

Andree Salvo

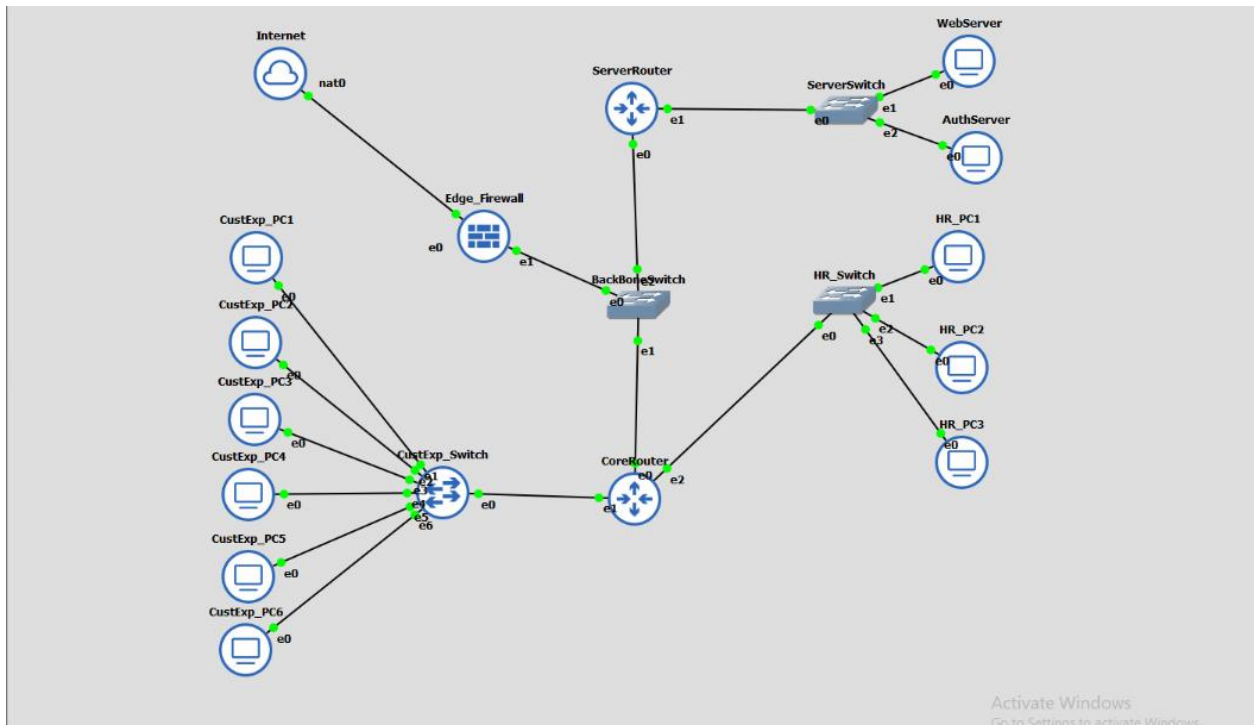
Southern New Hampshire University

CYB 310 – 7-2 Project Three Submission: Restructuring Status Report

Instructor: Raschid Muller

I. Network Reconfiguration

A. Network Diagram



B. Port assignment and VLAN assignment for each switch

Node properties ? X

BackBoneSwitch configuration

General

Name: BackboneSwitch

Console type: none

Settings

Port: 8

VLAN: 1

Type: access

QinQ EtherType: 0x8100

Add Delete

Ports

Port	VLAN	Type	EtherType
0	1	access	
1	1	access	
2	1	access	
3	1	access	
4	1	access	
5	1	access	
6	1	access	
7	1	access	

Reset OK Cancel Apply

Node properties ? X

CustExp_Switch configuration

General

Name: CustExp_Switch

Console type: none

Settings

Port: 8

VLAN: 1

Type: access

QinQ EtherType: 0x8100

Add Delete

Ports

Port	VLAN	Type	EtherType
0	20	access	
1	20	access	
2	20	access	
3	20	access	
4	20	access	
5	1	access	
6	1	access	
7	1	access	

Reset OK Cancel Apply

Node properties

HR_Switch configuration

General

Name:

Console type:

Settings

Port:

VLAN:

Type:

QinQ EtherType:

Ports

Port	VLAN	Type	EtherType
0	1	access	
1	1	access	
2	1	access	
3	1	access	
4	1	access	
5	1	access	
6	1	access	
7	1	access	

Node properties

ServerSwitch configuration

General

Name:

Console type:

Settings

Port:

VLAN:

Type:

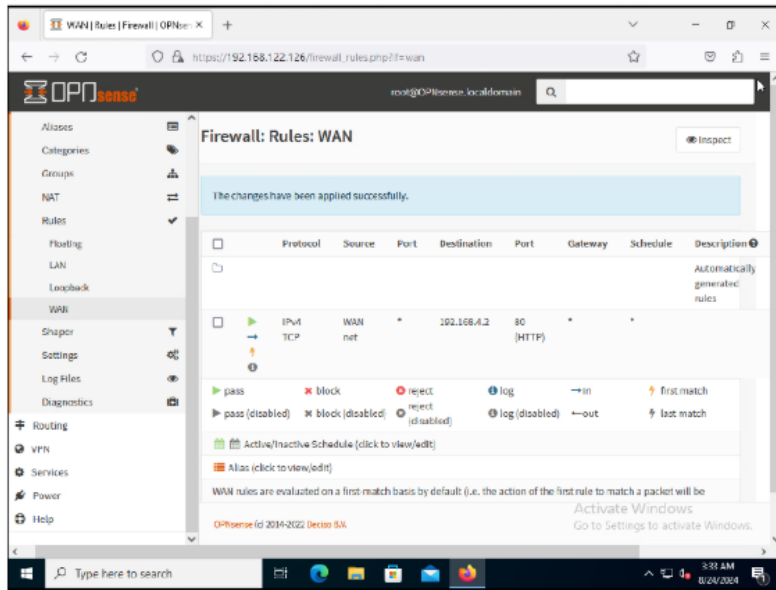
QinQ EtherType:

Ports

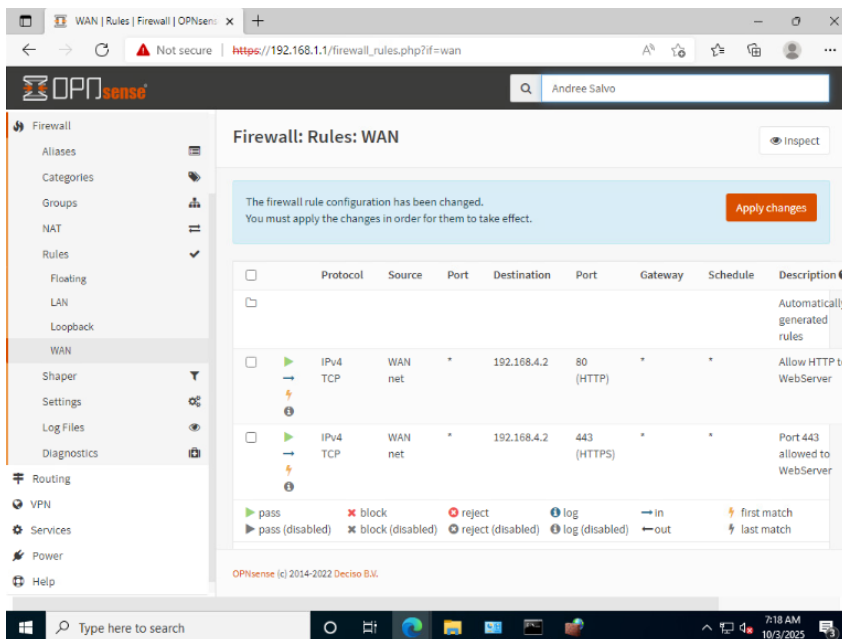
Port	VLAN	Type	EtherType
0	1	access	
1	1	access	
2	1	access	
3	1	access	
4	1	access	
5	1	access	
6	1	access	
7	1	access	

II. Traffic Flow Configuration: Include screenshots of the following:

A. Configure a firewall rule to allow port 80 HTTP from the WAN to the Web server.



B. Configure a firewall rule to allow port 443 HTTPS from the WAN to the Web server.



C. Configure a firewall rule to block port 80 HTTP from the WAN to any other system.

WAN | Rules | Firewall | OPNsense

Not secure | https://192.168.1.1/firewall_rules.php?if=wan

OPNsense

Firewall: Rules: WAN

The firewall rule configuration has been changed. You must apply the changes in order for them to take effect. [Apply changes](#)

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
<input type="checkbox"/>								Automatically generated rules
<input type="checkbox"/>	IPv4 TCP	WAN net	*	192.168.4.2	80 (HTTP)	*	*	Allow HTTP to WebServer
<input type="checkbox"/>	IPv4 TCP	WAN net	*	192.168.4.2	443 (HTTPS)	*	*	Port 443 allowed to WebServer
<input type="checkbox"/>	IPv4 TCP	WAN net	*	*	80 (HTTP)	*	*	Port 80 blocked from other systems

OPNsense (c) 2014-2022 Deciso B.V.

D. Configure a firewall rule to block port 443 HTTPS from the WAN to any other system.

WAN | Rules | Firewall | OPNsense

Not secure | https://192.168.1.1/firewall_rules.php?if=wan

OPNsense

Firewall: Rules: WAN

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
<input type="checkbox"/>								Automatically generated rules
<input type="checkbox"/>	IPv4 TCP	WAN net	*	192.168.4.2	80 (HTTP)	*	*	Allow HTTP to WebServer
<input type="checkbox"/>	IPv4 TCP	WAN net	*	192.168.4.2	443 (HTTPS)	*	*	Port 443 allowed to WebServer
<input type="checkbox"/>	IPv4 TCP	WAN net	*	*	80 (HTTP)	*	*	Port 80 blocked from other systems
<input type="checkbox"/>	IPv4 TCP	WAN net	*	*	443 (HTTPS)	*	*	Port 443 blocked from other system

OPNsense (c) 2014-2022 Deciso B.V.