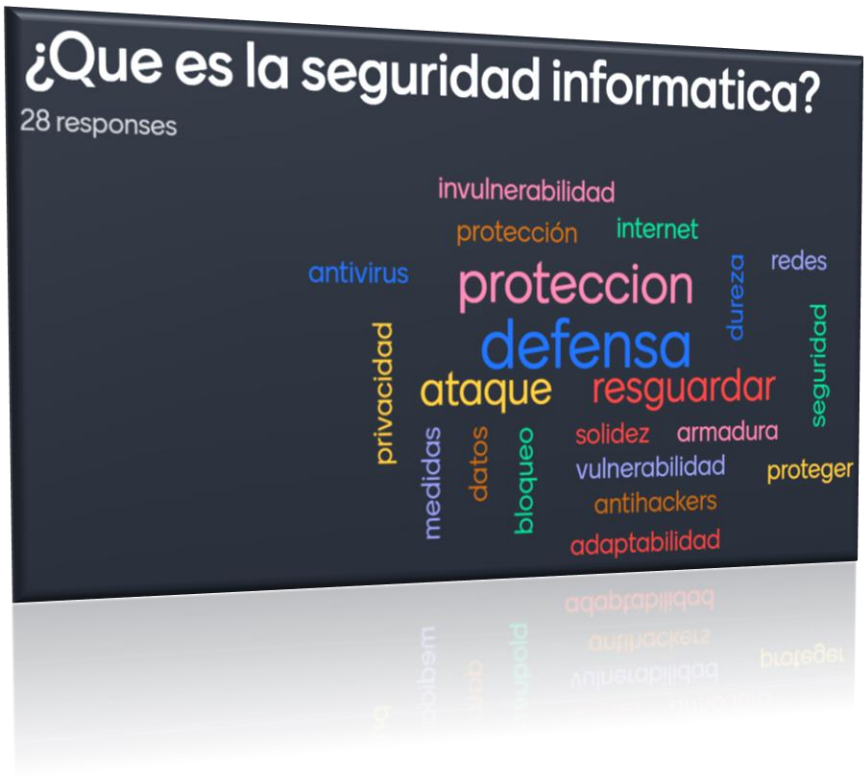
Universidad Paraguayo Alemana

UNIVERSIDAD PARAGUAYO ALEMANA
HEIDELBERG - ASUNCIÓN



Seguridad TICs

Prof.: Chrystian Ruiz Diaz

Contenido

Nota de Uso Académico

Este documento ha sido preparado exclusivamente para el uso académico del docente. Este documento no puede ser distribuido a ninguna otra parte ni utilizado para ningún otro propósito, diferente al establecido como alcance en el proyecto académico de la **UNIVERSIDAD PARAGUAYO ALEMANA**. El uso indebido del material fuera del ámbito académico no representa ninguna responsabilidad del docente.

Objetivos

Implementar seguridad perimetral con firewall "*Open Source*" con tres zonas; zona naranja para el servidor web accesible desde internet, zona verde la zona segura y la zona azul para las conexiones de personas/empresas externas.

Marco Teórico

VMware Workstation es un hipervisor que permite a los usuarios crear múltiples máquinas virtuales (VM) y utilizarlos simultáneamente junto con la máquina real. Cada máquina virtual puede ejecutar su propio sistema operativo, como Microsoft Windows, Linux o BSD. Como tal, VMware Workstation permite a una máquina física ejecutar múltiples sistemas operativos simultáneamente.

VMware Workstation soporta diferentes adaptadores de red, permite compartir unidades de disco y dispositivos USB desde la maquina real con la máquina virtual. Además, permite simular unidades de disco.

Existe una plataforma FREE para poder correr las diferentes máquinas virtuales llamada VMPlayer. Es posible descargarla en el siguiente link, tengan en cuenta que con esta solo se puede ejecutar una VM en forma simultánea, por lo que se recomienda realizar una suscripción a modo de prueba y tiene una validez de 60 días:

https://www.vmware.com/latam/products/workstation-player.html

Endian Firewall Community (EFW) es un producto de software de seguridad basado en Linux llave en mano diseñado para el hogar que puede transformar cualquier dispositivo de hardware no utilizado en una solución de Gestión Unificada de Amenazas (UTM) con todas las funciones. Endian Community está diseñado para simplificar la seguridad y ayudar a proteger las redes domésticas utilizando el poder del código abierto.

Materiales a utilizar

1. Descargar e instalar VMware (VMware ofrece 60 días "Trial" de sus productos)

https://www.vmware.com/

2. Descargar e instalar/montar Kali Linux

https://www.kali.org/downloads/

3. Descargar y montar Servidor Web Vulnerable

https://mega.nz/folder/l9UR0aLT

Clave de Cifrado= TpD0mySElIZWPbwtOwZ34A

OBS.: Estas tres primeras herramientas ya lo hemos utilizado en la clase práctica, las pueden reutilizar

4. Descargar e instalar/montar *Endian Firewall Community*

https://www.endian.com/de/community/download/

5. Del mismo link indicado en el ítem 3, descargar y montar una VM Windows 7 Ultimate x63

https://mega.nz/folder/l9UR0aLT

Clave de Cifrado= TpD0mySElIZWPbwtOwZ34A

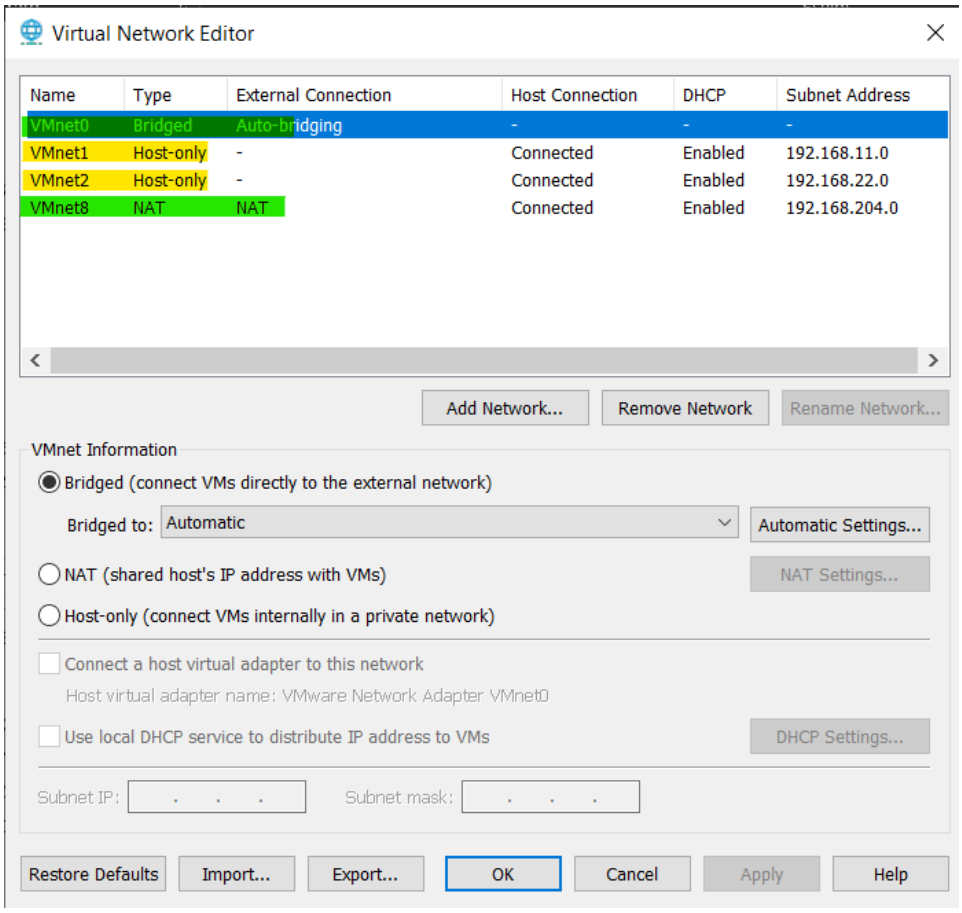
OBS.: Favor tener en cuenta que estas herramientas son utilizadas con fines estrictamente académicos, por lo que se las licencias y demás permisos son temporales. Esto a modo de facilitarles estas herramientas del trabajo practico y puedan centrarse en la elaboración en base a los objetivos propuestos.

Conexiones De Red

Este es el punto más importante en la manipulación de máquinas virtuales, dependiendo de cómo usemos las interfaces de red tendremos o no acceso a internet o acceso a máquinas virtuales en otros computadores.

Primero debe saber que VMware tiene varios switches virtuales a los cuales llama VMNet0, VMnet1… VMnet9. Por defecto VMnet0 hace un puente directo con una de las interfaces de red que tiene la máquina física, y usa la VMnet8 como interfaz de NAT. Esto se explicará con mayor detalle más adelante.

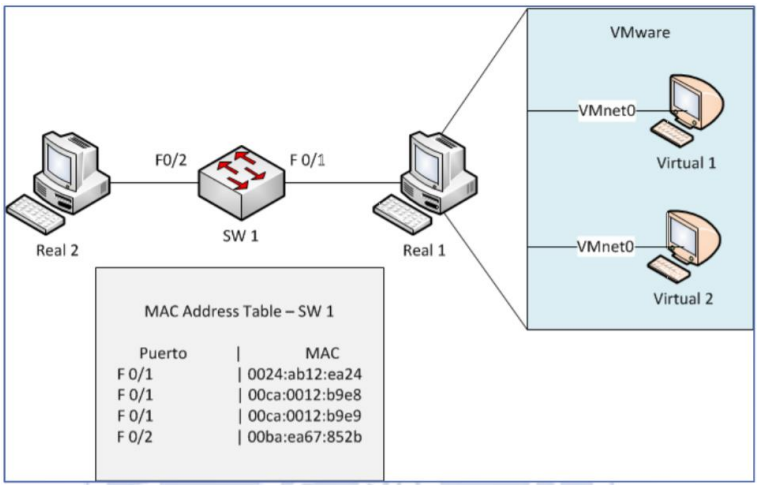
La central de administración de los switches de VMware se llama Virtual Network Editor, para hacer modificaciones debe ingresar por el menú de inicio -> todos los programas -> VMware y abrir el virtual Network Editor como administrador, de lo contrario no podrá realizar cambios en la configuración. Dentro de dichas opciones usted podrá llegar a crear un numero definido de switch virtuales o vnets.



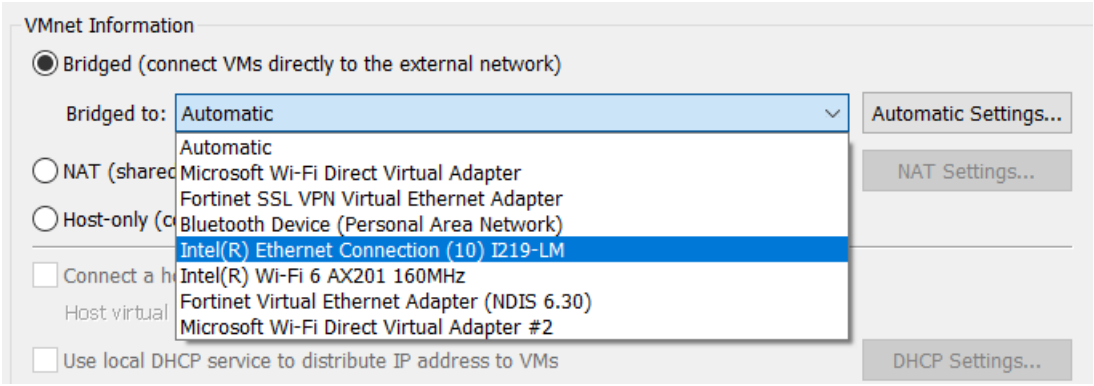
A continuación, se describen las opciones del Virtual Network Editor sobre cada VMnet.

VMnet 0

Por defecto esta interfaz se usa en modo Bridged, lo cual permite usar una interfaz física para conectar la maquina real a una infraestructura real.



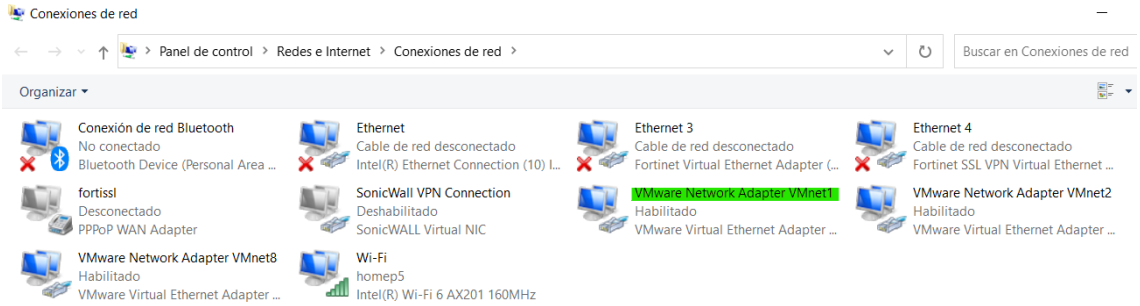
Uno de los problemas más comunes en el modo Bridged es que VMware toma automáticamente cualquier interfaz activa, es recomendable seleccionar de forma permanente la interfaz Ethernet de la maquina real.



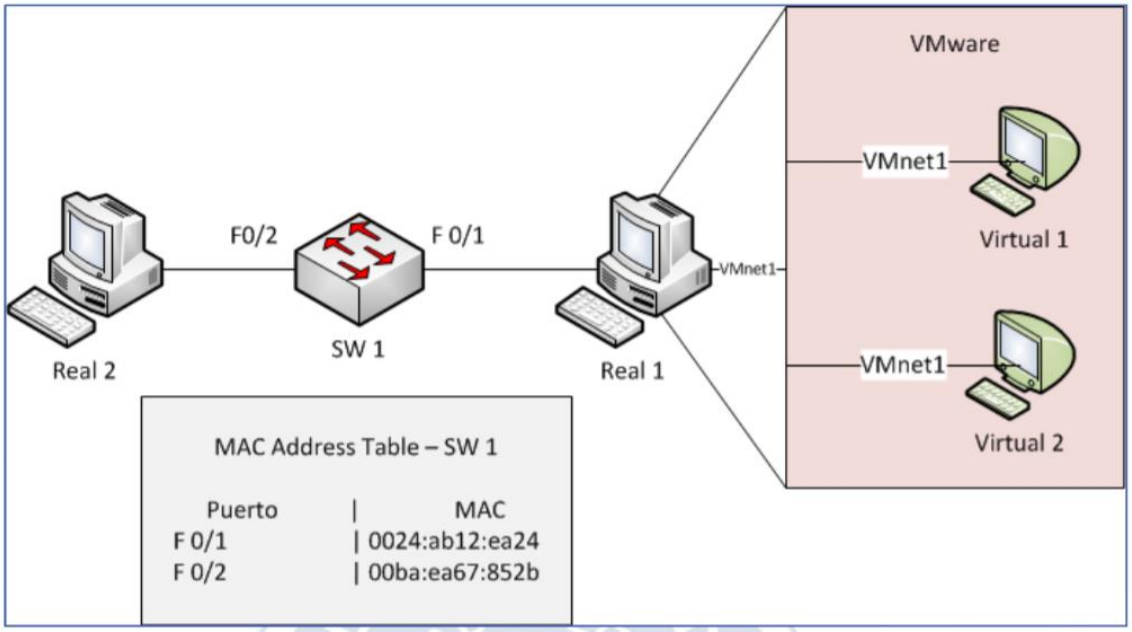
Cuando conecte una máquina virtual a la VMnet 0 = Bridged usará la tarjeta física del computador y tendrá acceso a toda la red. Es importante configurar un direccionamiento IP al interior de la máquina virtual que coincida con el direccionamiento de la red. Si al interior de la red hay un servidor DHCP, la máquina virtual puede usarlo para obtener sus valores de direccionamiento.

VMnet 1

Por defecto esta interfaz se usa en modo “Host only” para conectar la maquina real con las máquinas virtuales en una red que no tiene acceso a internet o a otra máquina real. La máquina real crea una interfaz virtual llamada VMnet1, puede ver esta interfaz en las conexiones de red.

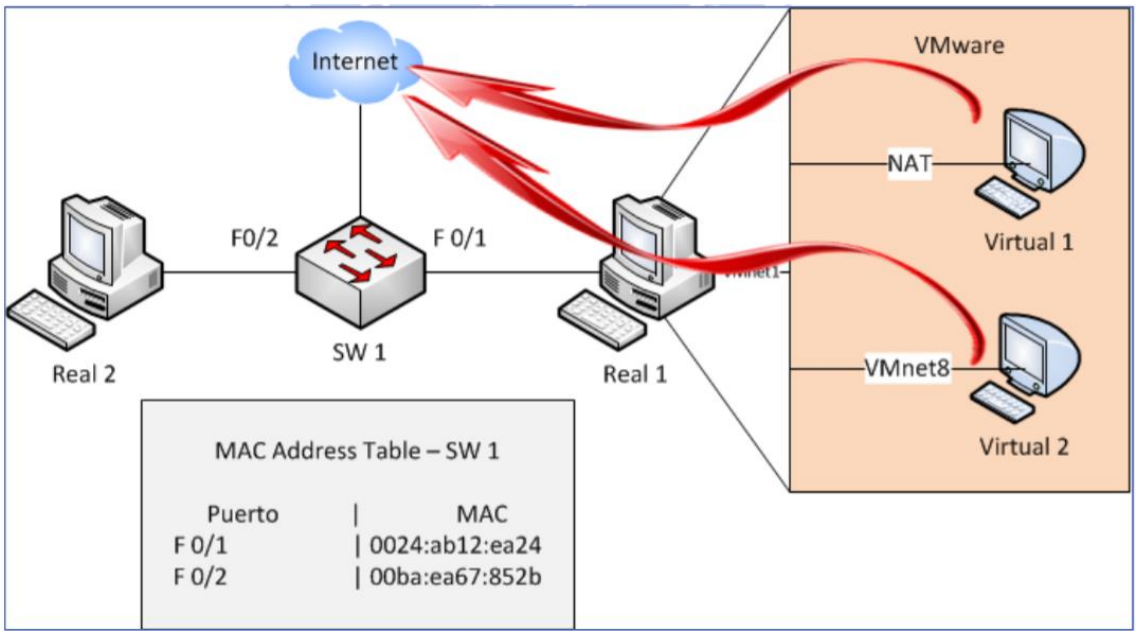


Esta interfaz tiene una dirección IP y una máscara de red que asigna de forma automática VMware. No asigne una dirección de Gateway esto podría afectar el enrutamiento de la máquina real. Para el caso de las imágenes presentadas en esta guía, si verifica el Virtual Network Editor, la dirección de red 192.168.230.0 es la red asignada a la VMnet 1. Cuando conecte una máquina virtual a esta VMnet, solo tendrá conexión entre la máquina real y la virtual. Todas las máquinas que estén en VMnet1 pueden verse entre sí.



VMnet 8

Esta interfaz también se llama NAT. Cuando conecta una máquina virtual a esta interfaz VMware usa un servidor DHCP el cual le asigna de forma dinámica dirección IP a cada máquina virtual. Por medio de esta interfaz la máquina virtual puede acceder a internet sin importar la fuente de internet que tenga la maquina Real (la máquina real puede estar conectada por Wifi, USB, Ethernet a internet) Todas las máquinas que estén en NAT pueden verse entre sí.

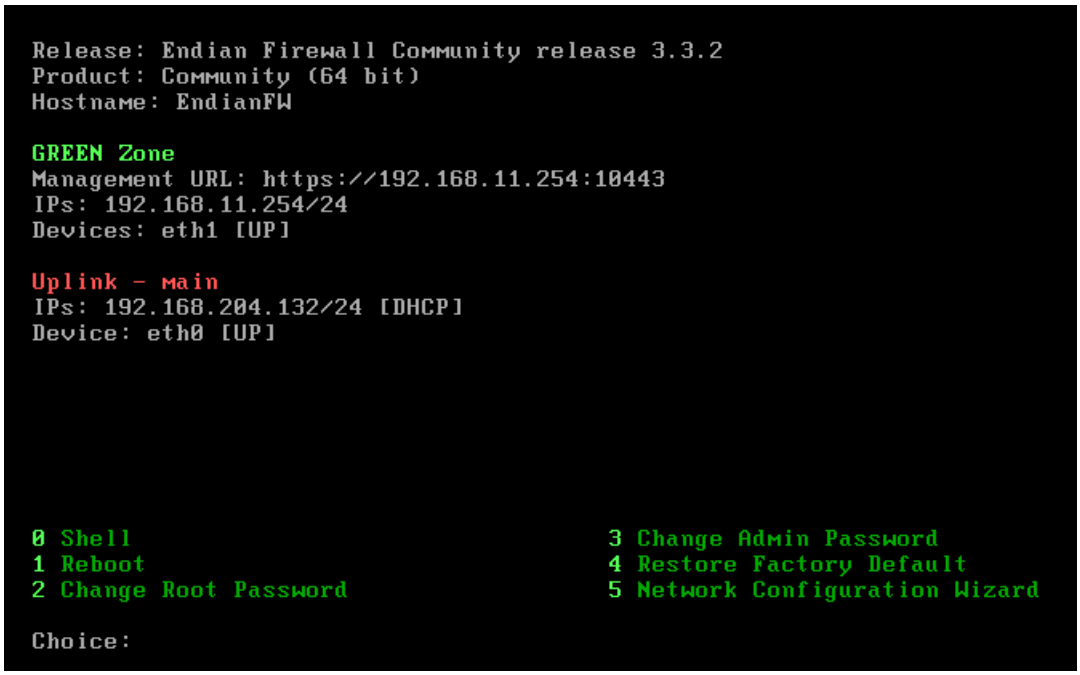


VMnet 3..7, 9

Las demás VMnet no tiene ninguna configuración por defecto, cada una es un switch virtual independiente y permite crear subredes a nivel de máquinas virtuales.

Endian Firewall Commnity

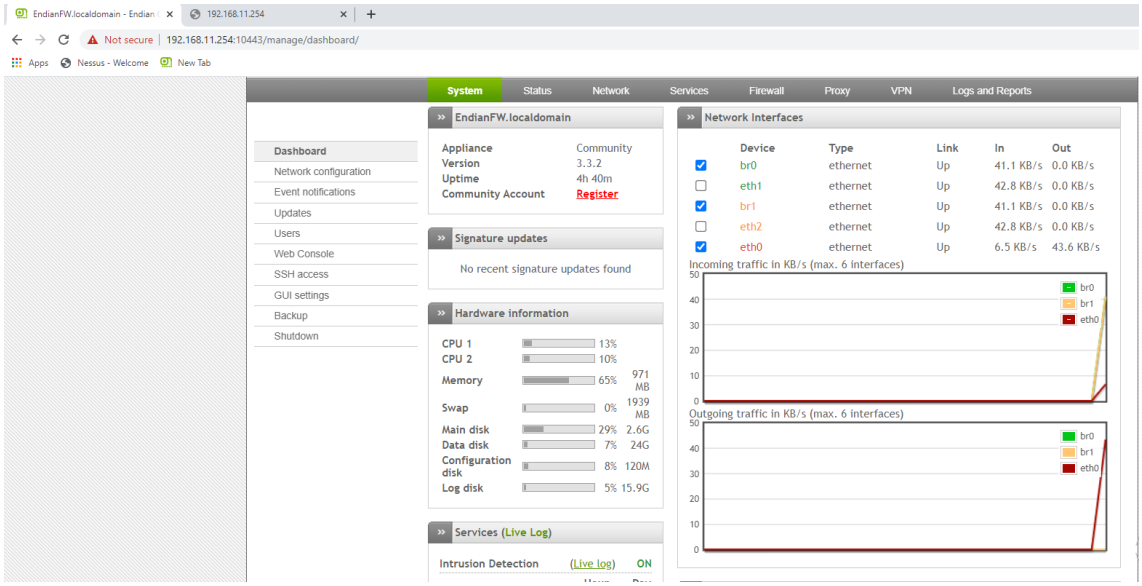
Una vez instalado la VM Endian, por consola quedaría de la siguiente manera:



En esta pantalla se indica la URL para realizar la configuración del firewal

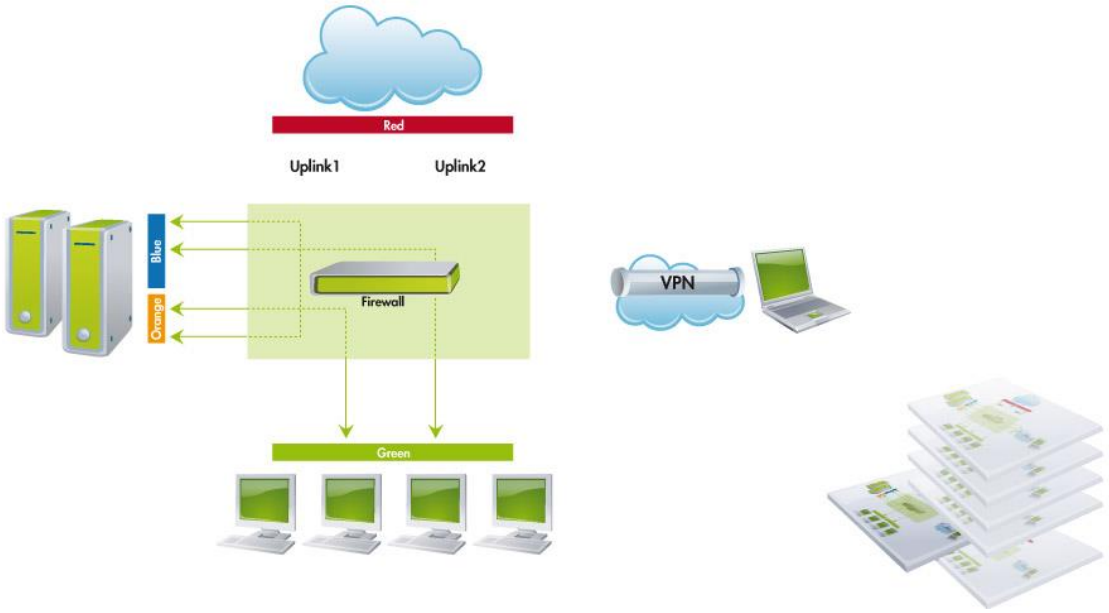
Entrando a la interfaz de configuración del Firewall (dependiendo desde la zona donde quieren acceder)

Nota: Esta pantalla es solo a modo de ejemplo, tanto la interfaz eth0, eth1, ethx y las direcciones IP dependen de como lo han configurando

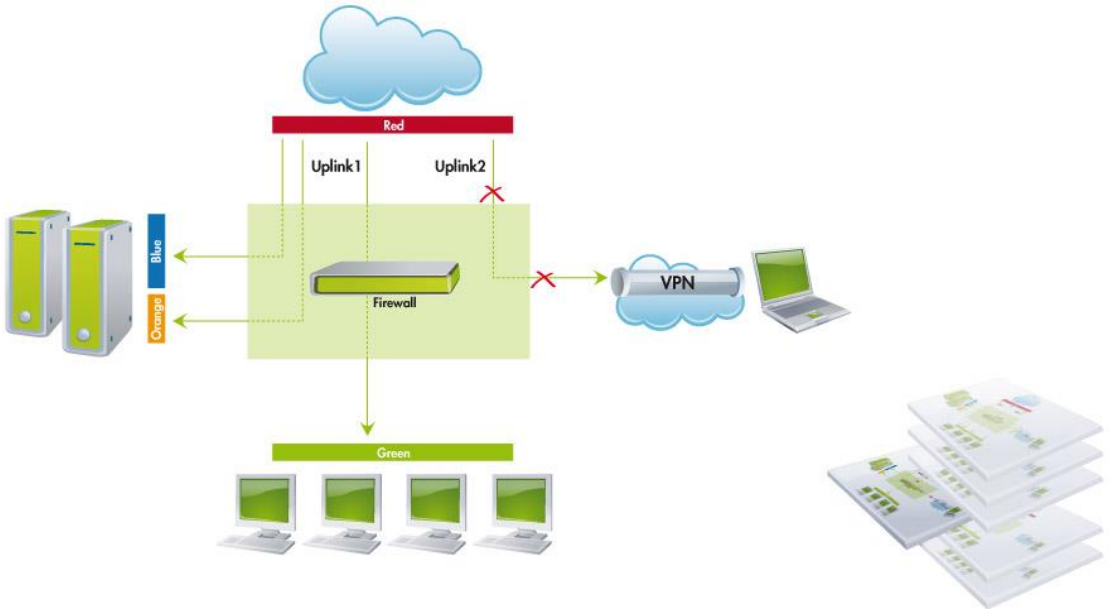


Mas abajo se grafica los modos de funcionamiento que soporta este firewall

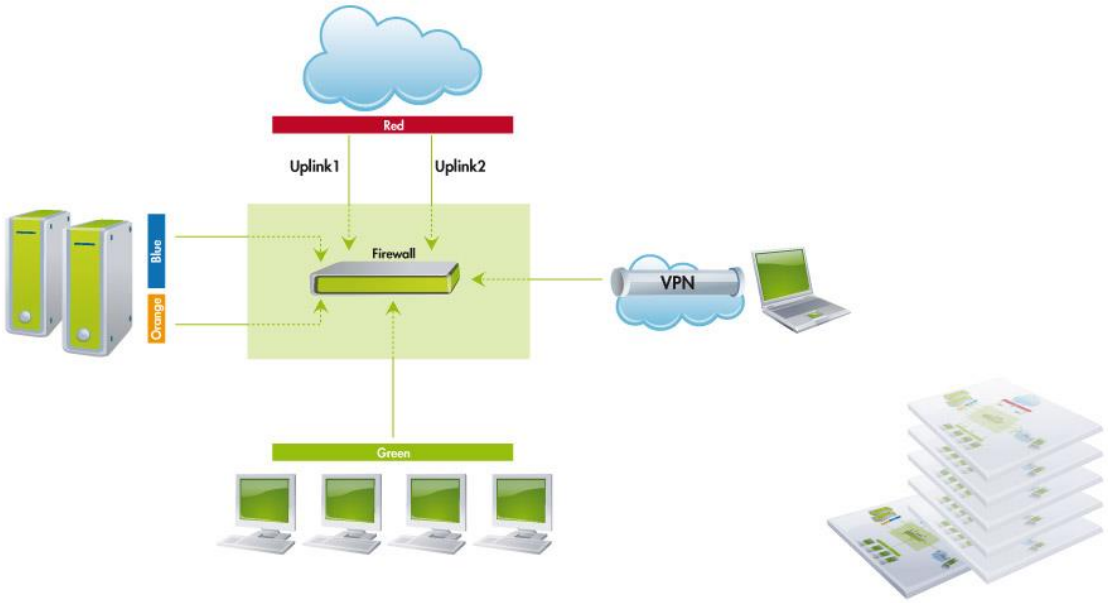
Inter-Zone traffic



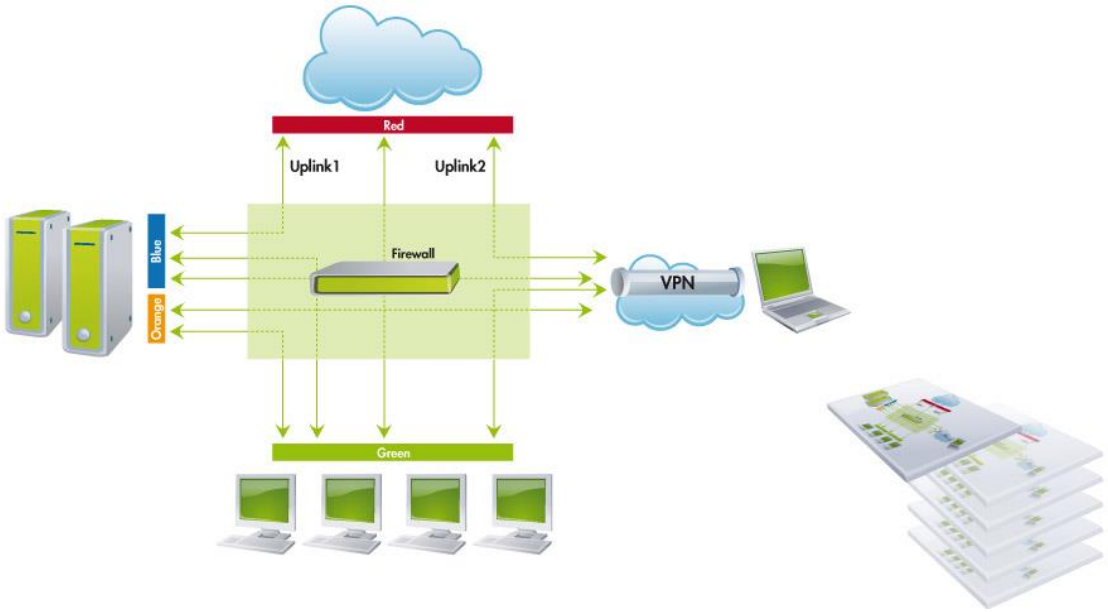
Routed Incoming Traffic



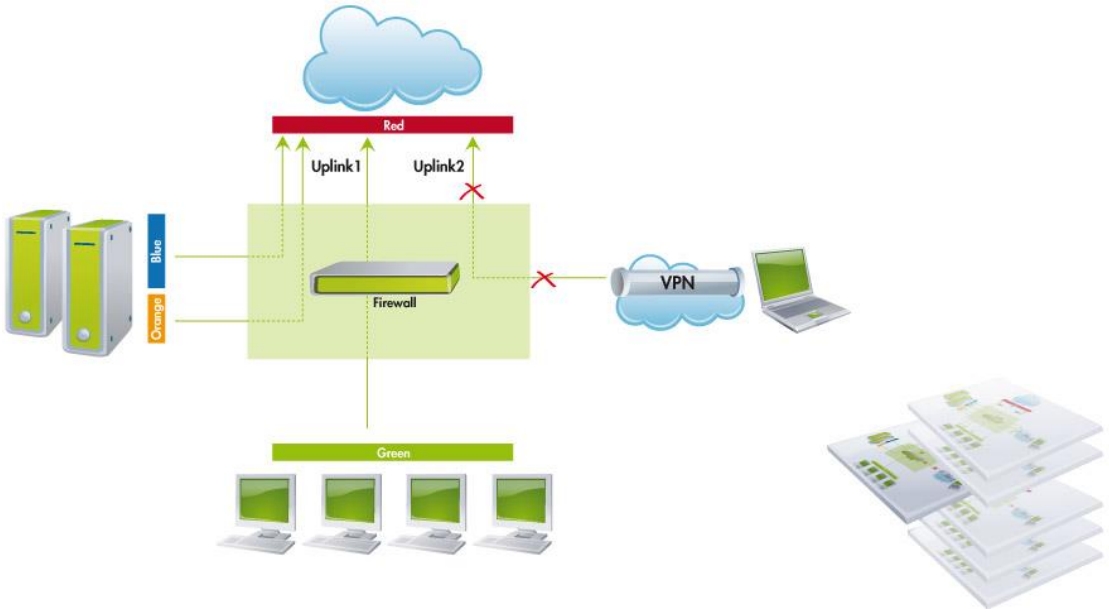
System access



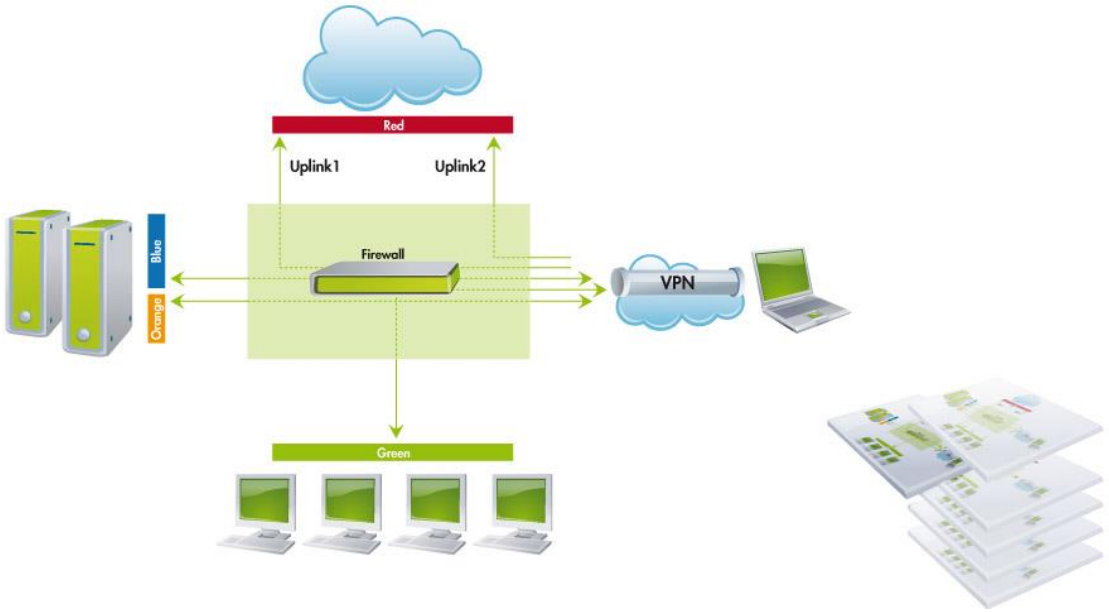
Port forwarding / NAT



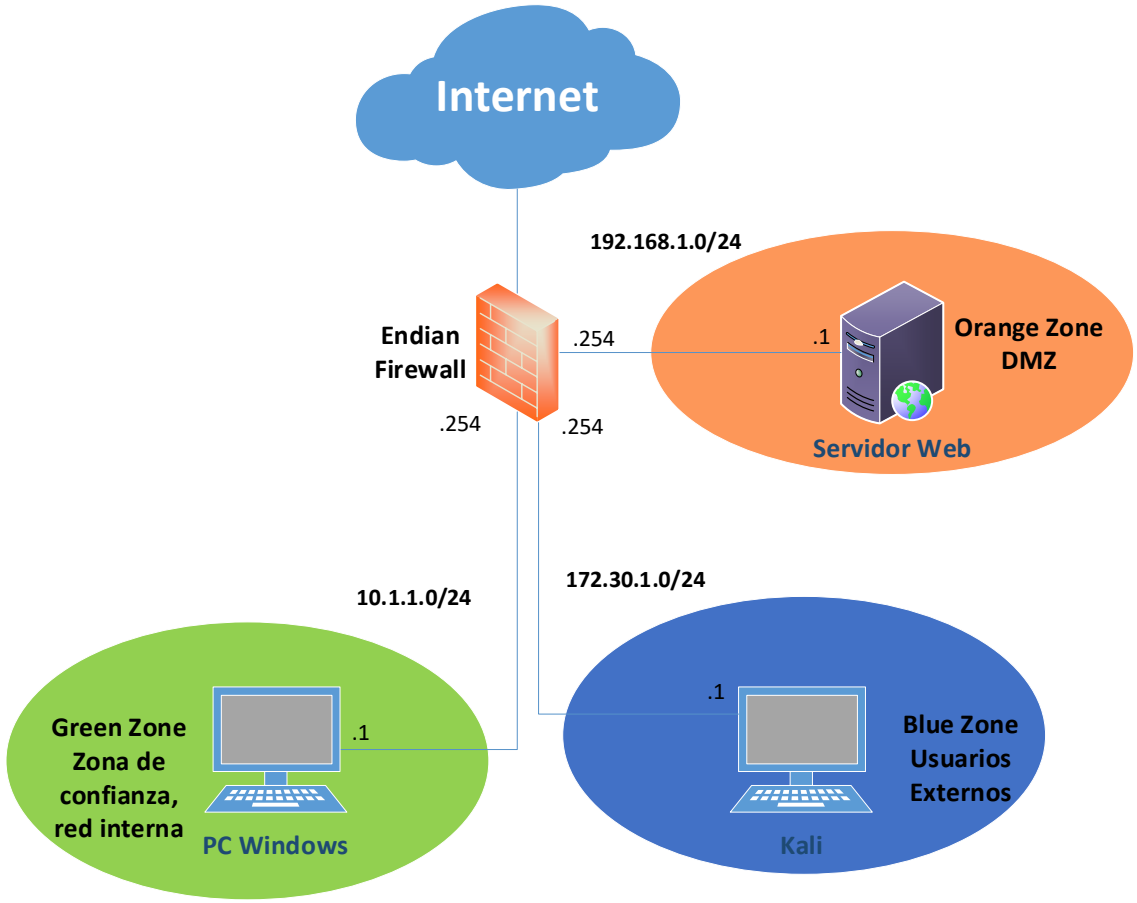
Outgoing traffic



VPN traffic



Arquitectura de Propuesta



Consideraciones:

I. El tercer octeto de cada segmento de red Ej. 192.168.xxx.0 tiene que ser de acuerdo a los dos últimos dígitos de se cedula de identidad, si termina en 99 seria 192.168.99.0, esto aplica para todas subredes.

II. El trabajo puede ser grupal, pero cada alumno deberá realizar en su propia maquina o de laboratorio, la entrega es individual y no se permite la entrega del mismo trabajo en la misma máquina.

III. Los avances de entrega serán indicadas por el profesor

