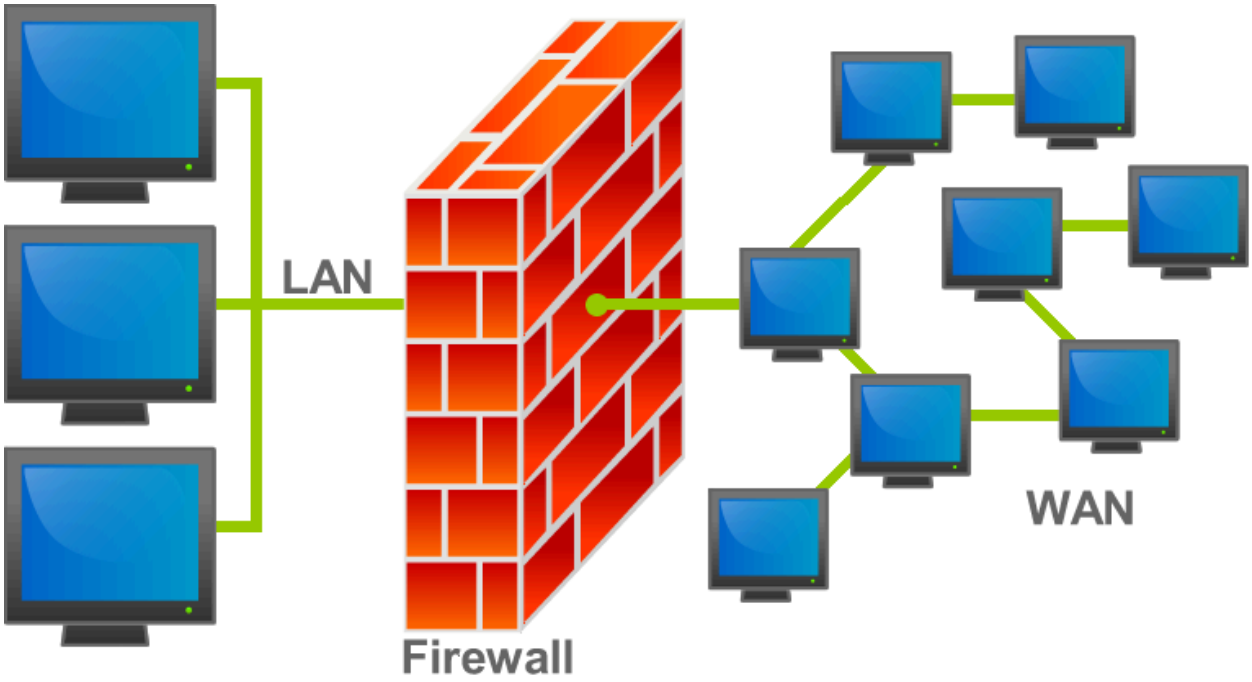
Laboratorio 6: Protección de redes mediante Firewall Cisco



Lara Reeves

2°C 2024
Redes Locales

1. Introducción

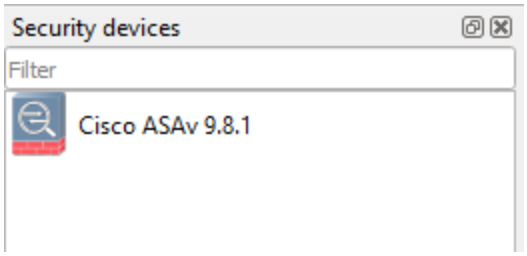
- Los Firewalls pueden ser implementados tanto en hardware como en software, en este caso, nos concentraremos claramente en la alternativa de software.
- Un Firewall o cortafuegos, añade seguridad a la red, pero de ninguna manera es la única herramienta que debemos utilizar.
- Por otro lado, tenemos a Cisco y sus Switches. Cisco es una empresa líder mundial en IT y el sector de redes, que se dedica principalmente a la interconexión de redes informáticas y comunicaciones.
- Aunque los dispositivos Cisco (tanto físicos como virtuales) no son gratuitos, resulta innegable su presencia en el mercado, e indispensable su aprendizaje para cualquier profesional del rubro.

2. Objetivo

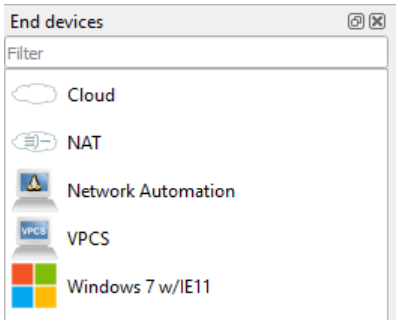
- Hacer una inducción en el mundo de la seguridad de las redes.
- Configurar desde cero un Firewall.

3. Procedimiento

- Se deben descargar e instalar dos appliances del marketplace de GNS3. Estas son Windows y Cisco ASAv. Adicionalmente se necesitará el archivo asav981.qcow2 para la imagen que utilizará Adaptive Security Virtual Appliance.

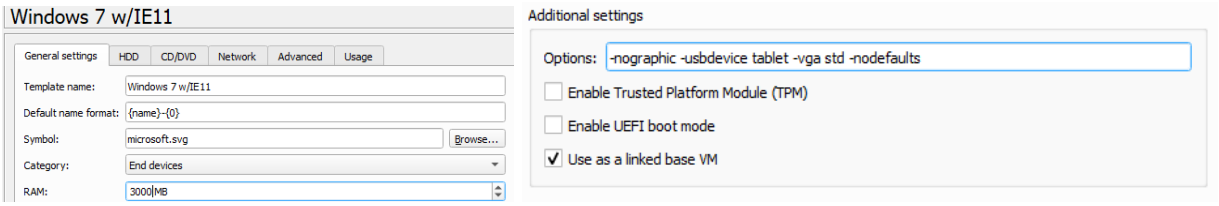


- Se debe importar la appliance de Windows. Para ello se recomienda tener el archivo IE11_-_Win7-disk1.vmdk previamente descargado en la misma carpeta, será necesario usar la opción Create a new version y darle OK. Una vez instalado el usuario para la vm es usuario y no posee password.

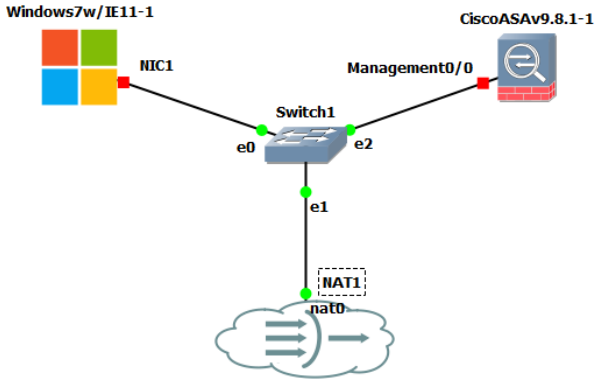


- Es necesario modificar el template de Windows 7. En la primera ocion se debe subir la

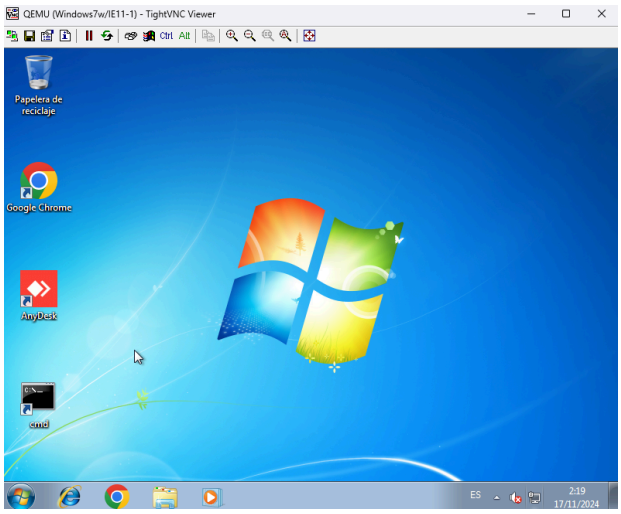
memoria RAM entre 2048 y 3000 para que windows 7 funcione fluido, y luego en la solapa advanced se debe ingresar la siguiente línea: *-nographic -usbdevice tablet -vga std -nodefaults* ya que sirve para manejar correctamente el windows.



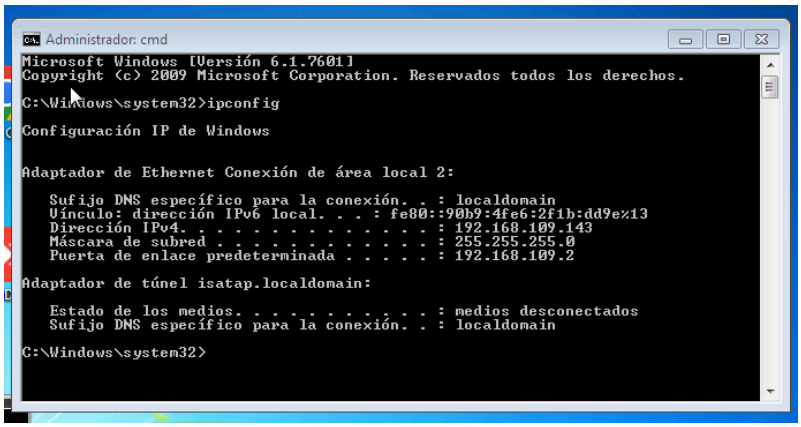
- Es necesario colocar el archivo descargado IE11_-_Win7-disk1.vmdk en la carpeta: C:\Users\<Usuario>\GNS3\images\QEMU
- Se crea una topología “incorrecta”, pero la cual es necesaria para terminar de configurar el entorno virtual.



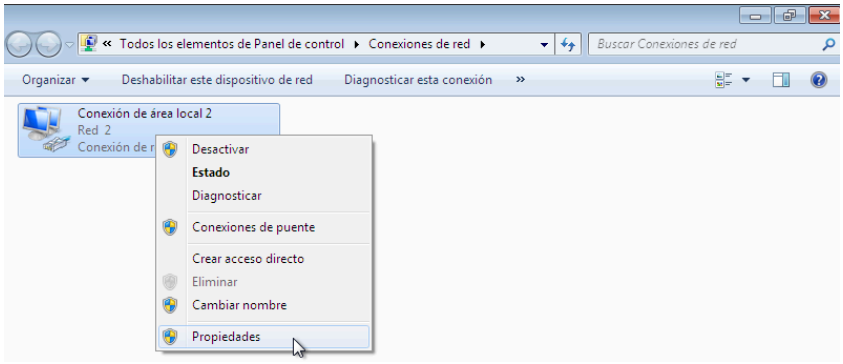
- Se inician todos los dispositivos y se deja que Windows instale todos sus drivers y actualizaciones, y se permite que CiscoASAv se reinicie 2 veces.



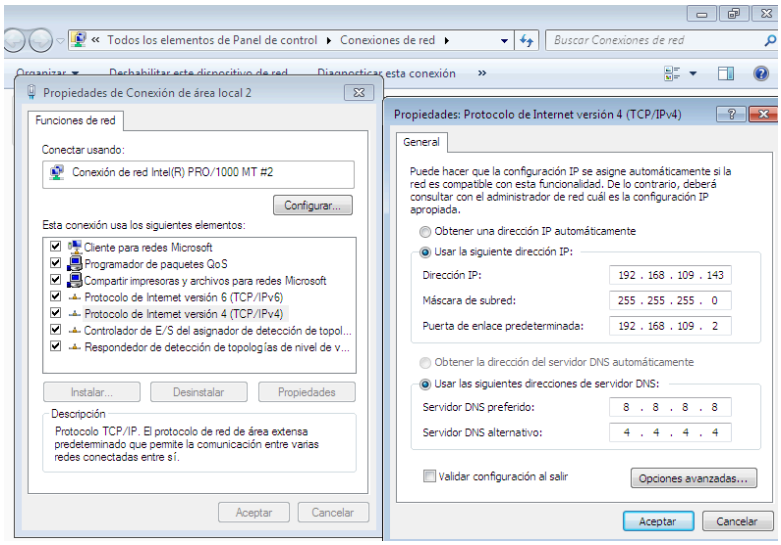
- Se abre la consola de comandos de Windows CMD. Una vez adentro se podrá ver que se le asignó una IP automáticamente vía DHCP.



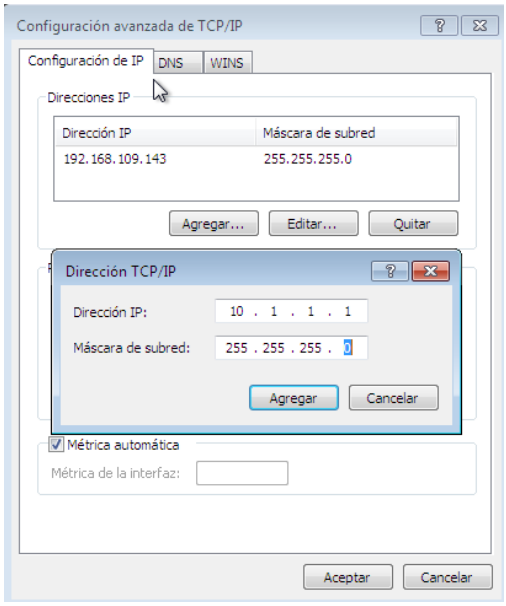
- Luego se configura la placa de forma estática, para ello se vuelve a ingresar a la ventana de ejecutar y se escribe ncpa.clp



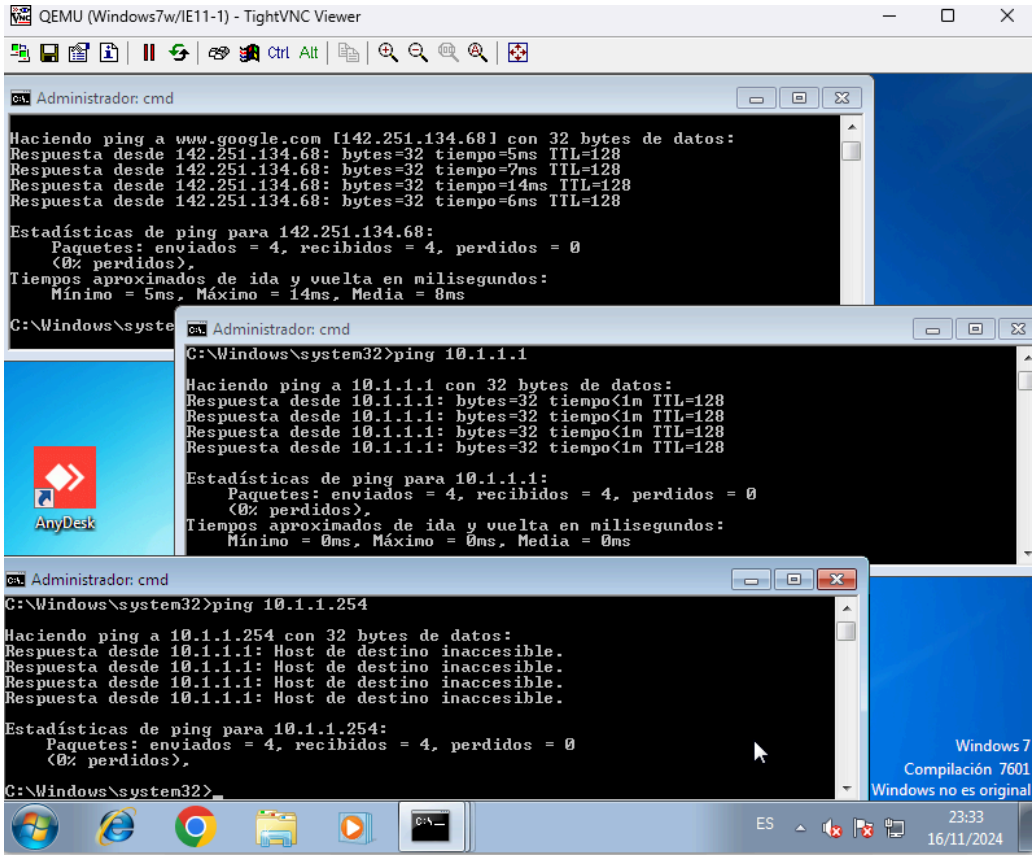
- La asignación estática se realiza a fin de que no cambie la dirección asignada al host de Windows.



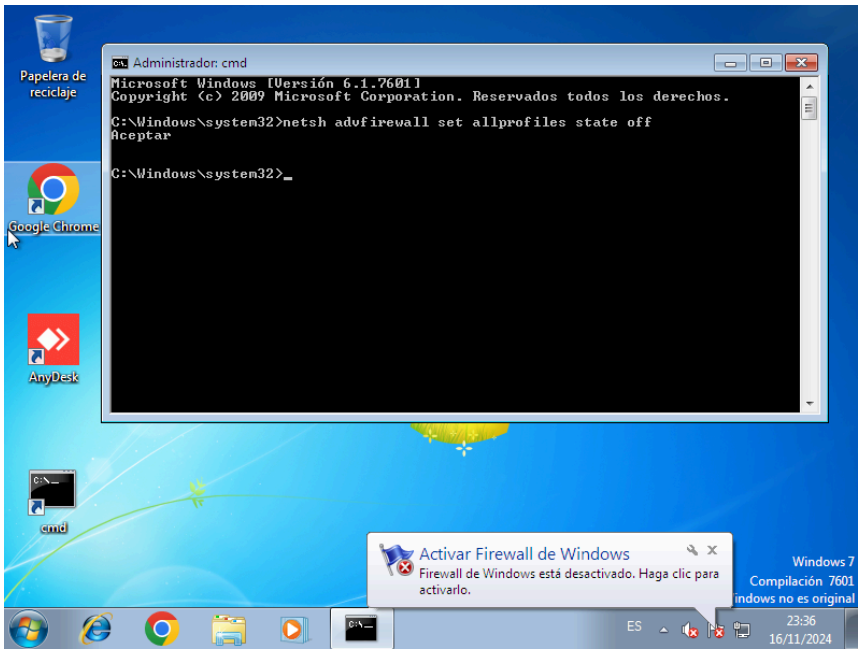
- Luego se hace clic en Opciones Avanzadas para ingresar otra dirección IP que será necesaria para comunicarse con Cisco ASAv.



- Una vez finalizados los pasos anteriores, se puede realizar un PING tanto a google, así como a la conexión interna, pero no al dispositivo Cisco.



- Ahora se procede a desactivar el firewall de Windows, ya que se utilizara el provisto por Cisco. Para realizar esto se utiliza el comando netsh advfirewall set allprofiles state off, el sul es ejecutado mediante una terminal CMD con privilegios de administrador. Una vez terminado el comando debe aparecer el mensaje de advertencia de que el firewall de windows fue desactivado.



- Se vuelve a la terminal de Cisco y se corren los siguientes comandos:

```
ciscoasa(config)# int g0/1
ciscoasa(config-if)# int g0/0
ciscoasa(config-if)#
Warning: ASAv platform license state is Unlicensed.
Install ASAv platform license for full functionality.

ciscoasa(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
ciscoasa(config-if)# ip address 10.1.1.254 255.255.255.0
ciscoasa(config-if)# no shut
ciscoasa(config-if)# end
ciscoasa# _
```

- Ahora se realiza PING a la VM de Windows:

```
ciscoasa# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

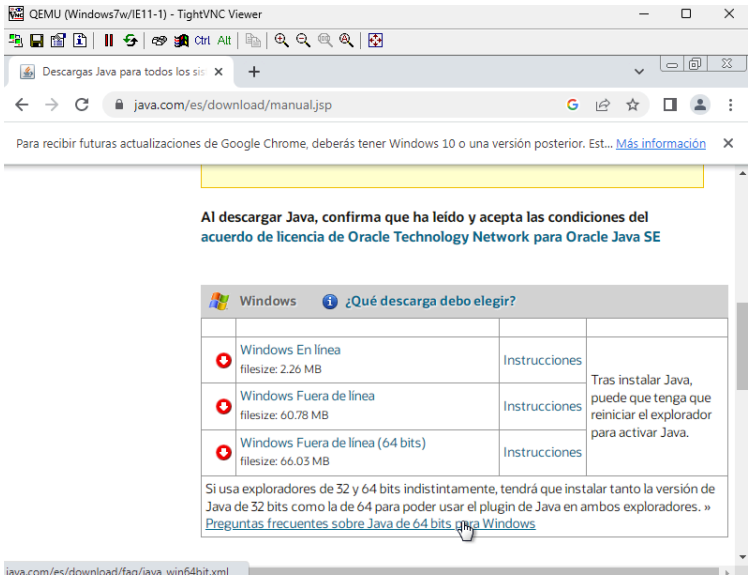
- Desde Windows a Cisco:

```
C:\Windows\system32>ping 10.1.1.254

Haciendo ping a 10.1.1.254 con 32 bytes de datos:
Respuesta desde 10.1.1.254: bytes=32 tiempo=1ms TTL=255
Respuesta desde 10.1.1.254: bytes=32 tiempo<1m TTL=255
Respuesta desde 10.1.1.254: bytes=32 tiempo<1m TTL=255
Respuesta desde 10.1.1.254: bytes=32 tiempo<1m TTL=255

Estadísticas de ping para 10.1.1.254:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms
```

- Se configura el Cisco ASAv

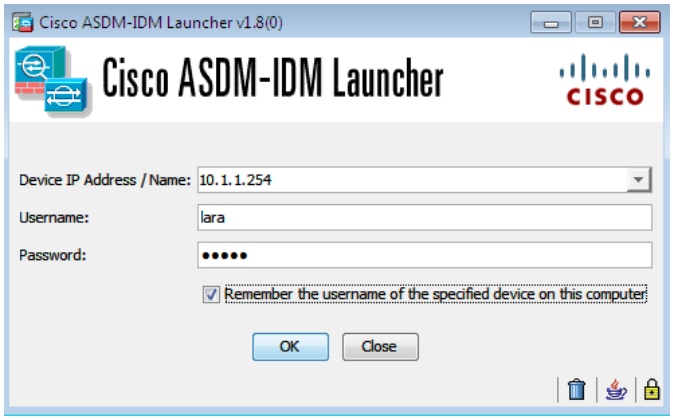
```
ciscoasa# conf t
ciscoasa(config)# username lara password cisco privilege 15
ciscoasa(config)# http server enable
ciscoasa(config)# http 0 0 inside
ciscoasa(config)# end
```

- Se procede con la instalación de Java en Windows, la opción a elegir es “Windows Fuera de línea”

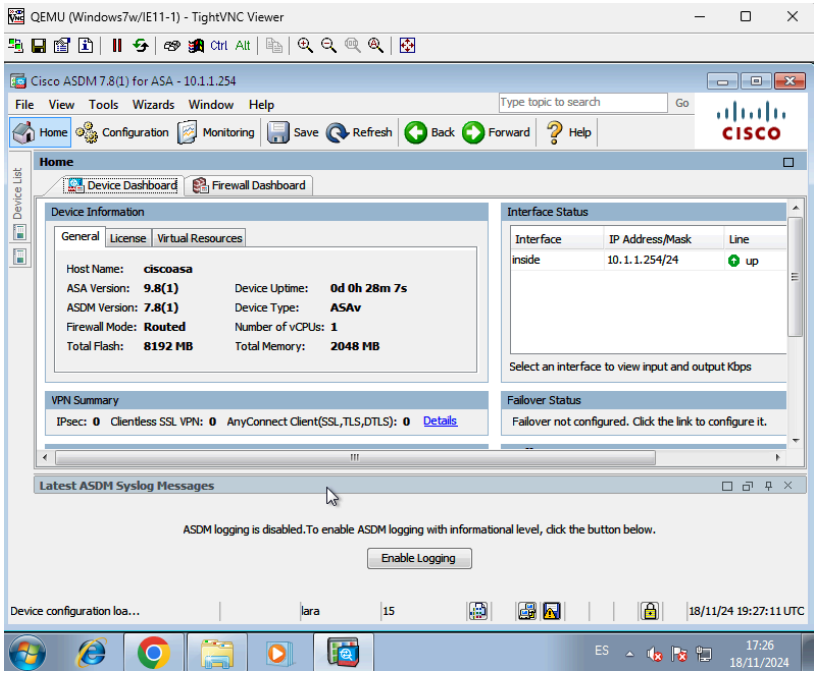


- Se instala el controlador de Cisco. Para ello debemos utilizar el usuario y contraseña que previamente se configuraron.

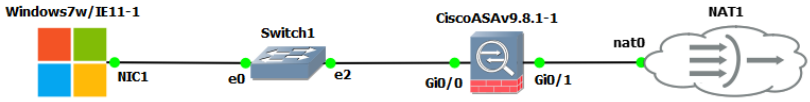
- Una vez instalado se ingresan los siguientes datos:



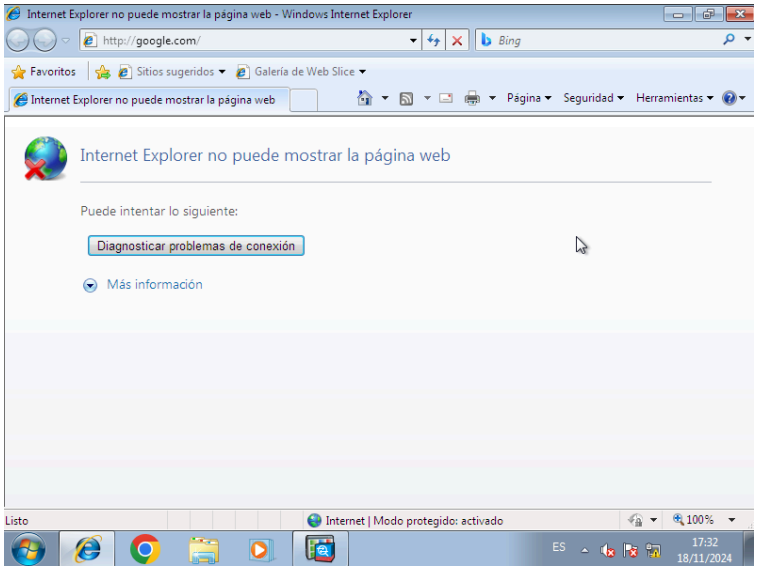
- Se debe ignorar el mensaje estilo popup que indica la falta de una licencia activa para ASAv, por lo cual el tráfico estará limitado, tanto en términos de velocidad, como número de conexiones, esto no es un impedimento para realizar el laboratorio. La aplicación nos dará información relevante como: versión, uso de recursos, uptime del dispositivo, etc. También se pueden habilitar los logs para mantener datos históricos de lo registrado por el dispositivo:



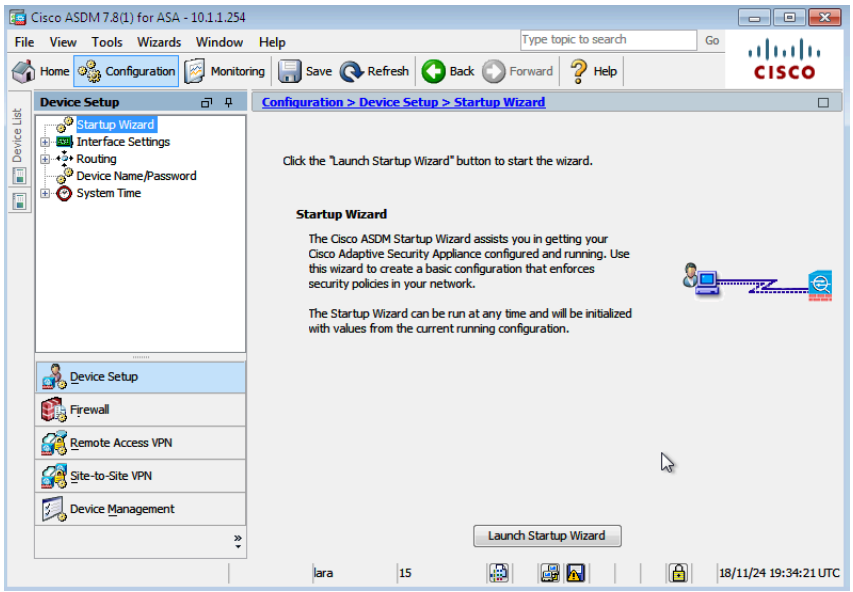
- Una vez realizadas todas las instalaciones necesarias se arregla la topología. De esta manera, lo que hacemos es que todo el tráfico desde y hacia el exterior tenga que pasar obligatoriamente por el Firewall de Cisco.

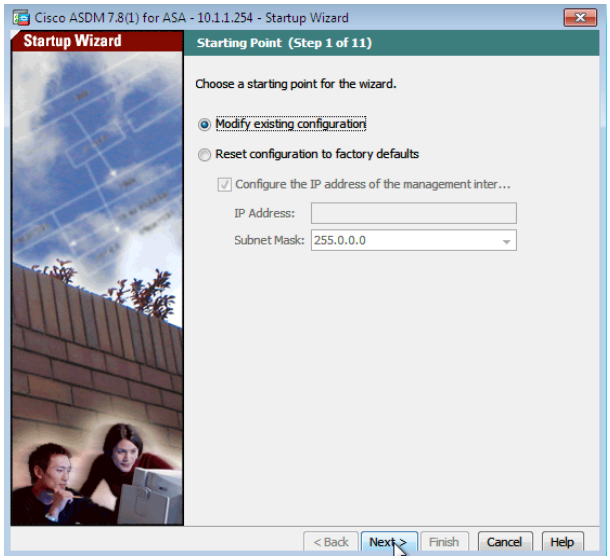


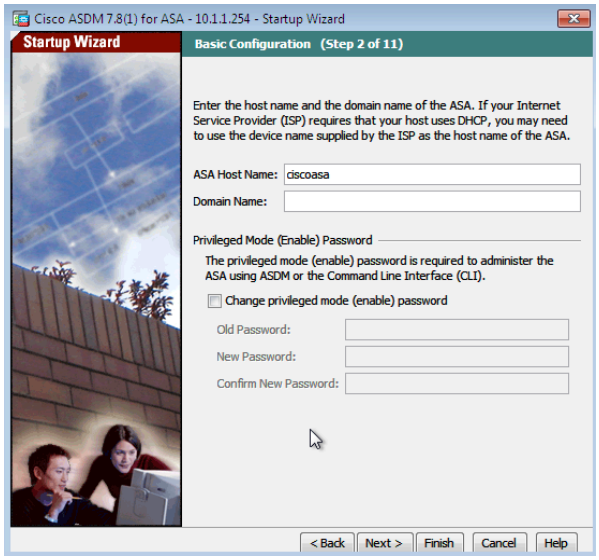
- Se necesita configurar el Firewall de tal manera que acepte tráfico saliente, porque si se intenta nuevamente acceder a alguna página de internet, no es posible:



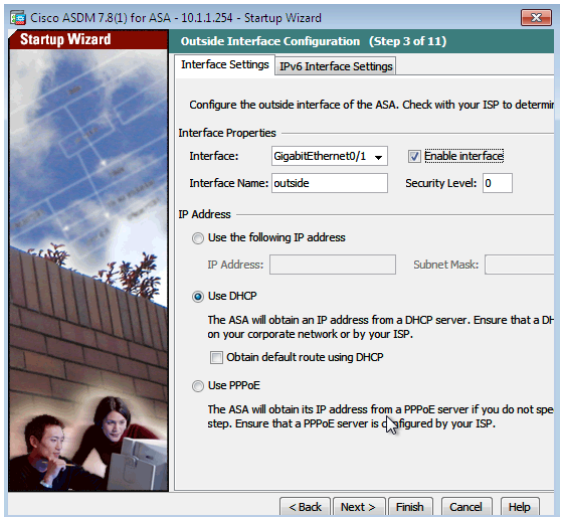
- Se realiza la configuración, para eso se vuelve a la aplicación Cisco ASDM. **Configuration > Launch Startup Wizard**:



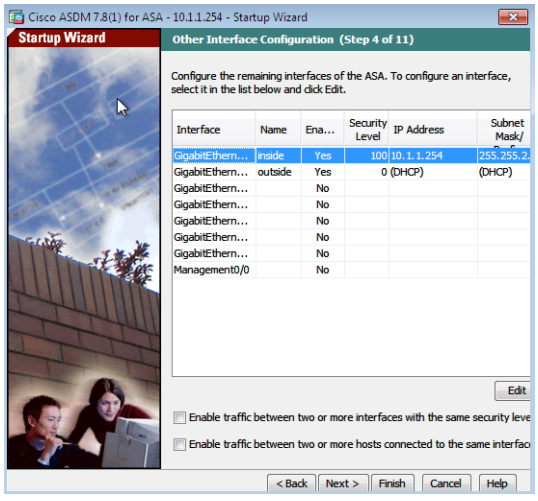




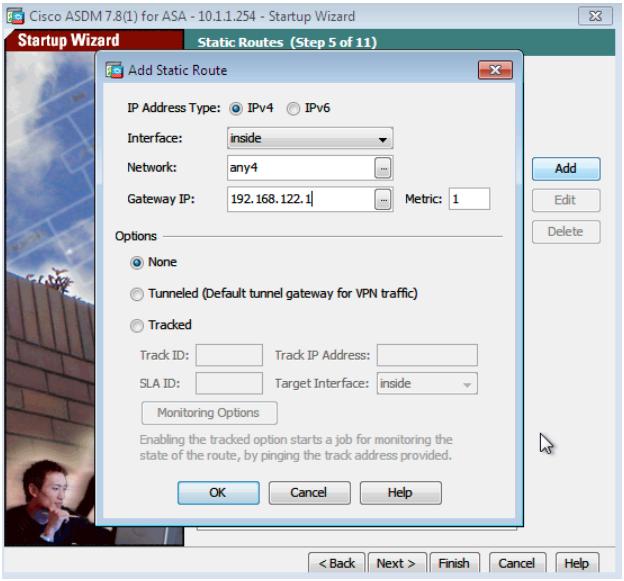
- Se crea la interfaz outside para permitir el tráfico entrante externo.



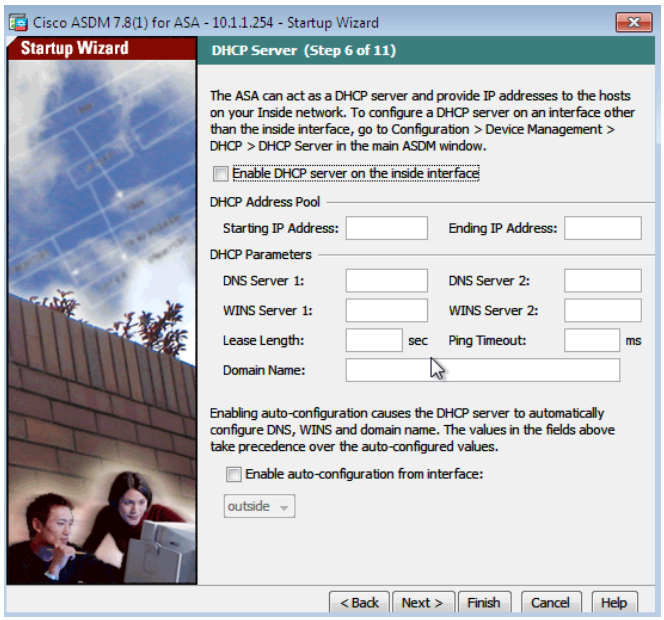
- Se va a las configuraciones que se habian hecho previamente en el adaptador inside



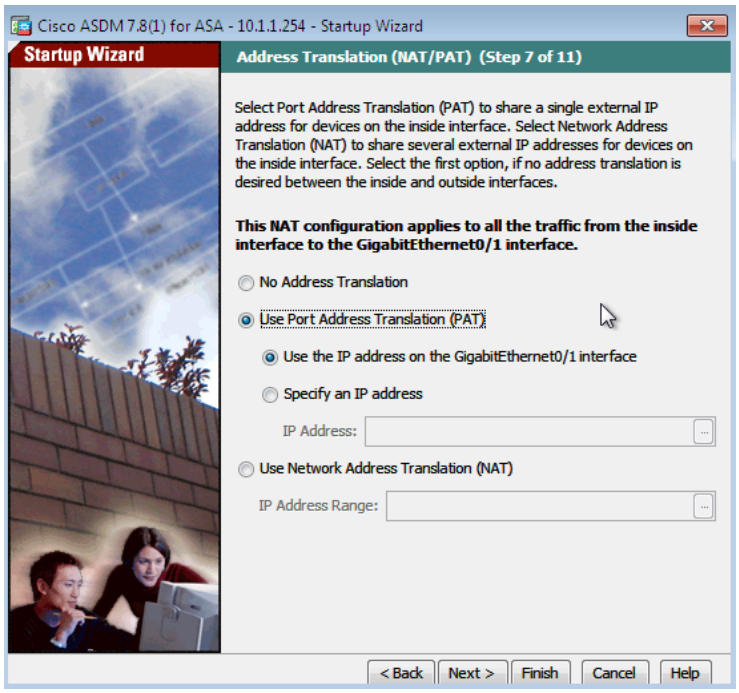
- Luego de hacer clic en next iremos a “Static Routes” y se define una ruta estática por defecto para el outside adapter.



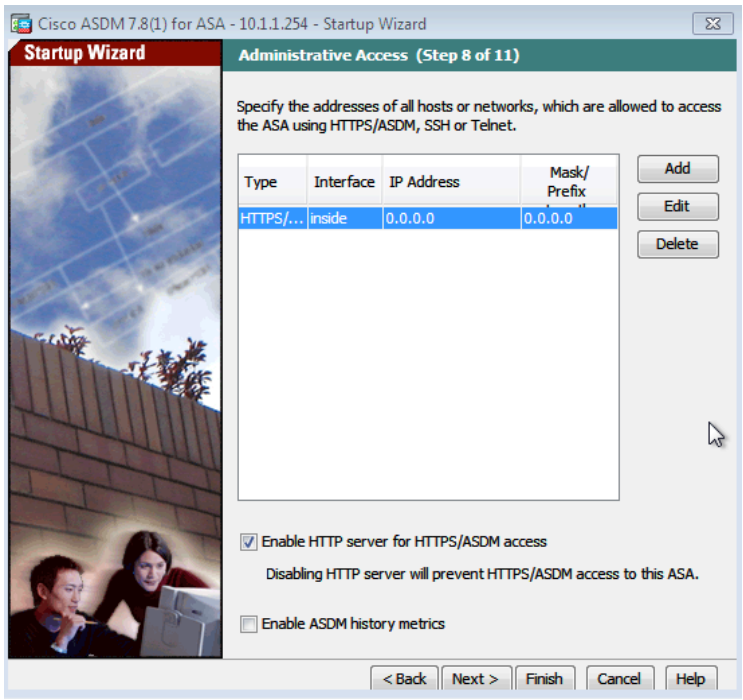
- No se habilita nada en la siguiente pantalla:



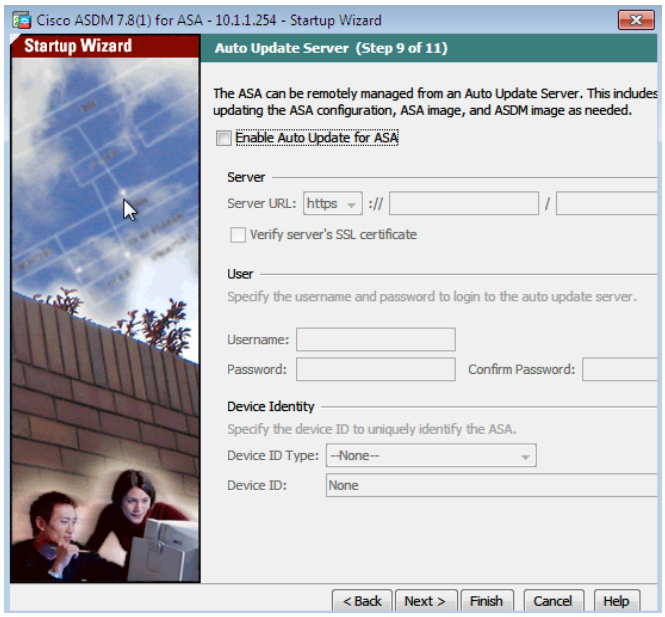
- Se habilita el Port Address Translation (PAT), para que el inside host pueda comunicarse con el exterior.

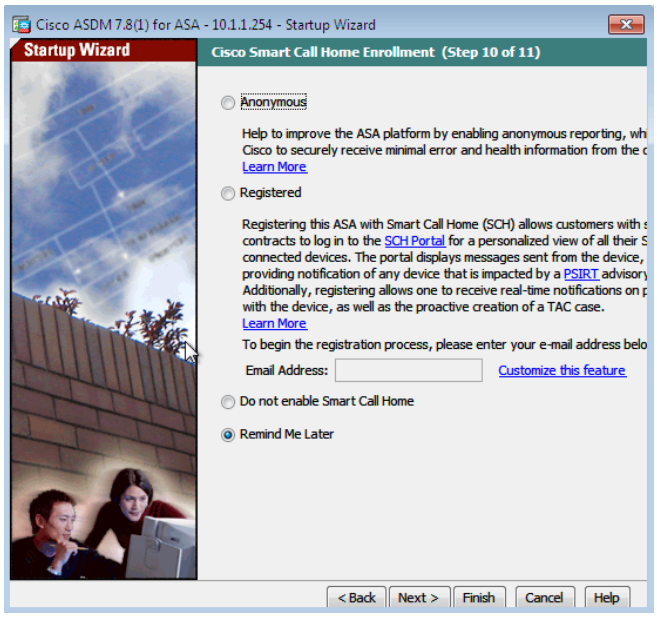


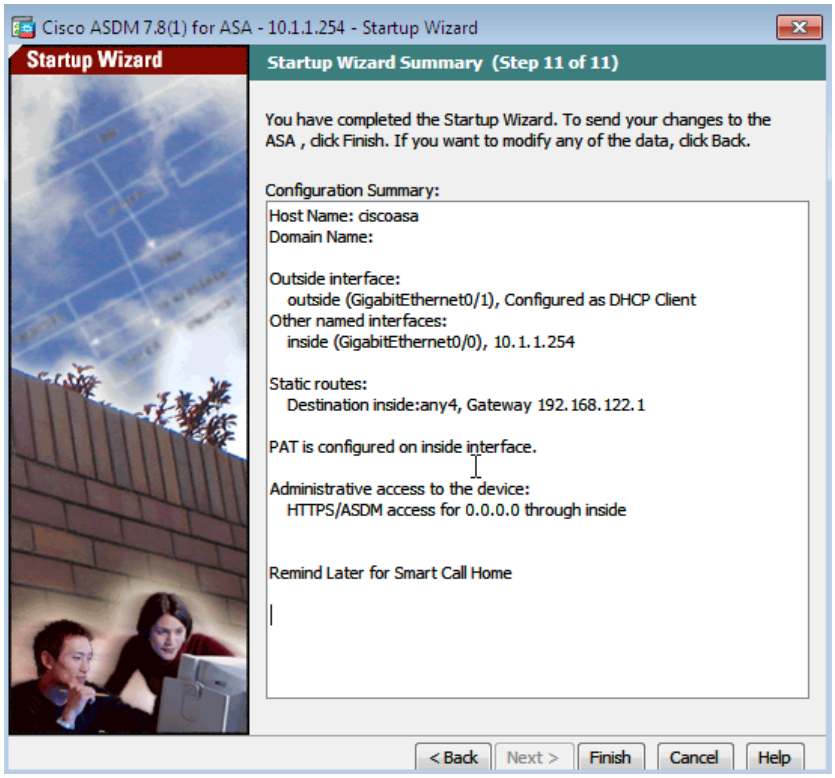
- Se mantiene habilitado el acceso mediante HTTP a Cisco ASAv.



- Se dejan las siguientes opciones como vienen por defecto, y se llega al resumen de la configuración.



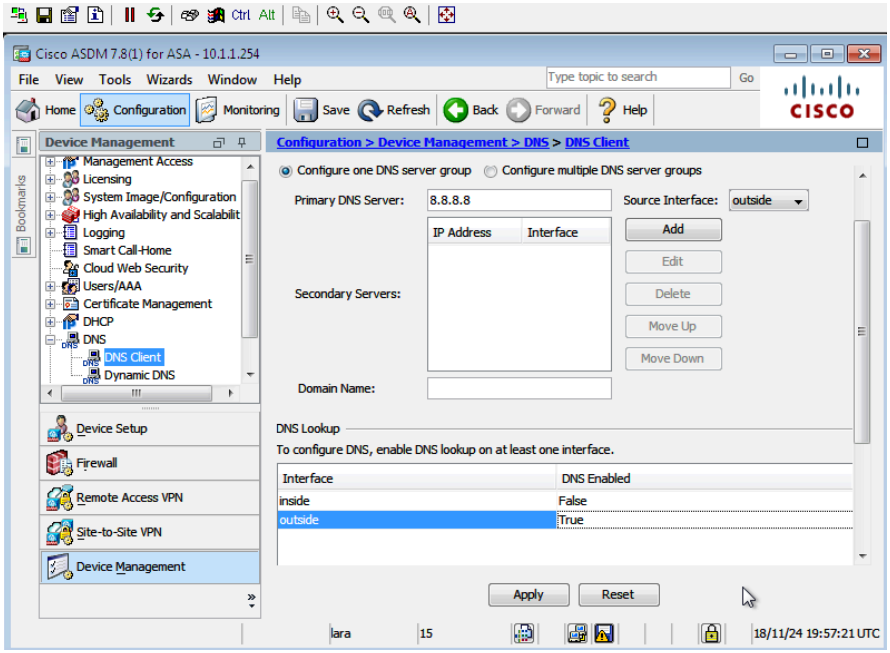




- se puede verificar mediante el comando sh run en la terminal Cisco ASAv que la interfaz de afuera fue generada

```
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.1.1.254 255.255.255.0
!
interface GigabitEthernet0/1
 nameif outside
 security-level 0
 ip address dhcp
!
```

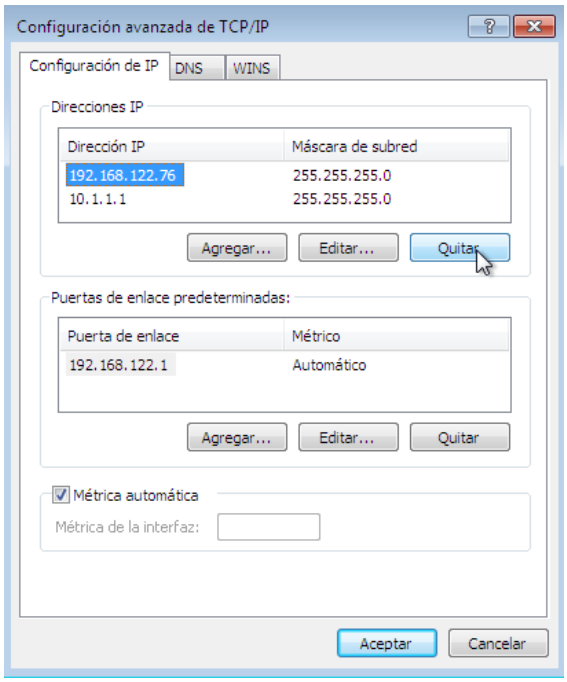
- Lo último que resta configurar es la configuración de DNS para el Firewall



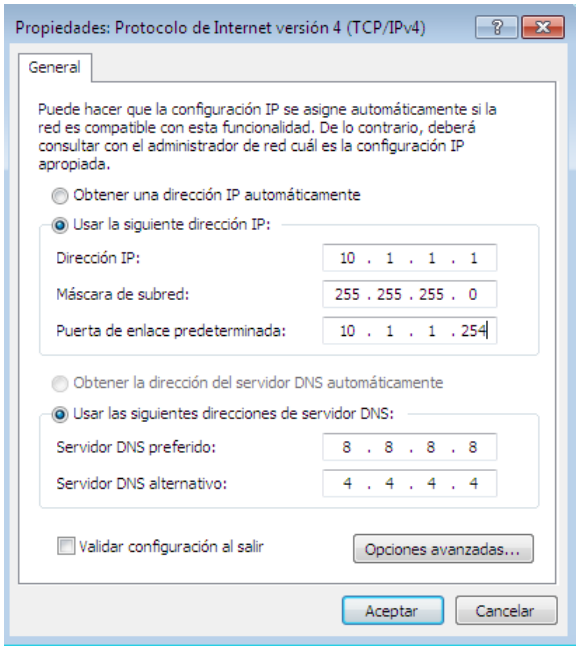
- Si se intenta hacer un ping a google, el resultado es positivo.

```
ciscoasa# ping www.google.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 142.251.134.68, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/12/20 ms
ciscoasa#
```

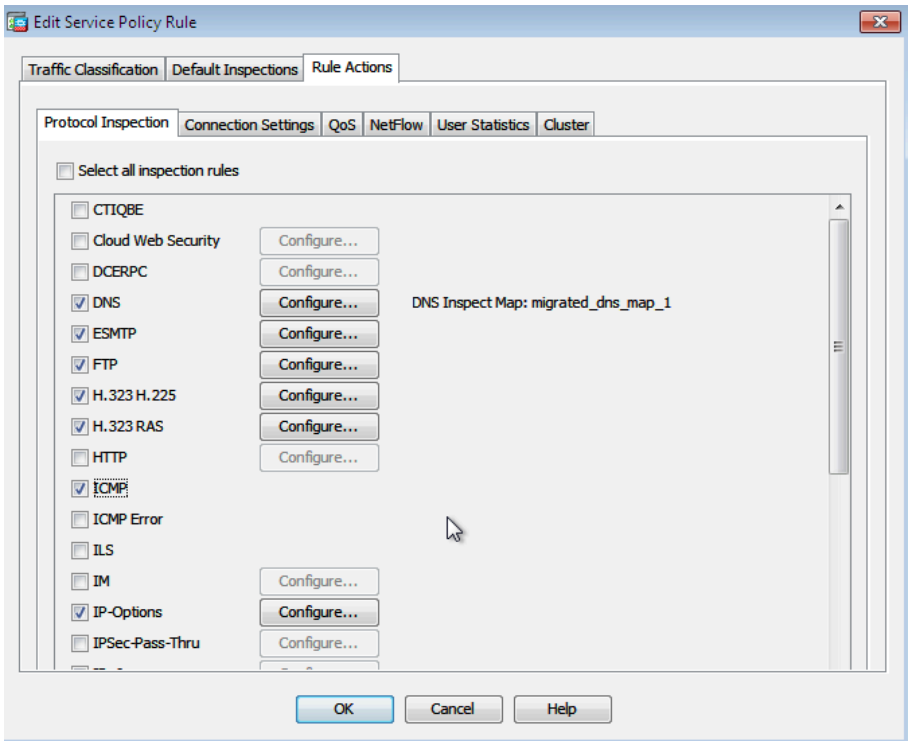
- Todavía no se puede conectar desde Windows. Para ello, se debe volver nuevamente a la configuración del Network Adapter, y modificar los siguientes parámetros: Removemos la antigua IP estática que habíamos configurado, dejando sólo 10.1.1.1:



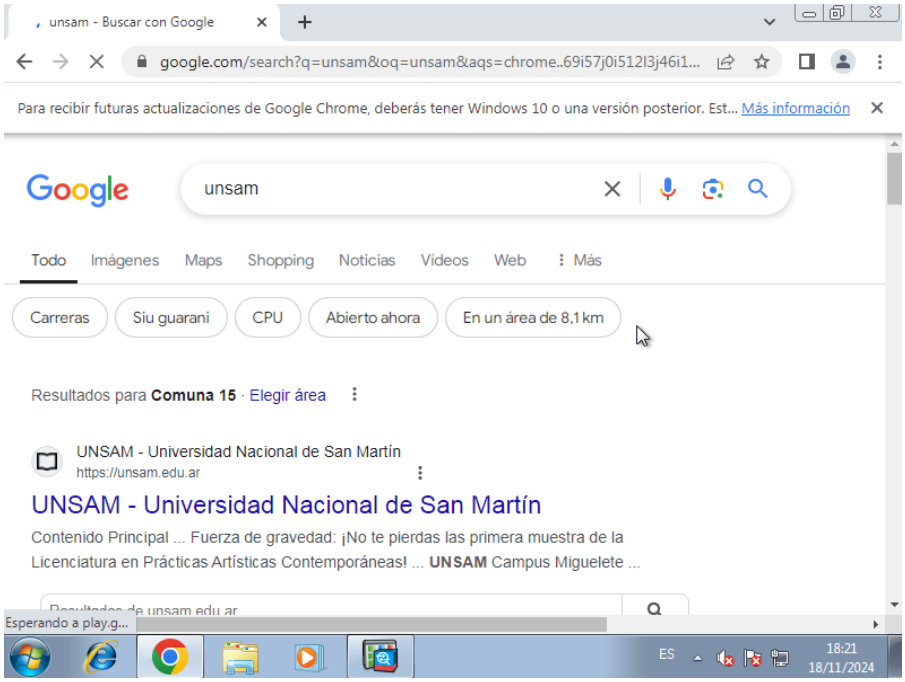
- Se modifica el Default gateway para que utilice el Firewall de Cisco



- Por último, se debe habilitar el tráfico ICMP, sino es descartado por defecto. Firewall → Service Policy Rule → Edit



- Una vez guardados los cambios, se puede acceder a Google



- Ahora

```
ciscoasa# conf t
ciscoasa(config)# object network obj-facebook.com
ciscoasa(config-network-object)# fqdn facebook.com
ciscoasa(config-network-object)# object network obj-wwwfacebook.com
ciscoasa(config-network-object)# fqdn www.facebook.com
ciscoasa(config-network-object)# object-group service my_facebook_service
ciscoasa(config-service-object-group)# service-object ip
ciscoasa(config-service-object-group)# service-object tcp destinarion eq http
                                                      ^
ERROR: % Invalid input detected at '^' marker.
ciscoasa(config-service-object-group)# service-object tcp destination eq http
ciscoasa(config-service-object-group)# service-object tcp destination eq https
ciscoasa(config-service-object-group)# exit
ciscoasa(config)#
```

```
ciscoasa(config)# object-group network blockfacebook
ciscoasa(config-network-object-group)# network-object object obj-facebook.com
ciscoasa(config-network-object-group)# network-object object obj-wwwfacebook.c$
ciscoasa(config-network-object-group)# end
ciscoasa#
```

```
ciscoasa# conf t
ciscoasa(config)# access-list acl-inside line 1 extended deny object-group my_$
ciscoasa(config)# access-list acl-inside line 2 extended permit ip any any log
ciscoasa(config)# access-group acl-inside in interface inside
ciscoasa(config)# end
ciscoasa# _
```

-

4. Cuestionario

1- ¿Por qué es “incorrecta” la topología utilizada en el paso Armado de Topología para Setup? Justifique.

La primera topología utilizada presenta una configuración incorrecta, ya que el NAT permite la conexión hacia el exterior y también facilita el acceso desde el exterior hacia la red interna. Sin embargo, al no estar conectado al firewall de Cisco, cualquier tráfico que ingrese desde el exterior puede acceder directamente a las redes internas, lo que genera una significativa vulnerabilidad en términos de seguridad.

En la segunda topología, al conectar el NAT al firewall, se establece una "barrera" que protege la red interna del acceso no autorizado desde la red externa, fortaleciendo así la seguridad del sistema.

2- ¿Qué diferencias encuentra entre el dispositivo de seguridad provisto por Cisco, y otra opción como podría ser la alternativa de Fortinet?

Criterio	Cisco ASAv	Fortinet
Arquitectura y Enfoque	Versión virtual del firewall Cisco ASA, diseñada para entornos de nube. Ofrece firewall avanzado, VPN y prevención de intrusiones, con integración fluida en soluciones Cisco.	Gestión unificada de amenazas (UTM) que combina firewall, VPN, antivirus y prevención de intrusiones en un solo dispositivo. Escalable para empresas de cualquier tamaño.
Facilidad de Uso y Configuración	Más complejo de configurar, dirigido a usuarios avanzados que aprovechen su potente CLI.	Interfaz gráfica intuitiva y fácil de usar, ideal para administradores que prefieren una gestión visual.
Rendimiento y Escalabilidad	Alto rendimiento en entornos virtuales y de nube. Integra perfectamente con otras soluciones de Cisco.	Escalable y capaz de manejar grandes volúmenes de tráfico. Ofrece firewall de próxima generación sin comprometer el rendimiento.
Costo	Precio generalmente más alto, adecuado para organizaciones con mayor presupuesto.	Solución más asequible, ideal para empresas con presupuestos ajustados.

3- ¿Por qué es importante contar con un Firewall entre la red interna y la red externa? ¿Qué otras medidas de seguridad podría tomar como administrador de una red?

Contar con un firewall entre la red interna y externa es fundamental para garantizar la seguridad de la infraestructura. Este dispositivo actúa como una barrera que filtra el tráfico, bloqueando accesos no autorizados y amenazas externas. Además, permite establecer políticas de control de acceso para asegurar que solo usuarios y dispositivos autorizados puedan interactuar con la red interna. Los firewalls también registran y monitorean el tráfico, detectando patrones sospechosos e intentos de intrusión, y ayudan a prevenir la fuga de datos sensibles.

Para complementar la seguridad, se pueden implementar medidas adicionales. Mantener sistemas actualizados con parches protege contra vulnerabilidades conocidas. La autenticación multifactor añade una capa de protección al acceso de sistemas críticos. Es crucial cifrar datos sensibles. Finalmente, realizar copias de seguridad regulares asegura la recuperación ante incidentes de seguridad.

4- ¿Por qué es importante contar con distintas opciones para automatizar redes?

En primer lugar, ofrece flexibilidad y adaptabilidad al permitir que los administradores elijan herramientas y bibliotecas según las necesidades específicas de su infraestructura, optimizando cada tarea. Además, reduce errores humanos al minimizar la intervención manual, lo cual es crucial en redes complejas donde los errores pueden ser costosos. También mejora la eficiencia al realizar tareas repetitivas rápidamente, liberando tiempo para actividades estratégicas.

La automatización garantiza consistencia en las configuraciones, siguiendo estándares predefinidos que fortalecen la seguridad e integridad de la red. Asimismo, facilita la escalabilidad, permitiendo gestionar redes más grandes sin aumentar significativamente los recursos humanos. Por último, fomenta la innovación y la mejora continua, brindando a los administradores la posibilidad de explorar y adoptar nuevas tecnologías para optimizar la gestión de redes.

5- ¿Contar con un Firewall es la solución a todos nuestros problemas? ¿Cómo combatiría un ataque originado desde nuestra misma red local (por ejemplo, un intento de hackeo desde un pendrive)?

Contar con un firewall no resuelve todos los problemas de seguridad en la red, ya que está diseñado principalmente para proteger contra amenazas externas. Sin embargo, ataques originados dentro de la red local, como aquellos mediante un pendrive infectado, requieren estrategias adicionales para una defensa integral.

Una medida clave es el uso de antivirus y antimalware actualizados en todos los dispositivos, para detectar y neutralizar software malicioso. Además, implementar políticas de control de dispositivos USB, como desactivar puertos no autorizados o monitorear su uso, puede prevenir la introducción de malware. También es útil incorporar sistemas de detección y prevención de intrusiones (IDS/IPS) que analicen actividades sospechosas y actúen en tiempo real.

5. Bibliografía

- Fortinet VS Cisco: ¿Cuál es la mejor opción? - Nsit
- Cisco Systems vs Fortinet 2024 | Gartner Peer Insights