Proposal No. 830929
Call H2020-SU-ICT-03-2018

Project start: 1 February 2019
Project duration: 42 months

Cyber Security for Europe

D7.3

Evaluation report on integration demonstration

Document Identification	
Due date	31 August 2021
Submission date	4th August 2021
Revision	1.3

Related WP	WP7	Dissemination Level	PU
Lead Participant	JAMK	Lead Author	Juha Piispanen (JAMK)
Contributing Beneficiaries		Related Deliverables	D7.1, D6.4

Abstract:

This deliverable introduces two use cases of cyber range technical federation and the requirements that were fulfilled and implemented in Flagship 1, a two-day online-only cyber security exercise organised by CyberSec4Europe in January 2021. In Flagship 1, there were total 36 participants from 22 affiliates across the Europe. The event utilised a cyber arena, realistic global cyber environment (RGCE) as a technical exercise environment. The participants of the event seamlessly connected to RGCE using a prepared virtual machine. The virtual machine was configured to use the implemented cyber range federation network. To enrich the exercise environment, Flagship 1 technical environment was extended with a commercial Amazon AWS cloud component running a testbed. Both the end-user connectivity and the extension of the cyber arena were implemented utilising an open-source software-only SD-WAN technology. The used technology performed reliably with low network latency and low CPU usage. It is estimated to be production-level maturity.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929.

Executive Summary

This deliverable describes the implementation of the two use cases and their requirements for cyber range technical federation: to offer end user access to a Cybersecurity exercise (CSE) environment and to extend a cyber range with a testbed to enrich an CSE contents. In Flagship 1, a CSE organised in CyberSec4Europe, a testbed was deployed to a commercial cloud.

Cyber Ranges are technical platforms that contain cyber-physical, simulated, emulated (or a combination of those) information or operational technology (IT/OT) systems, networks, processes and data. Cyber security research and development, certification and development of indivuals' and workforce knowledge, skills and abilities can take place in a cyber range. Cyber ranges can also be used for certification and to develop organisations preparedness responding to a cyber-attack or incident.
According to Karjalainen and Kokkonen (Karjalainen M. & Kokkonen T. 2020) the perspective and requirements for developing a cyber range are often narrow and limited to a specific area of interest. Cyber arenas are state-of-the-art modern and complex cyber security exercise platforms, containing e.g. simulated Internet and varied organisation environments (Karjalainen M. & Kokkonen T. 2020). Test beds are even more focused than cyber ranges, and they are used, for example, technology development, testing, and demonstration.

Meeting the needs and requirements of cyber range's end users and the event targeted at them, two or more cyber ranges, cyber arenas or testbeds can be interconnected, i.e. technically federated. Thus, the resulting federated cyber range can offer to the end users a technical platform that contains the features and the functionalities of the federated ranges, forming a single larger environment that the end users access and use. Technically, the federating of cyber ranges has been estimated to relieve the investment costs in technology and workforce salaries that the development of a cyber range requires (ECSO 2020). The concept of cyber range sharing and pooling has been recognised by various organisations, e.g. by the European Union (EU 2019) and European Defence Agency (EDA 2018).

CyberSec4Europe introduced requirements for cyber range technical federation in the PART B of the deliverable "D7.1 Report on existing cyber ranges, requirements" (CyberSec4Europe 2020). Two use cases and their requirements were implemented and demonstrated during Flagship 1, a two-day online only Cybersecurity Exercise (CSE), held in January 12-13 2021, organised by CyberSec4Europe and conducted by JAMK. In Flagship 1 there were 36 participants from 22 CyberSec4Europe affiliates across Europe. Flagship 1 utilised a Realistic Global Cyber Environment, a cyber arena developed, operated and owned by JYVSECTEC. Flagship 1 is reported in the deliverable "D6.4 Flagship 1" (CyberSec4Europe 2021).

Flagship 1 included tasks and learning objectives for technical experts and non-technicians. Because of this content decision, the provision of an access to the Flagship 1 environment that was as easy as possible was seen as an essential feature. For Flagship 1, the testbed was deployed to a commercial cloud to enrich an the event contents.

To define, model and organise the use cases and their respective requirements in Flagship 1, open-source software-only SD-WAN technology was utilised. The technology identification, the evaluation and the technology testing was performed prior selecting the implementation technology.

In a CSE, network reliability, throughput, latency and security are the key factors necessary not only to provide a smooth CSE experience to the participants, but also to fulfill the requirements a cyber range operator and owner has set. The demonstrated technology is estimated to be production-ready, that is it could be used to technically federate cyber ranges in cross-border events.

Document information

Contributors

Name	Partner
Jani Päijänen	JAMK

Reviewers

Name	Partner
Cham Nam Ngo	UNITN
Christos Douligeris	UPRC

History

Version	Date	Authors	Comment
0.1	1 April 2021	Jani Päijänen	Initial Document Structure.
0.2	3 June 2021	Juha Piispanen, Jani Päijänen	Document for language review.
0.3	8 June 2021	Jani Päijänen	Language corrections. Added chapter After Exercise Survey. Modifications to Executive summary.
0.4	28 June 2021	Jani Päijänen	Incorporated reviewer's comments in to the document. Added missing acronyms and terms. Changed two tables into pie-charts.
1.0	28 June 2021	Jani Päijänen	Lifted version number to 1.0.
1.1	29 June 2021	Jani Päijänen	Removed incorrectly inserted Annexes from the text. Changed version history month names to full months. Modified Refences formatting. Aligned the captions of tables with the deliverable template.
1.2	29 June 2021	Jani Päijänen	Corrected UNITN in the reviewers table. Layout modifications: added an empty line after the figures.
1.3	29 June 2021	Jani Päijänen	Removed an extra character from the header, and corrected two typos.
1.3	29 July 2021	Ahad Niknia	Final check and preparation for submission

Table of Contents

List of Figures

List of Tables

List of Acronyms

A	**AR**	Augmented Reality
C	**CSE**	Cyber Security Exercise
	CR	Cyber Range
E	**ECSO**	European Cyber Security Organisation
F	**FW**	Firewall
I	**ICS**	Industrial Control System
	IoT	Internet of Things
	IP	Internet Protocol
	IPSec	Internet Security Protocol
	IPv4	Internet Protocol version 4
	IPv6	Internet Protocol version 6
J	**JAMK**	JAMK University of Applied Sciences.
	JYVSECTEC	Jyväskylä Security Technology (JYVSECTEC) is the cyber security, artificial intelligence and data-analytics research development and training center in the Institute of Information Technology, part of JAMK, Finland.
L	**L2**	ISO's OSI model level 2
	L3	ISO's OSI model level 3
N	**NAT**	Network Address Translation
P	**P2P**	Peer-to-Peer
S	**SDN**	Software Defined Networking
	SD-WAN	Software Defined Wide Area Network
R	**RGCE**	Realistic Global Cyber Environment (RGCE) is JYVSECTEC planned, developed, operated and owned cyber arena.
	RTT	Round-Trip-Time
V	**VL1**	ZeroTier Virtual Layer 1, Peer to Peer transport layer
	VL2	ZeroTier Virtual Layer 2, The Ethernet virtualization layer
	VPN	Virtual Private Network
	VLAN	Virtual LAN

VR	Virtual Reality
VRF	Virtual Routing and Forwarding
VXLAN	Virtual Extensible Local Area Network

Glossary of Terms

A **Amazon AWS**

Amazon Web Services (AWS) is a pay-as-you-go metered service offering computing resources and APIs.

API

Application Programming Interface.

B **Bash**

Bash (Bourne Again Shell), is a Unix shell and command language.

Big Data

Big data refers to the collection, processing and analysis of different types data produced and collected from various types of sources, such as people, machines and sensors. The quantity of big data increases continuously.

C **Controller**

Software defined networks require a controller that controls the defined network address spaces, allows client device(s) to join the network and controls the defined network routings.

Cyber Arena

A realistic large-scale cyber range. Contains multiple independent or interdependent cyber ranges.

Cyber-physical device

Cyber-physical devices are network connected or connectable devices. They can be e.g. personal gadgets, like wearable health or activity monitoring devices, or industrial process automation devices.

Cyber Range

Cyber Ranges are simulated, emulated and/or cyber-physical environments that can be used for cyber security research and development, training, exercises, certification and education.

F **Federation Network**

A federation network is formed by the connected networks, their IP-address spaces, IP-addresses and IP address routings.

G **Green Team**

The technical support and maintenance team of a cyber range or of cyber arena during a CSE is called as green team.

S **Smart Grid**

A smart grid is intelligent energy distribution network that can automatically monitor energy flows and adjusts to changes in energy demand and supply.

T **Testbed**

Testbeds are specific technical environments to experiment, test or demonstrate a technology or its feasibility.

1 Cyber Range Technical Federation

In PART B of "D7.1 Report on existing cyber ranges, requirements" (CyberSec4Europe 2020) the term cyber range technical federation was introduced as an attempt to distinguish the interconnection of cyber ranges from the sharing of operational cyber range configuration data or data that is generated by activities performed in an event held in a cyber range. A cyber Range technical federation is recognised by the European Defence Agency (EDA 2018) and the European Union (EU 2019). A cyber range technical federation is an online activity, whereas cyber range operational federation can be an offline activity. Federating a cyber range with one or more testbeds, cyber ranges or cyber arenas forms a federation network. By accessing a federated network, the end users may gain access to a larger or to a more realistic cyber range than a single cyber range of the network could provide. Technically federating cyber ranges can relieve the investment costs in technology and workforce salaries that the development of a cyber range requires (ECSO 2020). Developing a cyber range that meets the set technical, operational and other requirements, requires skilled workforce and investment budget to acquire the required hardware and software, and to install, deploy and configure the cyber range for use.

In PART A of "D7.1 Report on existing cyber ranges, requirements" (CyberSec4Europe 2020), it was reported that the then-planned or the then-used cyber range interconnection technologies were SSH and IPSEC network tunnels, VPN solutions and SD-WAN. This deliverable focuses on the deployment and demonstration of an open-source based SD-WAN technology in a cyber range technical federation. The technology was demonstrated in Flagship 1, a CSE organised by CyberSec4Europe (CyberSec4Europe 2021). The demonstrator implemented two use cases from the requirements specification, PART B of "D7.1 Report on existing cyber ranges, requirements" (CyberSec4Europe 2020). The demonstrated use cases were:

1. Enhancing and enriching an existing cyber range with commercial cloud hosting services (Use Case 3: Adding Testbeds to a Cyber Range)
2. End-user connectivity (Remote user connectivity).

The implemented requirements specification's use case 3, "Adding Testbeds to a Cyber Range", included the technical federation of a commercial Amazon AWS cloud instance into the Flagship 1 technical exercise environment and the running of the exercise related service in the cloud. The remote users', i.e. participants', connectivity was implemented with a prepared VirtualBox 6.1.x virtual machine image, which the exercise attendees commissioned into their systems.

The Flagship 1 CSE technical environment and federation demonstration utilised Realistic Global Cyber Range (RGCE) (JYVSECTEC 2018). RGCE is a comprehensive cyber arena (Karjalainen M. & Kokkonen T. 2020). RGCE is developed, operated and owned by JYVSECTEC. RGCE runs in JYVSECTEC's datacentre.

Context of the demonstration

Flagship 1 was a two-day online-only cyber security exercise (CSE) organized by CyberSec4Europe task T6.4 of WP6. The participants of the event were CyberSec4Europe affiliates. The participants were divided into five teams by the CSE conductor, JYVSECTEC. Each team had equal tasks and objectives: to verify if the organisation (to which they were placed during the CSE) had faced a cyber-attack, and if so, follow the incident response plans provided by the conductor. The teams were offered modern cyber-incident investigation tools, which the individuals had to learn to use during the CSE. Had there been questions, each team had a designated coach during the whole CSE, whom they could consult to receive answers and support in exercise content related questions. There was a green team monitoring the Flagship 1 network and infrastructure. Had there been any issues, the CSE's green team would have investigated and resolved them. The participants were informed that they were simultaneously

participating in a cyber range technical federation demonstrator, but the demonstrator was not emphasised. After the exercise, the participants were asked to answer an anonymous survey. The survey had questions enquiring the experienced easiness in joining the federation network, and the reliability of network. The Flagship 1 CSE is documented in more depth in (CyberSec4Europe 2020).

2 Planning and Implementing CR Technical Federation

The technical federation planning started by searching, identifying and pre-evaluating open-source VPN or SD-WAN software, followed by comparing how the features of identified candidates met the requirements of the requirements specification listed in PART B of D7.1 Report on existing cyber ranges, requirements (CyberSec4Europe 2020). Two main candidates were identified and further evaluated: flexiWAN and ZeroTier One. After the two candidates were identified, they were tested. The testing started in Q2 2020.

flexiWAN Ltd is an Israel based company offering an open-source SD-WAN solution, flexiWAN (Flexiwan 2020). flexiWAN was released to production use in the end of 2019. It is available in hosted and self-hosted versions. At the time of the feature testing, flexiWAN was still at the beginning of its maturity, and some of the required features were missing. The biggest limitations, which were detected during the testing, were that in flexiWAN it was not possible to filter traffic between tunnels, and it was possible to have only one tunnel between sites. When the flexiWAN developers were enquired about this, they implied that multilink support was coming to flexiWAN; however, the developers could not provide an actual date when it could be available.

ZeroTier One (later referenced as ZeroTier) is an open-source VPN and SD-WAN software developed and open-sourced by ZeroTier Inc. ZeroTier uses P2P technology to connect endpoints together to form a network. ZeroTier uses a proprietary protocol that had similarities to VXLAN and IPsec. The protocol could be divided into VL1 and VL2 layers. ZeroTier's manual (ZeroTier 2020) describes the layers as "VL1 is the underlying peer-to-peer transport layer, the "virtual wire," while VL2 is an emulated Ethernet layer that provides operating systems and apps with a familiar communication medium.". VL1 had also zero-configuration capabilities, and it works like a DNS hierarchy. The base of the VL1 is a root server configured to each endpoint. The root server also contains the world definition that consisted of planet and moons. The public ZeroTier network has a single planet that is operated by ZeroTier Inc. The moons present the next level root servers that individuals can configure. With moons, individuals can reduce the dependency on the ZeroTier infrastructure.

ZeroTier's VL2 layer is a Virtual Extensible Local Area Network (VXLAN), which is like a network virtualization protocol with SDN capabilities. According to ZeroTier's manual, VL2 implements secure VLAN boundaries, multicast, rules, capability-based security, and certificate-based access control.

In the initial tests, it was seen that ZeroTier fulfilled more of the requirements of the requirements specification (CyberSec4Europe 2020) than flexiWAN. However, also ZeroTier had limitations, from which the most significant one was the missing centralised management interface. There existed a centralised management capability in the public version of the ZeroTier infrastructure; however, it could not be utilised, as it would have been in conflict with a requirement of JYVSECTEC's internal guidelines. The internal guidelines required to isolate the Flagship 1 federation network from the public Internet and thus prevented the usage of the ZeroTier's public infrastructure.

ZeroTier had a well-documented application programming interface (API), enabling to create a customised management system. After an extensive internal evaluation and testing ZeroTier was selected to be the technology to be adopted. The comparison regarding the fulfilment of requirements between flexiWAN and ZeroTier is presented in Table 1.

Requirement	FlexiWAN	ZeroTier
Specification 2.1: Overlay network MUST support L3 connectivity into a cyber range (i.e. routed connectivity between cyber ranges)	YES	YES
Specification 2.2: Overlay network SHOULD support L2 connectivity into a cyber range (i.e. extending L2 network between cyber ranges)	NO	YES
Specification 2.3: Overlay interface MUST support IPv4 and IPv6 connections in dual-stack	YES	YES
Specification 2.4: Overlay network MUST support IPv4 and IPv6 (cyber range Internet connectivity does not need to be dual-stack)	YES	YES
Specification 2.5: Overlay network MUST support the following topologies: point-to-point, hub-and-spoke, partial-mesh and full-mesh	NO	YES
Specification 2.6: Overlay network SHOULD support connectivity behind NAT/FW	YES	YES
Specification 2.7: Overlay network endpoint SHOULD be implemented either in hardware or in a virtual appliance	YES	YES
Specification 2.8: End-to-End Round-Trip-Time (RTT) MUST be less than 200ms	YES	YES
Specification 2.9: Overlay network must have centralised management to control interconnections between cyber ranges	YES	YES
Specification 2.10: Centralized management should be available to all cyber ranges	YES	YES
Specification 2.11: Overlay network MUST support segregation of concurrent exercises	NO	YES
Specification 2.12: Overlay network MUST be encrypted using industry standard protocols	YES	YES

Table 1: Requirements fulfilment comparison.

2.1 Federation Network Architecture

A requirement set in Flagship 1 by JYVSECTEC was to honour RGCE's self-suffiency, in other words, not to have any connection to the public Internet. To fulfil this requirement, a ZeroTier root server was created and deployed, and it was configured to the deployed ZeroTier endpoints in the Flagship 1 environment (Figure 1). The root server was deployed in Amazon's AWS. The rationale of using the commercial cloud provider Amazon AWS was that it provided better network redundancy and availability than JYVSECTEC's datacentre. A ZeroTier controller, controlling the federation network and the endpoints therein, and a federated testbed were also deployed in Amazon's AWS.

The network connections towards RGCE were split between two ZeroTier routers. One of the ZeroTier routers was designated to add the testbed to RGCE (AWS ZeroTier in Figure 1), and the other router was by the end user traffic (JAMK ZeroTier-2). The functionality could have been achieved using a

single ZeroTier router, but the deployed solution allowed load balancing and increased the network's redundancy. For the ease of the readers, actual IP addresses and network details are limited in this report.

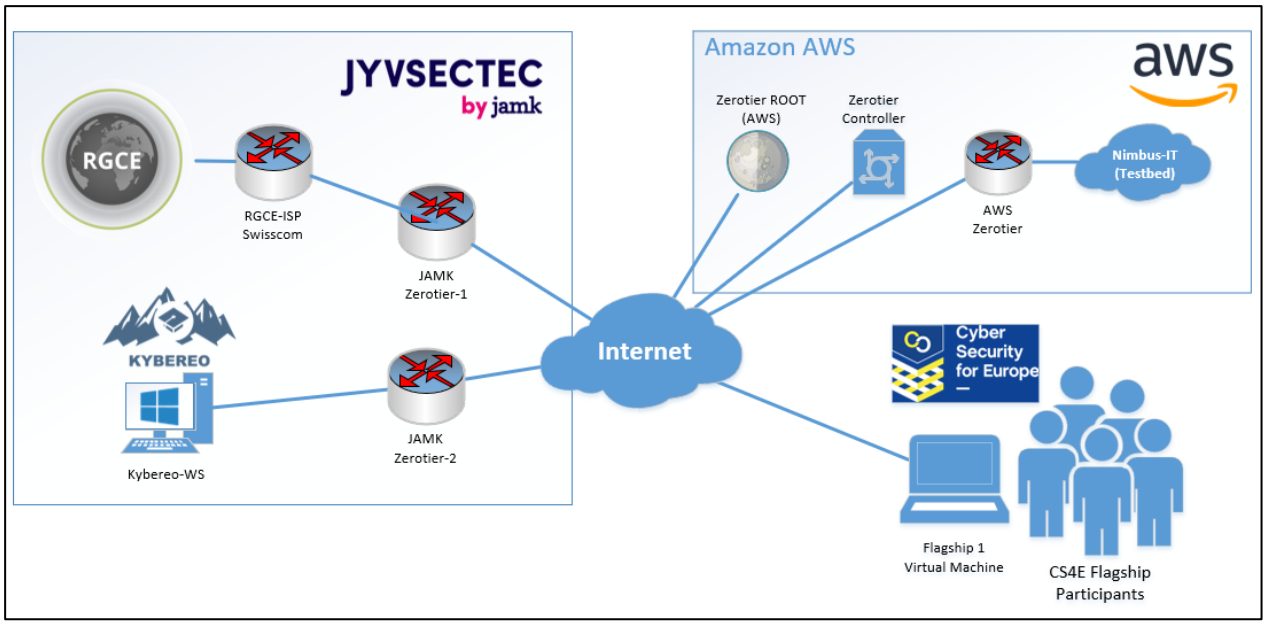


Figure 1: High-level network architecture.

RGCE is isolated from the Internet, i.e. no real Internet traffic enters or leaves the environment, but for a CSE it offers the global Internet's functionalities and services (JYVSECTEC 2018). For Flagship 1, two organisational environments, a train company environment and a university one were planned, developed and deployed in RGCE, which is located in JYVSECTEC's datacentre. A cloud provider environment (Nimbus-IT in Figure 1) was planned, implemented and deployed in Amazon's AWS. In Flagship 1, the Nimbus-IT had the role of a testbed in the federation network. Utilising the features of ZeroTier, RGCE (a cyber range) and Amazon AWS were technically federated.

In the Flagship 1 narrative, the participants were employees of the University of Kybereo. The participants connected directly but seamlessly to Kybereo's network through the federation network.

2.2 Tested use cases

Two use cases in PART B of the "D7.1 Report on existing cyber ranges, requirements" (CyberSec4Europe 2020) were showcased during the Flagship 1 federation demonstration. They were "Adding testbeds to a cyber range" and "End user connectivity". The use cases are described in the following subchapters.

2.2.1 Use case: Adding Testbeds to a Cyber Range

The use case "Adding testbeds to a cyber range" offers the use of domain specific characteristics such as testbeds or labs, to provide additional features that are not otherwise available in a cyber range. 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 not often designed for use in cyber exercises; however, they can be used as part of a CSE when connected to an appropriate cyber range. Connecting testbeds to a cyber range is typically carried out as a point-to-point connection, implemented e.g. by direct IPSEC, SSH or by a VPN tunnel.

2.2.2 Use case: End User Connectivity

In "D7.1 Report on existing cyber ranges, requirements" (CyberSec4Europe 2020), the individual end user connectivity was separated from the federation network. Following the selection of ZeroTier as the technical federation solution, it was understood that also the end user connectivity would be implemented with the same technology. The use case Demonstrating End User connectivity was planned to fulfil specifications 2.41 – 2.43:

- *Specification 2.41: Cyber range should have a registration portal.*
- *Specification 2.42: End user must be identified.*
- *Specification 2.43: Cyber range must deliver login information to end user.*

3 Demonstrating the implementation

The demonstration environment, including the federation network, was controlled by a single entity, JYVSECTEC. Had there been more entities or organisations forming the federation network, overlapping IP address spaces or conflicting IP addresses should have been negotiated and agreed. If there are more entities controlling the exercise or if there is more than one cyber range involved in the exercise, the technical addressing should be negotiated and agreed beforehand. The various topics, that need to be agreed upon, are listed in as checklist items in the PART B of "D7.1 Report on existing cyber ranges, requirements" (CyberSec4Europe 2020). The following is an exported snippet from the deliverable (CyberSec4Europe 2020), describing a rationale of a checklist item of agreeing Public Key Infrastructure (PKI) certificates and an actual checklist item:

> *In most cases, cyber ranges are built to mimic the real Internet; therefore,it is important to define also the Public Key Infrastructure (PKI). PKI is used to create certificates for example to websites so a 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: The needs of exercise organization public services' PKI-certification SHOULD be defined***

3.1 Controller system

Because of the requirement to honour the RGCE self-suffiency, utilising the public ZeroTier controller was not an option. By doing so, it would have created a live connection with the ZeroTier infrastructure and with the public Internet; therefore, the implementation of a self-created Zerotier network controller was undertaken. For demonstration purposes, it was decided to use Bash scripts to implement the controller. It was seen not necessary nor value adding to create a web-frontend for the controller functionality; the straightforward Bash scripts fulfilled the need to configure the ZeroTier network with a minimum effort spending. Having the functionality implemented by scripting, the authorisation and access control relied on the Operating System's functionalities instead of a potential web-framework provided functionality, had it been implement as a web-frontend.

ZeroTier had a well-documented API (ZeroTier 2020) that was utilised during the implementation. The API used HTTP GET and POST requests, and each of the requests had to include a Z-ZT1-Auth header. The Z-ZT1-Auth value was defined in ZeroTier's authtoken.secret file. A total of nine controller scripts were created (Table 2).

Script name	*Script description*
*addnetwork**	Add a network to the ZeroTier
delnetwork	Remove a network from ZeroTier
shownetworks	List the networks in the ZeroTier
addroute	Add a network route to the federation network
delroute	Remove a network route from the federation network
showroutes	List the network routes of the federation network
addmember / deploy	Add an endpoint to a federation network
delmember / drop	Remove an endpoint from a federation network
showmembers	List the endpoints of a federation network

Table 2: ZeroTier controller Bash scripts.

* Contents of the addnetwork script provided as an example.

```
#!/bin/bash
set -e
[[ $# -lt 3 ]] && echo -e "Usage: $0 {network name} {cidr}
{private?true/false}
If false, also specify {ipRangeStart} {ipRangeEnd}
Examples:
addnetwork some_public_mgmt 10.11.11.0/24 false 10.11.11.10
10.11.11.200
addnetwork some_private_network 10.22.22.0/24 true
" && exit
TOKEN=`sudo cat /var/lib/ZeroTier-one/authtoken.secret`
ID=`sudo ZeroTier-cli info | awk '{print $3}'`
DATA='{
"name": "'"$1"'",
"routes": [
{
"target": "'"$2"'"
}
],
'"`[[ $3 == "true"  ]]  &&
echo '"private"': true ||
echo '"v4AssignMode"': { '"zt"': true }, '"ipAssignmentPools"': [{
'"ipRangeStart"': '"'"$4"'"', '"ipRangeEnd"': '"'"$5"'"'}]`"'
}'
curl -X POST --header "X-ZT1-Auth: $TOKEN" -d "$DATA" \
"http://localhost:9993/controller/network/${ID}______"
```

3.2 Adding Testbeds to a Cyber Range

The aforementioned testbed was deployed in Amazon AWS as shown in Figure 2. Creating a federation network between a cyber range and a test bed, a customised minimalistic ZeroTier-router was built on

top of CentOS Linux. Two routers were deployed: JAMK Zerotier-1 and AWS Zerotier in Figure 2. With ZeroTier, the system requirements of the routers could be kept to a minimum: the routers had a single virtual CPU and one Gigabyte of memory.

The deployment process started by creating routers to JYVSECTEC's datacentre and to AWS. After the routers had been created, public IP addresses were assigned to them. ZeroTier should also work behind the NAT (Network Address Translation), but to avoid any connection issues public IPs were used. After the IP assignments, the routers connected to the ZeroTier Root, and the controller could now control the routers (JAMK Zerotier-1 and AWS Zerotier). A ZeroTier-JAMK-to-AWS-net (Zerotier-network in Figure 2) network was created, and both of these routers were added to this network.

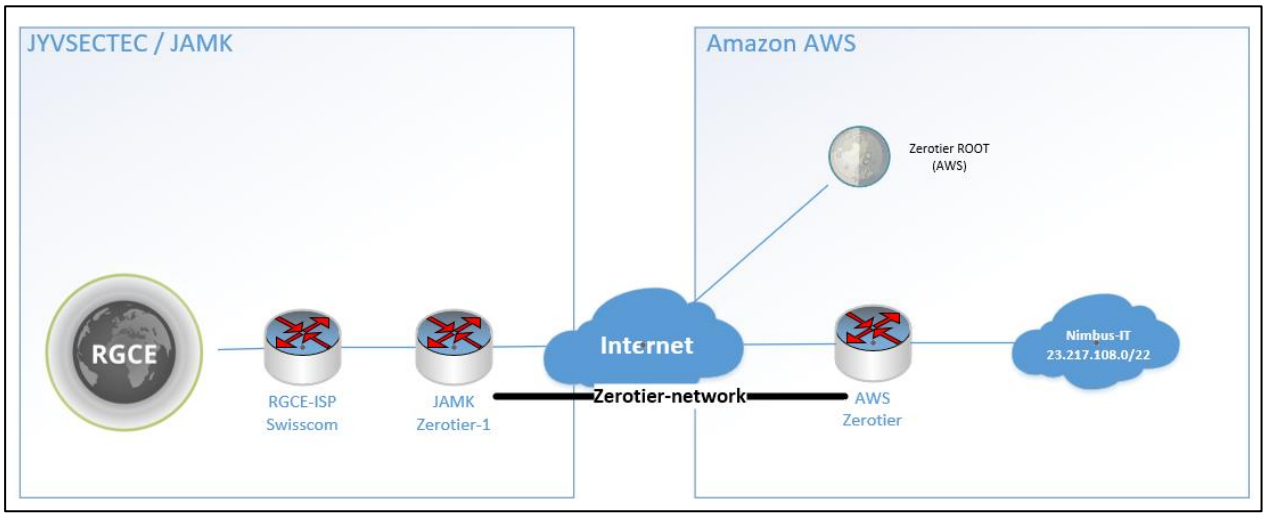


Figure 2: ZeroTier network between RGCE and Amazon AWS.

After both routers were connected to the ZeroTier federation network, static network routes were configured in both networks. For the JYVSECTECs router, a static route to 23.217.108.0/22 via the ZeroTier interface was configured. Because JYVSECTEC's RGCE mimics the real-life Internet and uses public IP addresses, a static default route to the AWS router routing all the traffic from AWS to JYVSECTEC (Figure 3) was created.

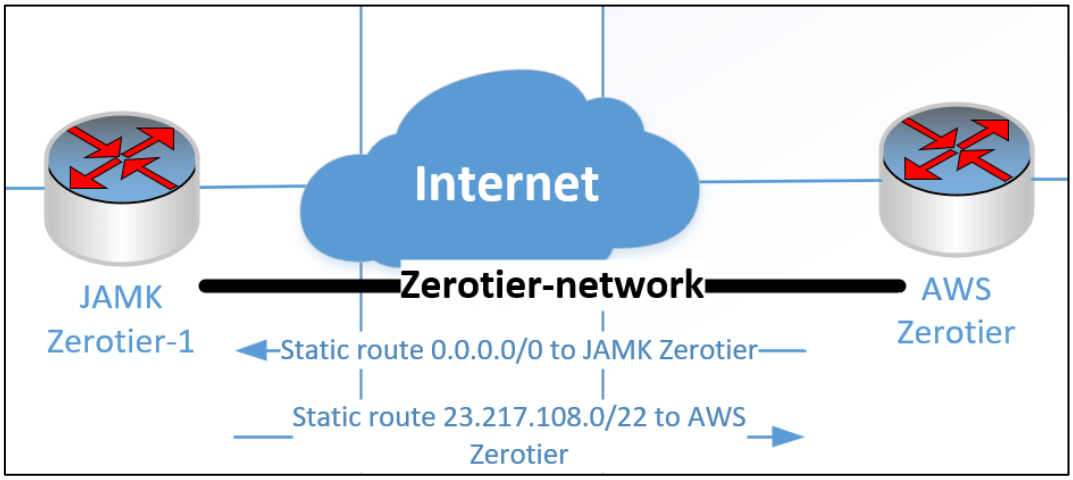


Figure 3: Federation routing.

One of the requirements of the overlay network was that it must support the segregation of concurrent exercises, Specification 2.11 in PART B of "D7.1 Report on existing cyber ranges, requirements" (CyberSec4Europe 2020). Even though in the Flagship 1 exercise only a single exercise was ongoing, the segregation in ZeroTier was tested. Rationale for this was to test and demonstrate the requirements specification. For the segregation, an additional overlay network, the "second exercise-net", was created, followed by adding two routers to this network as shown in Figure 4. After the routers had two separated overlay networks, Virtual Routing and Forwarding (VRF) was enabled and configured in the routers.

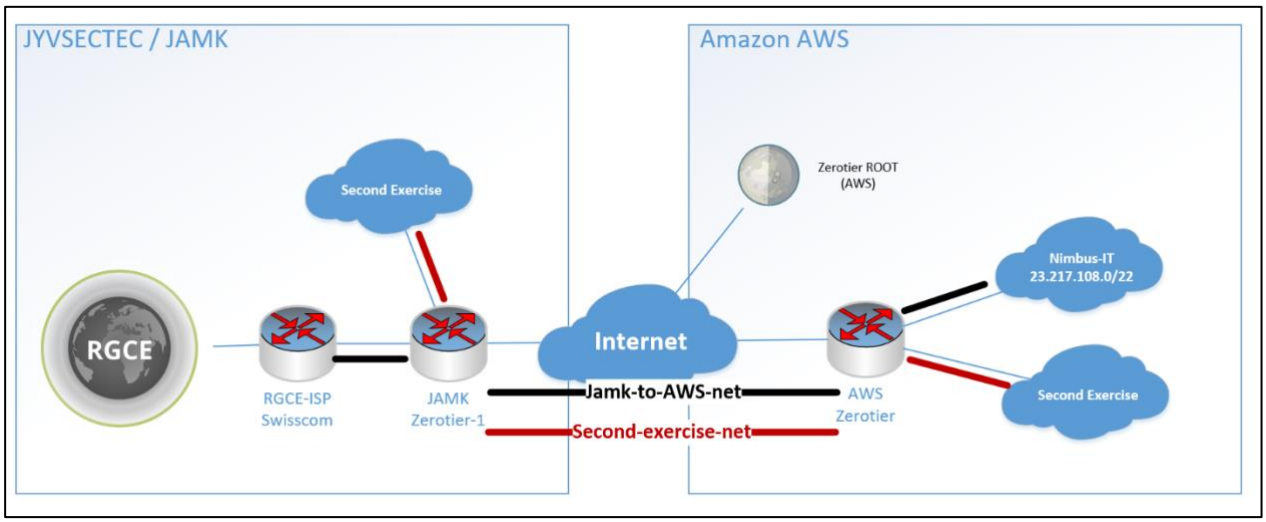


Figure 4: Segregation of concurrent exercises.

For the VRF separated routing tables were created in the routers, and ZeroTier's virtual network interfaces were added to these routing tables. For example, the traffic coming in from Nimbus-IT to AWS's ZeroTier router used the Flagship1 named routing table that had only the routes to the Flagship 1 exercise.

3.3 End User Connectivity

The end user connectivity was provided using a prepared custom made VirtualBox virtual machine. An image of the virtual machine was shared with the Flagship 1 participants. Once the image was commissioned by the participants in their VirtualBox installation, it provided connectivity the federation network. The reason for the custom-made virtual machine was that the users did not have to make any changes to their physical computers but they only had install the VirtualBox, if not already installed. From a CSE conductor's perspective, the arrangement enabled connecting to the virtual machines if it was necessary for troubleshooting purposes, had there been problems.

In the Flagship 1 registration form, the registrants were asked to measure and report their RTT and network throughput (Annex A: Determing the participants' network connection's RTT). The registrants were informed that RTT should be less 300 ms, but higher RTT values would not prevent their participation to the event. The suggested end user RTT (300 ms) was relaxed from the RTT stated in requirement specification (200 ms). The rational for relaxing the requirement was that at the time of the planning of the event, there were indicators hinting that as remote working due COVID-19 had grown, the network latencies had also grown in some but unspecified networks. The conductor had the goal to include the participants even if their reported RTTs would have been high, to not only test and demonstrate the federation network but also to provide an experience of a CSE in a cyber arena as well. The reported RTTs and network throughputs are listed in Annex B: Reported RTTs and Network Throughputs.

A total of 52 persons registered in Flagship 1, but not all were granted access to the event. The reason for limiting the number of persons in the event was primarily non-technical. The conductor's aim was to offer a beneficial CSE experience to the participants. This meant that the number of teams had to be

limited so that each of the teams could have a designated full-time coach, but also to keep the number of the members in a team manageable. Each teams' members' were planned to have meaningful tasks and objectives. Had the number of members in a team grown, there may have had faced the experience that "there is no things to do".

In Flagship 1, Linux Debian 10 was used as the base operating system, but it could have been be any other Linux distribution with a graphical user interface. The custom virtual machine included a prepared configuration for the ZeroTier federation network. When the virtual machine connected to a network, it automatically connected to the ZeroTier network (Figure 5).

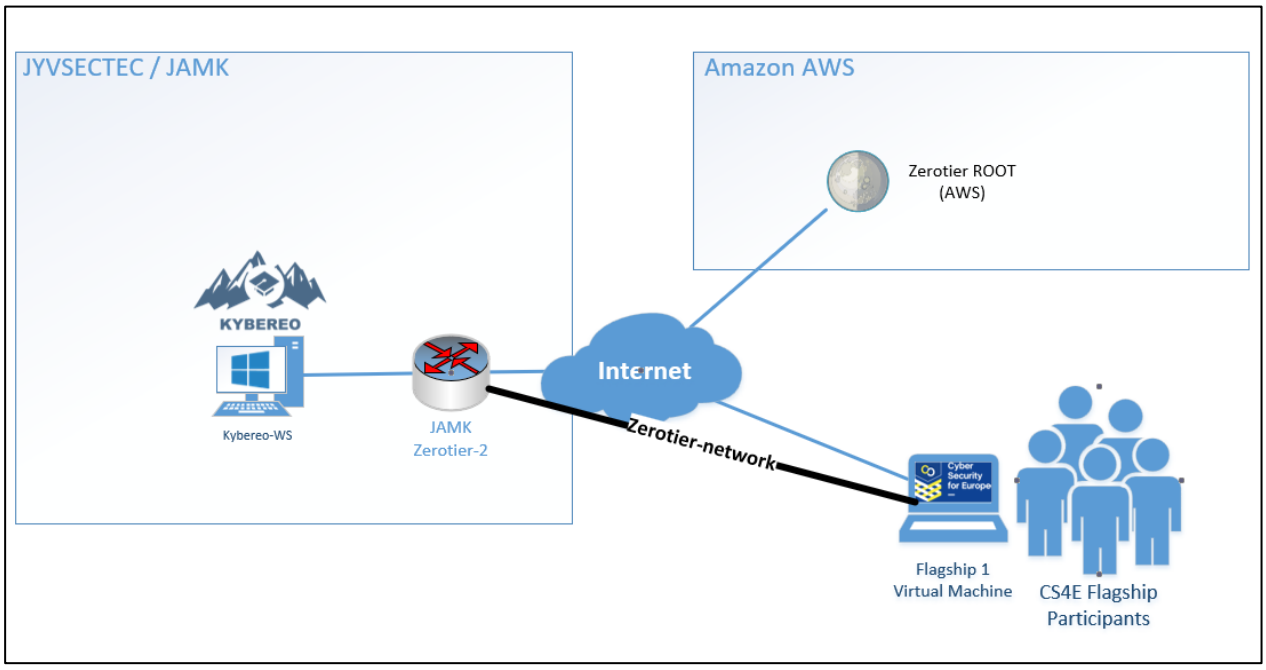


Figure 5: End-user federation network.

The first ZeroTier network functioned as a virtual lobby. In this network, the end users registered themselves in a developed federation portal using their ZeroTier address and a personal secret token. The tokens were sent to the participants before the exercise. The developed federation portal was hosted in the ZeroTier controller machine. The portal used the same ZeroTier controller scripts that were used to create the federation network controller. After the registration, the participants joined the actual ZeroTier end-user network and received their username and password pair for the exercise (Figure 6).

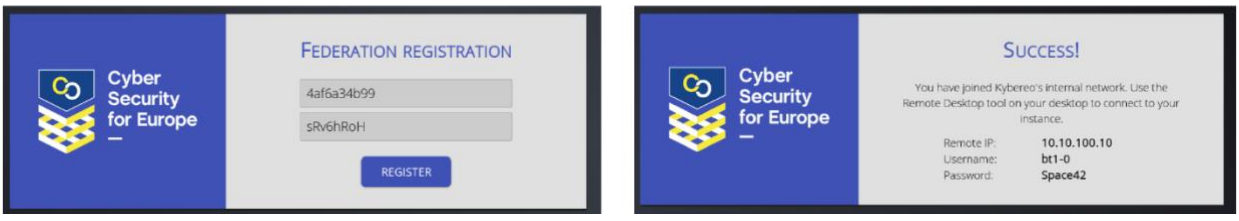


Figure 6: Federation portal.

A design idea for the end-users attending the event remotely was to make the connectivity technology as easy as possible, but still to respect the participants' privacy and to secure the intellectual property rights of the various parties. Trying to make the end-users expectations and steps clear, a workflow

diagram (Figure 7) was provided as part of the end users' connectivity guide (Annex C: Connecitivy Guide for Flagship 1 Participants).

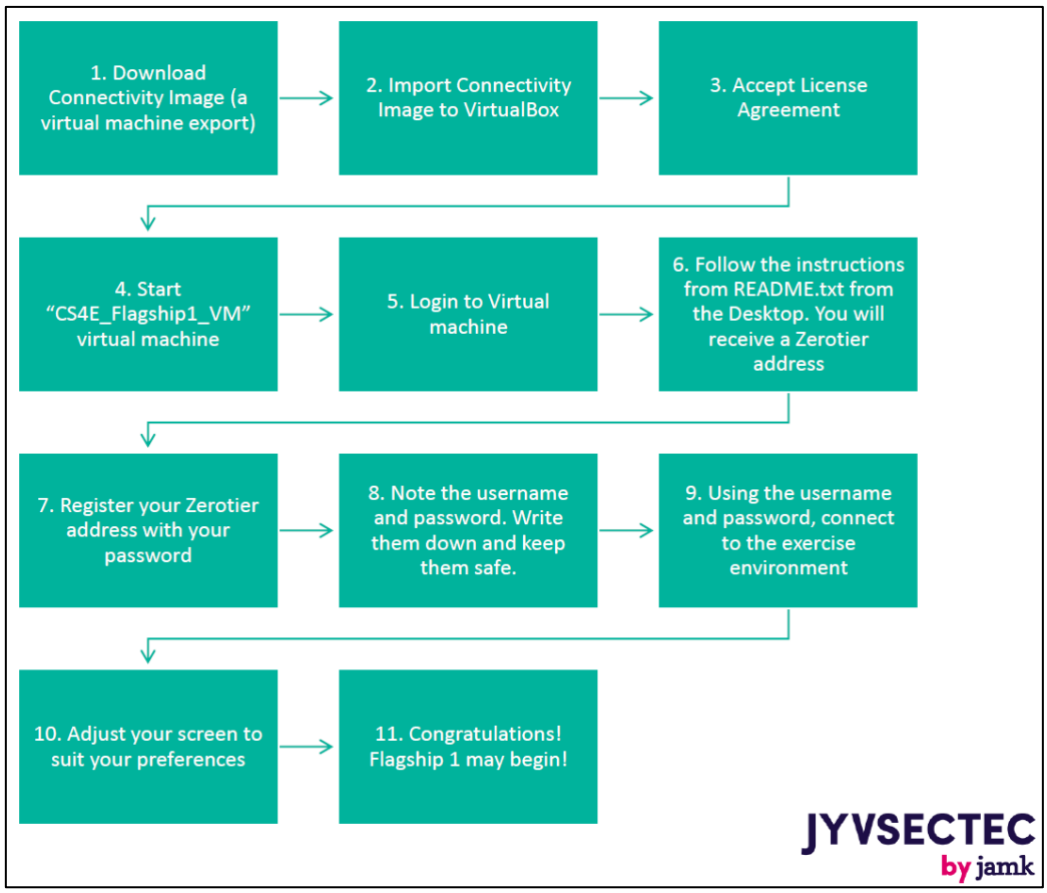


Figure 7: Provisioning workflow of the connectivity image.

3.4 Observations from the demonstration

During Flagship 1, a single user faced problems with connectivity. It was troubleshooted that the Internet connection the person was initially using had probably a double NAT, which prevented the usage of ZeroTier. The existence of the double NAT could not be verified, due time pressure to get the person into the event instead of trying to resolve the root cause of the issue. The fix was that the person was asked to switch to an alternative Internet connection, i.e. to another WLAN or mobile 4G Internet connection. By switching to another network connection, the participant was able to join to the federation network.

4 After exercise survey

After the Flagship 1 CSE, the participants were asked to respond to an anonymous survey. The survey contained questions related to the exercise network and connectivity and what kind of learning happened during the event. A total of 12 responses were received. The used survey system was Webropol (JAMK 2021). The participants were informed that they should do the survey in a single session, as an anonymous survey could not be saved. In addition, the participants were informed that responding the survey would take at least 30 minutes. It could be that the provided information raised the barrier too high for most of the participants to not to take the survey, or someone may had started responding to it but did not finish it. Due the nature of survey, there is no statistics about possible unfinished responses.

4.1 Federation network and remote connection

The survey topic "Federation network and remote connection" (Table 3) contained five assertions: the pre-exercise connectivity guide was sufficient, the VirtualBox image (CS4E_Flagship1_vm) was easy to deploy, The registration process to federation network was clear, Connecting to the cyber environment (Kybereo) with Remote Desktop was easy and The connectivity to the cyber environment (Kybereo) was reliable and the latency (perceived delay between an activity you performed and visual feedback in the environment) was satisfactory. Each assertion had four answer options: Disagree, Partially disagree, Partially agree and Agree.

All 12 respondents selected the "Agree" option to "Pre-exercise connectivity guide was sufficient" and to "The VirtualBox image (CS4E_Flagship1_vm) was easy to deploy" assertions. To the assertion "The registration process to federation network", two (16.7%) respondents selected Partially agree and ten (83.3%) selected Agree. To the assertion "Connecting to cyber environment (Kybereo) with Remote Desktop was easy", Partially disagree was selected by one (8.3%), Partially agree was selected by three (25.0%) and Agree by eight (66.7%) respondents. The assertion "The connectivity to the cyber environment (Kybereo) was reliable and latency (perceived delay between an activity you performed and visual feedback in the environment) was satisfactory" option Partially agree was selected by eight (66.7%) and Agree was selected by four (33.3%) respondents.

Assertion	Disagree	Partially disagree	Partially agree	Agree	Average	Median
Pre-exercise connectivity guide was sufficient	0.0 %	0.0 %	0.0 %	100.0 %	4.0	4.0
The VirtualBox image (CS4E_Flagship1_vm) was easy to deploy	0.0 %	0.0 %	0.0 %	100.0 %	4.0	4.0
The registration process to federation network was clear	0.0 %	0.0 %	16.7 %	83.3 %	3.8	4.0
Connecting to cyber environment (Kybereo) with Remote Desktop was easy	0.0 %	8.3 %	25.0 %	66.7 %	3.6	4.0
The connectivity to the cyber environment (Kybereo) was reliable and latency (perceived delay between an activity you performed and visual feedback in the environment) was satisfactory	0.0 %	0.0 %	66.7 %	33.3 %	3.3	3.0

Table 3: Reported perceived clarity of Flagship 1 connectivity (N=12).

4.2 Did you have problems with the virtual machine or with the federation network?

To the question "Did you have problems with virtual machine or federation network", option Yes was selected by four (33.3%) and option No was selected by eight (66.7%) respondents (Figure 8).

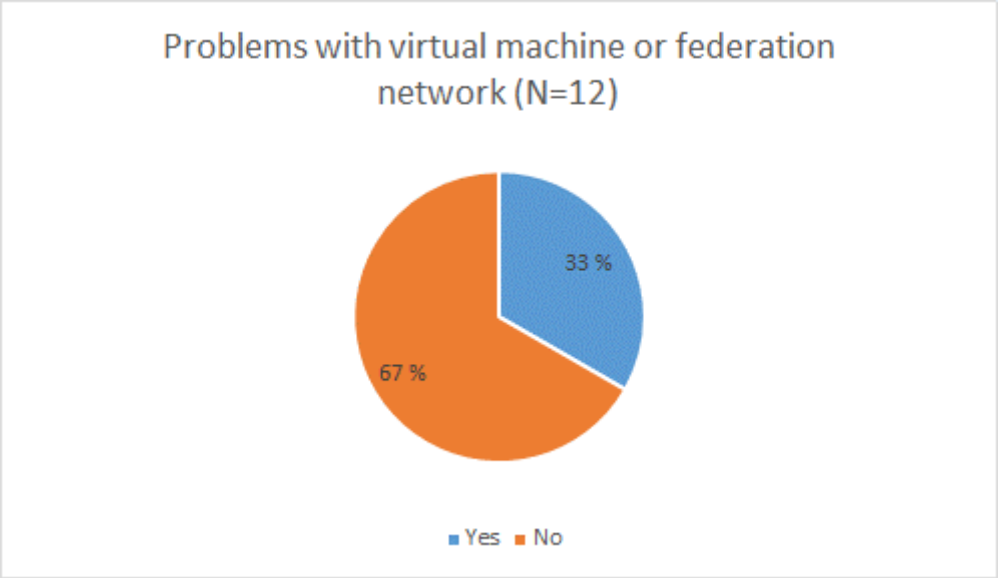


Figure 8: Problems with virtual machine or federation network (N=12).

Had the respondent selected the option Yes, then those respondents were enquired to select the used host Operating System (Figure 9) and provide a description of the problem they had faced (Table 4).

The reported host operating systems, of which the four participants had selected the option Yes to the question "Did you have problems with virtual machine or federation network", selected option Windows three times (75.0 %) and the option MacOS once (25.0 %). The option of Linux received no responses.

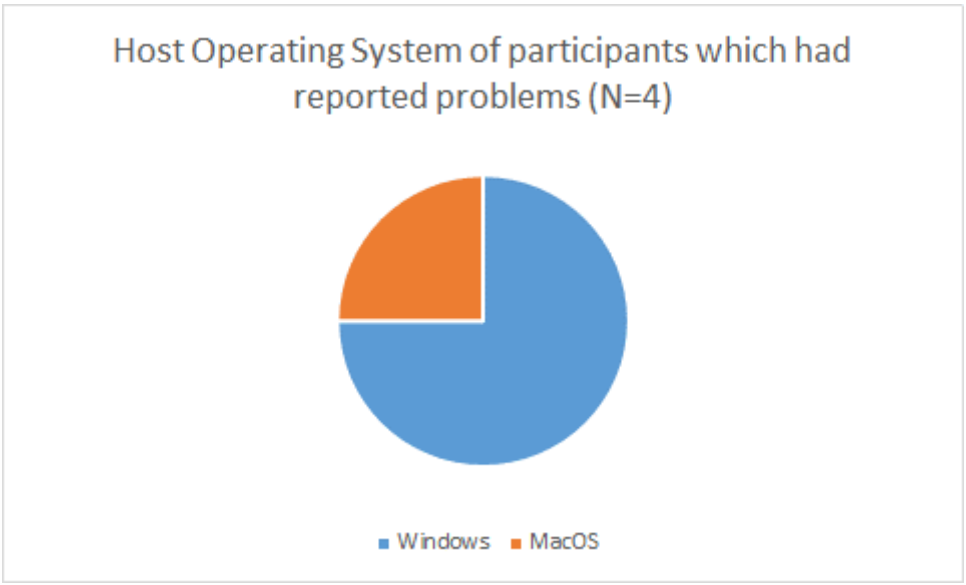


Figure 9: Host Operating System of participants which had reported problems (N=4).

The perceived problems the four participants reported are listed in Table 4. One respondent reported facing some issues with Remote Desktop, One respondent reported issues with the exercise network connectivity, one respondent had a flicker screen issue, and one respondent had initially received an invalid secret token.

Responses
Some issues with the Remote Desktop
Sometimes the exercise network encountered connectivity issues.
I had the flickering issue. With that, it would have been impossible to participate. Luckily, I was given instructions on how to fix this issue and I managed to do this before the event. I think the connectivity test that was done before the event was actually a very good thing, as this way we did not have to spend event time on debugging this.
initially, my access token was invalid

Table 4: Reported problems with Virtual Machine or Federation network (N=4).

5 Conclusions

In the online-only Cyber Security Exercise (CSE), Flagship 1, specific parts of the requirement specification (CyberSec4Europe 2020) were demonstrated. The demonstration, a cyber range technical federation, was implemented by using open-source ZeroTier SD-WAN technology. ZeroTier was used in two use cases: extending an existing cyber range and providing end user connectivity.

In accessing the federated network, the end users connected seamlessly to a virtual lobby, which was located in the federation network. Once they had entered with their user names and pre-CSE provided personal token, the participants were able to access the technical CSE environment transparently. An existing cyber arena, JYVSECTEC's RGCE, was extended with various features located in a testbed running in Amazon AWS. RGCE and the testbed were interconnected with a federated network.

The demonstration highlighted that using open-source software-only SD-WAN technology to implement a cyber range technical federation can be cost-effective, as there are no external costs caused by renting, purchasing or investing in commercial software or hardware solutions. However, there are some costs generated by the work required to plan and implement the federation. In this case, there were also costs generated to develop the nine SD-WAN Controller scripts.

It must be remarked that the deployment of an SD-WAN solution to technically federate testbeds, cyber ranges or arenas requires in-depth knowledge of IP traffic routing to plan and implement federation networks and IP traffic flow between the networks and the endpoints therein. This is due to the nature of IP networks and network routing; however, it does not depend on the commerciality status of an SD-WAN solution.

The technical CSE environment, RGCE, was controlled by the event conductor, therefore the IP address space and the network routing arrangements were easy to manage. Had there been two or more cyber ranges or arenas operated by different entities to be federated in the CSE, the IP addresses and network routings should have been agreed upon, as stated in the requirement specification, PART B of "D7.1 Report on existing cyber ranges, requirements" (CyberSec4Europe 2020).

During the CSE, the federation networks operated reliably at high throughput, low latency and low CPU consumption as monitored live during the event. From the participants' perspective there may have been occasional latencies in the connectivity. Luckily, there were no severe latencies, even though the RTT was relaxed. In an online CSE, like the FlagShip 1, the participants' network latency may influence the participants' perceived quality of the CSE. Unfortunately, there is not much a CSE conductor can do about participants' network latency. The federation network live monitoring indicated no decrease of

network throughput or rise of the network latency or the CPU utilisation, therefore the perceived latencies might have been related to the Internet connection a participant used, but not to the federation network. The majority of the registrants of Flagship 1 reported that the connection used during registration had a RTT less than 200 ms. A strict RTT requirement for the CSE participants, that is for the end-users, may provide a better CSE experience, but it may prevent some potential participants from joining the CSE.

The implemented requirements of (CyberSec4Europe 2020) were valid. A positive deviation from the requirements specification was that even the end user connectivity was possible to be implemented using the demonstrated technology. The technology used in the demonstrator is estimated to be production-ready to be used in cross-border cyber range and cyber arena events.

Future research

The requirements specification, PART B of "D7.1 Report on existing cyber ranges, requirements" (CyberSec4Europe 2020) contains use cases and requirements that were not demonstrated. The now-demonstrated technical solution, ZeroTier, could be further extended to be used in cross-border CSEs incorporating two or more cyber ranges and arenas, and thus, to demonstrate more use cases and their respective performance as expected from the requirements specification.

There are, however, new emerging technologies based on WireGuard (Donenfeld 2020), a software defined network (SDN) technology built into the Linux Kernel, solutions being also available on Microsoft's Windows and Apple's MacOS. The authors have identified promising WireGuard based open-source implementations innernet by tonari (tonari 2021) and netmaker by Falconcat Inc. (Falconcat 2021) that could be evaluated when implementing a cyber range technical federation.

References

CyberSec4Europe. (2020, August 31). "D7.1 Report on existing cyber ranges, requirements". Retrieved June 3, 2021, from https://cybersec4europe.eu/wp-content/uploads/2020/09/D7.1-Report-on-existing-cyber-ranges-and-requirement-specification-for-federated-cyber-ranges-v1.0_submitted.pdf

CyberSec4Europe. (2021, February 24). "D6.4 Flagship 1". Retrieved June 7, 2021, from https://cybersec4europe.eu/wp-content/uploads/2021/06/D6.4-Flagship-1-v1.1-submitted.pdf

Donenfeld J.A. (2020, June 1). "WireGuard: Next Generation Kernel Network Tunnel". Retrieved June 3, 2021, from https://www.wireguard.com/papers/wireguard.pdf

EDA. (2018, September 13). Cyber Ranges Federation Project reaches new milestone. Retrieved June 8, 2021, from https://eda.europa.eu/news-and-events/news/2018/09/13/cyber-ranges-federation-project-reaches-new-milestone

EU. (2019, November 4). "Finland's Presidency of the Council of the European Union Cyber Ranges Federation – Towards Better Cyber Capabilities Through Cooperation". Retrieved June 8, 2021, from https://eu2019.fi/en/-/cyber-ranges-federation-yhteistyolla-kohti-parempaa-kyberkyvykkyytta

flexiWAN. (2020). "SD-WAN and SASE Open Source". Retrieved June 8, 2021, from https://flexiwan.com/sd-wan-open-source/

tonari. (2021, March 29). "Introducing 'innernet'". Retrieved June 8, 2021, from https://blog.tonari.no/introducing-innernet.

JAMK (2021). "Webropol Survey programme login". Retrieved June 28, 2021 from https://webropol.jamk.fi/

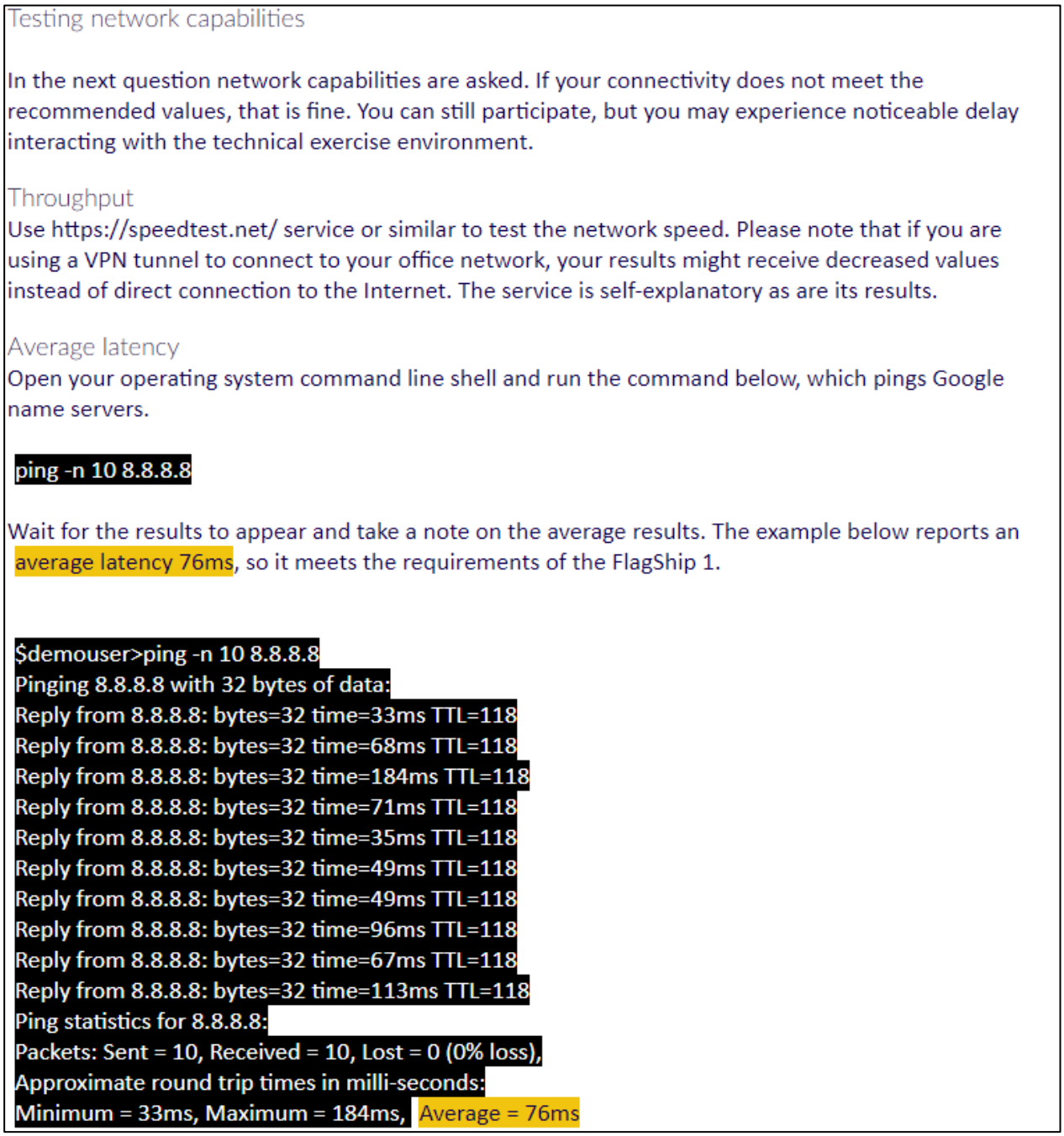
JYVSECTEC (2018). "Cyber Range White Paper". Retrieved March 10, 2021, from https://jyvsectec.fi/wp-content/uploads/2018/10/JYVSECTEC-cyber-range.pdf

Karjalainen, M. and Kokkonen, T. (Sep. 2020). Comprehensive Cyber Arena; The Next Generation Cyber Range, 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 7-11 Sept. 2020 Sep. 2020, IEEE, pp. 11-16. doi: 10.1109/EuroSPW51379.2020.00011

Falconcat (2021). "netmaker github repository". Retrieved June 8 2021, from https://github.com/gravitl/netmaker

ZeroTier. (2020). "ZeroTier Manual". Retrieved June 3, 2021, from https://www.ZeroTier.com/manual/#4_1

Annex A: Determing the participants' network connection's RTT



Testing network capabilities

In the next question network capabilities are asked. If your connectivity does not meet the recommended values, that is fine. You can still participate, but you may experience noticeable delay interacting with the technical exercise environment.

Throughput

Use https://speedtest.net/ service or similar to test the network speed. Please note that if you are using a VPN tunnel to connect to your office network, your results might receive decreased values instead of direct connection to the Internet. The service is self-explanatory as are its results.

Average latency

Open your operating system command line shell and run the command below, which pings Google name servers.

```
ping -n 10 8.8.8.8
```

Wait for the results to appear and take a note on the average results. The example below reports an average latency 76ms, so it meets the requirements of the FlagShip 1.

```
$demouser>ping -n 10 8.8.8.8
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=33ms TTL=118
Reply from 8.8.8.8: bytes=32 time=68ms TTL=118
Reply from 8.8.8.8: bytes=32 time=184ms TTL=118
Reply from 8.8.8.8: bytes=32 time=71ms TTL=118
Reply from 8.8.8.8: bytes=32 time=35ms TTL=118
Reply from 8.8.8.8: bytes=32 time=49ms TTL=118
Reply from 8.8.8.8: bytes=32 time=49ms TTL=118
Reply from 8.8.8.8: bytes=32 time=96ms TTL=118
Reply from 8.8.8.8: bytes=32 time=67ms TTL=118
Reply from 8.8.8.8: bytes=32 time=113ms TTL=118
Ping statistics for 8.8.8.8:
Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 33ms, Maximum = 184ms, Average = 76ms
```

Annex B: Reported RTTs and Network Throughputs

Network throughput (down/up) MBps	Average latency (ms)
123	5000
33/9	80
10/10	123
0	0
At least 10/5	<300ms
89.73/83.42	34
109.80 / 39.81	34.135
7	56
68/10	14
50	11ms
30/10	29
210	14
40/40	17
71.14/17.88	30ms
140/19	36
571.44/735.74	34.759
5 Mbps	39ms
30.6/9.5	29.526
40	17
20/10	50
86.66/9.94	25 ms
440/900	11
95/9	27.485

15	170
17/14	23
30/15	30ms
27/3	30
30/22	29
100/10	52.982
70	180
10/5	3
20	28
94/10	9(unloaded)/68(loaded)
106/9.6	76
20	13
10	59.01
136/12	31.245
90.61/104.79	20
90	4
300/50	7
15/15 Mbps	80
100/100	5
100/10	7
80/71 Mbps	101ms
200/260	7
30/10	106
requirement met	requirement met
28.4 Mbps	26ms
63.16/10.28	12
11/5	89

100/20	100
50	13

Annex C: Connecitivy Guide for Flagship 1 Participants

Contents

- System requirements
- Prerequisites
- Provisioning workflow overview
- Provisioning guide
- Guide for reconnecting
- Decommissioning workflow overview
- Decommissioning guide
- Troubleshooting

16.12.2020

JYVSECTEC by jamk

System Requirements

Component	Minimum	Recommended
Virtualisation software	VirtualBox 6.1.x installed	
CPU	64-bit Intel i5 2,7 GHz or equivalent	
RAM	6 GB	
Free disk space	20 GB	
Internet	Yes	Yes
Sound	Audio Out & In via a headset	Yes
Headset	1x	Yes
Display	1x 1366×768	2x 1920×1080 (FullHD)
Mouse	Trackpad/touchpad	External mouse
Keyboard	1x	

16-12-2020

JYVSECTEC by jamk

Prerequisites to connect

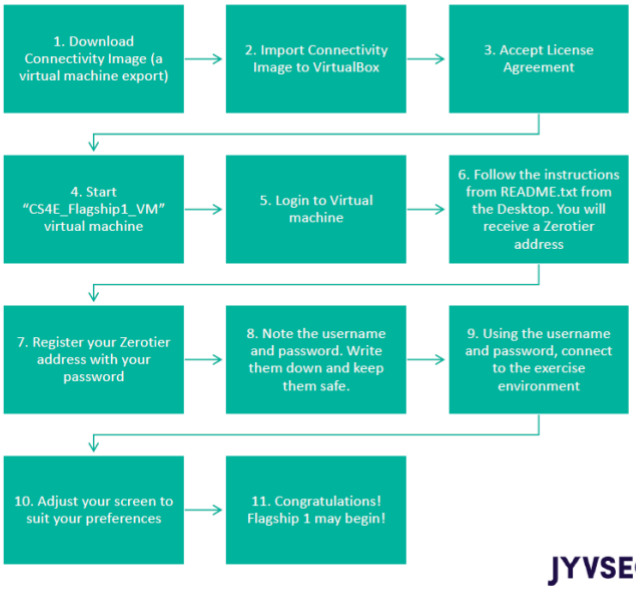
- Prerequisite is that your system has
  - VirtualBox 6.1.x Installed
- Please note that Installation requires Administrator rights
- Depending on your organization's security policy **you may need to contact your IT support to assist you with the installation**

16.12.2020

JYVSECTEC by jamk

Provisioning Exercise environment connectivity, the workflow

PRE-exercise



16.12.2020

JYVSECTEC by jamk

1. Download Connectivity Image (a virtual machine export)

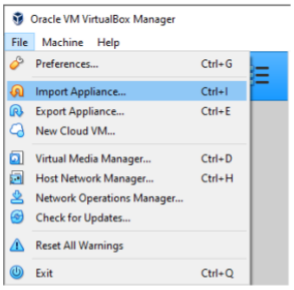
- The virtual machine image is available HERE
- Image size is about 2,4 GB
- Image is designed for Oracle VirtualBox, but it may also work with other hypervisors
- Oracle VirtualBox can be downloaded from https://www.virtualbox.org/wiki/Downloads

16-12-2020

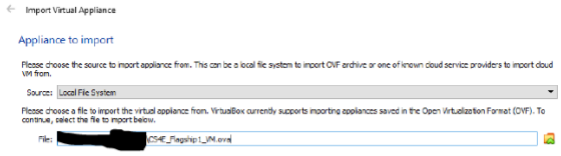
JYVSECTEC by jamk

2. Import Connectivity Image to VirtualBox

- The first thing to do is to import the downloaded VM-image to VirtualBox
- Select *File* → *Import Appliance* (Ctrl + i)



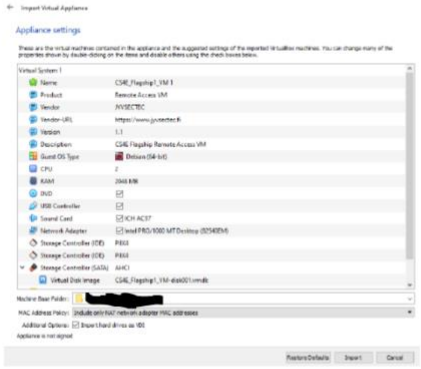
- Select the downloaded VM-image and click *Next*



16-12-2020

2. Import Connectivity Image to VirtualBox

- Next window is *Appliance settings*
- Make sure that the machine base folder is pointing to a drive that has enough free space for the VM
  - VM's disk takes roughly 6 GB disk space
- Other settings can be left to default
  - (Optional) *If you have spare resources on your computer, you can add more RAM (4096 MB)*
- Lastly click *Import*

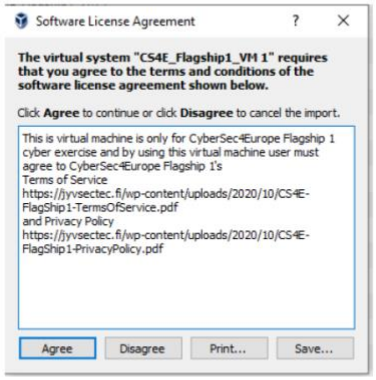


16-12-2020

JYVSECTEC by jamk

3. Accept License Agreement

- When the machine is imported to Virtual Box, Virtual box displays a License Agreement for the user to accept
- License Agreement must be accepted to use the virtual machine

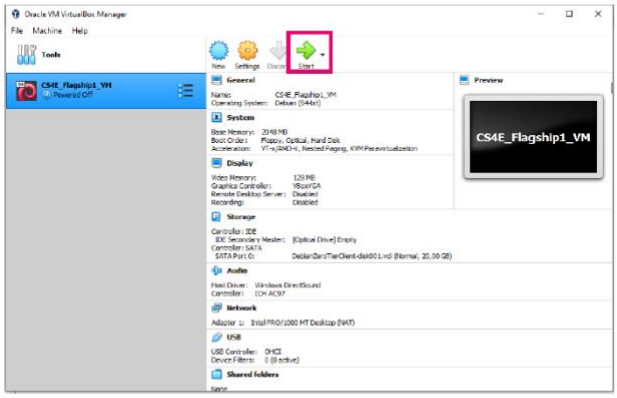


16-12-2020

JYVSECTEC by jamk

4. Start “CS4E_Flagship1_VM” virtual machine

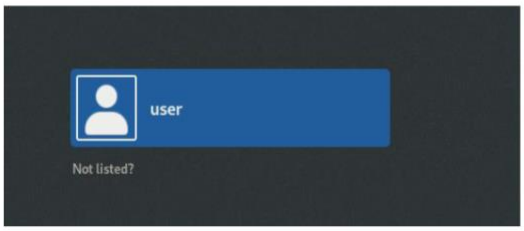
- After the import is done, the virtual machine is showing on the left side of VirtualBox’s main window
- To start the VM click the green arrow



JYVSECTEC by jamk

5. Login to Virtual machine

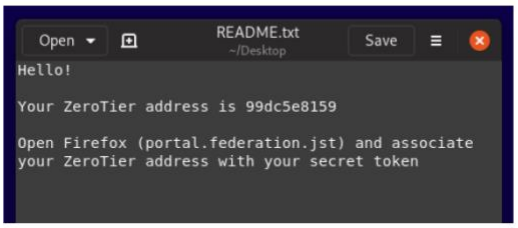
- Select the default user (*user)* and use password ***cs4e*** for logging in



JYVSECTEC by jamk

6. Follow the instructions from README.txt from the Desktop.

- After logging in, double click on ***README.txt*** on the desktop and copy the ZeroTier address



16.12.2020

JYVSECTEC by jamk

7. Register your Zerotier address with your password

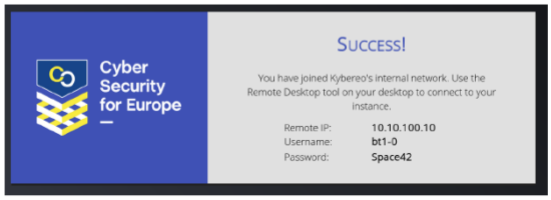
- Open Firefox (*on your virtual machine*), and the registration portal should open
- Insert the ZeroTier address from the **README.txt** and associate it with your personal **secret token** (received earlier via SMS)

16-12-2020

JYVSECTEC by jamk

8. Note the username and password. Write them down and keep them safe.

- After registering, the form should display the necessary credentials to connect to your personal instance in Kybereo's internal network
- You can check the credentials later by revisiting on https://portal.federation.jst
- You are now ready to connect to Kybereo!

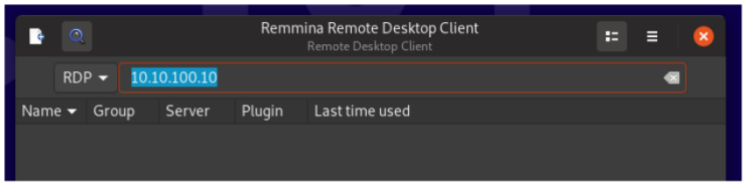


16-12-2020

JYVSECTEC by jamk

9. Using the username and password, connect to the exercise environment

- Double click on ***Remote Desktop*** shortcut either on your desktop or on the quick launch bar
- Enter the **Remote IP** address received from the registration portal and hit enter

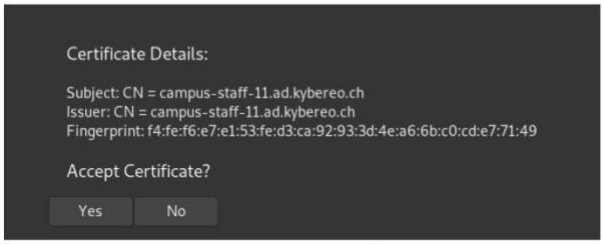


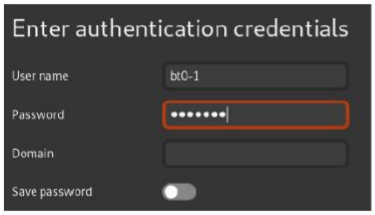
16-12-2020

JYVSECTEC by jamk

9. Using the username and password, connect to the exercise environment

- When connecting for the first time, a certificate popup appears
- Accept the certificate
- Now you can input the **username** and the **password** from the registration portal
- Leave the *domain* empty
- Save the password if you wish



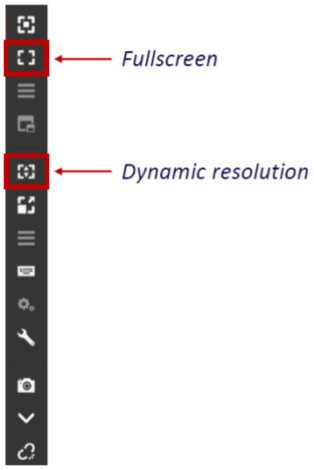


16-12-2020

JYVSECTEC by jamk

10. Adjust your screen to suit your preferences

- Toggle fullscreen and dynamic resolution update to get the best possible view

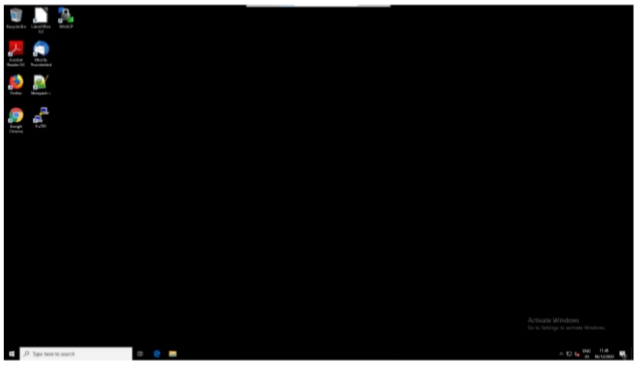


16-12-2020

JYVSECTEC by jamk

11. Congratulations! Flagship 1 may begin!

- If all goes well, you should have the following view
- You are now successfully connected to Kybereo, which means that you are ready to start the investigation!
- Enjoy the Flagship 1 exercise!



16-12-2020

JYVSECTEC by jamk

Reconnecting to exercise

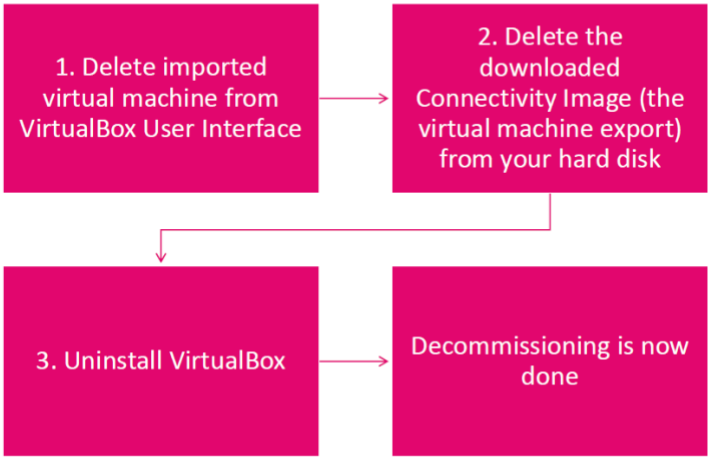
- Virtual Machine will connect automatically to exercise network when the virtual machine boot up
  - So users can shutdown virtual machine after day 1 and reconnect to exercise by starting the virtual machine

16.12.2020

JYVSECTEC by jamk

Decommissioning Exercise environment connectivity, the workflow

POST-exercise

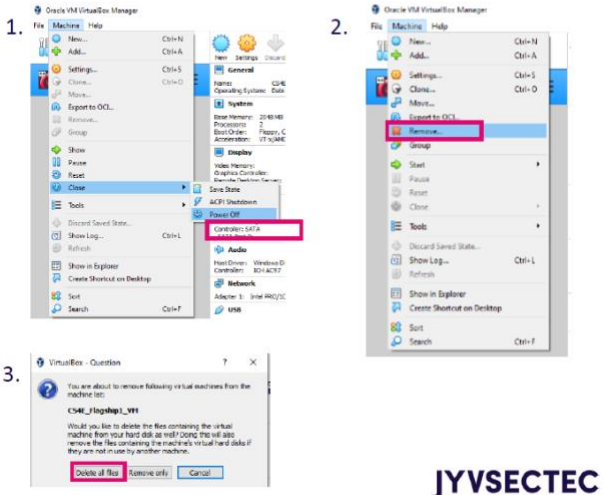


16.12.2020

JYVSECTEC by jamk

1. Delete imported virtual machine from VirtualBox User Interface

1. Power off the virtual machine by selecting *Machine and Close → Power Off* (or right clicking the virtual machine and selecting *Close → Power Off*)
2. Delete virtual machine selecting *Machine and Remove (or* right clicking the virtual machine and selecting *Remove)*
3. Select *delete all data* from the dialog box

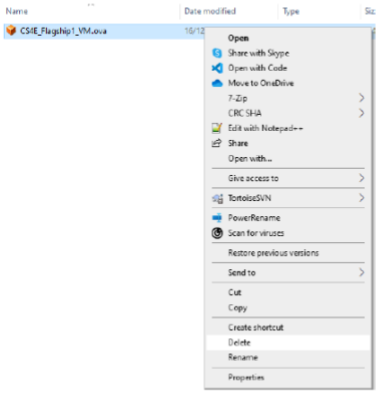


16.12.2020

JYVSECTEC by jamk

2. Delete the downloaded Connectivity Image (the virtual machine export) from your hard disk

- Go to download folder and delete the *CS4E_Flagship1_VM.ova*



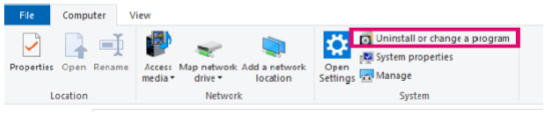
16.12.2020

JYVSECTEC by jamk

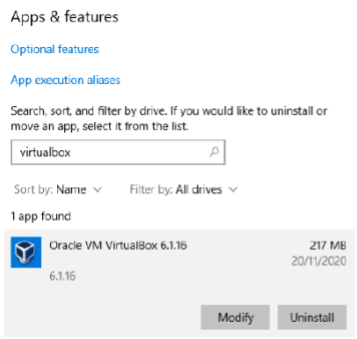
2. Delete the downloaded Connectivity Image (the virtual machine export) from your hard disk

1. Open Windows file explorer and select from the top toolbar *Uninstall or change a program*
2. Type Virtualbox to search bar and click *Oracle VM VirtualBox* and select *Uninstall*
3. Follow the uninstaller's instructions

1.

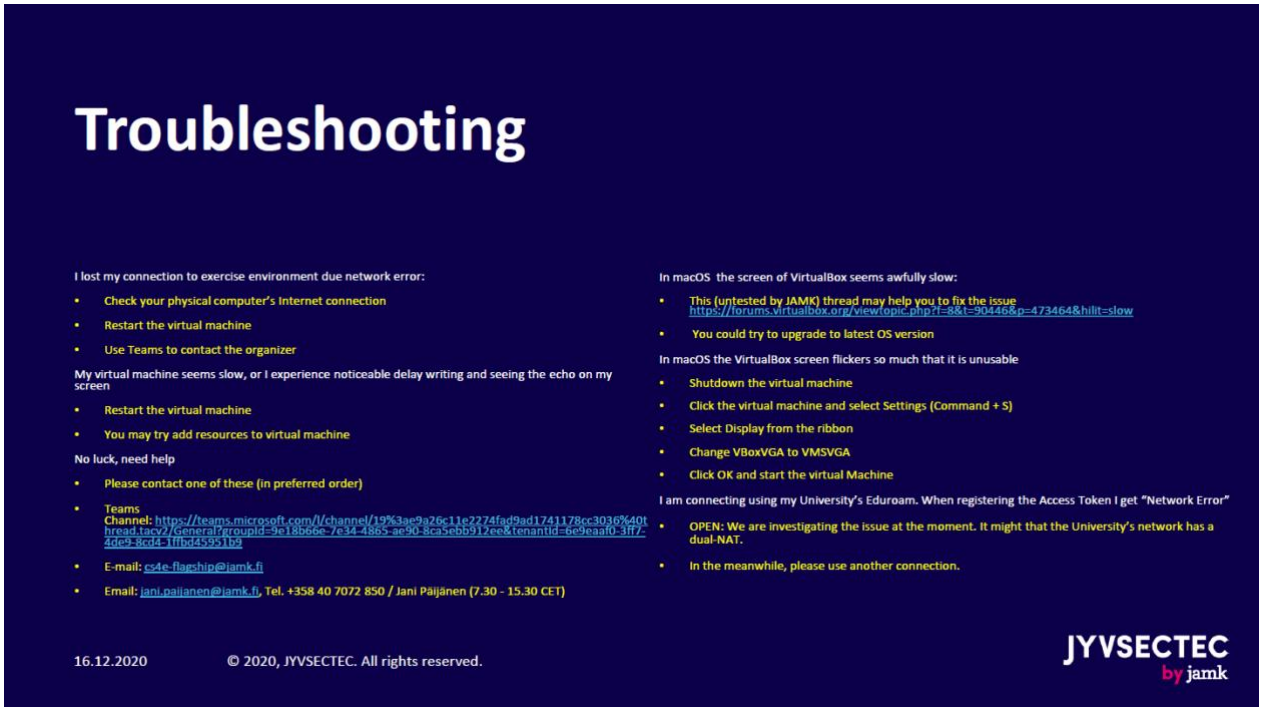


2.



16.12.2020

JYVSECTEC by jamk


Troubleshooting
I lost my connection to exercise environment due network error:
Check your physical computer's Internet connection
Restart the virtual machine
Use Teams to contact the organizer
My virtual machine seems slow, or I experience noticeable delay writing and seeing the echo on my screen
Restart the virtual machine
You may try add resources to virtual machine
No luck, need help
Please contact one of these (in preferred order)
Teams
Channel: https://teams.microsoft.com/l/channel/19%3ae9a26c11e2274fad9ad1741178cc3036%40thread.tacv2/General?groupId=9e18b66e-7e34-4865-ae90-8ca5ebb912ee&tenantId=6e9eaaf0-3ff7-4de9-8cf4-1ffbd45951b9
E-mail: cs4e-flagship@jamk.fi
Email: jani.paijanen@jamk.fi, Tel. +358 40 7072 850 / Jani Päijänen (7.30 - 15.30 CET)
In macOS the screen of VirtualBox seems awfully slow:
This (untested by JAMK) thread may help you to fix the issue https://forums.virtualbox.org/viewtopic.php?f=8&t=90446&p=473464&hilit=slow
You could try to upgrade to latest OS version
In macOS the VirtualBox screen flickers so much that it is unusable
Shutdown the virtual machine
Click the virtual machine and select Settings (Command + S)
Select Display from the ribbon
Change VBoxVGA to VMSVGA
Click OK and start the virtual Machine
I am connecting using my University's Eduroam. When registering the Access Token I get "Network Error"
OPEN: We are investigating the issue at the moment. It might that the University's network has a dual-NAT.
In the meanwhile, please use another connection.
16.12.2020
© 2020, JYVSECTEC. All rights reserved.
JYVSECTEC
by jamk