

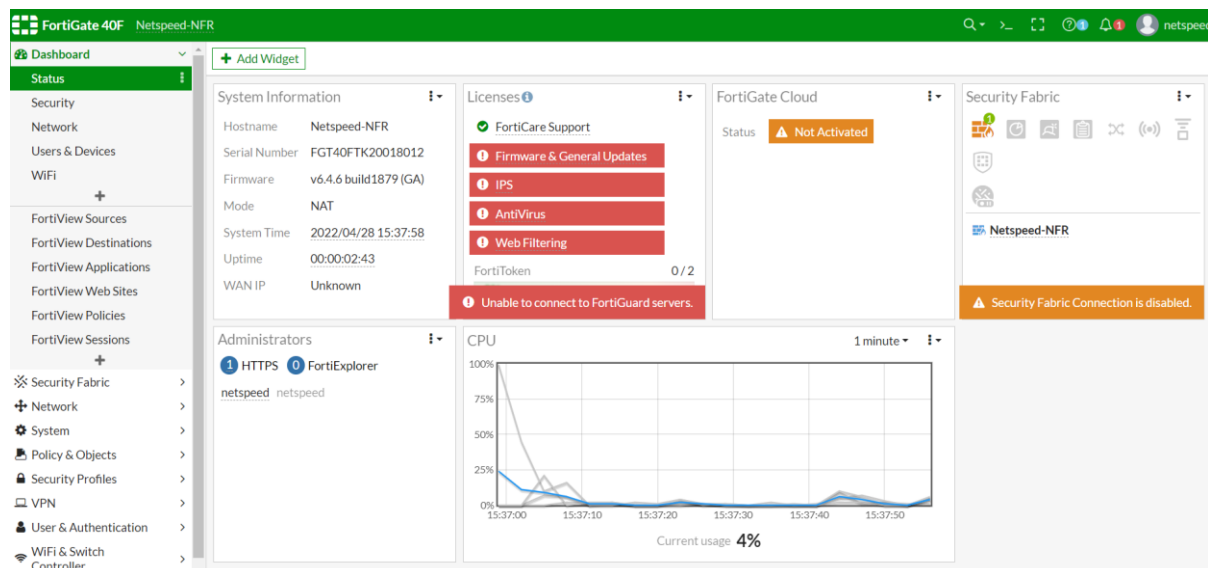
Configuración de VLANs GUI

1. Configuración de router FortiGate



Conectamos nuestro portatil al Puerto 1 con un cable de red. Si el DHCP esta activado nos dara la IP 192.168.1.1/24 y podremos acceder al router por la IP 192.168.1.99/24

Una vez queramos acceder al router, las credenciales default son usuario admin y contraseña password.



Lo primero al entrar en el router es cambiar el hostname, creacion primero de un perfil de usuario con los permisos que queramos darles en este caso es con permisos para la administracion del router y luego crearemos un usuario que le asignaremos ese perfil (perfil netspeed y usuario netspeed) cuando lo creamos el default admin desaparece y ya solo podremos acceder con netspeed a no se que creamos otro usuario.

System Settings

Host name

Netspeed-NFR

System Time

Current system time

2022/04/25 11:17:53

Time zone

(GMT) Dublin, Edinburgh, Lisbon, London, Canary Is.

Set Time

NTP

PTP

Manual settings

Select server

FortiGuard

Custom

Sync interval

60

Minutes (1 - 1440)

Setup device as local NTP server

Listen on Interfaces

fortilink

Administration Settings

HTTP port

80

Redirect to HTTPS

HTTPS port

443

Port conflicts with the SSL-VPN port setting

SSH port

22

Telnet port

23

Edit Admin Profile

Name

netspeed

Comments

0/255



Access Permissions

Access Control	Permissions	Set All
Security Fabric	<div><div>None</div><div>Read</div><div>Read/Write</div></div>	
FortiView	<div><div>None</div><div>Read</div><div>Read/Write</div></div>	
User & Device	<div><div>None</div><div>Read</div><div>Read/Write</div></div>	
Firewall	<div><div>None</div><div>Read</div><div>Read/Write</div><div>Custom</div></div>	
Log & Report	<div><div>None</div><div>Read</div><div>Read/Write</div><div>Custom</div></div>	
Network	<div><div>None</div><div>Read</div><div>Read/Write</div><div>Custom</div></div>	
System	<div><div>None</div><div>Read</div><div>Read/Write</div><div>Custom</div></div>	
Security Profile	<div><div>None</div><div>Read</div><div>Read/Write</div><div>Custom</div></div>	
VPN	<div><div>None</div><div>Read</div><div>Read/Write</div></div>	
WiFi Switch	<div><div>None</div><div>Read</div><div>Read/Write</div></div>	

OK

Cancel

Edit Administrator

Username  netspeed  [Change Password](#)

Type **Local User**

- Match a user on a remote server group
- Match all users in a remote server group
- Use public key infrastructure (PKI) group

Comments Write a comment... 0/255

Administrator Profile netspeed

☐ Two-factor Authentication

☐ Restrict login to trusted hosts

Luego vamos a LAN y configuramos la LAN con otra Direccion IP ponemos la 192.168.1.1/24. Damos el rango de DHCP para 192.168.1.100 – 192.168.1.250 mascara 255.255.255.0

Ahora crearemos las diferentes interfaces virtuales para las diferentes VLANs para ello nos vamos al apartado de New Interface.

New Interface

Name Guest

Alias Guest

Type **VLAN**

Interface **lan**

VLAN ID 100


Role **LAN**

Address

Addressing mode **Manual** DHCP Auto-managed by FortiIPAM PPPoE

IP/Netmask 192.168.100.1/24

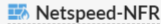
Create address object matching subnet ☒


Name  Guest address



Destination 192.168.100.1/24



Secondary IP address ☐

FortiGate

 **Netspeed-NFR**

 [Documentation](#)


 [Online Help](#) 

 [Video Tutorials](#) 

Seleccionamos el tipo como VLAN la interface donde estará será en LAN y el ID de la VLAN con la que podremos identificarla mas tarde. La IP de la puerta de enlace de la VLAN será 192.168.100.1/24 y el DHCP será del 100.100 al 100.250

☒ **DHCP Server**


Address range 192.168.100.100-192.168.100.250




Netmask 255.255.255.0

Default gateway **Same as Interface IP** [Specify](#)

DNS server **Same as System DNS** [Same as Interface IP](#) [Specify](#)

Lease time  ☒ 604800 second(s)

 **Advanced**

Esto lo hacemos con las demás VLANs hemos puesto de ejemplo la de Guest, con la de Voice donde irán los Teléfonos IP será la VLAN 200 con IP 192.168.200.1/24 rango de direcciones 200.100-200.250, la VLAN 999 Management donde iran los APs y otros dispositivos de la red tendrá IP 192.168.99.1/24 con el mismo rango de direcciones.

Ahora vamos a añadir las políticas de filtrado de paquetes. El filtrado será de esta manera:

- LAN to WAN: Office 365 services, HTTP and HTTPS
- Guest to WAN: any to any
- Management to WAN: any to any
- Management to LAN: any to any
- Management to Guest: any to any


Configuración de LAN to WAN:

Edit Policy


Name ⓘ

Office365-Lan-to-Wan


Incoming Interface

 lan


Outgoing Interface

 wan


Source

 lan


Destination


 Microsoft-Office365

Schedule

 always

Action

 ACCEPT

 DENY


Inspection Mode

Flow-based

Proxy-based

Firewall / Network Options

NAT




IP Pool Configuration

Use Outgoing Interface Address

Use Dynamic IP Pool

Preserve Source Port



Protocol Options

PROT

default

Edit Policy

Name	HTTP/s-Lan-to-Wan	
Incoming Interface	lan	
Outgoing Interface	wan	
Source	lan	
Destination	all	
Schedule	always	
Service	HTTP HTTPS	
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY	
Inspection Mode	<input checked="" type="checkbox"/> Flow-based <input type="checkbox"/> Proxy-based	

Firewall / Network Options

NAT ☒

IP Pool Configuration ☒ Use Outgoing Interface Address ☐ Use Dynamic IP Pool

Preserve Source Port ☐

Protocol Options

Configuración de Guest to WAN:

New Policy

Name	Guest	
Incoming Interface	Guest (Guest)	
Outgoing Interface	wan	
Source	all	
Destination	all	
Schedule	always	
Service		
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY	
Inspection Mode	<input checked="" type="checkbox"/> Flow-based <input type="checkbox"/> Proxy-based	

Firewall / Network Options

NAT ☒

IP Pool Configuration ☒ Use Outgoing Interface Address ☐ Use Dynamic IP Pool

Preserve Source Port ☐

Protocol Options

Security Profiles

AntiVirus ☐

Configuración de Management to WAN:

Lo mismo que lo anterior pero sustituimos en el incoming interface por Management

Configuración de Management to LAN y LAN to Management:

Edit Policy

Name	lan->mngmt
Incoming Interface	lan
Outgoing Interface	Management (Management)
Source	all
Destination	all
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	<input checked="" type="checkbox"/> Flow-based <input type="checkbox"/> Proxy-based

Firewall / Network Options

NAT ☒

IP Pool Configuration ☒ Use Outgoing Interface Address ☐ Use Dynamic IP Pool

Preserve Source Port ☐

Protocol Options

ID: 9

Last used: N/A

First used: N/A

Hit count: 0

Active sessions: 0

2 minutes ago → now

Total bytes: 0 B

Current bandwidth: 0 B/s

[Documentation](#)

[Online Help](#)

De mngmt seria lo mismo pero al revés.

Cambiamos el puerto para la administración del router por el 8889

Creación de permisos de VPN, creando un grupo. Lo anadimos que el puerto sea el 8443

SSL-VPN Settings

No SSL-VPN policies exist. Click here to create a new SSL-VPN policy using these settings

Connection Settings

Listen on Interface(s): lan, wan

Listen on Port: 8443

Web mode access will be listening at <https://192.168.1.1:8443> <https://10.6.1.118:8443>

Redirect HTTP to SSL-VPN ☐

Restrict Access: ☒ Allow access from any host ☐ Limit access to specific hosts

Idle Logout ☒

Inactive For: 300 Seconds

Server Certificate: Fortinet_Factory

You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). It is recommended to purchase a certificate for your domain and upload it for use.

Todos los filtros tendremos que ponerle una barrera de seguridad que lleva el firewall de FortiGate, ya que hace la función de IPS, IDS y AntiMalware.

Security Profiles

AntiVirus	<input checked="" type="checkbox"/>	AV default	
Web Filter	<input checked="" type="checkbox"/>	WEB default	
DNS Filter	<input checked="" type="checkbox"/>	DNS default	
Application Control	<input checked="" type="checkbox"/>	APP default	
IPS	<input checked="" type="checkbox"/>	IPS default	
SSL Inspection		SSL certificate-inspection	

Logging Options

Log Allowed Traffic ☒ Security Events All Sessions

Comments 0/1023

Enable this policy ☒

Creamos el grupo y anadimos al usuario netspeed al grupo de VPN de forma que así podremos usarlo.

Damos los permisos de full Access portal

Edit SSL-VPN Portal

Name

full-access

Limit Users to One SSL-VPN Connection at a Time

☐

☒ Tunnel Mode

Enable Split Tunneling

☒

Routing Address

+

Source IP Pools

SSLVPN_TUNNEL_ADDR1

x

+

Tunnel Mode Client Options

Allow client to save password

☒

Allow client to connect automatically

☐

Allow client to keep connections alive

☐

DNS Split Tunneling

☐

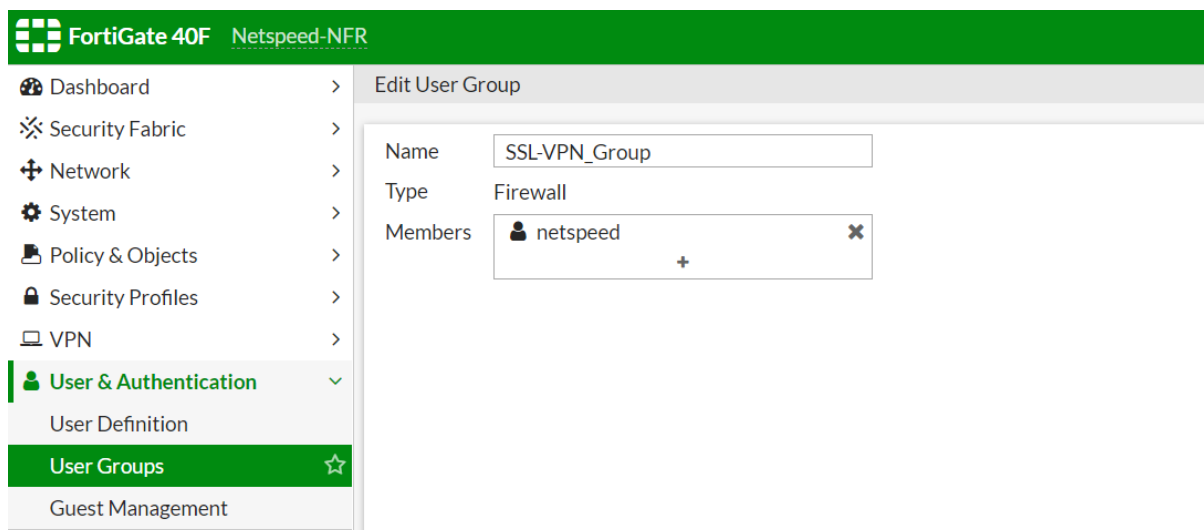
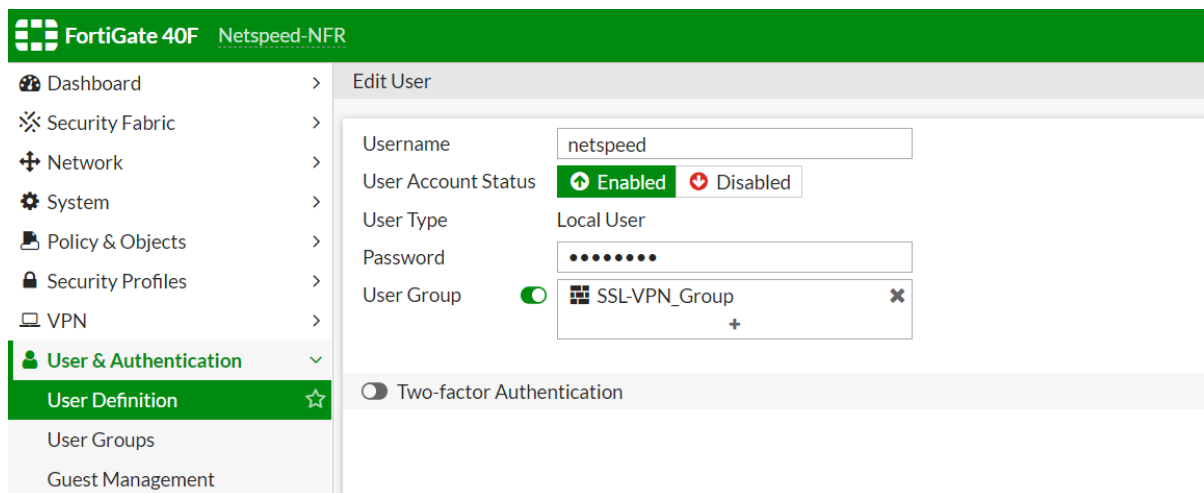
☐ Host Check

☐ Restrict to Specific OS Versions

☒ Enable Web Mode

Portal Message

SSL-VPN Portal



2. Configuración Switch

Conectamos un cable del puerto 2 al switch vemos que le da primero una IP de la lan, ya que antes tenemos que configurar el switch para que este en la VLAN 999.

Le dará una IP 192.168.1.X de forma que entraremos al switch desde esa IP. Las credenciales son admin y blank

Lo primero que vamos a hacer nada mas entrar en el switch es entrar en el apartado de VLAN para crear las VLANs.

Network > VLAN

Summary

Device

Network

VLAN

VLAN Interface

Voice VLAN

MAC

MSTP

Link Aggregation

LACP

LLDP

ARP Management

ARP Anti-Attack

IGMP Snooping

MLD Snooping

IPv4 Routing

IPv6 Routing

Select VLAN

Create

Port Detail

Detail

Modify VLAN

Modify Port

Remove

Create:

VLAN IDs: Example: 3, 5-10

Create

ID	Description
1	VLAN 0001

Modify VLAN description (Note: you can do this later on the Modify VLAN page)

Modify the description of the selected VLAN:

ID	Description
<input type="text"/>	<input type="text" value="VLAN 0001"/> (1-32 Chars.)

Apply

Vemos en la foto la VLAN 1 que seria la vlan que viene predeterminada como la administrativa.

Realizamos esto con las demás VLANs

Untaggeamos los puertos 1 y 8 para las vlans 1 y 999.

Network > VLAN

Summary

Device

Network

VLAN

VLAN Interface

Voice VLAN

MAC

MSTP

Link Aggregation

LACP

LLDP

ARP Management

ARP Anti-Attack

IGMP Snooping

MLD Snooping

IPv4 Routing

IPv6 Routing

DHCP

Service

Diagnostics Tools

Authentication

Select VLAN

Create

Port Detail

Detail

Modify VLAN

Modify Port

Remove

Please select a VLAN to modify:

999 - VLAN 0999

Modify Description (optional)

VLAN 0999 (1-32 Chars.)

Apply

Select membership type:

☒ Untagged ☐ Tagged ☐ Not A Member

Select ports to be modified and assigned to this VLAN:

☒ 1 ☒ 3 ☒ 5 ☒ 7 ☒ 8 ☐ 9 ☐ 10

Select All Select None

Note: You can assign multiple ports in different membership types to this VLAN.

Summary

Untagged Membership	Tagged Membership
GE1/0/1, GE1/0/8	

Apply Cancel

Para realizar configuraciones mas completas vamos a la modificación de puertos:

Select VLAN	Create	Port Detail	Detail	Modify VLAN	Modify Port	Remove
-------------	--------	-------------	--------	-------------	-------------	--------

Select Ports

1

3

5

7

2

4

6

8

9

10

HPE 1920-8G-PoE...

Select All

Select None

Not available for selection

Select membership type:

☒ Untagged
 ☐ Tagged
 ☐ Not A Member
 ☐ Link Type
 ☐ PVID

Enter VLAN IDs to which the port is to be assigned:

VLAN IDs: Example: 1,3,5-10

Selected ports:

Untagged Membership

Apply

Cancel

La configuración final sería PVID de los puertos 1 y 8 sería la vlan 1 ya que es la administrativa digamos es la que establece una conexión router-switch y taggeamos en esos puertos la vlan que queremos que nos de la IP en este caso la VLAN 999.

El puerto 8 sera el que ira conectado al router y el puerto 1 el que ira conectado con el AP. Podemos realizar la misma configuración para otros puertos para la demás VLANs de la misma forma que este. Tenemos que tener siempre la vlan administrativa conetada con el router a través de PVID y untaggeada.

También taggearemos estos puertos con los demás VLANs para que todo el trafico pueda pasar por estos puertos digamos que esta configurado troncalmente.

3. Configuración de AP

Una vez que tenemos conectados el AP al switch va a obtener una IP también sin estar en la VLAN toda la configuraciones vienen con la VLAN 1.

Tenemos que entrar en el AP, con credenciales admin y contraseña es el numero de serie.

Lo primero que haremos es irnos a la configuración del AP en Access Points y cambiar el Uplink a la VLAN 999 que es la management.

The screenshot shows the 'Edit Access Point 7c:57:3c:cd:f9:ae' configuration page. The left sidebar contains a navigation menu with 'Configuration' selected, and sub-items like 'Access Points', 'System', 'RF', 'Security', 'IDS', 'Routing', 'Tunnelling', 'Services', 'DHCP Server', 'Maintenance', and 'Support'. The main content area is titled 'Edit Access Point 7c:57:3c:cd:f9:ae' and has a tabbed interface with 'General', 'Radio', 'Installation Type', and 'Uplink' tabs. The 'Uplink' tab is active, showing fields for 'Uplink management VLAN' (set to 999), 'Eth0 bridging' (disabled), and 'USB port' (enabled). Below these are sections for 'PEAP User' (Username, Password, Retype) and 'Upload Certificate' (URL, Certificate type set to CA, and an 'Upload Certificate' button).

Ya únicamente vamos a utilizar el AP para crear varios punto de accesos dentro y separar las redes.

The screenshot shows the Aruba Virtual Controller configuration interface. The top header includes the 'aruba' logo, 'VIRTUAL CONTROLLER', and the identifier 'SetMeUp-CD:F9:AE'. The left sidebar has 'Configuration' selected, with sub-items like 'Networks', 'Access Points', 'System', and 'RF'. The main content area is titled 'edit Prueba' and has a tabbed interface with 'Basic', 'VLAN', 'Security', and 'Access' tabs. The 'Basic' tab is active, showing the 'Name & Usage' section with fields for 'Name' (set to Prueba), 'Type' (set to Wireless), and 'Primary usage' (set to Employee).

aruba

VIRTUAL CONTROLLER

SetMeUp-CD:F9:AE

Dashboard

Configuration

Networks

Access Points

System

RF

Security

IDS

edit Prueba

1 Basic

2 VLAN

3 Security

4 Access

Client IP & VLAN Assignment

Client IP assignment

☐ Virtual Controller managed

☒ Network assigned

Client VLAN assignment

☐ Default

☒ Static

☐ Dynamic

VLAN

2000

En client VLAN le damos a static para elegir la VLAN (vlan 2000 que hice de prueba)

aruba

VIRTUAL CONTROLLER

SetMeUp-CD:F9:AE

Dashboard

Configuration

Networks

Access Points

System

RF

Security

IDS

Routing

Tunneling

Services

DHCP Server

Maintenance

About

edit Prueba

1 Basic

2 VLAN

3 Security

4 Access

Security Level

Security Level

Personal

Key management

WPA2-Personal

Passphrase format

8-63 chars

Passphrase

Retype

MAC authentication

☐

Blacklisting

☐

Enforce DHCP

☐

Fast Roaming

802.11r

☐

802.11k

☐

802.11v

☐

aruba

VIRTUAL
CONTROLLER

SetMeUp-CD:F9:AE

Dashboard

Configuration

Networks

Access Points

System

RF

Security

IDS

edit Prueba

1 Basic

2 VLAN

3 Security

4 Access

Access Rules

Access Rules

Download roles

No restrictions on access based on destination or type of traffic

Y ya seria todo, tener en cuenta la salida a WAN en los filtrados del firewall. s