

Firewall Fortigate

November 8, 2021

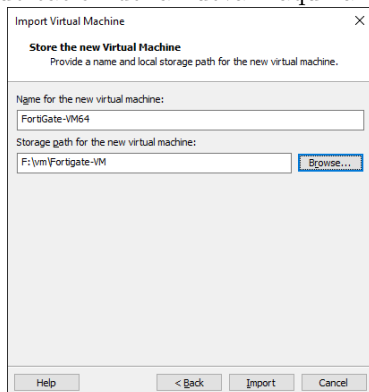
Fortinet nos permite descargar y utilizar la máquina virtual de forma gratuita durante dos semanas . Significa que no tiene que comprar nada para probar algunas funciones en su VM.

1 Instalacion

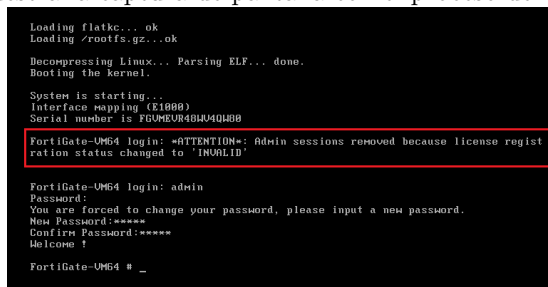
Lo primero que debe hacer es ir a support.fortinet.com y crear una cuenta gratuita.

Extraiga el archivo descargado y haga doble clic en el archivo de la máquina virtual.

Esto abrirá la ventana Importar máquina virtual donde deberá especificar la ubicación de la nueva máquina virtual:



Ahora puede iniciar la VM y acceder a la consola CLI. El nombre de usuario predeterminado es admin y la contraseña está en blanco. En el primer inicio de sesión, se le pedirá que establezca la nueva contraseña. A continuación se muestra la captura de pantalla con el proceso de inicio de sesión inicial.

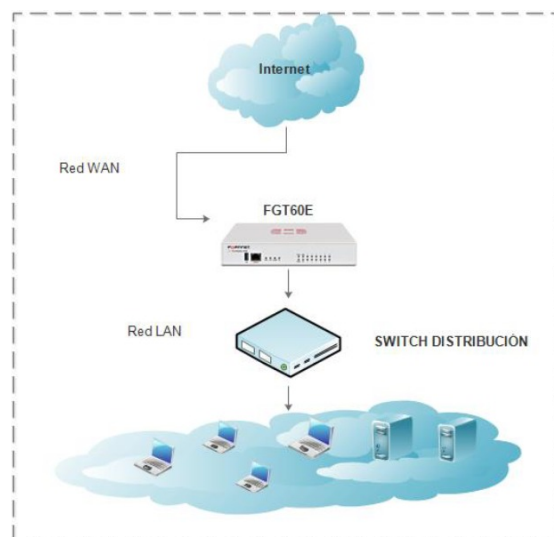


De forma predeterminada, todos los adaptadores de red de la máquina virtual están en modo puente, esto significa que una de las interfaces obtendrá una dirección IP de su enrutador (servidor DHCP), que proporciona acceso a Internet a su computadora. Una vez que sepa la dirección IP de Fortigate-VM, puede iniciar sesión en su interfaz web. Si tuvo un error relacionado con la licencia, mencionado anteriormente

Este error tiene algo que ver con la sincronización horaria. La forma más fácil de hacer que funcione es simplemente realizar un restablecimiento de fábrica de Fortigate-VM. El comando se ejecuta el restablecimiento de fábrica

Después del proceso de restablecimiento, deberá volver a iniciar sesión con las credenciales predeterminadas (administrador y contraseña en blanco). Proporcione la nueva contraseña y busque la dirección IP de la interfaz como se describió anteriormente. Ahora podrá acceder a la GUI y comenzar a configurar el dispositivo.

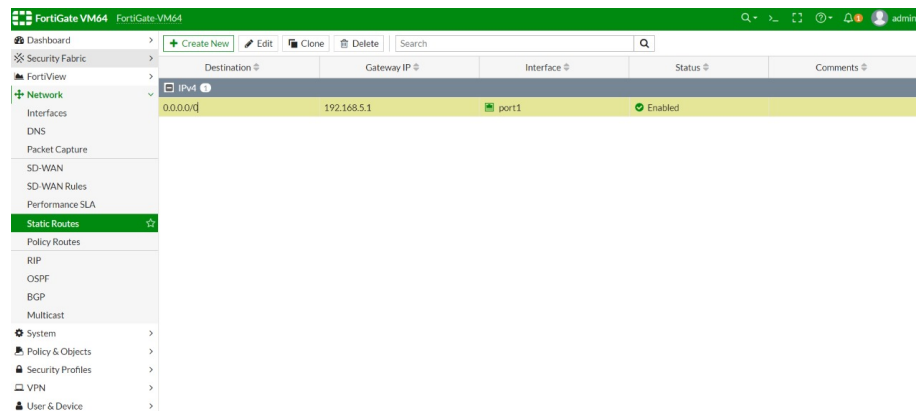
2 Topologia para el Firewall



3 Politicas Firewall

ruta estatica para navegacion de firewall y red lan

se debe de configurar un gateway por el cual nuestro firewall perimitral tendra acceso a internet por medio de este a traves de politica brindaremos navegacion y acceso de red a los equipos conectados a la red Lan y DMZ.



configuracion de interfaces

interfas WAN

se configuro la interfaz Wan en el puerto 1 de nuestro firewall asignando una IP de nuestro segmento del router de casa, esto para utilizar el router de casa como puerta de salida del firewall.

```

idbth (kbps). Used to estimate link utilization.
vrrp-virtual-mac          Enable/disable use of virtual MAC
for VRRP.
role                      Interface role.
snmp-index               Permanent SNMP Index of the interf
ace.
preserve-session-route   Enable/disable preservation of ses
sion route when dirty.
auto-auth-extension-devi Enable/disable automatic authoriza
tion of dedicated Fortinet extension device on this interface.
ap-discover              Enable/disable automatic registrat
ion of unknown FortiAP devices.
switch-controller-igmp-s Switch controller IGMP snooping pr
nooping-proxy.
switch-controller-igmp-s Switch controller IGMP snooping fa
st-leave.

FortiGate-UM64 (port1) # set mode
static      Static setting.
dhcp       External DHCP client mode.
pppoe      External PPPoE mode.

FortiGate-UM64 (port1) # set mode static

FortiGate-UM64 (port1) # set ip 192.168.5.250 255.255.255.0_

```

interfas LAN

se configuro el puerto 2 de nuestro firewall como segmento LAN asignando la red 192.168.44.0/24 para los equipos windows server y windows endpoint los cuales pertenecen a nuestro segmento de red interna.

```

edit "port2"
    set vdom "root"
    set ip 192.168.44.250 255.255.255.0
    set allowaccess ping https ssh
    set type physical
    set alias "Lan Internal"
    set device-identification enable
    set role lan
    set snmp-index 2
next

```

Interfas DMZ

se configuro el puerto 3 de nuestro firewall como segmento DMZ asignando la red 10.10.10.0/24 para los equipos Linux en los cuales se encuentran servicios criticos tales como base de datos y servidores FTP. Esta zona se encuentra aislada de la RED LAN y para acceder a ella se deben de solicitar permisos al administrador del FW para que cree politicas de acceso, indicando que equipos se van a conectar y protocolos a utilizar.

The screenshot shows the 'Edit Interface' configuration for a FortiGate device. The interface is named 'DMZ (port3)' with an alias 'DMZ'. It is configured as a 'Physical Interface' with a role of 'DMZ'. The addressing mode is set to 'Manual' with an IP address of '10.10.10.250' and a netmask of '255.255.255.0'. Under 'Administrative access', IPv4 protocols are configured: HTTPS and PING are checked, while SSH, SNMP, RADIUS Accounting, Security Fabric Connection, FMG-Access, and FTM are unchecked. LLDP settings for both Receive and Transmit are set to 'Use VDOM Setting'. The 'Device detection' option is enabled.

Creacion de objetos

Según buenas practicas en equipos como firewall perimetral es recomendado crear objetos especificos para brindar accesos a los equipos a los diferentes destinos. Se crearon objetos como RED LAN, Servidor Ubuntu, RED DMZ entre otros.

Name	Type	Details	Interface	Visibility	Ref
FABRIC_DEVICE	Subnet	0.0.0.0/0		Visible	0
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0		Hidden	0
RED_DMZ	Subnet	10.10.10.0/24		Visible	0
RED_Lan	Subnet	192.168.44.0/24		Visible	3
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	SSLVPN tunnel interface (ssl.root)	Visible	2
Ubuntu	Subnet	10.10.10.130/32		Visible	3
all	Subnet	0.0.0.0/0		Visible	3
gmail.com	FQDN	gmail.com		Visible	1
login.microsoft.com	FQDN	login.microsoft.com		Visible	1
login.microsoftonline.com	FQDN	login.microsoftonline.com		Visible	1
login.windows.net	FQDN	login.windows.net		Visible	1
none	Subnet	0.0.0.0/32		Visible	0
wildcard.digipbox.com	FQDN	*digipbox.com		Visible	0
wildcard.google.com	FQDN	*google.com		Visible	1

Creacion politicas de acceso

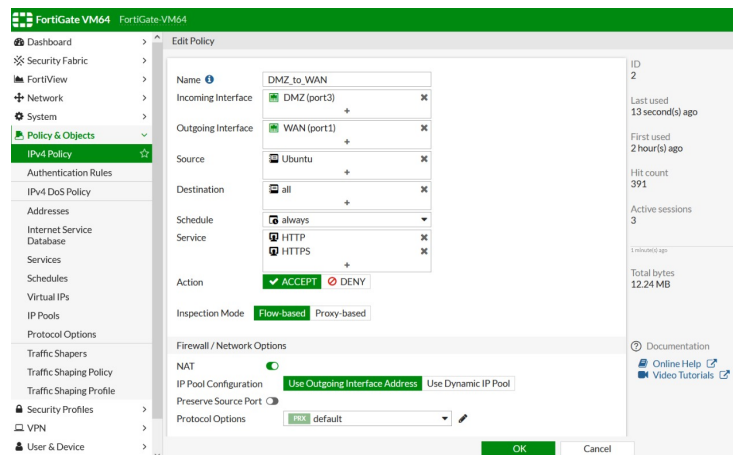
Creacion politicas de acceso RED LAN

Se configuraron politicas de acceso a internet para los equipos conectados a la RED LAN, para esto fue necesario especificar las interfaces de entrada y salida así como que dispositivos tienen permisos y cuales no, en este tipo de reglas se pueden aplicar politicas de seguridad como perfiles UTM, en el cual se pueden configurar servicios y aplicaciones ya sea que se necesiten permitir o bloquear, en nuestro caso no fue posible activar este tipo de seguridad por temas de licenciamiento.

Name	Incoming Interface	Outgoing Interface	Source	Destination	Schedule	Service	Action	Inspection Mode	Firewall / Network Options
Navegacion_LAN	Lan_Internal (port12)	WAN (port1)	RED_Lan	all	always	ALL	ACCEPT	Flow-based	NAT: Use Outgoing Interface Address, IP Pool Configuration: Use Dynamic IP Pool, Preserve Source Port: Off, Protocol Options: default

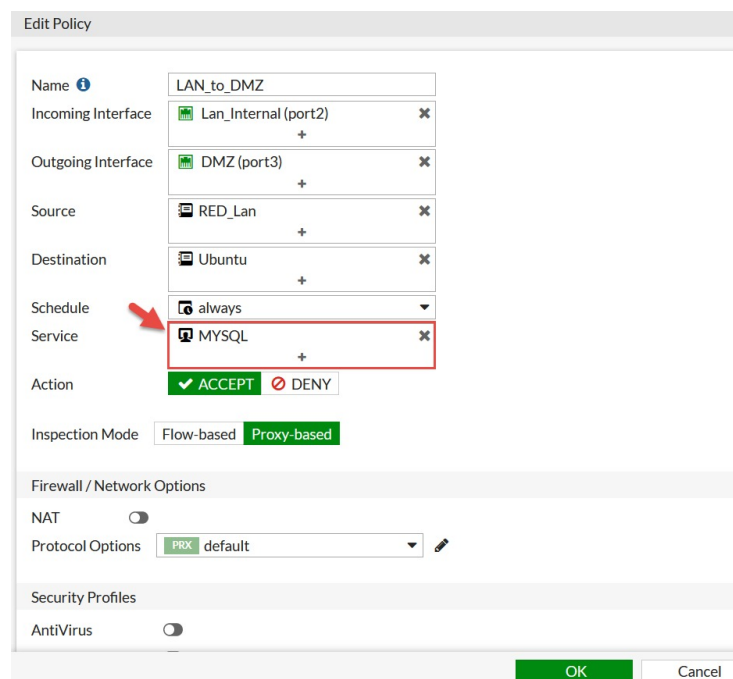
Creacion politicas de acceso RED DMZ

Se configuraron politicas de acceso a internet para los equipos conectados a la RED DMZ, para esto fue necesario especificar las interfaces de entrada y salida así como que dispositivos tienen permisos y cuales no, esta politica se creó más cerrada por motivos de los servicios que se encuentran en la misma, cabe mencionar que esta zona no tiene acceso full a la zona LAN esto por motivos de seguridad.



Comunicación red LAN con DMZ

Por políticas de seguridad la RED lan no debe de compartir todos los recursos con la RED DMZ, esto para evitar cualquier tipo de fuga de información o infección que se pueda dar en cualquier red, el firewall tiene como funcion brindar accesos o denegar permisos a los usuarios, para nuestro proyecto se creó una politica para comunicación entre RED LAN y DMZ únicamente permitiendo el servicio de mysql y ICMP, esto para mitigar cualquier riesgo o vulnerabilidad que utilice puertos inusuales.



Monitorio de red

Una de las muchas bondades de un firewall perimetral es la reporteria, por medio de esta nosotros podemos verificar tanto como vitalidad y accesos de los usuarios, en nuestro firewall configuramos un dashboard el cual utilizaremos para verificar el estado de las interfaces y el estado del firewall, monitoreando su performance como cpu, memoria ram y throughput de las interfaces configuradas.

