

# **Nimble Troubleshooting and Firewall Configuration**

# MINT 709 - Capstone Project by Prabin Joshi



**Master of Science in Internetworking** 

**Department of Computing Science** 

**University of Alberta** 

Supervisor

Dr. Mike MacGregor

# Table of Contents

1.	Introduction	5
1.1	SCOPE OF THE PROJECT	5
1.2	PURPOSE OF THE PROJECT	6
2. M	ODULE DESCRIPTIONS	6
2.1	Understanding and Implementing User and Group Policy Management	9
2.1	.1 Motivation	11
2.1	Learning Objectives	11
2.2	Implementing VLAN on Nimble	12
2.2	2.1 Motivation	14
2.2	2.2 Learning Objectives	14
2.3	Understanding Port Forwarding and its Implementation	15
2.3	3.1 Motivation	17
2.3	3.2 Learning Objectives	17
2.4	Monitoring Nimble with pfTop	17
2.4	4.1 Motivation	17
2.4	1.2 Learning Objectives	19
2.5	Connecting Nimble to the Internet	19
2.5	5.1 Motivation	21
2.5	5.2 Learning Objectives	21
2.6	Restricting Websites Access with Nimble	22
2.6	5.1 Motivation	24
2.6	5.2 Learning Objectives	24
2.7	Creating a Network on UniFi	24
2.7	7.1 Motivation	24
2.7	7.2 Learning Objectives	26
2.8	Restricting Device Access with Nimble	26
2.8	3.1 Motivation	28
2.8	3.2 Learning Objectives	28
2.9	Implementing Firewall Policy on UniFi	28
2.9	9.1 Motivation	28

	2.9.2 L	earning Objectives	
2	2.10 Cre	ate and Restore Backup on Nimble	30
	2.10.1	Motivation	32
	2.10.2	Learning Objectives	32
2	2.11 Kno	owledge Sharing on Security and Monitoring	33
	2.11.1	Motivation	34
	2.11.2	Learning Objectives	34
3.	CONCLU	JSIONS	35
4.	REFERE	NCES	35

# Table of Figures

Figure 1: Block Diagram of Nimble and its Roles	6
Figure 2: Data Flow of Nimble	7
Figure 3: User Manager	9
Figure 4: Group Manager	9
Figure 5: Privilege Management	10
Figure 6: Creating a VLAN	. 11
Figure 7: Interface Assignment	12
Figure 8: DHCP Server IP Pool	.12
Figure 9: Firewall Rules	13
Figure 10: Port Forwarding in Nimble	14
Figure 11: Configuring Port Forwarding	. 15
Figure 12: Firewall Policy	. 15
Figure 13: pfTop Configuration	.17
Figure 14: pfTop Rules Monitoring	.17
Figure 15: Using Filter Expression on pfTop	18
Figure 16: Netgate Router Ports Overview	.19
Figure 17: Connection Monitoring	. 19
Figure 18: Firewall Policy for WAN	20

Figure 20: Host Addition.22Figure 21: Firewall Rules.22Figure 22: Creating a Network using UniFi Controller.24Figure 23: Creating Wi-Fi Network.24Figure 24: Firewall Rules.25Figure 25: Restriction using Logical Address.26Figure 26: Active Firewall Policy.26Figure 27: Implementation of Firewall rules on UniFi devices.28Figure 28: Creating Firewall Rule.28Figure 30: Factory Reset.30Figure 31: Reset Process.31Figure 32: Restoring Backup.32Figure 33: Capturing Traffic.33Figure 34: Analyzing the Traffic.34	Figure 19: Firewall Aliases	21
Figure 22: Creating a Network using UniFi Controller.24Figure 23: Creating Wi-Fi Network.24Figure 24: Firewall Rules.25Figure 25: Restriction using Logical Address.26Figure 26: Active Firewall Policy.26Figure 27: Implementation of Firewall rules on UniFi devices.28Figure 28: Creating Firewall Rule.28Figure 29: Creating Backup.29Figure 30: Factory Reset.30Figure 31: Reset Process.31Figure 32: Restoring Backup.32Figure 33: Capturing Traffic.33	Figure 20: Host Addition	22
Figure 23: Creating Wi-Fi Network.24Figure 24: Firewall Rules.25Figure 25: Restriction using Logical Address.26Figure 26: Active Firewall Policy.26Figure 27: Implementation of Firewall rules on UniFi devices.28Figure 28: Creating Firewall Rule.28Figure 29: Creating Backup.29Figure 30: Factory Reset.30Figure 31: Reset Process.31Figure 32: Restoring Backup.32Figure 33: Capturing Traffic.33	Figure 21: Firewall Rules	22
Figure 24: Firewall Rules.25Figure 25: Restriction using Logical Address.26Figure 26: Active Firewall Policy.26Figure 27: Implementation of Firewall rules on UniFi devices.28Figure 28: Creating Firewall Rule.28Figure 29: Creating Backup.29Figure 30: Factory Reset.30Figure 31: Reset Process.31Figure 32: Restoring Backup.32Figure 33: Capturing Traffic.33	Figure 22: Creating a Network using UniFi Controller	24
Figure 25: Restriction using Logical Address26Figure 26: Active Firewall Policy26Figure 27: Implementation of Firewall rules on UniFi devices28Figure 28: Creating Firewall Rule28Figure 29: Creating Backup29Figure 30: Factory Reset30Figure 31: Reset Process31Figure 32: Restoring Backup32Figure 33: Capturing Traffic33	Figure 23: Creating Wi-Fi Network	24
Figure 26: Active Firewall Policy.26Figure 27: Implementation of Firewall rules on UniFi devices.28Figure 28: Creating Firewall Rule.28Figure 29: Creating Backup.29Figure 30: Factory Reset.30Figure 31: Reset Process.31Figure 32: Restoring Backup.32Figure 33: Capturing Traffic.33	Figure 24: Firewall Rules	25
Figure 27: Implementation of Firewall rules on UniFi devices28Figure 28: Creating Firewall Rule28Figure 29: Creating Backup29Figure 30: Factory Reset30Figure 31: Reset Process31Figure 32: Restoring Backup32Figure 33: Capturing Traffic33	Figure 25: Restriction using Logical Address	26
Figure 28: Creating Firewall Rule.28Figure 29: Creating Backup.29Figure 30: Factory Reset.30Figure 31: Reset Process.31Figure 32: Restoring Backup.32Figure 33: Capturing Traffic.33	Figure 26: Active Firewall Policy	26
Figure 29: Creating Backup.29Figure 30: Factory Reset.30Figure 31: Reset Process.31Figure 32: Restoring Backup.32Figure 33: Capturing Traffic.33	Figure 27: Implementation of Firewall rules on UniFi devices	28
Figure 30: Factory Reset.30Figure 31: Reset Process.31Figure 32: Restoring Backup.32Figure 33: Capturing Traffic.33	Figure 28: Creating Firewall Rule	28
Figure 31: Reset Process.   31     Figure 32: Restoring Backup.   32     Figure 33: Capturing Traffic.   33	Figure 29: Creating Backup	29
Figure 32: Restoring Backup	Figure 30: Factory Reset	30
Figure 33: Capturing Traffic	Figure 31: Reset Process	31
	Figure 32: Restoring Backup	32
Figure 34: Analyzing the Traffic	Figure 33: Capturing Traffic	33
	Figure 34: Analyzing the Traffic	34

# 1. Introduction

Despite significant advances in technology and its widespread application in our society, many still do not have access to the Internet. This is primarily due to approaches taken for infrastructure rollout or failure to connect more sparsely populated areas [4]. As per Wakoma, Nimble uses the concept of a wireless mesh network to create a decentralized network infrastructure that is portable and, most importantly, an offline-first network. In the present world, the concept of portable wireless infrastructure helps to build communities that don't; have access to proper wired infrastructure. A wireless mesh network has a rich interconnection among devices, and it adopts a self-form, self-heal approach, which means that if one node fails to operate, the rest of the nodes or devices can still communicate with each other either directly or through intermediate nodes [5]. As there are a growing number of challenges in the deployment of wired infrastructure due to geographical issues, etc., wireless technology is needed to reach every corner of the world and keep people connected. Wakoma is trying to solve this problem by enabling communities to build their infrastructure that works offline and connects back to the Internet [4].

The Nimble network is an open-source network that can be built and deployed locally [6]. Users connected to the Nimble network can have access to a lot of services, such as video, voice, and text chat, video streaming and downloading, file sharing, eLearning module and website building and learning, collaborative spreadsheet and document creation, eBook reading, gaming, and much more, completely offline [4]. All these features can be accessed entirely offline and help people to stay connected with each other. The users on the Nimble network can easily connect to the Internet by plugging it into the network. Nimble units are portable and can be moved around or left in place to grow sustainable and scalable networks [6]. Over time, Nimble increases Internet demand and access by making it relevant, practical, and affordable to local communities [4].

# **1.1 SCOPE OF THE PROJECT**

The Nimble Troubleshooting and Firewall Configuration course is designed to provide users with no prior experience in Nimble implementation with a general understanding of its structure and technical aspects. The course offers comprehensive coverage of the different services and devices used to create a complete Nimble, covering fundamental to moderate complexity topics and providing hands-on practical demonstrations of modules to equip users with the experience needed to successfully configure, monitor, and upgrade their Nimble.

#### **1.2 PURPOSE OF THE PROJECT**

The goal of this project is to equip users with the fundamental knowledge necessary to operate the Nimble. This course offers hands-on implementation of technology concepts supported by interactive short video vignettes. By focusing on the application of Intranet technology with an offline-first network and implementation modules, users gain the technical knowledge to independently implement the Nimble, enabling large-scale deployment for remote smaller communities and providing a strong infrastructure for building a community wireless mesh network. The bundled solution of Nimble and the hands-on modules provides end users with easy access to resources and timely configuration, enabling them to utilize the full range of features that Nimble has to offer.

# 2. MODULE DESCRIPTIONS

The Nimble Troubleshooting and Firewall Configuration course consists of 11 modules focused on policy implementation, configuration, monitoring, and backup, as well as topics focused on how to stay secure and how the activity of users is monitored on a day-to-day basis. Figure 1 shows the block diagram representation of Nimble with the functions of each component. The functions of each individual component help in the application of the offline first network by integrating together to perform as a bundled solution. Such solutions help remote communities by being portable as well as eliminating the great need for the Internet and, at the same time, allowing individuals living in those communities to access the services locally without the need for expensive Internet plans. The offline first ideology uses the services run locally on Nimble to provide an offline way of communicating with people without the need for the Internet [1]. The services can be used for various communication services like video chat, messaging, streaming, etc.

Figure 2 represents a data flow diagram of Nimble. It explains how Nimble works and how it is connected to provide various services to end users. It uses colour-coded symbols to help end users understand the workflow of Nimble. This Nimble unit consists of devices like routers, switches, servers, access points, etc., to facilitate the offline first ideology. The platform used to run the Nimble services is an open-source project called 'Lokal', developed by Wakoma Incorporated and available on GitHub as 'GitHub-Wakoma'. It is designed to be platform-agnostic and serves as an open-source solution to connect various open-source services and applications. The 'Lokal' platform allows content creation, curation, and sharing without relying on the Internet. Branded as 'Lokal Services Global Impact', the platform operates on the philosophy of making a positive impact. It is compatible with online and offline environments due to its compatibility with a range of hardware and operating systems.

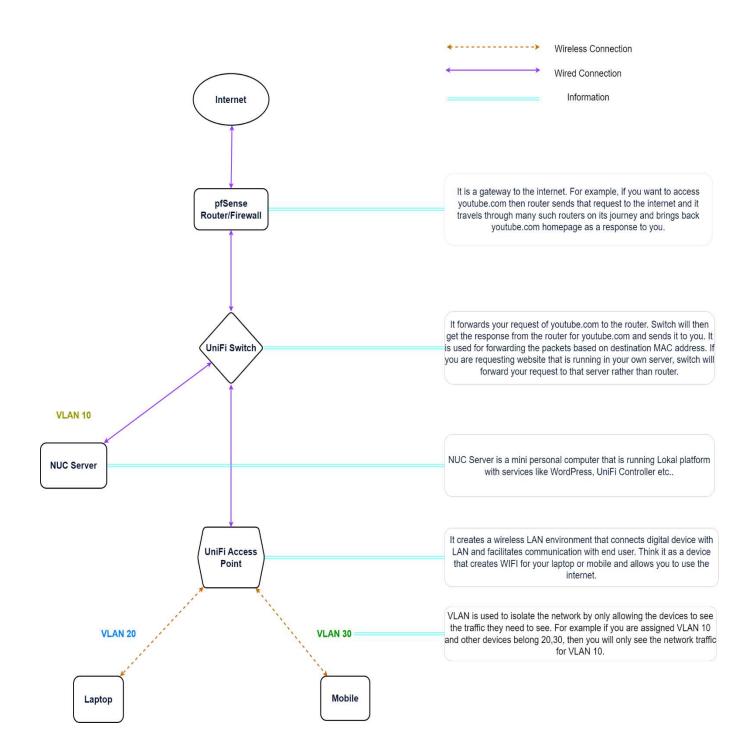


Figure 1: Block Diagram of Nimble and its Roles

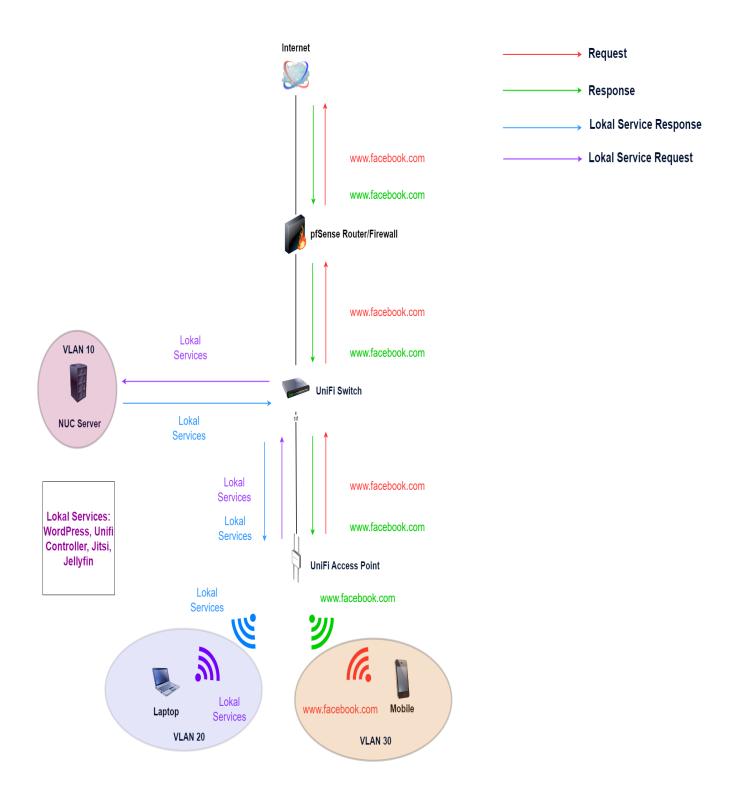


Figure 2: Data Flow of Nimble

As a customizable open-source software and service platform, 'Lokal' enables communities and organizations to produce, consume, and interact both online and offline. The 'Lokal' platform prioritizes offline functionality, offering a wide range of services, including video and audio calls, messaging, music, e-learning, e-books, network monitoring, Wikipedia, file-sharing, social networking, wireless network management, media streaming, and more. Platform installation is straightforward, requiring only a single line of code. Currently, the 'Lokal' platform runs on modern Linux OS, specifically Ubuntu, and is an ideal solution for remote communities with unreliable Internet connections.

This course consists of 11 fundamental modules focused on providing the end-user with hands-on experience in Nimble operation. A general overview of the topic, along with technical implementation, is provided to give users fundamental skills and hands-on training to use Nimble on their own. The module list is as follows:

- Understanding and Implementing User and Group Policy Management
- Implementing VLAN on Nimble.
- Understanding Port Forwarding and its Implementation.
- Monitoring Nimble with pfTop.
- Connecting Nimble to the Internet.
- Restricting Websites Access with Nimble.
- Creating a Network on UniFi.
- Restricting Device Access with Nimble.
- Implementing Firewall Policy on UniFi.
- Create and Restore Backup on Nimble.
- Knowledge Sharing on Security and Monitoring.

# 2.1 Understanding and Implementing User and Group Policy Management

This module is designed to provide users with an understanding of how to manage users and groups on Nimble. Policy-level management of users and groups determines who should have access to what resources and this module defines such policies. A general understanding of access management policies involves dividing a group of people into various subgroups based on their access rights, as well as defining policies based on roles. Examples of this are given in the figures below.

By the end of this module, users will be able to describe and complete tasks related to creating users and groups and assigning privileges based on the requirements. They will also be able to demonstrate measurable and observable output while understanding the concept of different privilege rules.

DNWT-pfSense.localdomain - Sys × +	https://192.168.5.1/system_usermanager.php			1	<ul> <li>- a</li> <li> a</li> </ul>
		VPN <del>+</del> Status <del>+</del> Dia	gnostics + Help +		0 €÷
System / User Manag	er / Users				0
Users Groups Setting	Authentication Servers				
Users	Full name	Status	Groups	Actions	
admin 🖓	System Administrator	~	admins	Add	T Delete
0					
	Netgate pfSense Plus is developed and mai	ntained by Netgate. © ESF 2004	- 2022 View license.		

Figure 3: User Manager

	anager / Groups / Edit	8
Users Groups	Settings Authentication Servers	
Group Properties		
Group name	dashboard	
Scope	Local	
	Warning: Changing this setting may affect the local groups file, in which case a reboot may	be required for the changes to take effect.
Description	\$	
	Group description, for administrative information only	
Group membership	admin	*
	Not members Members	-
	>>> Move to 'Members'	
		NOT MEMDERS
	Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.	

Figure 4: Group Manager

DNWT-pfSense.localdomain -	5ys × +	∨ – Ø X
⊲ ⊳ c	A Not secure https://192.168.5.1/system_groupmanager_addprivs.php?groupid=2	IV 🖬 🐨 🗉
pfisense -	► System ▼ Interfaces ▼ Firewall ▼ Services ▼ VPN ▼ Status ▼ Diagnostics ▼ Help ▼	<b>\$0</b> •
System	/ User Manager / Groups / Edit / Add Privileges	Θ
Users	Groups Settings Authentication Servers	
Group Pri	Group dashboard	
Assigne	d privileges       User - System: Copy files to home directory (chrooted scp)         User - System: Shell account access       User - System: Shell account access         User - VPN: IPsec xauth Dialin       User - VPN: IPsec Xauth Dialin         User - VPN: IPPO Dialin       User - VPN: DPOD Dialin         WebCfg - AJAX: Get Queue Stats       WebCfg - AJAX: Get Queue Stats         WebCfg - AJAX: Get Service Providers       WebCfg - AJAX: Get Service Providers         WebCfg - Dashboard (ell)       WebCfg - Dashboard (ell)         WebCfg - Diagnostics: ARP Table       WebCfg - Diagnostics: Rack Re Restore         WebCfg - Diagnostics: Configuration History       WebCfg - Diagnostics: Configuration History         WebCfg - Diagnostics: NSL Lookup       T         Hold down CTRL (PC//COMMAND (Mac) key to select multiple items.       T	

Figure 5: Privilege Management.

# 2.1.1 Motivation

The motivation of this module is to provide users with simplified approaches to implementing policies and maintaining access rights. In addition, the module aims to equip users with the skills and knowledge necessary to train others on policy design and monitoring. By the end of this module, users will have a better understanding of the importance of having policies in place and be able to perform real-world test cases through hands-on demonstrations.

#### 2.1.2 Learning Objectives

After completing this module, users should be able to execute the following tasks:

- a. Create, update, and delete Users, Groups.
- b. Understand the privilege access management.
- c. Grant access to users and groups based on roles.
- d. Define policy for groups.

#### 2.2 Implementing VLAN on Nimble

This module gives users with the knowledge and skills to implement VLAN on Nimble. It covers concepts related to the configuration and implementation of VLAN in Nimble. VLANs allow a switch to act like many switches, which means that one switch can handle many different networks or groups of computers that are unable to talk to each other. This helps to divide a big network into smaller parts for better organization and security. When switches are connected, computers on the same VLAN can be on different switches and still communicate. A single port on a device can also be used to talk to computers on different VLANs. The module provides a hands-on demo on creating VLANs, assigning them to interfaces, implementing firewall policies, and IP address assignments. The snapshots can be found in the figures below.

By the end of this module, users will be able to describe VLAN and its terminologies. They will also gain ideas on configuring interfaces and proper VLAN assignments. They will be able to implement firewall policies along with managing a pool of IP addresses with the introduction of a DHCP server and its benefits.

DNWT-pfSense.localdomain - Into × +			o x
	ecure   https://192.168.5.1/interfaces_vlan_edit.php   😳		••• E
pfsense + System	Interfaces - Firewall - Services - VPN - Status - Diagnostics - Help -	<b>≜</b> 1) ↔	
Interfaces / VLAN	ls / Edit	≢ ₩ 0	
VLAN Configuration			
Parent Interface	mvneta0 (f0:ad:4e:19:27:3e)  VIAN capable interfaces will be shown.		
VLAN Tag	[40]         I           802.1Q VLAN tag (between 1 and 4094).		
VLAN Priority	0 802.1Q VLAN Priority (between 0 and 7).		
Description	Description A group description may be entered here for administrative reference (not parsed).		
	Save		
	Netgate pfSense Plus is developed and maintained by Netgate. © ESF 2004 - 2023 View license.		

Figure 6: Creating a VLAN

DNWT-pfSense.localdomain - Inter × +		v – o x
	68.5.1/interfaces_assign.php	I 🐨 E
pfisense + System + Interfaces +	Firewall + Services + VPN + Status + Diagnostics + Help +	â () 🗭
Interfaces / Interface Assignme	ents	Litt 😧
Interface Assignments Interface Groups	Wireless VLANs QinQs PPPs GREs GIFs Bridges LAGGs	
Interface	Network port	
WAN	VLAN 4090 on mvneta0 (WAN)	•
LAN	VLAN 4091 on mvneta0 (LAN)	Delete
OPT	VLAN 4092 on mvneta0 (OPT)	Celete
PFSENSE_NUC_VLAN10	VLAN 10 on mvneta0 (PFSENSE_NUC_VLAN10)	Celete
PFSENSE_STAFF_VLAN20	VLAN 20 on mvneta0 (PFSENSE_STAFF_VLAN20)	Delete
PFSENSE_GUEST_VLAN30	VLAN 30 on mvneta0 (PFSENSE_GUEST_VLAN30)	✓
Available network ports:	VLAN 40 on mvneta0 (TEST_VLAN)	✓ + Add
Save	$\bigcirc$	
Interfaces that are configured as members of a lag	gg(4) interface will not be shown.	
		÷



WT-pfSens	e.localdomain - Ser 🗙 🕂						٥	
⊳ c	🛛 🔺 Not	secure   https://192.168.5.1/	ervices_dhcp.php?if=opt5		10			
	BOOTP	Ignore BOOTP queries				_		
	Deny unknown clients	Allow all clients		~				
		interface, any DHCP client v	vith a MAC address listed on any s		interface. If set to Allow known clients from any ress. If set to Allow known clients from only this scope/range.			
	Ignore denied clients	<ul> <li>Denied clients will be igr</li> </ul>	ored rather than rejected.					
		This option is not compatib	le with failover and cannot be enab	oled when a Failover Peer IP address is	s configured.			
	Ignore client identifiers	<ul> <li>If a client includes a union</li> </ul>	que identifier in its DHCP request, t	hat UID will not be recorded in its leas	e.			
			/hen a client can dual boot using d official DHCP specification.	ifferent client identifiers but the same	hardware (MAC) address. Note that the resulting			
	Subnet	192.168.40.0						
	Subnet mask	255.255.255.0						
	Available range	192.168.40.1 - 192.168.40.1	254					
	Range	192.168.40.10		192.168.40.250		)		
		From		То				
	Additional Pools							
	Add	+ Add pool						
		If additional pools of addre	sses are needed inside of this subr	et outside the above Range, they may	be specified here.			
		Pool Start	Pool End	Description	Actions			

Figure 8: DHCP Server IP Pool

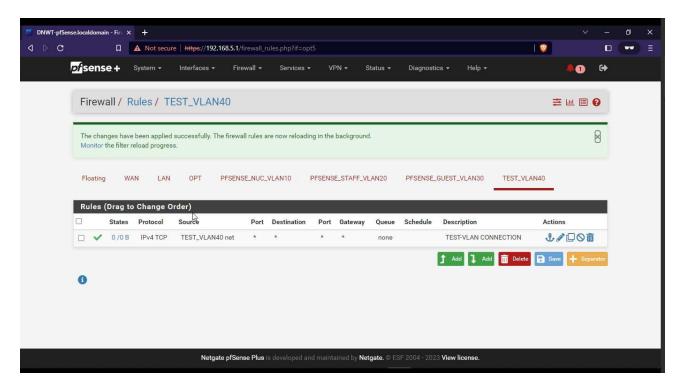


Figure 9: Firewall Rules

#### 2.2.1 Motivation

The motivation of this module is to provide users with knowledge of using VLAN and its implementation. The main goal of this module is to help users understand the significance of VLAN in managing network traffic and how it can be used to improve the performance of the Nimble network. By providing a comprehensive overview of the VLAN concept and its implementation, this module will enable users to successfully integrate VLAN in the Nimble network and configure firewall rules to enhance the flow of network traffic.

2.2.2 Learning Objectives

After completing this module, users should be able to execute the following tasks:

- a. Creating VLANs and assigning appropriate VLAN tags.
- b. Understanding the concept of VLAN and basic VLAN terminologies.
- c. Configuring interfaces and proper VLAN assignments.
- d. Implementing Firewall rules and policies.
- e. Selecting an appropriate pool of IP addresses.

#### 2.3 Understanding Port Forwarding and its Implementation.

This module provides the user with the basic concept of Port Forwarding. It covers concepts related to the implementation of port forwarding in Nimble. This will guide users to understand why it is required and how to implement that in Nimble. Port Forwarding is a technique that will help external devices access devices or computer services on a private network. Port forwarding is a way to connect a device on your private network (like your home network) to the Internet. This allows other people on the Internet to access things on your device, like a game or a website. Port forwarding maps an "Internet door" (called a port) to your device so that when someone knocks on that door, it goes directly to your device. However, this can also be dangerous if not set up properly, as someone could access your device without your permission. An example of this concept is provided with the hands-on demo. The snapshots can be found in the figures below.

By the end of this module, users will be able to get hands-on experience with port forwarding and understand its implementation. Users will also gain ideas on choosing appropriate ports as per the standards and rules in place for the use of ports for private and public use. They will be able to implement port forwarding to connect with devices behind a different network.

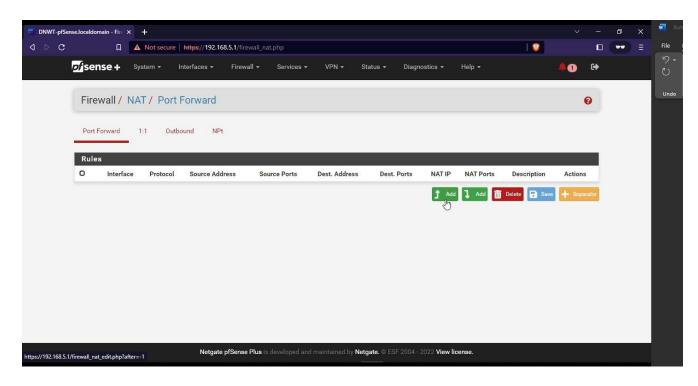


Figure 10: Port Forwarding in Nimble

📕 DNWT-pfSense.localdomain - Fire 🗙 🕂							v –	٥	×
	secure   https://192.168.5.1/fir	ewall_nat_edit.php?after=-1							
pfsense+ System +	Interfaces <del>+</del> Firewa	ll ← Services <del>-</del> V	/PN + Status +	Diagnostics •	• Help <del>•</del>	<b>40</b>	•		Â
Firewall / NAT / F	Port Forward / Edit						0		
Edit Redirect Entry									
Disabled	Disable this rule								
No RDR (NOT)	<ul> <li>Disable redirection for traf This option is rarely needed.</li> </ul>	100	igh knowledge of the im	plications.					
Interface	WAN Choose Wich interface this r	ule applies to. In most cases	▼ s "WAN" is specified.						ł
Address Family	IPv4 Select the Internet Protocol v	ersion this rule applies to.	~						
Protocol	TCP Choose which protocol this ru	ile should match. In most ca	► ases "TCP" is specified.						
Source	Display Advanced								
Destination	Invert match.	WAN address Type		► Ade	dress/mask	X	*		
Destination port range	Other 🗸	Custom	Other To port	♥ Cu:	stom				

Figure 11: Configuring Port Forwarding

_	_	ie +				Services -	- VPN		tus 🕶	Diagnosti	cs + Help +	<b>40</b> G
F	irew	all / F	Rules /	WAN								Liii 🗐 😰
	oatin ules	-	AN LA		E_NUC_	VLAN10	PFSENSE_	STAFF_VLA	N20	PFSENSE_	GUEST_VLAN30	
o		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	×	0 /0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	\$
	×	0 /0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	\$
	~	0 /0 B	IPv4 TCP	*	*	192.168.5.7	32400	*	none		NAT Port Forward For MY PC	℄ℰⅅѺ菌
											1 Add 1 Add 🔟 Delete	🖏 Save 🕇 + Separato
0							ß					

Figure 12: Firewall Policy

#### 2.3.1 Motivation

The motivation behind this module is to provide users with the knowledge and skills to use port forwarding and its implementation. The module will help users understand why and when we use port forwarding and how it can help gain access to services or devices located behind a different private network. This module will enable users to plan which services to connect using port forwarding, as well as gain the necessary skills to integrate it into the Nimble network.

#### 2.3.2 Learning Objectives

After completing this module, users should be able to perform the following tasks:

- a. Understand the concept of Port Forwarding.
- b. Understand the concept of NAT.
- c. Implement Port Forwarding on Nimble.

# 2.4 Monitoring Nimble with pfTop

In this module, users will learn how to monitor Internet activity on a Nimble network and use tools such as pfTop to gain insights into network traffic. Through the use of visuals, users will learn to quickly make sense of network activity and respond to any issues that arise. Specifically, users will be trained in using pfTop, a network traffic monitoring and statistics plugin in pfSense, to analyze and monitor network traffic in Nimble. The module will guide users through the process and provide snapshots of the tools used. By the end of the module, users will be able to:

- a. Use pfTop to monitor the traffic.
- b. Use filter expression to analyze the traffic and makes changes as required.

#### 2.4.1 Motivation

The motivation of this module is to provide users with knowledge of pfTop and its implementation in Nimble. This module will help users to gain insights into their network traffic and its statistics. Users will learn how to implement the pfTop plugin through the pfSense portal to analyze their network traffic.

DNWT-pfSense.localdomain - Dia 🗙 🕂								٥	×
	2 168 5 1/diag often ohn					0			
	2.100.3.1/diag_prop.php								
of sense + System - Interfaces -	Firewall - Services -	VPN - Status -	Diagnostic	s <del>-</del> Hel	lp <del>-</del>		•		<u>^</u>
				ar enga					
Diagnostics / pfTop							9		- 11
blaghootios, phrop									- 11
							 _		- 8
pfTop Configuration				N					- 8
View default				43					- 11
default		~							
	at net 208.123.73.0/24								
click for filter help	0								
Sort by Butes									
Sort by Bytes		*							
Maximum # of States									
Maximum # of States 100		~							
Output									
pfTop: Up State 1-93/93, View: default, O			100	EV0	DUTC	DV755			
PR DIR SRC tcp In 192,168.5,19:59193	DEST 192.168.5.1:443	STATE ESTABLISHED:ESTABLISHED	AGE 00:00:54	EXP	PKTS	BYTES 2324188			
ipv6-icmp Out fe80::f2ad:4eff:fe19:273e[4			00:47:13		6424	356584			
ipv6-icmp Out fe80::f2ad:4eff:fe19:273e[4		NO TRAFFIC:NO TRAFFIC	00:47:13		2777	199944			
ipv6-icmp Out fe80::f2ad:4eff:fe19:273e[1		NO TRAFFIC:NO TRAFFIC	00:15:58	00:00:07	132	12672			
ipv6-icmp In fe80::f2ad:4eff:fe19:273e[1		NO TRAFFIC:NO TRAFFIC	00:15:58	00:00:07	132	12672			
tcp In 192.168.5.19:59186	192.168.5.1:443	FIN WAIT 2:FIN WAIT 2	00:00:59		15	2896			
tcp In 192.168.5.19:59192	192.168.5.1:443	FIN WAIT 2: FIN WAIT 2	00:00:54		14	2856			
udp In 192.168.10.10:58972	192.168.10.1:53	MULTIPLE:MULTIPLE		00:00:34	14	1098			
ude Te 100 169 10 10/25142	101 169 10 1.52	MULTIDI SIMULTIDI S	00101116		11	2050			-

Figure 13: pfTop Configuration

se.localdomain - D	ia × +								
0	A Not s	secure https://192.16	8.5.1/diag	pftop.phr			1 🐨		
Diagnoon			9						
pfTop Conf	iguration								
	View	rules				V			
	View	Tules				<b>`</b>			
	_		_	_	_		_	_	
Output									
pfTop: Up Rul	e 1-128/128,	View: rules							
RULE ACTION	DIR LOG Q	IF PR K	PKTS	BYTES	STATES	MAX INFO			
0] Pass	Any		0	0	0	all			
1 Pass	Any		0	0	0	all			
2 Block	In Log Q		37	3809	0	drop inet from 169.254.0.0/16 to any			
3 Block	In Log Q		0	0	0	drop inet from any to 169.254.0.0/16			
4 Block	In Log		0	0	0	drop inet all			
5 Block	Out Log		0	0	0	drop inet all			
6 Block	In Log		652	125522	0	drop inet6 all			
7 Block	Out Log		0	0	0	drop inet6 all			
8 Pass	Any Q	ipv6-icmp K	909	89226	0	inet6 all			
9 Pass	Any Q	ipv6-icmp K	0	0	0	inet6 all			
10 Pass	Any Q	ipv6-icmp K	7	496	0	inet6 all			
11 Pass	Any Q	ipv6-icmp K	6	424	0	inet6 all			
12 Pass	Out Q	ipv6-icmp K	0	0	0	inet6 from fe80::/10 to fe80::/10			
13 Pass	Out Q	ipv6-icmp K	0	0	0	inet6 from fe80::/10 to fe80::/10			
14 Pass	Out Q	ipv6-icmp K	1	96	0	inet6 from fe80::/10 to fe80::/10			
15 Pass	Out Q	ipv6-icmp K	0	0	0	inet6 from fe80::/10 to fe80::/10			
16 Pass	Out Q	ipv6-icmp K	0	0	0	inet6 from fe80::/10 to fe80::/10			
17 Pass	Out Q	ipv6-icmp K	0	0	0	inet6 from fe80::/10 to ff02::/16			
18 Pass	Out Q	ipv6-icmp K	0	0	0	inet6 from fe80::/10 to ff02::/16			
19 Pass	Out Q	ipv6-icmp K	330	31680	0	inet6 from fe80::/10 to ff02::/16			
20 Pass	Out Q	ipv6-icmp K	0	0	0	inet6 from fe80::/10 to ff02::/16			
21 Pass	Out Q	ipv6-icmp K	0	0	0	inet6 from fe80::/10 to ff02::/16			
22 Pass	In Q	ipv6-icmp K	0	0	0	inet6 from fe80::/10 to fe80::/10			
23 Pass	In O	ipv6-icmp K	0	0	0	inet6 from fe80::/10 to fe80::/10			

Figure 14: pfTop Rules Monitoring

pfTo	p Configuration									
	View	default		~						
	Filter expression	host 192 168	10.1 and proto udp							
		click for filter h	11 secondar	J						
	Sort by	Bytes		~						
IVIa	aximum # of States	100								
		100		~						
0.11		100								
Outp	out	100		•				_		
pfTop	: Up State 1-7/7 (1					540	DUTC			
pfTop PR	: Up State 1-7/7 (1 DIR SRC	02), Vi <mark>e</mark> w: defa	DEST	STATE	AGE	EXP	PKTS 23	BYTES 1932	-	
pfTop PR udp	: Up State 1-7/7 (1 DIR SRC In_ 192.168.10	02), View: defa 1.10:43893	DEST 192.168.10.1:53	STATE NO_TRAFFIC:SINGLE	00:01:57	00:00:27	23	1932		
pfTop PR udp udp	: Up State 1-7/7 (1 DIR SRC	02), View: defa 1.10:43893 1.10:51516	DEST	STATE NO_TRAFFIC:SINGLE MULTIPLE:MULTIPLE	00:01:57 0 <mark>0:01:5</mark> 8					
pfTop PR udp	: Up State 1-7/7 (1 DIR SRC In 192.168.10 In] 192.168.10	02), View: defa 1.10:43893 1.10:51516 1.10:46245	DEST 192.168.10.1:53 192.168.10.1:53	STATE NO_TRAFFIC:SINGLE	00:01:57 00:01:58 00:01:38	00:00:27 00:00:56	23 25	1932 1833		
pfTop PR udp udp udp	: Up State 1-7/7 (1 DIR SRC In 192.168.10 In 192.168.10 In 192.168.10	02), View: defa 1.10:43893 1.10:51516 1.10:46245 1.10:59398	DEST 192.168.10.1:53 192.168.10.1:53 192.168.10.1:53	STATE NO <u>T</u> RAFFIC:SINGLE MULTIPLE:MULTIPLE NO <u>T</u> RAFFIC:SINGLE	00:01:57 00:01:58 00:01:38 00:01:48	00:00:27 00:00:56 00:00:27	23 25 20	1932 1833 1660		
pfTop PR udp udp udp udp	: Up State 1-7/7 (1 DIR SRC In 192.168.10 In 192.168.10 In 192.168.10 In 192.168.10	02), View: defa .10:43893 .10:51516 .10:46245 .10:59398 .10:38300	DEST 192.168.10.1:53 192.168.10.1:53 192.168.10.1:53 192.168.10.1:53	STATE NO_TRAFFIC:SINGLE MULTIPLE:MULTIPLE NO_TRAFFIC:SINGLE NO_TRAFFIC:SINGLE	00:01:57 00:01:58 00:01:38 00:01:48 00:01:46	00:00:27 00:00:56 00:00:27 00:00:27	23 25 20 22	1932 1833 1660 1562		
pfTop PR udp udp udp udp udp udp	: Up State 1-7/7 (1 DIR SRC In 192.168.10 In 192.168.10 In 192.168.10 In 192.168.10 In 192.168.10	02), View: defa .10:43893 .10:51516 .10:46245 .10:59398 .10:3300 .10:40507	DEST 192.168.10.1:53 192.168.10.1:53 192.168.10.1:53 192.168.10.1:53 192.168.10.1:53	STATE NO_TRAFFIC:SINGLE MULTIPLE:MULTIPLE NO_TRAFFIC:SINGLE NO_TRAFFIC:SINGLE	00:01:57 00:01:58 00:01:38 00:01:48 00:01:46 00:01:48	00:00:27 00:00:56 00:00:27 00:00:27 00:00:27	23 25 20 22 21	1932 1833 1660 1562 1428		
pfTop PR udp udp udp udp udp udp udp	: Up State 1-7/7 (1 DIR SRC In 192.168.10 In 192.168.10 In 192.168.10 In 192.168.10 In 192.168.10 In 192.168.10	02), View: defa .10:43893 .10:51516 .10:46245 .10:59398 .10:3300 .10:40507	DEST 192.168.10.1:53 192.168.10.1:53 192.168.10.1:53 192.168.10.1:53 192.168.10.1:53 192.168.00.1:53	STATE NO_TRAFFIC:SINGLE NO_TRAFFIC:SINGLE NO_TRAFFIC:SINGLE NO_TRAFFIC:SINGLE NO_TRAFFIC:SINGLE MULTIPLE:MULTIPLE	00:01:57 00:01:58 00:01:38 00:01:48 00:01:46 00:01:48	00:00:27 00:00:56 00:00:27 00:00:27 00:00:27 00:00:27 00:00:56	23 25 20 22 21 23	1932 1833 1660 1562 1428 1413		

Figure 15: Using Filter Expression on pfTop.

# 2.4.2 Learning Objectives

After completing this module, users will be able to analyze the network traffic and rules using pfTop. Users will be able to use filter expressions to perform extensive analysis of the generated traffic. They will also be able to monitor firewall rules and take necessary actions as required.

# 2.5 Connecting Nimble to the Internet

While the Nimble ideology is based on an offline-first network, this module provides users with the knowledge needed to connect Nimble to the Internet, should they choose to do so. Nimble is a solution designed to provide offline communication, eliminating the need for the Internet. However, for users who want to take advantage of the Internet connectivity, this module provides guidance on how to set up and configure a connection. With a focus on remote communities, Nimble is deployed to work in both online and offline modes. The snapshot of the tools and process is given in the figures below. This module will help users to do the following tasks:

a. Connecting Nimble to the Internet.

b. Monitoring the Connections and Implementing WAN firewall policy.



Figure 16: Netgate Router Ports Overview.

DNWT-pfSense.	ocaldomain - Stat 🔃 UniFi Network	DNWT-pfSense.localdomain - S	state	Netgate 110	pisense+ security e	DNWT-pfSense.loo	aldomain × +		- 0	
ı⊳ c	A Not secure <u>https://192.168.5</u>	.1					1 🥹			
Version	22.05-RELEASE (arm64) built on Wed Jun 22 18:56:18 UTC 2022	S sshd S	ecure \$	Shell Daemon	C®	LAN		lan (in) elan	(out)	-
	FreeBSD 12.3-STABLE	🥑 syslogd S	ystem	Logger Daem	on Co				6.0	k
	The system is on the latest version.	🥑 unbound D	NS Re	solver	Co					
	Version information updated at Mon Jan 30 16:09:18 MST 2023 😴	Interfaces			100				4.0	k
СРՍ Туре	ARM Cortex-A53 r0p4 2 CPUs: CPU 0: ARM Cortex-A53 r0p4 affinity: 0	🕂 WAN	1	1000baseT <full- duplex&gt;</full- 	10.0.0.245 2604:3d09:8480:3				2.0k	
	CPU 1: ARM Cortex-A53 r0p4 affinity: 1 SafeXcel Crypto: Yes (inactive)	I LAN	1	1000baseT <full-< td=""><td>192.168.5.1</td><td>30:09</td><td>30:50</td><td>31:40</td><td>32:09</td><td></td></full-<>	192.168.5.1	30:09	30:50	31:40	32:09	
Hardware crypto	Inactive			duplex>		PFSENSE	_NUC_VLAN1	opt2 (in) 😑 opt2	(out)	
Jptime	00 Hour 29 Minutes 51 Seconds	I OPT	4	none	192.168.6.1				0.0	
Current late/time	Mon Jan 30 16:32:04 MST 2023	PFSENSE_NUC_VLAN10	1	1000baseT <full- duplex&gt;</full- 	192.168.10.1				-2.0	ж
DNS server(s)	<ul> <li>127.0.0.1</li> <li>64.59.184.13</li> <li>64.59.190.242</li> <li>8.8.4.4</li> </ul>	PFSENSE_STAFF_VLAN20	1	1000baseT <full- duplex&gt;</full- 	192.168.20.1				-4.0	
	• 0.0.4.4 • 8.8.8.8	<b>.</b>	↑		192.168.30.1	30:09	30:50	31:40	32:09	
ast config	Mon Jan 30 16:07:39 MST 2023	PFSENSE_GUEST_VLAN3	)	<full- duplex&gt;</full- 		PFSENSE	_STAFF_VLAN	🛿 😡 dət3 (in) 🛛 🛑 opt3	(out)	k
State table size	0% (193/98000) Show states	TEST_VLAN40	1	1000baseT <full- duplex&gt;</full- 	192.168.40.1				0.0	
MBUF Usage	6% (1276/20490)	C LAN Uplink	1	Ethernet	n/a				-10	

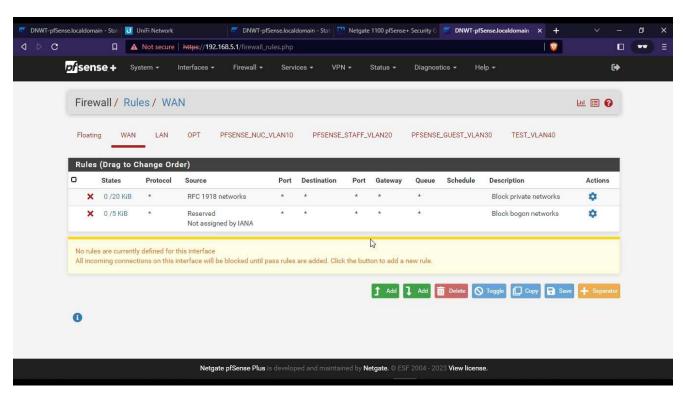


Figure 17: Connection Monitoring

Figure 18: Firewall Policy for WAN

#### 2.5.1 Motivation

The motivation of this module is to help users with connecting the Nimble to the Internet. It will provide guidance on the necessary steps to be taken and rules to be followed while emphasizing the associated risks of transitioning from an offline-first network to an open Internet approach.

#### 2.5.2 Learning Objectives

After completing this module, users will have hands-on experience with the process required to connect to the Internet and gain insights into the standards used for IP addresses to make such a connection. Additionally, users will learn about applying appropriate firewall policies to facilitate connections with the outside network.

# 2.6 Restricting Websites Access with Nimble

Restricting user's Internet access can increase productivity and protect your network from viruses and malicious content found on some websites. There are various ways to perform this operation, such as allowing access to all URLs except the ones you block or blocking all URLs and only allowing specific websites to enter your network. In this module, we focus on allowing all websites and blocking only specific websites from entering your network. The snapshot of this demo is given in the figures below.

After completing this module, users will have hands-on experience with the concept of aliases, as well as defining firewall rules to protect their network from external interference. Users will also gain ideas on the advantages of applying these policies to better protect their network and facilitate URL management on the network.

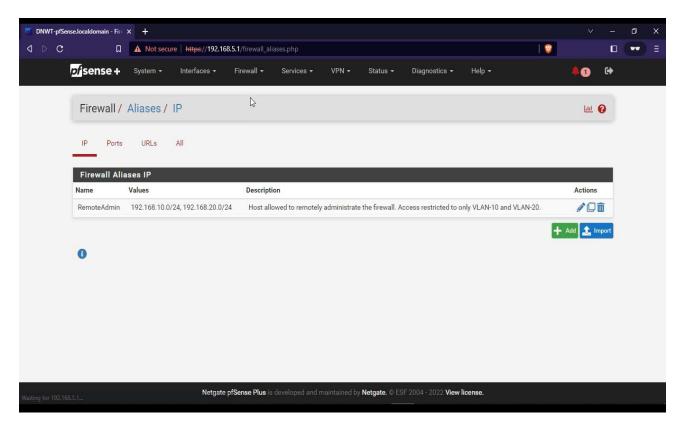


Figure 19: Firewall Aliases

NWT-pfSense.localdomain - Fire X	+		C
D C 🛛 🔺	Not secure   https://192.168.5.1/firewall_aliases_e	dit.php?tab=ip	
Firewall / Alia	ses / Edit		Θ
Properties			
Na	Blocked Website		
	The name of the alias may only consist of the second seco	e characters "a-z, A-Z, 0-9 and _".	
Descripti	List of websites to be blocked		
	A description may be entered here for admir	istrative reference (not parsed).	
Ту	De Host(s)	~	
Host(s)			
н	re-resolved and updated. If multiple IPs are r	: be specified by their IP address or fully qualified domain na etumed by a DNS query, all are used. An IP range such as 19 d a list of individual IP addresses will be generated.	
IP or FQ	www.facebook.com	Facebook website	Delete
	www.twitter.com	Twitter website	T Delete
	Save + Add Host	ed and maintained by <b>Netgate.</b> ⊕ ESF 2004 - 2022 <b>View lice</b>	nse

Figure 20: Host Addition

	Firew	vall / Rule	s/ LAN								≢ 💷 🗏 🌘
[		wall rule config anges must be a									Apply Changes
	Floatin	g WAN	LAN	OPT	PFSE	NSE_NUC_VLAN10	PF	SENSE_ST	AFF_VLAN20	PFSENSE_GUEST_VLAN30	
		(Drag to Ch									
-		States	Protocol	source	Port	Destination	Port	Gateway	Queue Schedule		Actions
		0 /0 B 16 /2.79 MiB	IPv4 TCP			Blocked_Websites	*	*	none	Restrict the access to unwanted website	08 801
			IPv6 *	LAN net		*	*	*	none	Default allow LAN to any rule Default allow LAN IPv6 to any rule	±≠□0ī €≠□0ī
		0700	IF VO	LAN HEL					none	Add 1 Add 1 Delete	
	0			4							Save - Separ

Figure 21: Firewall Rules

#### 2.6.1 Motivation

The motivation of this module is to help users block unwanted websites from their network. This module will help users understand the security aspects of their network by keeping it safe from malicious websites and increasing productivity. Restricting certain websites from entering the network is important to increase the safety and security of the network.

#### 2.6.2 Learning Objectives

Users will be able to perform the following tasks:

- a. Defining the websites that need to be blocked from entering the network.
- b. Understanding aliases and their implementation.
- c. Defining firewall policy to block the websites.

# 2.7 Creating a Network on UniFi

This module provides knowledge on how to create networks on UniFi devices using a platform called as UniFi controller. All UniFi equipment can be managed using a single interface, which

offers intuitive configuration options as well as robust device control and monitoring.[1]. The controller, also referred to as UniFi Network Application hosts the feature allowing users to control UniFi devices like Switch, Aps, etc. In this module, we will learn about creating networks and assigning the networks to wireless services. The snapshot of the demo is given in the figures below. Users will be able to perform the following tasks:

- a. Creating networks using UniFi network application.
- b. Creating Wireless SSID using UniFi controller.
- c. Managing the networks using the controller.
- d. Managing the network based on AP groups.

#### 2.7.1 Motivation

The motivation of this module is to help users to provide a hands-on demo to create networks using UniFi controllers on UniFi devices. This module aims to equip users with the knowledge required to implement and maintain networks on these devices and troubleshoot any problems related to network creation using UniFi Network Application.

DN	WT-pfSense.localdomain -	- Status: 📔 😈 UniFi Network		× +								- ť	3 X
4 0	> C	Not secure http://www.accure.com/accure	ps://unifi.lokal	l.network/manage/d	efault/settings/ne	tworks				1			=
0	Network												٢
œ					Not seeing every	thing? Go to Classic							$\times$
	Q Search Setting												
o∰ ⊚	💮 WiFi			Networks 💽									
ه	U Security			NAME *	ROUTER ~	SUBNET ~	IP LEASES ~	INTERNET ~	BACKUP ~	VPN ~	CONTENT FIL	TER	
<u>000</u>				<ul> <li>LAN</li> <li>pfsense-Gue</li> </ul>			0 (248)						
$\odot$	System Sett			pfsense-NU				- 🖖					
0	Controller Version			pfsense-Staf									
۵ ث													
													•

Figure 22: Creating a Network using UniFi Controller

🗾 DN	WT-pfSense.localdomain - Status:   🚺 UniFi Network	× +				- 0	×
1 لە	C 🛛 🗘 Not secure   https://	/unifi.lokal.network/manage/default	t/settings/wifi			•••	
0	Network						٢
(DP)		0 N	lot seeing everything? Go to Clas:			is again	×
— ©							
ر چ	WiFi       A       Networks	WiFi 💽			New WiFi Network		
ត្រ	Security     Security     Internet		TWORK - AP GROUP		WIFI EXPERIENCE		
ф О	응 System Settings		sense-Staff-VLA All APs				
Ð   Ø	Controller Version 6.2.26	Guest Hotspot 💽					
0							

Figure 23: Creating Wi-Fi Network.

#### 2.7.2 Learning Objectives

After completing this module, users will understand how to use the controller to configure networks for UniFi devices. Users will also be able to maintain their networks depending on their use cases.

# 2.8 Restricting Device Access with Nimble

Nimble does not offer the option to restrict access for a device attempting to connect to the network or to block it using MAC addresses. Instead, Nimble uses logical addresses to restrict access, and this module will guide users through the process of implementing this concept. It is important to note that blocking a particular IP address may not necessarily restrict the device from connecting to the network. As logical addresses can change, unlike physical addresses, users may need to block a pool of IP addresses or an entire subnet of IP addresses. Additionally, a device may still connect by switching the connection, so monitoring traffic is essential to ensure proper network management. This module will provide hands-on experience for restricting a specific IP address. The snapshot of the demo is included in the figures below.

After completing this module, users will possess the skills required to manage their network access rules and control device connections to their network. They will also be able to filter good and bad traffic using logical addresses and protect their network from unwanted access.

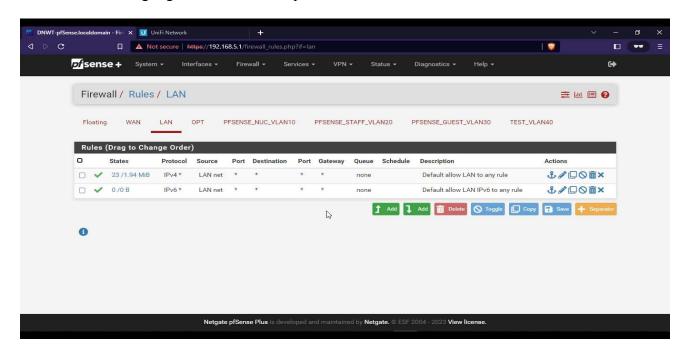


Figure 24: Firewall Rules

📕 DNWT-pfSense.localdomain - Fin 🗙 🚺 U	niFi Network	+					٥	×
	t secure   https://192.168.5.1/fi	rewall_rules_edit.php?if=lan&afi	er=-1		<b>V</b>			
	onoocene mendee nom a	men puoketo maot come to mat	on uno ruio.			-		^
Address Family	IPv4		~					
	Select the Internet Protocol v	rersion this rule applies to.						
Protocol	TCP		~					
	Choose which IP protocol thi	s rule should match.						
Source						- 1		
Source		10 - 10 - 10 - 10 - 10 - 10 - 10 - 10 -				_		
Source	Invert match	Single host or alias	*	172.16.5.64	1	~		
	Cisplay Advanced							
	The Source Port Range for a its default value, any.	connection is typically random	and almost never equal to the	destination port. In most cases this setti	ing must remain	at		
	no ocidan valoc, any.					_		
Destination								
Destination	Invert match	any	×	Destination Address	1	~		
Destination Port Range	(other) 🗸		(other) 🗸					
	From	Custom	То	Custom				
	Specify the destination port of	or port range for this rule. The "1	o" field may be left empty if or	nly filtering a single port.				
						- 1		
Extra Options								
Log	Log packets that are hand	dled by this rule						
			gging for everything. If doing a	lot of logging, consider using a remote s	syslog server (see	6		
	the Status: System Logs: Set	tings page).						
<b>N</b> 1.11	(							*

Figure 25: Restriction using Logical Address.

2	sens	e + Syster	m 🔻 İnte	erfaces <del>-</del> F	irewall	<ul> <li>Servic</li> </ul>	es 🕶	VPN 🗸	Status 🕶	Diagnostics 👻	Help 🕶			•
F	Firew	all / Rules	/ LAN									ŧ	E 🔟 🗐	0
				essfully. The fire	wall rul	es are now rele	bading	in the back	ground.					
1	Monitor	the filter reload	progress.											0
	Floating	WAN	LAN	OPT PFSE	NSE_N	UC_VLAN10	PF	SENSE_STA	FF_VLAN20	PFSENSE_GUEST	_VLAN30 TEST_	VLAN40		
				Ň										
F	Rules	(Drag to Cha	nge Order	)										
		(Drag to Cha States	nge Order Protocol	) Source	Port	Destination	Port	Gateway	Queue Schee	lule Description		Action	s	
	)				Port *	Destination	Port *	Gateway *	Queue Scheo none	dule Description			s Do <b>đ</b>	
0	)	States	Protocol	Source							w LAN to any rule	£ Ø		
0	) > × > •	States 0 /0 B	Protocol IPv4 TCP	Source 172.16.5.64	*	*	*	*	none	Default allo	w LAN to any rule w LAN IPv6 to any rule	\$ Ø \$ Ø	°00	×
	) > × > ~	States 0 /0 B 26 /2.03 MiB	Protocol IPv4 TCP IPv4 *	Source 172.16.5.64 LAN net	*	*	*	*	none none none	Default allo Default allo	w LAN IPv6 to any rule	\$# \$# \$#	00 00 00 00	×
	) > × > ~	States 0 /0 B 26 /2.03 MiB	Protocol IPv4 TCP IPv4 *	Source 172.16.5.64 LAN net	*	*	*	*	none	Default allo Default allo		\$# \$# \$#	00 00 00 00	×

Figure 26: Active Firewall Policy

#### 2.8.1 Motivation

The motivation of this module is to help users with the knowledge and hands-on demo to block unwanted devices from their network or devices trying to connect to their network using logical addresses. Providing users with the technical information necessary to execute this policy. Also provides users to manage their network access rules.

#### 2.8.2 Learning Objectives

Users will be able to perform the following tasks:

- a. Use of firewalls to restrict devices.
- b. Understand the concept of logical address and physical address.
- c. Implement a firewall policy to protect network infrastructure.

# 2.9 Implementing Firewall Policy on UniFi

This module provides knowledge on how to create firewall rules on UniFi devices using a platform called UniFi Controller. All UniFi equipment can be managed using a single interface, which offers intuitive configuration options as well as robust device control and monitoring [1]. The controller, also referred to as UniFi Network Application hosts the feature that allows users to control UniFi devices such as switches and access points. In this module, we will learn about creating firewall rules and implementing them on UniFi devices through UniFi Controller. The snapshot of the demo is given in the figures below. After completing this module, users will have the necessary skills to create, manage, and monitor firewall rules in their UniFi-managed networks. They will also understand the difference between established and invalid states.

#### 2.9.1 Motivation

This module aims to provide users with a hands-on demonstration of how to create networks on UniFi devices using the UniFi controller. It will equip users with the necessary knowledge and skills to implement, maintain, and troubleshoot their networks using the UniFi Network Application.

Un Un	iFi Network × +						٥	×
<b>d</b> 1	C 🛛 🗘 Not secure   http://www.secure	ps://unifi.lokal	.network/manage/default/settings/security/threat-management	1			•••	
0	Network						(	•
OP			1 Not seeing everything? Go to Classic Settings		Don't show	this agair		×
 ©	Q Search Settings		Internet Threat Management					
ဝ-ြို့	🔅 WiFi		Firewall					
0	Networks		Rules					
[6]	🛞 Internet							
<u>ollo</u>	System Settings		All Rules Internet LAN Guest Internet v6 LAN v6	Gues	tv6			
0	Advanced Features		RULE INDEX ENABLED DESCRIPTION ACTION C	COUNT	ТҮРЕ			
Ø								
ے ب	Controller Version 6.2.26							
(1)			Groups					

Figure 27: Implementation of Firewall rules on UniFi devices

😈 Un	iFi Network X UniFi Gateways -	Introduction to Firew +			~		٥	×
4	C 🛛 🗘 🔺 Not secure   htt	tps://unifi.lokal.network/manage/default/s	settings/security/threat-management/firewall/rule/form/new	🦁			•••	
0	Network							٢
œ		Not	seeing everything? Go to Classic Settings		Don't show	w this agai		×
- ©	Q Search Settings		Create New Rule					
ૡ૽	🔶 WiFi	Description	Allowed Established States					
0	Networks	Enabled						
ما ال	internet	Rule Applied	Refore Predefined Rules					
Õ	System Settings	Action	Accept					
$\oslash$		IPv4 Protocol						
Û.	Controller Version 6.2.26	Source				~		
0				Cancel	Apply C	hanges		

Figure 28: Creating Firewall Rule

# 2.9.2 Learning Objectives

Users will be able to perform the following tasks:

- a. Creating firewall rules using the UniFi network application.
- b. Implementing firewall policies for different internal and external interfaces.
- c. Monitoring the policy using the controller.
- d. Understanding the concept of established and invalid states.

# 2.10 Create and Restore Backup on Nimble

The critical aspect of every deployment is the planning and response for failover. If a live system goes down, it hampers the overall operation and possibly may result in loss of data or the devices getting crashed. It is important to be able to have a backup in place and restore it in case a failure occurs. This module will help users in this scenario with a hands-on demonstration and the technical skills required to perform this operation. Backup and restore is done with the pfSense router and a snapshot of which is given in the figures below.

After completing this module, users will be able to restore their network device from a hard reset and regain their data using previously stored backup information. They will also be able to recover their device from any misconfiguration using the backup file.

← → C A A Not secure   https://	//192.168.5.1/diag_backup.php	i£ ☆ 🛛 🔮
of sense + System -	Interfaces - Firewall - Services - VPN - Status - Diagnostics - Help -	<b>41</b> 🕩
Diagnostics / Bac	kup & Restore / Backup & Restore	Θ
Backup & Restore Co	nfig History	
Backup Configuration		
Backup area	All V	
Skip packages	Do not backup package information.	
Skip RRD data	Do not backup RRD data (NOTE: RRD Data can consume 4+ megabytes of config.xml space!)	
Include extra data	□ Backup extra data. Backup extra data files for some services.	
Encryption	Encrypt this configuration file.	
	Lownload configuration as XML	
Restore Backup		
	Open a Netgate pfSense Plus configuration XML file and click the button below to restore the configuration.	
Restore area		

# Figure 29: Creating Backup

- > C 🟠 A Not secure Https://192.168.5.1/diag_defaults.php	Ê	☆		۲
💋 Sense + System + Interfaces + Firewall + Services + VPN + Status + Diagnostics + Help +	1	•		
Diagnostics / Factory Defaults		0		
Factory Defaults Reset				
Resetting the system to factory defaults will remove all user configuration and apply the following settings: <ul> <li>Reset to factory defaults</li> </ul>				
LAN IP address will be reset to 192.168.1.1     System will be configured as a DHCP server on the default LAN interface     Reboot after changes are installed     WAN interface will be set to obtain an address automatically from a DHCP server     webConfigurator admin username will be reset to 'admin'     webConfigurator admin password will be reset to 'pfsense'				
Are you sure you want to proceed?				
Netgate pfSense Plus is developed and maintained by Netgate. © ESF 2004 - 2022 View license.				
config-DNWT-pfSxml			Show	all

Figure 30: Factory Reset

Netgate pfSense Plus.home.arpa	+	~	-	٥	×
$\leftrightarrow$ $\rightarrow$ X $\triangle$ Not secure	https://192.168.1.1	e	☆		:
	Welcome to Netgate pfSense Plus!       Image: Constraint of the initial setup wizard starts.         One moment while the initial setup wizard starts.       Image: Constraint of the initial setup wizard starts.         Embedded platform users: Please be patient, the wizard takes a little longer to run than the normal GUI.       Image: Constraint of the initial page.         To bypass the wizard, click on the Netgate pfSense Plus logo on the initial page.       Image: Constraint of the initial page.				



Skip RRD data	🔽 Do not backup RRD da	192.168.1.1 says		
12. 		Are you sure you wish to restore configuration?		
Include extra data	<ul> <li>Backup extra data.</li> <li>Backup extra data files for</li> </ul>	Салсе		
Encryption	Encrypt this configurat	ion file.		
	🛓 Download configurati	on as XML		
Restore Backup				
	Open a Netgate pfSense F	Plus configuration XML file and click the button below to restore the configuration.		
Restore area	All	~		
Configuration file	Choose File config-DN	WT7132402.xml		
Switch	Preserve switch config	juration.		
Encryption	Configuration file is en	crypted.		
	<b>D</b> Restore Configuration The firewall will reboot aff	er restoring the configuration.		

#### 2.10.1 Motivation

The motivation of this module is to assist users with maintaining a backup of their network device and restoring it in case of failure. These skills will provide users with the technical knowledge necessary to recover successfully from an event. This module provides a hands-on demonstration to share knowledge on restoring their network from potential data loss.

#### 2.10.2 Learning Objectives

Users will be able to perform the following tasks:

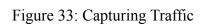
- a. Create the backup file.
- b. Resetting the device.
- c. Restore the device using the backup file.

#### 2.11 Knowledge Sharing on Security and Monitoring

The module is designed to provide users with knowledge about security and the fact that they are not anonymous on the Internet. It is more of a knowledge-sharing module than an implementation module that shows users, through a hands-on demo, how they can be tracked and have their activities monitored by external parties. The module provides a general overview of data traffic monitoring and how to remain secure and protected from unwanted parties. The snapshot is included in the figures below.

Upon completing the module, users will be able to understand how to keep their network secured and protect their privacy. They will also gain knowledge on how they can be tracked by external parties. This will help build a solid foundation for being aware of such situations and taking necessary actions when appropriate.

13902 6.722379       13.107.42.12       10.0.0.15       TCP       1514       120 443       443 + 55376       [ACK] Seq=15273922 Ack=253 Win=16380 Len=1460 [TCP segment of a reassembled         13908 6.722445       10.0.0.15       13.107.42.12       TCP       54       128 55376       55376       443 [ACK] Seq=15273922 Ack=253 Win=16695 Len=0         13904 6.722458       13.107.42.12       10.0.0.15       TCP       1514       120 443       443 + 55376 [ACK] Seq=1527382 Ack=253 Win=16695 Len=0         13905 6.722605       10.0.0.15       13.107.42.12       TCP       54       128 55376       55376 + 443 [ACK] Seq=15278642 Ack=253 Win=16695 Len=0         13906 6.724163       13.107.42.12       10.0.0.15       TCP       1514       120 443       443 + 55376 [ACK] Seq=15278642 Ack=253 Win=16695 Len=0         13906 6.724263       13.107.42.12       10.0.0.15       TCP       1514       120 443       443 + 55376 [ACK] Seq=1527802 Ack=253 Win=16695 Len=0         13906 6.724263       10.0.0.15       13.107.42.12       TCP       54       128 55376       55376 + 443 [ACK] Seq=257802 Ack=253 Win=16695 Len=0         13906 6.724264       10.0.0.15       13.107.42.12       TCP       54       128 55376       55376 + 443 [ACK] Seq=257802 Ack=253 Win=16695 Len=0         13906 6.724264       10.0.0.15       13.107.42.12       TCP<	Apply a display filter <	:Ctrl-/>					E 2
13980 6, 722379 13.107.42.12 10.6.0.15 10.74.2.12 10.6.0.15 10.74.2.12 10.6.0.15 10.8.0.12 10.8.0.15 10.8.0.0	. Time	Source	Destination	Protocol	Length Time	to Live Source Port	Info
13989 6,722445       18.0.0.15       13.107.42.12       TCP       54       128 5576       5376       4.43       [ACX] Seq-327382       Min-16599 Len-0         13984 6,722558       13.107.42.12       18.0.0.15       TCP       151       120 443       443       +5376       [ACX] Seq-327582       Ack-253 Min-16599 Len-0         13986 6,72463       13.107.42.12       10.0.0.15       TCP       1514       120 443       443       +5376       [ACX] Seq-1327882       Ack-253 Min-16598 Len-0         13986 6,72463       13.107.42.12       10.0.0.15       TCP       1514       120 443       443       +5376       [FM, CS] Seq-1327882       Ack-253 Min-16598 Len-0         13986 6,72452       13.107.42.12       10.0.0.15       TCP       1514       120 443       443       +5376       [FM, CS] Seq-1327832       Ack-253 Min-16598 Len-0         13986 6,72452       13.107.42.12       10.0.0.15       TCP       1514       120 443       443       +5376       [FM, CS] Seq-1327832       Ack-253 Min-16598       Len-046       [TCP segment of a reascembled]         13986 6,72452       13.107.42.12       10.0       interface       VinceWPF (92016548-CC01-4437-894A-3C5C648C54C2), ide-626       Seq 147       Seq 147       Seq 147       Seq 147       Seq 147       Seq 147	13901 6.722379	13.107.42.12	10.0.0.15	SSLv2	1514	120 443	Encrypted Data [TCP segment of a reassembled PDU]
<pre>13946 6.722588 13.107.42.12 10.0.0.15 TCP 1514 120 443 443 + 55376 [XC] Seq-1527582 Ack-253 Win-1588 Len-1460 [TCP segment of a reassembled 13965 6.722685 13.107.42.12 10.0.0.15 TCP 1514 120 443 443 + 55376 [ACK] Seq-15276842 Ack-253 Win-16580 Len-1460 [TCP segment of a reassembled 13966 6.724163 13.107.42.12 10.0.0.15 TCP 1514 120 443 443 - 55376 [ACK] Seq-15276842 Ack-253 Win-16580 Len-1460 [TCP segment of a reassembled 13966 6.724163 13.107.42.12 10.0.0.15 TCP 1514 120 443 443 - 55376 [ACK] Seq-15276842 Ack-253 Win-16580 Len-1460 [TCP segment of a reassembled 13966 6.724163 13.107.42.12 10.0.0.15 TCP 1514 120 443 443 - 55376 [ACK] Seq-15278042 Ack-253 Win-16580 Len-1460 [TCP segment of a reassembled 13986 6.72458 13.107.42.12 10.0.0.5 TCP 1514 120 443 443 - 55376 [ACK] Seq-15278042 Ack-253 Win-16580 Len-1460 [TCP segment of a reassembled 13986 6.72458 13.107.42.12 bits), 1514 bytes captured (12112 bits) on interface \Device\WPF_(92016548-CCD1-4437-894A-3C56648C54C2), id 0 thermet Protocol Version 4, for: 13.107.42.12, bst: 10.0.0.15 Transmission Control Protocol, Src Port: 443, Dst Port: 55376, Seq: 1, Ack: 1, Len: 1460 Frasport Layer Security</pre>	13902 6.722379	13.107.42.12	10.0.0.15	TCP	1514	120 443	443 + 55376 [ACK] Seq=15273922 Ack=253 Win=16380 Len=1460 [TCP segment of a reassembled
13985 6.722065 10.0.0.15 13.107.42.12 TCP 54 128 55376 55376 + 443 [ACK] Seq=253 Ack=15276842 Ukin=16695 Len-0 13980 6.724163 13.107.42.12 10.0.0.15 TCP 1514 120 443 + 43 + 55376 [FM, ACK] Seq=15276842 Ack=253 Ukin=16380 Len=1460 [TCP segment of a reassembler 13980 6.724263 10.0.0.15 13.107.42.12 TCP 54 128 55376 55376 + 443 [ACK] Seq=15276842 Ack=253 Ukin=16380 Len=1460 [TCP segment of a reassembler 13980 6.724236 10.0.0.15 13.107.42.12 TCP 54 128 55376 55376 + 443 [ACK] Seq=253 Ack=15279762 Ukin=16538 Len=40 13980 6.724236 11.107.42.12 10.0.0.15 TCP 1514 120 443 443 + 55376 [SM, CK] Seq=253 Ack=15279762 Ukin=16585 Len=0 13980 6.724360 13.107.42.12 J10 40 15 TCP 1514 120 443 443 + 55376 [SM, CK] Seq=253 Ack=15279762 Ukin=16585 Len=0 13980 6.724360 13.107.42.12, Dt: 10.0.0.15 TCP 1514 120 443 443 + 55376 [SM, CK] Seq=253 Ack=15279762 Ukin=16587 Len=0 Trans 1: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\WPF (9201548-CCD1-4437-B94A-3CSC648C54C2), id 0 thermet II, sr: ARBISOG or Jinis Jiais (0), bst: TnetLoc-T2:10iar7 (76:0:c:Bi:f2:10ia7) Internet Protocol, Sr: Drotool, Sr: Port: 443, Dst Port: 55376, Seq: 1, Ack: 1, Len: 1460 Transport Layer Security 0 78 0c b8 f2 10 a7 10 55 11 af 3d 36 08 00 45 00 x x·····V v=6·-E· 0 66 d6 95 0b d6 48 02 29 02 66 02 55 05 18 0 79 70 27 26 120 24 fd 64 24 25 40 (fd 04 15) 0 78 0c b8 f2 10 a7 10 55 11 af 3d 36 08 ad 9 0 x ····V v=6·-E· 0 78 0c b8 f2 10 a7 10 55 11 af 16 c 19 70 53 ······ P····) f ·V··· 0 76 4d 44 0c cc 06 c f0 73 0f 74 43 35 7a c 2d 9 (ff······ st#cz···· 0 93 80 16 c 36 95 97 27 27 45 0b 80 4 d6 98 ad 99 ······ Hu··· 0 76 4d 54 0c cc 60 c f0 73 0f 74 45 08 6d 40 ······ 0 93 80 16 c 36 97 09 12 cs 74 54 04 19 1 (cs 13 7 % ······ 460 ·········· 0 93 80 16 cs 16 57 75 20 Lib 4d 6d 56 8f ad 96 ···································	13903 6.722445	10.0.0.15	13.107.42.12	TCP	54	128 55376	55376 + 443 [ACK] Seq=253 Ack=15275382 Win=16695 Len=0
13906 6.724163 13.107.42.12 10.0.0.15 TCP 1514 120 443 443 + 55376 [ACK] Seq-15276042 Ack-253 Win-16300 Len-1460 [TCP segment of a reassembled 13006 6.724163 13.107.42.12 10.0.0.15 TCP 1514 120 443 443 + 55376 [PSH, ACK] Seq-1527302 Ack-253 Win-16300 Len-1460 [TCP segment of a reassembled 13006 6.724163 13.107.42.12 10 10.0.0.15 TCP 54 128 53376 5443 [ACK] Seq-15276042 Ack-253 Win-16300 Len-1460 [TCP segment of a reassembled 13006 6.724163 13.107.42.12 10 10.0.0.15 TCP 54 128 53376 5443 [ACK] Seq-15276042 Ack-253 Win-16300 Len-1460 [TCP segment of a reassembled 13006 6.724163 13.107.42.12 10 10.0.0.15 TCP 1514 120 443 443 + 55376 f442 [ACK] Seq-15276042 Ack-253 Win-16300 Len-1460 [TCP segment of a reassembled 13006 6.72450 13.107.42.12 10.0.0.15 TCP 1514 120 443 443 + 55376 f442 [ACK] Seq-15276042 Ack-253 Win-16300 Len-1460 [TCP segment of a reassembled 13006 6.72450 13.107.42.12 10.000 [ACK] TCP 1514 120 443 443 + 55376 [ACK] Seq-153760763 Ack-253 Win-16300 Len-1460 [TCP segment of a reassembled 13006 6.72450 [ACK] Seq-15376 [ACK] Seq-153776 [ACK] Seq-15376 [ACK] Seq-153776 [ACK] Seq-15376 [A	13904 6.722558	13.107.42.12	10.0.0.15	TCP	1514	120 443	443 + 55376 [ACK] Seq=15275382 Ack=253 Win=16380 Len=1460 [TCP segment of a reassembled
<pre>13907 6.724163 13.107.42.12 10.0.0.15 TCP 1514 120 443 443 + 55376 [PSH, ACK] Seq=15278392 Ack=253 Min=16380 Len=1460 [TCP segment of a reasce 13908 6.724236 10.0.0.15 13.107.42.12 TCP 54 120 5337 55376 + 443 [ACK] Seq=253 Ack=15279762 Ack=253 Min=16380 Len=1460 [TCP segment of a reasce manual and 6.724236 11.077.02 12 10 0.0.15 TCP 1514 120 443 443 + 55376 [PSH, ACK] Seq=253 Ack=15279762 Ack=253 Min=16380 Len=1460 [TCP segment of a reasce manual and 6.724236 11.077.02 12 10 0.0.15 TCP 1514 120 443 443 + 55376 [PSH, ACK] Seq=253 Ack=15279762 Ack=253 Min=16380 Len=1460 [TCP segment of a reasce thermet 11, Src: ARRISGro_mf:3d:36 (10:56:11:afi:3d:36), Dst: IntelCor_f2:10:a7 (78:0c:b8:f2:10:a7) Internet Protocol Version 4, Src: 13.107.42.12, Dst: 10.0.0.15 Internet Protocol, Src Port: 443, Dst Port: 55376, Seg: 1, Ack: 1, Len: 1460 Fransport Layer Security</pre>	13905 6.722605	10.0.0.15	13.107.42.12	TCP	54	128 55376	55376 + 443 [ACK] Seq=253 Ack=15276842 Win=16695 Len=0
13980 6.724236 13 107 42 12 13 107 42 13 107 42 14 10 10 14	13906 6.724163	13.107.42.12	10.0.0.15	TCP	1514	120 443	443 + 55376 [ACK] Seq=15276842 Ack=253 Win=16380 Len=1460 [TCP segment of a reassembled
13000 6 77436       13 107 42 12       10 0 0 15       TFP       1514       120 443       443 + 55376 [4FV] Sonut5279762 drbs253 Winz163R0 [env1460 [TFP comment of a reaccembler of a reaccemble	13907 6.724163	13.107.42.12	10.0.0.15	TCP	1514	120 443	443 + 55376 [PSH, ACK] Seq=15278302 Ack=253 Win=16380 Len=1460 [TCP segment of a reasse
<pre>&gt;</pre>	13908 6.724236	10.0.0.15	13.107.42.12	TCP	54	128 55376	55376 → 443 [ACK] Seg=253 Ack=15279762 Win=16695 Len=0
<pre>thernet II, Src: ARRISGro_af:3d:36 (10:56:111:af:3d:36), Dst: IntelCor_f2:10:a7 (78:0c:b8:f2:10:a7) Internet Protocol Version 4, Src: 13.107.42.12, Dst: 10.0.0.15 Transmission Control Protocol, Src Port: 443, Dst Port: 55376, Seq: 1, Ack: 1, Len: 1460 Transport Layer Security 0 78 0c b8 f2 10 a7 10 56 11 af 3d 36 08 00 45 00 x ····· V ···=6··E· 0 65 dc 8b 55 40 00 78 06 30 40 0d 5b 20 0c 0a 00 ···· V0 ···=6··E· 0 65 dc 8b 55 40 00 78 06 30 40 0d 5b 20 0c 0a 00 ···· V0 ···=6··E· 0 65 dc 8b 55 40 00 77 06 30 40 0d 5b 20 0c 0a 00 ···· V0 ···=6··E· 0 80 0f 61 bb df 50 b9 34 89 29 92 66 c0 55 50 18 ····· P···)·f·VP· 0 80 0f 61 bb df 50 b9 34 89 29 92 66 c0 55 50 18 ····· P···)·f·VP· 0 7b 4d e4 0e cc e0 cc f0 73 0f 74 23 3c 7a c2 d9 (M····s t tsc:··· 0 92 b5 c3 ee 13 89 71 ea 7a ff 11 6c e1 91 70 53 ·····q· z··1··p5 0 93 a0 16 c5 eb f6 57 75 2d b8 40 db 89 88 d9 8a ····· Mu ·-@··· 0 25 20 21 fc 43 55 8b 96 99 69 c5 77 44 41 a 85 4f 77 ····· NMi 0 9c 58 80 59 5b db 91 36 90 80 db 64 44 1a 95 4f 77 ····· NMi 0 9c 58 80 59 5b db 91 36 90 80 db 64 44 1a 95 4f 77 ····· NMi 0 9c 58 80 59 5b db 91 36 90 80 db 64 44 1a 85 4f 77 ····· NMi 0 9c 58 80 59 5b db 91 36 90 80 db 64 44 1a 85 4f 77 ····· NMi 0 9c 58 80 59 5b db 91 36 90 80 db 64 44 1a 85 4f 77 ······ NMi 0 9c 58 80 59 5b db 91 36 90 80 db 64 44 1a 85 4f 77 ······ NMi 0 9c 58 80 59 5b db 91 36 90 80 db 64 44 1a 85 4f 77 ······ NMi 0 9c 58 80 59 5b db 91 36 90 80 db 64 44 1a 85 4f 77 ······· NMi 0 9c 58 77 70 11 35 5b ed ea e7 3a a3 3f 8c d6 26 b4 ···································</pre>	13989 6 774368	13 107 42 12	10 0 0 15	TCP	1514	120 443	443 + 55376 [ACK] Sen=15070760 Ark=053 Win=16380 Len=1460 [TCP segment of a reassembler
0       0	Transport Layer 5	ecurity					
0       0	Transport Layer 3	ecurity					
0       7b 4d e4 be cc e0 cc f0       73 6f 74 23 3c 7a c2 d9       (M+s-tec)         69       64 99 9c cc 5f 87 78 27       c2 63 12 24 fe 04 c4 19       idx <sup>2</sup> - c 5         93       80 16 c5 eb f6 57 75       2b 84 04 b0 89 88 ad 98	18 78 0c b8 f2 1	0 a7 10 56 11 af 3d 3			-		
0       69       64       99       92       c5       f8       78       72       c2       63       12       24       fe       04       c4       19       id      x*       c5	08 78 0c b8 f2 1 08 05 dc 8b 56 4	0 a7 10 56 11 af 3d 3 0 00 78 05 30 40 0d 6	b 2a 0c 0a 00 ····\	@·x· 0@·k*			
9 2 b 5 c 3 ee 13 89 71 ea 7a ff 11 6c e1 91 70 53	00 78 0c b8 f2 1 10 05 dc 8b 56 4 20 00 0f 01 bb d	0 a7 10 56 11 af 3d 3 0 00 78 05 30 40 0d 6 8 50 b9 a4 89 29 92 6	b 2a 0c 0a 00 ····\ 6 c0 56 50 18 ····	(@·x·0@·k* ·P···)·f·	VP ·		
9       38       16       15       16       57       52       38       40       16       51       77         2       52       52       92       91       fc       43       85       86       96       95       74       48       49       57       75       24       84       96       91       fc       43       87       72       74       66       16       17       96       84       96       16       76       78       ~       ~       Mile       0         9       cs       85       55       bd       18       86       64       44       18       64       79       ×       ~       <	<ul> <li>78 @c b8 f2 1</li> <li>95 dc 8b 56 4</li> <li>90 @f 01 bb d</li> <li>3f fd 25 ba 0</li> <li>7b 4d e4 0e c</li> </ul>	0 a7 10 56 11 af 3d 3 0 00 78 06 30 40 dd 6 8 50 b9 a4 89 29 92 6 0 00 1c 66 7c 05 1e b c 60 cc f0 73 0f 74 2	b 2a 0c 0a 00 ···· 6 c0 56 50 18 e ac c9 9b b0 ? % 3 3c 7a c2 d9 {M··	@ x 0@ k* ·P···) f· ···n  ···· s·t#<	VP		
25       92       91       fc       43       85       8e       b9       69       57       72       74       64       b9       17       58 <t< td=""><td>78 0c b8 f2 1 10 05 dc 8b 56 4 20 00 0f 61 bb d 3f fd 25 ba 0 75 40 ec 69 76 44 0e c 50 69 64 99 9c c</td><td>0 a7 10 56 11 af 3d 3 0 00 78 06 30 40 0d 6 8 50 b9 a4 89 29 92 6 0 00 1c 6e 7c 05 1e b c e0 cc f0 73 0f 74 2 5 f8 78 27 c2 63 12 2</td><td>b 2a 0c 0a 00 6 c0 56 50 18 e ac c9 9b b0 ?% 3 3c 7a c2 d9 {M 4 fe 04 c4 19 id</td><td>@-x-0@-k* -P)-f- </td><td>VP-</td><td></td><td></td></t<>	78 0c b8 f2 1 10 05 dc 8b 56 4 20 00 0f 61 bb d 3f fd 25 ba 0 75 40 ec 69 76 44 0e c 50 69 64 99 9c c	0 a7 10 56 11 af 3d 3 0 00 78 06 30 40 0d 6 8 50 b9 a4 89 29 92 6 0 00 1c 6e 7c 05 1e b c e0 cc f0 73 0f 74 2 5 f8 78 27 c2 63 12 2	b 2a 0c 0a 00 6 c0 56 50 18 e ac c9 9b b0 ?% 3 3c 7a c2 d9 {M 4 fe 04 c4 19 id	@-x-0@-k* -P)-f- 	VP-		
0       49       59       79       72       7c       46       b9       10       90       75         0       9c       58       65       56       b9       13       69       80       d6       44       14       64       54       75       75       10       10       00	88         78         9c         b8         f2         1           10         95         dc         b8         56         4           20         90         9f         a1         b4         a2           30         3f         fd         25         ba         a4           40         7b         4d         e4         9c         c         c         56         69         64         99         c         c         55         c3         e4         2b         c5         c3         e4         bc         c         c         55         c3         e4         bc         c         c         55         c3         e4         bc         c         c         c3         c5         c3         e4         bc         c         c         c5         c5         c4         c3         c5         c3         e4         c4         bc         c         c         c5         c5         c4         c4         bc         c         c5         c5         c5         c4         c5         c5         c5         c5         c5         c5         c4         c5         c5         c5         c4         c5 </td <td>0 a7 10 56 11 af 3d 3 0 00 78 05 30 40 0d 6 8 50 b9 34 89 29 92 6 0 00 1c 60 7c 05 1e b c e0 cc f0 73 0f 74 2 5 f8 78 27 c2 63 12 2 3 89 71 ea 7a ff 11 6</td> <td>b 2a 0c 0a 00 6 c0 56 50 18 e ac c9 9b b0 ?% 3 3c 7a c2 d9 {M 4 fe 04 c4 19 id c e1 91 70 53</td> <td>@ x 0@ k* P···) f ···n   ···· s t#&lt; ·x' c \$ ···q z · 1</td> <td>vP z · pS</td> <td></td> <td></td>	0 a7 10 56 11 af 3d 3 0 00 78 05 30 40 0d 6 8 50 b9 34 89 29 92 6 0 00 1c 60 7c 05 1e b c e0 cc f0 73 0f 74 2 5 f8 78 27 c2 63 12 2 3 89 71 ea 7a ff 11 6	b 2a 0c 0a 00 6 c0 56 50 18 e ac c9 9b b0 ?% 3 3c 7a c2 d9 {M 4 fe 04 c4 19 id c e1 91 70 53	@ x 0@ k* P···) f ···n   ···· s t#< ·x' c \$ ···q z · 1	vP z · pS		
9 c 58 05 95 bd 9b 13 69       80 db 64 44 1a 05 4f 79       X ····i · · dD··Oy         0 5b 1e eb af 9e b9 1e 82 c6 84 3f be c6 f7 88 b2       [····································	88         78         9c         b8         f2         1           10         95         dc         b8         56         4           20         90         9f         91         bb         d           31         fd         25         ba         94         40         c           36         7b         4d         e4         ec         c         56         69         64         99         c         c           92         2b         53         e1         c5         e1         76         93         a8         16         c5         e5	0 a7 10 56 11 af 3d 3 0 00 78 06 30 40 0d 6 8 50 b9 a4 89 29 92 6 0 00 1c 6e 7c 05 1e b c e0 cc f0 73 0f 74 2 5 f8 78 27 c2 63 12 2 3 89 71 ea 7a ff 11 6 b f6 57 75 2d b8 44 0	b 2a 0c 0a 00 6 c0 56 50 18 e ac c9 9b b0 3 3c 7a c2 d9 4 fe 04 c4 19 id c e1 91 70 53 b 0a 98 ad 9a	@ x 0@ k* P· ) f · n   · · · · · · · · · · · · · · · · ·	vP z pS		
0       Sb 1e eb af 9e b9 1e 82       c6 84 3f be c6 f7 80 b2       [?]         0       7b ad 5e a2 5e bb e5 e5       19 14 4b d3 1f 05 a6 7f       [?]         0       16 77 69 a3 0c 06 60 66 dc cc de 7f 53 77 98 d7       [?]         0       95 75 76 b1 19 5b eb ea e7 3a a3 3f 8c d6 26 b4       up-[?]         0       9a d2 61 6d 9f dd b5 8a f8 ff 5f 33 77 98 a	<ul> <li>78 @c b8 f2 1</li> <li>65 dc 8b 56 4</li> <li>20 @f f0 1 bb d</li> <li>36 3f fd 25 ba @</li> <li>76 d4 90 c</li> <li>69 64 99 9c c</li> <li>60 92 b5 c3 ec 1</li> <li>76 93 @0 16 c5 2</li> <li>25 02 91 fc 4</li> </ul>	0 a7 10 56 11 af 3d 3 0 00 78 06 30 40 0d 6 5 50 b9 a4 89 29 26 0 00 1c 60 7c 65 1e 0 0 00 1c 66 7c 65 1e 0 c e0 cc f0 73 0f 74 2 5 f6 78 27 c2 63 12 2 3 89 71 ea 7a ff 11 6 b f6 57 75 2d b8 40 d 3 85 8e b9 69 c9 57 4	b 2a 0c 0a 00	@ x 0@ k* P ) f n   s t#< x' c \$ q z 1 Wu - @ C i WE@	vP z pS Q		
0       7b ad 5e a2 5e bb e5 e5       19       14 4b d3       1f 05 a6 7f       {	68         78         8c         b8         f2         1           10         05         dc         b8         56         4           20         00         0f         f1         b1         b4           30         3f         fd         25         ba           440         7b         4d         e4         ec           50         69         64         99         cc         c           60         92         b5         c3         e1         177           93         a0         16         c5         e         189         25         92         17         72         7           96         c4         95         79         72         7         7         7	0 a7 10 56 11 af 3d 3 0 00 78 06 30 40 0d 6 5 9 09 34 89 29 26 0 00 1c 66 7C 65 1e b c e0 cc f0 73 0f 74 2 5 f8 78 27 c2 63 12 2 3 89 71 ea 7a ff 11 6 b f6 57 75 2d b8 40 d 3 85 8e b9 69 c9 57 4 c 45 b0 1e 17 b8 8d 9	b 2a 0c 0a 00	@ x 0@ k* P ) f 1 s t#< x c \$ q z 1 Wu - @ C i WE@ F 0	vP z Q KM		
© 95 75 76 bl 19 59 eb ea e7 3a a3 3f 8c d6 26 b4 - upp-[- <sup>*</sup> +:-}-&- 9 sa d2 61 6d 9f dd b5 8a f8 ff 5f 33 7f 45 79 98am	00         78         0c         b8         f2         1           10         05         dc         b8         56         4           20         00         of         f1         b5         d3         f4         f2         ba         0           40         05         dc         f4         f5         ba         0         44         0e         c           50         69         64         99         c         f6         99         c         f6         16         5         6         64         99         c         f6         16         16         c         16         17         93         00         fc         5         6         64         99         c         58         16         16         5         16         16         5         16<	0 a7 10 56 11 af 3d 3 0 00 78 05 30 40 0d 6 5 0 b9 a4 89 29 92 6 0 00 1c 66 7c 05 1e b c e0 cc f0 73 0f 74 2 5 f8 78 27 c2 6 3 12 2 3 89 71 ea 7a ff 11 6 b f5 77 52 db 8 40 d 3 85 8e b9 69 c9 57 4 c 46 b0 1e 17 b9 8d 9	b 2a 0c 0a 00	<pre>@ x 0@ k* P ) f 1 s t#c x' c \$ q z 1 Wu - @ C i WE@ F dD</pre>	vp - z p5 - Q - KM - Oy		
0 9a d2 61 6d 9f dd b5 8a f8 ff 5f 33 7f 45 79 98 am	00         78         0c         b8         f2         1           10         05         dc         b8         56         4           20         00         0f         f1         b1         b5           30         3f         fd         25         b3         b7         b1         b5           40         70         b4         44         0e         c         99         c         69         92         b5         c3         e4         16         c5         93         a0         16         c5         25         92         1f         c4         92         c         25         92         1f         c4         92         c         25         92         1f         c4         92         c         93         a0         16         c5         92         1f         c4         92         c         25         92         1f         c4         92         c5         95         50         50         50         50         50         55         16         55         16         55         16         55         16         55         16         55         16         55         16	0 a7 10 56 11 af 3d 3 0 00 78 06 30 40 0d 6 8 50 b9 a4 89 29 26 0 0 00 1c 60 7c 05 1e 0 c e0 cc f0 73 0f 74 2 5 f8 78 27 c2 63 12 2 3 89 71 ea 7a ff 11 6 b f6 57 75 2d b8 40 d 3 85 8e b9 69 95 77 4 c 46 b0 1e 17 b9 3d 9 d 9b 13 69 80 db 64 4 e b9 1e 82 c6 64 3 fb	b 2a 0c 0a 00	() x 0() k P ) f s t#c x' c \$ q z 1 Wu - () C i WE() F i dD ?	vP z pS Q KM Oy		
9 4e dd 74 59 b8 8e 6e c7 b2 97 73 94 37 53 67 12 N+tY+n++s-75g	88         78         9c         b8         f2         1           10         95         dc         b8         56         4           20         90         9f         10         b6         64         92         b5         b8         44         40         c         56         64         93         36         fd         25         b8         44         44         40         c         56         69         95         56         4         93         a0         16         c5         e         93         a0         16         c5         e         92         b5         c3         e1         c7         93         a0         16         c5         e         92         b5         c3         e1         c4         95         77         7         a0         e         c4         95         p5         b6         b6         b6         s5         b1         e         b1         e         a1         95         b5         b6         b5         b6         b5         b6         b7         b3         b6         55         b6         b6         b7         b3         b6         55         b6         <	0         a7         10         56         11         af         3d           0         00         78         05         30         40         6d         5           0         00         12         6d         7         70         5         12           0         00         12         6d         73         97         42         12         12         12         12         12         7         7         7         12         12         13         38         7         16         7         7         17         16         16         16         57         75         2d         18         40         43         38         86         19         9         7         4         14         16         17         18         40         43         38         86         16         17         19         34         40         43         15         16         17         13         16         86         16         16         17         17         13         16         16         16         17         13         13         13         13         13         16         16         17         13	b 2a 0c 0a 00	() x 00 k P ) f s t#<: x' c \$ q z 1 Wu - 0 C i WE0 F i dD X	vP - z - 0y		
	78         0c         b5         f2         1           110         05         dc         8b         56         4           20         00         07         10         b5         64           20         30         3f         fd         25         ba           303         3f         fd         25         ba         9           50         69         44         26         bc         5         69         64         99         92         c         360         92         b5         c3         e1         11         37         93         30         16         c5         e2         92         c4         95         79         72         77         79         32         95         50         15         16         57         94         56         95         50         15         16         77         64         56         95         50         15         16         77         72         72         72         72         72         72         72         72         72         72         72         72         72         72         72         72         72         72	0 a7 10 56 11 af 3d 3 0 00 78 06 30 40 0d 6 5 50 b9 a4 89 29 26 0 00 12 60 77 05 1e 0 0 00 1c 6c 77 05 1e 0 c e0 cc f0 73 0f 74 2 5 f6 78 27 c2 6 31 22 3 89 71 ea 7a ff 11 6 b f6 57 75 2d b8 40 d 3 85 8e b9 69 c9 57 4 c 46 b0 1e 17 b9 8d 9 d 91 33 69 8d b6 44 4b d c 99 1e 82 c6 84 3f b e bb c5 5 19 14 4b d c 96 60 6a 6d cc de 7	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	@ x 0@ k P ) f s t#c x' c \$ q z 1 Wu - @ C i WE@ [F i dD ? ^ K 	νР z - φS - Q - КМ - Оу		
7d 24 16 c1 58 43 60 d8 1d 46 96 b2 40 2a 39 68 }\$ XC F @*9h	100         78         0c         b8         f2         1           110         05         dc         b8         56         4           120         00         0f         11         b5         40           120         00         0f         11         b5         40           120         00         0f         11         b5         40           120         00         0f         15         ba         0           150         69         64         99         cc         16         16         c5           150         69         64         99         cc         16         16         c5         16         16         c5         16         16         c5         16 <td>0 a7 10 56 11 af 3d 3 0 00 78 06 30 40 6d 6 5 00 b9 a4 89 29 92 6 0 00 1c 6e 7c 05 1e 0 0 00 1c 6e 7c 05 1e 0 c e0 cc f0 73 0f 74 2 5 f8 78 27 c2 63 12 2 3 89 71 ea 7a ff 11 6 5 f5 75 2d b8 4d d 3 85 8e b9 69 c9 57 4 c 46 b0 1e 17 b8 8d 9 d 9b 13 69 8d b6 64 3f b e b0 e5 c6 19 14 4b 0 c 06 00 6a 6d cc de 7 9 5b eb ea e7 3a a3 3 f dd b5 8a f8 ff 5f 3</td> <td><math display="block">\begin{array}{cccccccccccccccccccccccccccccccccccc</math></td> <td>@ x 0@ k* P ) f ' n   s t#&lt;: x' c\$ q z 1 WU - @ C C i WE@  F i dD  j m Si       </td> <td>vp pS Q KM Oy N 8 Ey</td> <td></td> <td></td>	0 a7 10 56 11 af 3d 3 0 00 78 06 30 40 6d 6 5 00 b9 a4 89 29 92 6 0 00 1c 6e 7c 05 1e 0 0 00 1c 6e 7c 05 1e 0 c e0 cc f0 73 0f 74 2 5 f8 78 27 c2 63 12 2 3 89 71 ea 7a ff 11 6 5 f5 75 2d b8 4d d 3 85 8e b9 69 c9 57 4 c 46 b0 1e 17 b8 8d 9 d 9b 13 69 8d b6 64 3f b e b0 e5 c6 19 14 4b 0 c 06 00 6a 6d cc de 7 9 5b eb ea e7 3a a3 3 f dd b5 8a f8 ff 5f 3	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	@ x 0@ k* P ) f ' n   s t#<: x' c\$ q z 1 WU - @ C C i WE@  F i dD  j m Si       	vp pS Q KM Oy N 8 Ey		
	88         78         9c         b8         f2         1           18         65         66         67         15         56         4           20         60         67         61         56         4         8         6         67         54         56         4         36         6         36         9         9         36         6         55         5         6         6         9         9         5         6         6         9         9         9         6         6         9         9         5         6         6         9         9         5         6         6         9         9         5         6         6         9         9         5         6         6         6         9         9         5         6         16         7         9         3         16         5         9         16         7         16         9         16         7         16         9         16         7         16         16         16         16         9         16         17         16         16         16         16         16         16         16         16 </td <td>0 a7 10 56 11 af 3d 3 0 00 78 06 30 40 6d 6 5 00 b9 a4 89 29 92 6 0 00 1c 6e 7c 05 1e 0 0 00 1c 6e 7c 05 1e 0 c e0 cc f0 73 0f 74 2 5 f8 78 27 c2 63 12 2 3 89 71 ea 7a ff 11 6 5 f5 75 2d b8 4d d 3 85 8e b9 69 c9 57 4 c 46 b0 1e 17 b8 8d 9 d 9b 13 69 8d b6 64 3f b e b0 e5 c6 19 14 4b 0 c 06 00 6a 6d cc de 7 9 5b eb ea e7 3a a3 3 f dd b5 8a f8 ff 5f 3</td> <td><math display="block">\begin{array}{cccccccccccccccccccccccccccccccccccc</math></td> <td>@ x 0@ k* P ) f ' n   s t#&lt;: x' c\$ q z 1 WU - @ C C i WE@  F i dD  j m Si       </td> <td>vp pS Q KM Oy N 8 Ey</td> <td></td> <td></td>	0 a7 10 56 11 af 3d 3 0 00 78 06 30 40 6d 6 5 00 b9 a4 89 29 92 6 0 00 1c 6e 7c 05 1e 0 0 00 1c 6e 7c 05 1e 0 c e0 cc f0 73 0f 74 2 5 f8 78 27 c2 63 12 2 3 89 71 ea 7a ff 11 6 5 f5 75 2d b8 4d d 3 85 8e b9 69 c9 57 4 c 46 b0 1e 17 b8 8d 9 d 9b 13 69 8d b6 64 3f b e b0 e5 c6 19 14 4b 0 c 06 00 6a 6d cc de 7 9 5b eb ea e7 3a a3 3 f dd b5 8a f8 ff 5f 3	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	@ x 0@ k* P ) f ' n   s t#<: x' c\$ q z 1 WU - @ C C i WE@  F i dD  j m Si       	vp pS Q KM Oy N 8 Ey		



	Capture Analyze Statist	and the second	is Tools H	elp				
			0.77	- 6				
and an and a second and	<b>X</b> 🖸 <b>Y</b> 🗢 🖷 🗄	કે 🔽 📰 જે જે	. Q. II				_	_
Apply a display filter <ct< th=""><th>rl-/&gt;</th><th></th><th></th><th></th><th></th><th></th><th></th><th>-</th></ct<>	rl-/>							-
Time	Source	Destination	Protocol	Length Time to	o Live Source Port	Info		
274 33.251030	10.0.0.15	18.211.145.151	TCP	55	128 56728	56728 + 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]		E
275 33.281725	10.0.0.15	44.242.50.20	TCP	55	128 56729	56729 → 443 [ACK] Seq=1 Ack=1 Win=509 Len=1 [TCP segment of a reassembled PDU]		
276 33.320676	52.70.76.76	10.0.0.15	TCP	66	232 443	443 → 56726 [ACK] Seq=1 Ack=2 Win=127 Len=0 SLE=1 SRE=2		
277 33.322835	44.242.50.20	10.0.0.15	TCP	66	229 443	443 + 56729 [ACK] Seq=1 Ack=2 Win=184 Len=0 SLE=1 SRE=2		
278 33.324263	18.211.145.151	10.0.0.15	TCP	66	232 443	443 → 56728 [ACK] Seq=1 Ack=2 Win=115 Len=0 SLE=1 SRE=2		
279 33.396050	SamsungE_b3:4d:d3	Broadcast	ARP	60		Who has 10.0.0.1? Tell 10.0.0.129		
280 33.772752	10.0.0.15	52.203.77.241	TCP	55	128 56731	56731 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]		-
281 33.839913	52.203.77.241	10.0.0.15	TCP	66	232 443	443 → 56731 [ACK] Seq=1 Ack=2 Win=115 Len=0 SLE=1 SRE=2		
282 34 6744R4	10 0 0 133	224 A A 251	MONS	154	255	Standard query AvAAAA PTR companion-link ten local "OU" question PTR homekit	trn 1	-
	ol Protocol, Sec Port		=6x					
	00 80 06 35 42 0a 0		@··· 58····					
	bb c3 ff b0 5d 00 f		····· ·]··×	P-				
02 01 32 50 00 0	00 00	• • 2P	<u>.</u>					

Figure 34: Analyzing the Traffic.

#### 2.11.1 Motivation

The motivation of this module is to help guide users about the importance of understanding real-world scenarios and protecting information from third parties. Providing users with information on how they can be monitored and tracked.

2.11.2 Learning Objectives

Users will be able to perform the following tasks:

- a. Gain knowledge of Traffic Monitoring
- b. Learn about implementing security practices.

# 3. CONCLUSIONS

To conclude, this Nimble course uses short video vignettes to provide users with both knowledge and hands-on experience with various platforms. The idea of using videos to share information with end users provides additional resources for them to gain an in-depth understanding of Nimble, making it an effective way to enrich the user's learning experience. This method can help supplement key concepts of Nimble, provide real-life examples, and demonstrate problem-solving techniques. Users can learn about Nimble and gain technical expertise at their own pace, with the course providing a common platform for learning about different concepts used in Nimble. This interactive learning experience provides users with more efficient processing and memory recall.

The key observations from producing this course on Nimble are that it provides clarification for difficult concepts, including relevant content for the learning goals of each module, highlighting key information from specific topics, and communicating the learning objectives and motivation for each topic. This form of communication helps to build a stronger and more skilled community to operate Nimble successfully.

# 4. **REFERENCES**

- 1. Taneja, A., "Intranet and its application 'Community Networks' to overcome Digital Divide"2022. [Online]. Available: https://doi.org/10.7939/r3-rby4-a929.
- 2. Virtual LANs (VLANs) Netgate, "pfSense Documentation," 19 Jan 2021. [Online] Available: https://docs.netgate.com/pfsense/en/latest/vlan/index.html.
- 3. Why Videos are important in Education. 2023. [Online] Available: https://www.nextthoughtstudios.com/video-production-blog/2017/1/31/why-videos-are-i mportant-in-education.
- 4. "IEEE CTU Summit 2021- Wakoma Nimble," Wakoma (2021, January 21). [Online] Available: https://www.youtube.com/watch?v=wjBn3O5Ksgg.
- 5. "Wireless Mesh Network", Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/Wireless\_mesh\_network
- 6. "Nimble," Wakoma. [Online] Available: https://wakoma.co/nimble/.