

MANUAL DE CONFIGURACIÓN DE VDOM EN FORTIGATE
ANEXO

PRESENTADO POR:
DAVID ALEJANDRO TORRES RONCANCIO
JOSE FELIPE ZAMBRANO PEREZ

MODERNIZACION TECNOLÓGICA DE LA INFRAESTRUCTURA DE LOS SERVICIOS DE
SEGURIDAD PERIMETRAL PARA LA RED CORPORATIVA

UNIVERSIDAD EL BOSQUE
FACULTAD DE INGENIERÍA ELECTRÓNICA
ESPECIALIZACIÓN EN SEGURIDAD DE REDES TELEMATICAS
BOGOTÁ, COLOMBIA
[12/06/2020]

Dominios Virtuales (VDOMs)

Los VDOM o virtual domain es una funcionabilidad que ofrece Fortinet gratuitamente en sus dispositivos Fortigate tanto en equipos appliance como virtuales, esta función nos permite crear instancias de Fortigate, cada instancia es opera de manera independiente tanto de administración como de reglas de acceso, rutas, VPNs y UTM.

Consiste en dividir de manera lógica el dispositivo con el fin de tener varios Fortigate que operen en diferentes modos en el mismos hardware o máquina virtual, permite segmentar flujos de trafico de diferentes redes y poder separar la administración de los usuarios de seguridad.

En Fortinet por defecto se puede configurar o crear máximo 10 VDOMs en un dispositivo desde el modelo 60D en adelante, para las modelos anteriores tiene un máximo 5 VDOMs, si desea tener un número mayor de estos Virtual domain debe adquirir licencias con el fabricante.

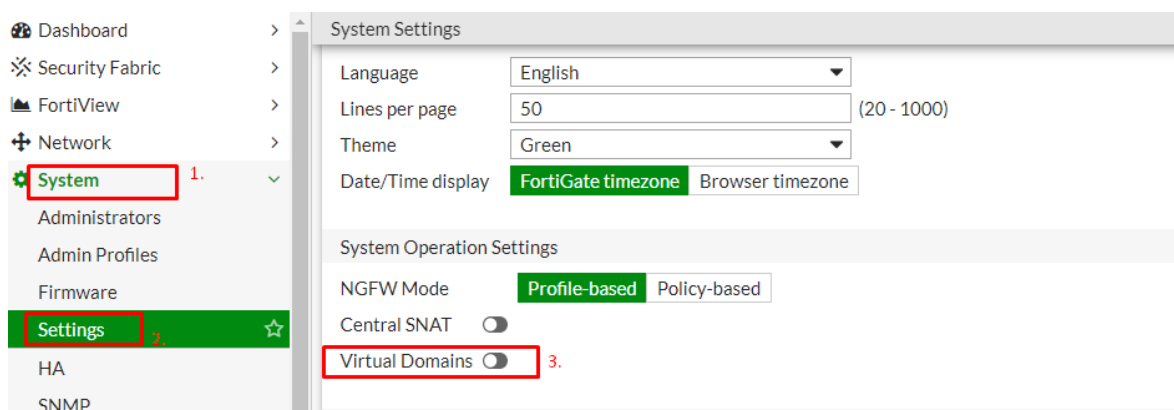
el VDOM "root" es el encargado de la administración de hacer tareas "globales" la conectividad a Fortiguard para actualizaciones, peticiones DNS, logs, clúster, aunque esto se puede cambiar vía GUI de acuerdo a las necesidades requeridas.

En la configuración de los virtual domain se tiene la opción de configurar usuarios específicos para cada VDOM, siempre y cuando no se le habilite la opción del perfil de administración de "super_admin" ya que un usuario con este rol tiene acceso a todos los VDOMs.

A continuación, se detallará el proceso de creación y configuración de los dominios virtuales.

Paso 1.

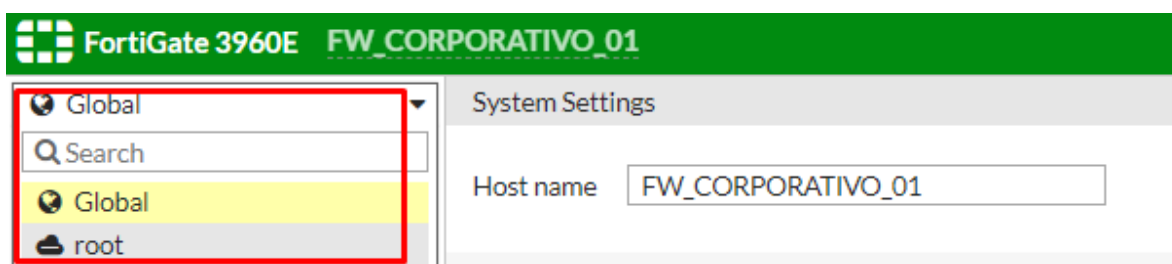
La primera configuración consiste en habilitar la función de VDOM en el Fotigate ya que por defecto viene deshabilitado, para ello seleccionamos System > Settings > Virtual Domains y se gurda configuración.



Al aplicar el cambio se cerrará automáticamente la sesión del usuario administrador que se tenía activa con el fin de aplicar la configuración realizada correspondiente a la activación de los VDOMs.

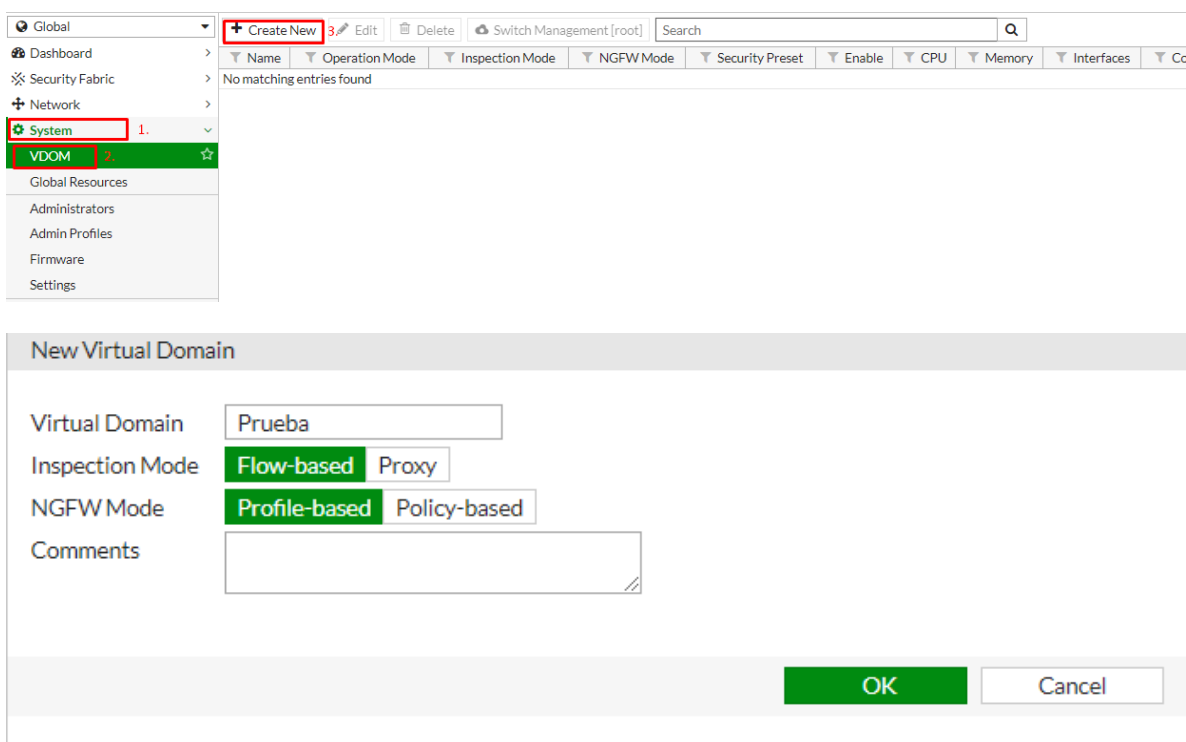
Paso 2.

Al iniciar sesión en el Fortigate se evidenciará en la parte superior derecha un menú de despliegue con los VDOM creados.



Paso 3.

Para crear un nuevo VDOM seleccionamos System > VDOM > Create New.



Al realizar la creación del VDOM podemos realizar ciertas configuraciones del virtual domain de acuerdo a las necesidades requeridas para ellos editamos el VDOM.

Global

+ Create New

Edit

3 Delete

Switch Management [root]

Search

Q

Dashboard

Security Fabric

Network

System

VDOM

Global Resources

Name	Operation Mode	Inspection Mode	NGFW Mode	Security Preset	Enable	CPU	Memory
Prueba	NAT	Flow-based	Profile-based	Custom	<input checked="" type="checkbox"/>	0%	0%

Se puede customizar ciertas configuraciones correspondientes a políticas, usuarios, VPN y logs con el fin de definir las características en la cual trabaja la nueva instancia configurada.

Edit Virtual Domain Settings

Virtual Domain: Prueba
Inspection Mode: **Flow-based** Proxy
NGFW Mode: **Profile-based** Policy-based
Comments:

Resource Usage

Reset All

Resource	Current Usage	Global Maximum	Override Maximum	Guaranteed
Active Sessions	0% (0)	No Limit Set	<input type="checkbox"/>	
Policy & Objects				
Firewall Policies	0% (0)	41024	<input type="checkbox"/>	
Firewall Addresses	0% (41)	41024	<input type="checkbox"/>	
Firewall Address Groups	0% (0)	10692	<input type="checkbox"/>	
Firewall Custom Services	0% (87)	No Limit Set	<input type="checkbox"/>	
Firewall Service Groups	0% (4)	No Limit Set	<input type="checkbox"/>	
Firewall One-time Schedules	0% (0)	No Limit Set	<input type="checkbox"/>	
Firewall Recurring Schedules	0% (2)	No Limit Set	<input type="checkbox"/>	
User & Device				
User	0% (0)	No Limit Set	<input type="checkbox"/>	
User Groups	0% (0)	No Limit Set	<input type="checkbox"/>	
Concurrent Explicit Proxy Users	0% (0)	8000	<input type="checkbox"/>	
VPN				
SSL-VPN	0% (0)	No Limit Set	<input type="checkbox"/>	
VPN IPsec Phase1 Tunnels	0% (0)	2000	<input type="checkbox"/>	
VPN IPsec Phase2 Tunnels	0% (0)	2000	<input type="checkbox"/>	
VPN IPsec Phase1 Interface Tunnels	0% (0)	No Limit Set	<input type="checkbox"/>	
VPN IPsec Phase2 Interface Tunnels	0% (0)	No Limit Set	<input type="checkbox"/>	
Dial-up Tunnels	0% (0)	No Limit Set	<input type="checkbox"/>	
Log & Report				
Log Disk Quota (MB)	0% (0)	No Limit Set (MB)	<input type="checkbox"/>	

Paso 4.

Administración de VDOMs, de acuerdo a la configuración realizada ya se podrá administrar de forma independiente cada VDOM lo cual es necesario tener en cuenta que hay configuraciones que solo se deben realizar en cada virtual domain y otras configuraciones que se aplican de forma global, y esta afectara a todos los VDOMs.

Listado de configuraciones que se aplicaran de forma global para todo los VDOMs.

Sistema

- Interfaces Físicas y virtuales.
- DNS configuración.
- Nombre del equipo.
- Hora del Sistema.
- Versión Firmware.
- Idle Tiempo de autenticación.
- HA.
- SNMP.
- Reemplazar mensajes.

Usuarios

- Perfilamiento de usuario.

UTM

- Antivirus.

Logs y reportes

- Log de configuración.

Paso 5.

Se configura una interfaz de gestión para la administración del virtual domain donde seleccionamos el VDOM de administración (Global) > networks > Interfaces y seleccionamos el puerto MGMT (puede escoger cualquier otro puerto) se debe habilitar el acceso a HTTPS, PING y SSH.

Global

Dashboard

Security Fabric

Network

Interfaces

DNS

System

Log & Report

Edit Interface

Interface Name mgmt (00:09:0F:09:54:01)

Alias

Link Status Up

Type Physical Interface

Virtual Domain root

Role LAN

Dedicated Management Port

Address

Addressing mode Manual DHCP Dedicated to FortiSwitch

IP/Network Mask 192.168.1.99/255.255.255.0

Administrative Access

IPv4

HTTPS

SSH

HTTP

SNMP

PING

FTM

FMG-Access

CAPWAP

RADIUS Accounting

FortiTelemetry

DHCP Server

Networked Devices

Device Detection

Admission Control

Security Mode None

Secondary IP Address

OK Cancel

Paso 6.

Creación de usuario por VDOM se debe seleccionar System > Administrators > create new > administrator donde seleccionamos el usuario la contraseña y el perfil de usuario en la parte de Virtual Domains seleccionamos el VDOMs al cual quiere tener acceso.

Global

Dashboard

Security Fabric

Network

System

VDOM

Global Resources

Administrators

Admin Profiles

Firmware

Settings

HA

SNMP

Replacement Messages

FortiGuard

Advanced

Feature Visibility

Certificates

SDN Connectors

Log & Report

New Administrator

User Name prueba1

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

Password

Confirm Password

Comments Write a comment...

Administrator Profile prof_admin

Virtual Domains

Prueba

root

Email Address

SMS

Two-factor Authentication

Restrict login to trusted hosts

Restrict admin to guest account provisioning only

OK Cancel

Referencias

<https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/938921/creating-per-vdom-administrators>

http://docshare.tips/coacutemo-configurar-dominios-virtuales-vdoms-en-un-fortigate_5a80f0ab08bbc50e28c24040.html

<https://fortixpert.blogspot.com/2016/12/gestionando-fortigates-individualmente.html?view=classic>