Horizon 2020

Innovative Tools for Cyber-Physical Energy Systems

Secure self-healing software-defined industrial OT networks in extreme environments

Ørsted Secondment Logbook

Editor	Agrippina Mwangi
Deliverable type	Ørsted Secondment LogBook
Contractual Delivery date	1st October 2024
Actual Delivery date	
Number of pages	?
Keywords	offshore wind, cyber security, autonomous networks, industrial OT Networks, software-defined networking
Authors	Agrippina Mwangi
	León Navarro-Hilfiker
Supervised by	Lukasz Brewka
	Mikkel Gryning
	Elena Fumagalli
	Madeleine Gibescu

Executive Summary

This report addresses ...

Table of Contents

Abbreviations

SDN   Software Defined Networking

1 Research Objective

- To design and test a self-healing module for software-defined Industrial OT networks in extreme environments.

2 Related works

3 Experimental Setup

This section highlights a step-by-step guide on how to develop the self-healing module on Microsoft Azure Sandbox and the stress tests conducted to evaluate the network performance with/without the self-healing module.

3.1 MS-Azure Resource Group Design and VM Instantiation

- Create an account in Microsoft Azure Portal

- A resource group A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. To create a resource group on the MS-Azure portal:

  – Go to *"create a resource"*. Search for *"Resource Group"* on the Marketplace and create a *"Resource Group"*. Type a unique name for your resource group and choose the resource details region closest to you.

- Create a Virtual Network and a Subnet. Virtual Networks make it easy for you to take advantage of the scalable, on-demand infrastructure of Azure while providing connectivity to data and applications on-premises, including systems running on Windows Server, mainframes, and UNIX as defined in Figure 2.

- Protect a subnet using a Network Security Group

- Deploy Bastion to connect to a virtual machine

- Create an Ubuntu Server Virtual Machine

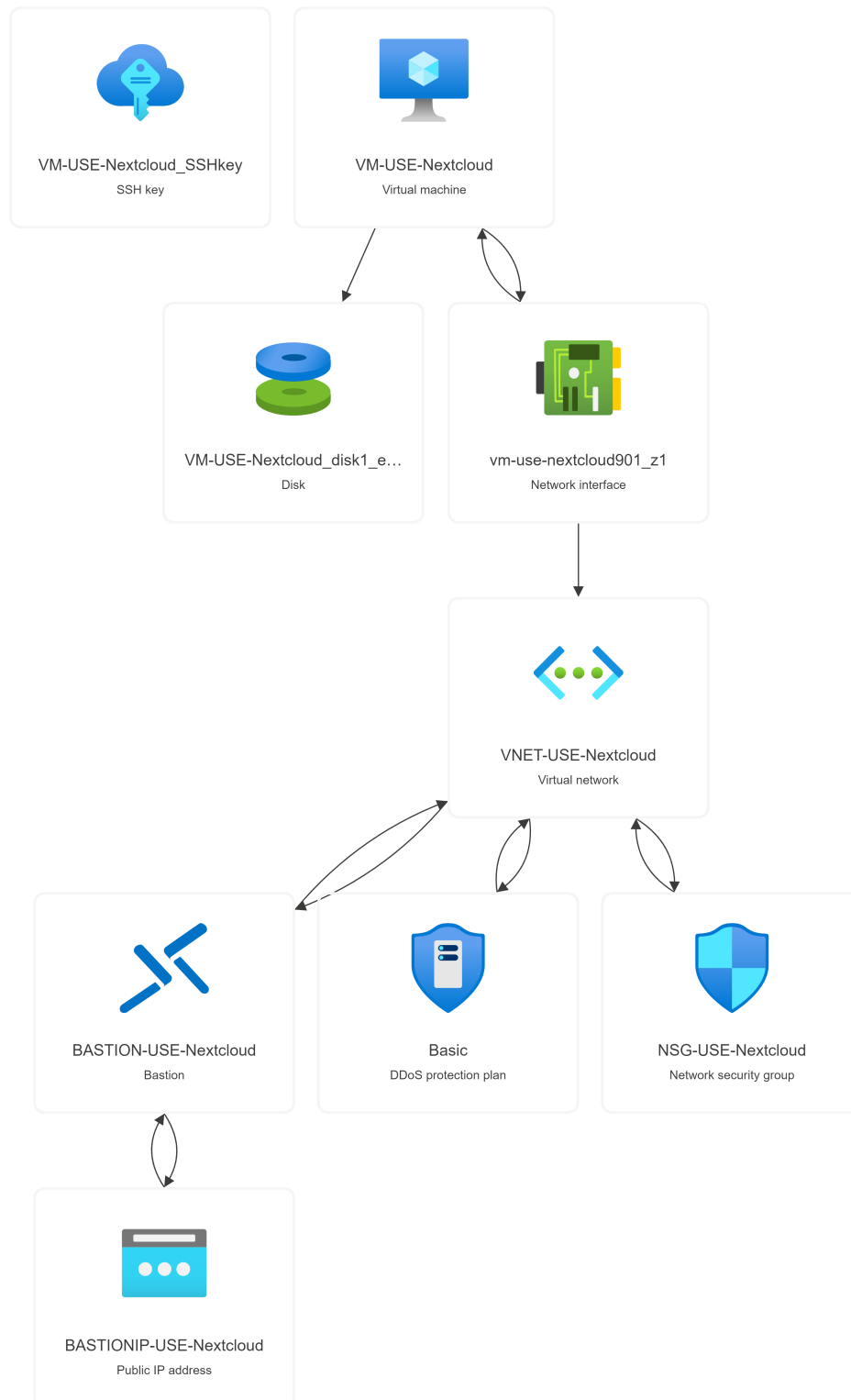- Install Mininet and ONOS via SSH using Bastion

Figure 1: Caption

IP addresses

Address space	192.168.0.0/16 (65,536 addresses)
Subnet	SNET_AS1_WF1OSS1 (192.168.0.0/19) (8,192 addresses)
Subnet	SNET_AS2_WF2OSS2 (192.168.32.0/19) (8,192 addresses)
Subnet	SNET_AS1_WF3OSS3 (192.168.64.0/19) (8,192 addresses)
Subnet	SNET_Onshore_Control_Center (192.168.96.0/19) (8,192 addresses)
Subnet	SNET_Cloud_Control_Center_EXT (192.168.128.0/20) (4,096 addresses)

Figure 2: Offshore wind farm application scenario VNET Subnets for the communicating AS

- Publish an IP
- Create a DNS label

3.2 Topology Design and Scripting

Creating a customized mininet topology.

3.3 Self-healing Module Design and Testing

4 Results

5 Discussion

6 Conclusion

7 References