addition to mandatory BGP attributes also routing policies and bandwidth limits should be defined. It is possible that cyber ranges can have same IP addresses in use and therefore routing policies must be define. On those routing policies the IP addresses that are exchanged are defined. The physical bandwidth of the cyber range's Internet

connections set limits to the exercise bandwidth. The exercise bandwidth should always be under the Internet connection's bandwidth. This results in the following checklists:

Checklist 1.2: BGP neighbor configuration SHOULD be agreed upon

Checklist 1.2.1: ISP BGP properties SHOULD be specified (Autonomous System number, public IP addresses, ISP name)

Checklist 1.2.2: ISP BGP neighbor IP addresses SHOULD be exchanged between cyber range operators

Checklist 1.2.3: ISP BGP neighbor routing policy SHOULD be defined

Checklist 1.2.4: Numbering schemas SHOULD be evaluated for overlapping IP subnet or AS number

Checklist 1.2.5: Exercise bandwidth between ISPs SHOULD be defined

4.2 Scenario 2

Connecting exercise organization environment to Internet Service Provider of another cyber range

In this scenario, two or more exercise organizations are connected to the exercise ISP of another cyber range based on exercise scenario. This kind of interconnection requires information of exercise organization's technical connectivity to exercise ISP which are same than in the real world, including IP-addresses and first hop connectivity information. In some cases, the exercise organization requires more than just an Internet access to exercise's "Internet", then the specified architectures and protocols must be agreed on by participating cyber ranges. When the exercise organization only requires Internet access to the exercise's Internet, the following checklists need to be taken into consideration:

Checklist 2.1: First hop connectivity information SHOULD be defined

Checklist 2.2: Bandwidth to ISP SHOULD be defined

Checklist 2.3: Routing from organization perimeter to ISP SHOULD be defined

Checklist 2.4: Organization name and ISP name SHOULD be exchanged

Checklist 2.5: Exercise specific public IP addresses for organization environment SHOULD be defined

In order to use Domain Name System in the exercise organization, DNS architecture must be defined. The organization needs to know ISP's DNS servers and organization have to inform about DNS delegations to the exercise's ISP. It is also important that both side of the exercise are in the same time, so the Network Time Protocol (NTP) servers must also be defined. These result in the following checklist:

Checklist 2.6: Exercise ISPs infrastructure (DNS servers, NTP, etc.) services SHOULD be exchanged

Checklist 2.7: Exercise organization environment's public DNS architecture SHOULD be defined and the needed DNS delegations should be agreed on

Checklist 2.8: Exercise organization's domain name SHOULD be specified for the exercise

In most cases cyber ranges is built to mimic the real Internet, therefore also the Public Key Infrastructure (PKI) is important to define. PKI is used to create certificates for example to websites so user can see that the webpage is trusted. If the exercise organization wants to get their website or other services to be trusted, they must get their certificates from the cyber range.

Checklist 2.9: Exercise organization's public services' PKI-certification needs SHOULD be defined

However, if the exercise organization has multiple sites, the requirements for exercise ISP connectivity might be more complex and require more detailed information

on the connectivity between the exercise organization's sites. This kind of connectivity inside cyber ranges can be implemented in multiple ways, which results the following checklists:

Checklist 2.10: Exercise organization's sites SHOULD be described

Checklist 2.11: Exercise organization's routing policy between its sites SHOULD be defined

Checklist 2.12: Exercise organization's preferred VPN solution SHOULD be described and SHOULD be agreed on

The checklists 2.10 – 2.12 are meant for fictional or simulated organizations that are inside Cyber Range. Therefore, the checklist 2.12 "preferred VPN solution" means VPN technology like IPsec used inside Cyber Range (not VPN or overlay solution to connect Cyber Ranges).

4.3 Scenario 3

Connecting exercise organization as a part of other cyber range's exercise organization

In this scenario, CR1's exercise organization needs to be extended with CR4's exercise organization (see Figure 12). CR4's exercise organization has some functionalities that are needed to connect to CR1's exercise organization. When joining another's cyber range's organization, the organization's information has to be about changes between ranges, in including an agreement on IP addresses and if cyber ranges use the same IP addresses, there may be a need for IP address changes or NAT. If the organization uses some kind of domain such as Active Directory, the information needed to join the domain has to be exchanged between ranges. This kind of scenario creates following checklists:

Checklist 3.1: IP address scheme SHOULD be agreed on and defined

Checklist 3.2: Appropriate network configurations SHOULD be specified

Checklist 3.3: Need and method to integrate workstations to Active Directory or equivalent domain SHOULD be defined

Checklist 3.4: In a case of overlapping IP addressing the appropriate NAT design SHOULD be agreed on

4.4 Scenario 4

Connecting specified device/service as part of other cyber range

In this scenario, CR3's service will used as part of CR4's Cyber Range (see Figure 12). For example, the traffic generator that is owned by CR3 is used in CR4's exercise. In order to connect the device or service to another cyber range, the connectivity information has to be exchanged between cyber ranges. A device or service may need some specific requirements for connectivity to work properly, such as bandwidth and these requirements should be defined. Because the service is owned and administrated in another cyber range, the cyber range that uses the device or service has to know the credentials and instructions in order to use the device or service properly. This creates the following checklists:

Checklist 4.1: First hop connectivity information SHOULD be defined

Checklist 4.2: Bandwidth requirement to first hop SHOULD be defined

Checklist 4.3: Appropriate credentials for the usage of the service SHOULD be provided

Checklist 4.4: In a case of overlapping IP addressing the appropriate NAT design SHOULD be agreed on

Checklist 4.5: Appropriate instructions and technical configurations SHOULD be provided

5 Demonstration

One of the objects of the thesis's was to design high level technical plan for the demonstration of the federation of cyber ranges. Demonstration's objectives are to test all the use cases that was defined in chapter three and show that federated cyber ranges can be used on a cyber security exercise and that already made scenarios can be adapt to federation. These use cases dictate that the demonstration scenario is capably to test defined topologies: point-to-point, hub and spoke and mesh.

In figure 16 is the physical topology of the demonstration. The demonstrations contain three cyber ranges so the defined topologies can be tested.

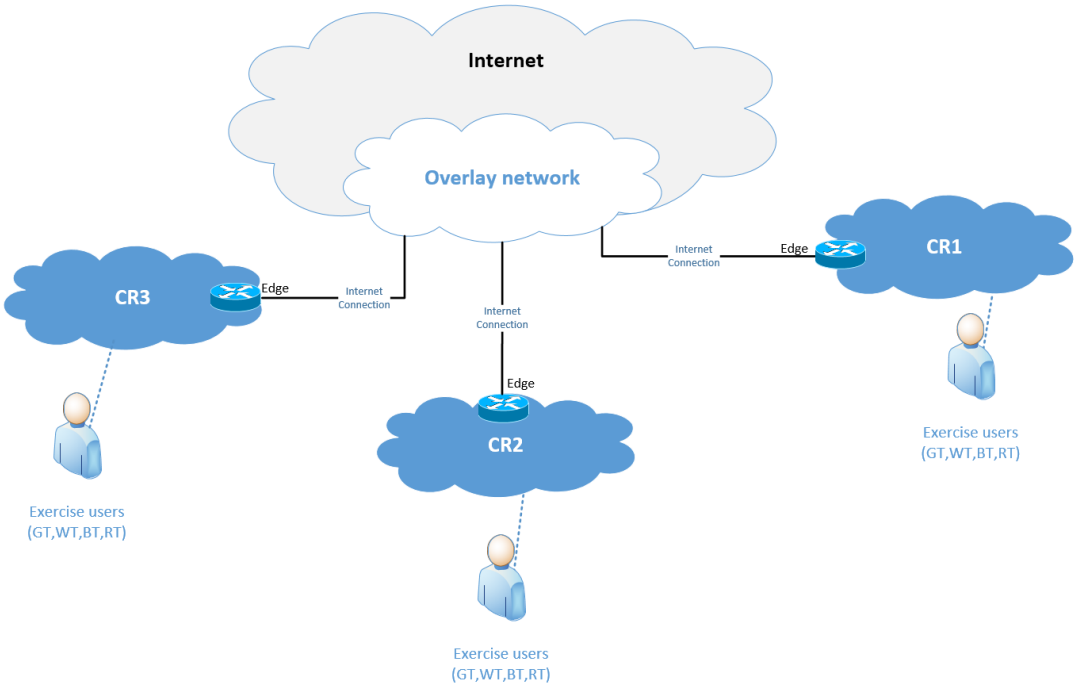

Figure 16 Demonstration's physical topology

These participating cyber ranges connects to the overlay network. For the demonstration the overlay network uses Internet for the underlay network so the cyber ranges only need Internet connection. The Internet is most cost-effective technic for the underlay network. Cyber ranges Internet connection have to meet the requirements that was specified in chapter four.

For the exercise's scenario is used existing scenario that JYVSECTEC has already use in RGCE. Now this scenario is divided for three different cyber ranges. The Exercise's scenario includes white, blue and red team. In the exercise blue team is defending automation organization that has office and automation environments. These environments separated from each other and are connected by MPLS-VPN. This scenario is using the scenario 3 in chapter 4, where exercise organization is extended to other cyber range. (Figure 17)

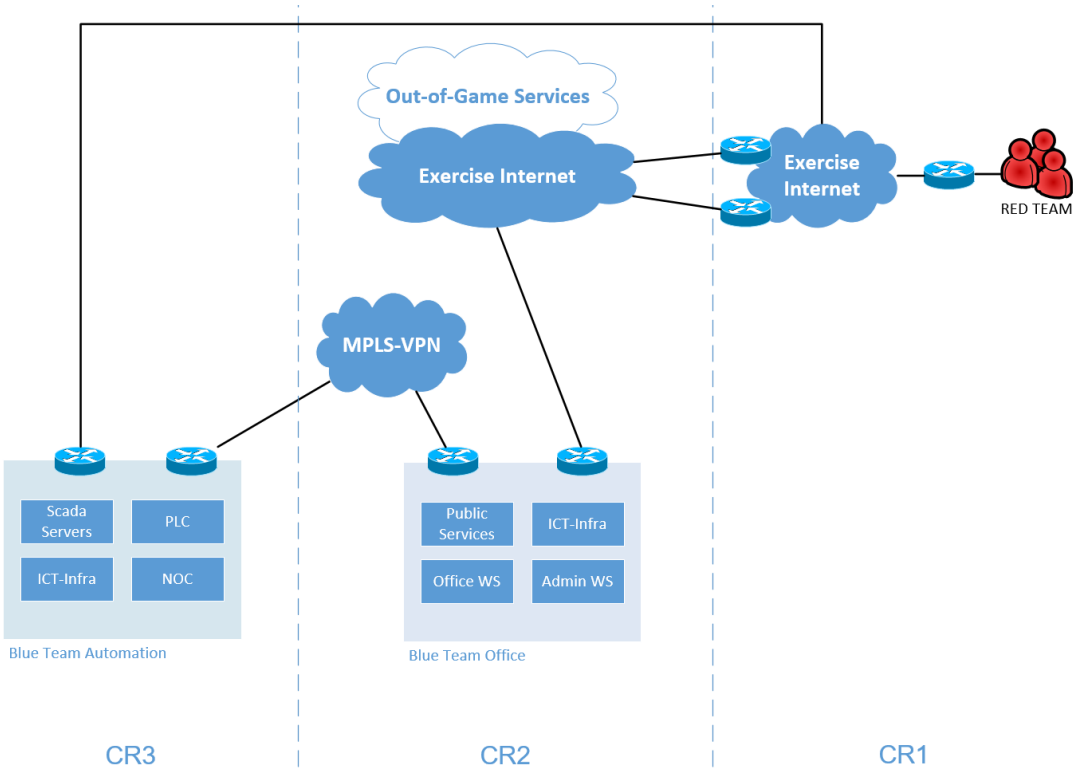

Figure 17 Exercise topology of demonstration

Cyber range 2 is the main range in the scenario and it contains the blue team's office environment, exercise Internet and Out-of-Game Services. Out-of-Game services includes exercise control systems used by white team and Out-of-Game communication services. To test chapters four's scenario 1, the exercise Internet is extended to CR1. Red team is located only in CR1. Even though red team's physical location is in CR1, red team executed attacks to services that are inside of CR2 and CR3 through the exercise Internet. Blue team's automation environment is in CR3. The automation environment's exercise Internet traffic is going through the CR1, so the overlays topology is mesh because every cyber range is connected to each other.

Figure 18 shows the exercise topology on overlay's perspective. Every line in Figure 18 presents a network that is defined inside of the overlay network.

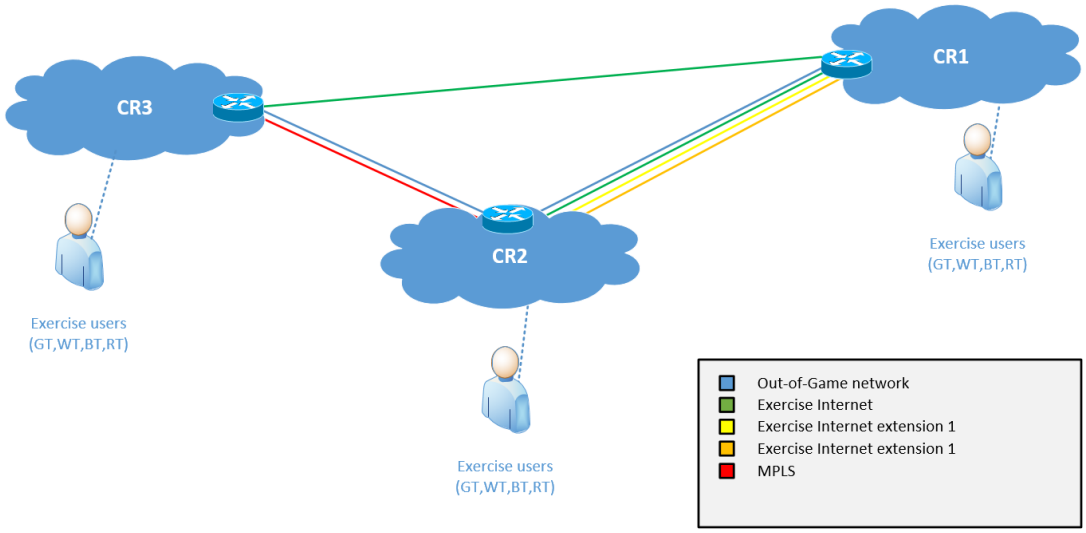

Figure 18 Demonstration's overlay network

As can be seen the overlays topology is full mesh. Since the topology is full mesh, other topologies that were defined in chapter can be also tested when some parts of the exercise topology are disconnected from the overlay network. For example, if the CR3's automation environment's exercise Internet traffic is disconnected from CR1 and then rerouted directly to CR2 the topology is then hub and spoke.

6 Conclusions

The goal of this master's thesis was to define use cases and requirements for technical federation of cyber ranges. Overall the defined use cases and requirements will help JYVSECTEC in a next step. With the result of the thesis vendors and service providers can be contacted and start to plan technical demonstration and tests. However, these results are only the starting point and the requirements should be updated after the technical demonstration and before the final solution and production use.

In this research the qualitative research method was used with inductive analysis. Most of the material that was used in this master's thesis was academic researches or network vendor's publications. For technical topics RFC documents was also used. Most of the referenced material was written on cyber security exercises or cyber ranges. There very few sources for technical federation and that is why many network vendors' publications was used. Those publications were more for companies that wants to connect different branches together. That is the reason why many of the defined requirements was based on author's own experience and knowledge of cyber ranges and cyber security exercises. The qualitative research and inductive analysis supported this kind of approach well. Most of the problems during the research were a result of author's lack of experience in research. Also, the timetable was very tight and with a better planning, there could have been time to evaluate some vendor's product and test defined requirements in real life.

The master's thesis resulted in use cases, list of requirements and checklist. The list of requirements included 17 different requirements for the interconnection of cyber ranges. After the initial technical connection, there are many different aspects that must be considered before the federation is usable. The purpose of the checklist is to notice these aspects or problems and help connect different cyber ranges functions together.

When considering these defined requirements for the federation, the best solution for the overlay network is SD-WAN. SD-WAN uses different kind of protocols often those that were discussed in chapter 2 and combine these protocols to easily handled network. With ease of use, the centralized management and support to create

different kind of topologies and networks inside of overlay network will be much more efficient and flexible than the protocols by themselves. The next step is to make a technical demonstration and update the requirements based on the experiences of the technical demonstration.

References

Cisco 2013. VXLAN Overview: Cisco Nexus 9000 Series Switches. Accessed 12 November 2018. Retrieved from https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/white-paper-c11-729383.html

Cisco 2018a. Cisco SD-WAN Solution overview. Accessed 14 October 2018. Retrieved from https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-sd-wan-sol-overview-cte-en.pdf?oid=otren012099

Cisco 2018b. Point-to-Point GRE over IPSec Design and Implementation. Accessed 28 October 2018. Retrieved from https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/P2P_GRE_IPSec/P2P_GRE/2_p2pGRE_Phase2.html#wpxref46836

Thomas, D. 2006. A General Inductive Approach for Analyzing Qualitative Evaluation Data. American Journal of Evaluation, Vol. 27 No. 2.

Davis, J., Magrath, S. 2013. A Survey of Cyber Ranges and Testbeds. Department of Defence, Australian Government.

duConet 2017. IPsec: Crypto Maps, GRE and VTI. Accessed 18 November 2018. Retrieved from https://duconet.com/ipsec-crypto-maps-gre-vti/

ENISA 2015. The 2015 Report on National and International Cyber Security Exercises. Accessed 30 November 2018. Retrieved from https://www.enisa.europa.eu/publications/latest-report-on-national-and-international-cyber-security-exercises

European Commission 2013. Cybersecurity Strategy of the European Union:

An Open, Safe and Secure Cyberspace. Accessed 9 December 2018. Retrieved from http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

Fall, R. W, Richard,Stevens. 2012. TCP/IP Illustrated, Volume 1. San Francisco. Addison-Wesley.

Gartner 2018. IT Glossary. Accessed 12 October 2018. Retrieved from https://www.gartner.com/it-glossary/software-defined-wan-sd-wan

Imperva 2018. GRE Tunnel for Humans: Making Sense of Generic Routing Encapsulation. Accessed 15 November 2018. Retrieved from https://www.incapsula.com/blog/what-is-gre-tunnel.html

Juniper 2018. Understanding VXLANs. Accessed 4 November 2018. Retrieved from https://www.juniper.net/documentation/en_US/junos/topics/topic-map/sdn-vxlan.html

JYVSECTEC – Jyväskylä Security Technology. 2018a. JYVSECTEC's website. Accessed 1 October 2018. Retrieved from https://www.jyvsectec.fi

JYVSECTEC – Jyväskylä Security Technology. 2018b. JYVSECTEC CYBER RANGE, RGCE and solutions. Accessed 10 November 2018. Retrieved from https://jyvsectec.fi/wp-content/uploads/2018/10/JYVSECTEC-cyber-range.pdf

Kick, J. 2014. Cyber Exercise Playbook. The Mitre Corporation.

MEF 2017. Understanding SD-WAN Managed Services. Accessed 19 October 2018. Retrieved from http://www.mef.net/resources/download?id=45&fileid=file1

NIST – National Institute of Standards and Technology 2018. Cyber Ranges. Accessed on 30 November 2018. Retrieved from https://www.nist.gov/sites/default/files/documents/2018/02/13/cyber_ranges.pdf

Nuage 2016. Evolution of Wide Area Networking. Accessed 17 October 2018. Retrieved from http://www.nuagenetworks.net/wp-content/uploads/2015/08/PR1506012099EN_NN-VNS_Enterprise_CaseStudy.pdf

RFC7348. 2014. Virtual eXtensible Local Area Network. Accessed 12 November 2018. Retrieved from https://tools.ietf.org/html/rfc7348

RFC5406. 2009. Guidelines for Specifying the Use of IPsec Version 2. Accessed 1 November 2018. Retrieved from https://tools.ietf.org/html/rfc5406

RFC6071. 2011. IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap Accessed 1 November 2018. Retrieved from https://tools.ietf.org/html/rfc6071

SDxCentral. What is sofware defined networking. Accessed 12 October 2018. Retrieved from https://www.sdxcentral.com/sdn/definitions/what-the-definition-of-software-defined-networking-sdn/

Secretariat of the Security Committee. 2013. Finland's Cyber Security Strategy. Accessed 12 December 2018. Retrieved from https://turvallisuuskomitea.fi/wp-content/uploads/2018/09/Cyber-Strategy-for-Finland.pdf

Teare, D. 2010. Implementing Cisco IP Routing. Indianapolis. Cisco Press.

Vallaots, A. 2017. Federation of Cyber Ranges. Master's Thesis. Institute of Computer Science. University of Tartu.