EJERCICIO 2

1. OBJETIVO:

En el presente ejercicio se procederá a configurar un túnel VPN “Acceso Remoto”. Esta práctica trata de representar un escenario en el que un técnico de una empresa externa tiene que tener acceso a la máquina de su cliente para darle servicio remoto. Empleará el sistema corporativo que tiene su cliente.

2. PASOS A SEGUIR:

Nos conectaremos al equipo FGT-01 y FGT-02 en alguna de sus interfaces con las credenciales admin/icslab.

Cargaremos el fichero de configuración para borrar la configuración del otro grupo. Para ello iremos al menú de “admin” en la esquina superior derecha y localizaremos la palabra “Restore” y elegiremos el fichero de configuración “FGT-01-Inicio ejercicio” y “FGT-02-Inicio ejercicio”. El equipo se reiniciará.

Verificaremos que sólo hay una regla configurada que es la que permite la comunicación desde la red interna hacia el exterior. No se permite el tráfico entrante a los equipos de la máquina en los segmentos 10.2.201.0/24 y 10.2.202.0/24.

En primer lugar, crearemos un grupo en “User and Authentication” llamado “icslab-vpn-users”.

Luego crearemos dos usuarios que llamaremos “vpn01” y “vpn02” y los haremos miembros del grupo que hemos creado anteriormente. La contraseña será “icslab2025$”

Allí nos dirigiremos al menú “VPN – IPSec Tunnels” para configurar el equipo para que reciba conexiones entrantes empleando el protocolo IPSec.

En la parte superior pincharemos en “Create New – IPSec Tunnel”.

Una vez allí le daremos las siguientes características:

- Le llamaremos vpn-ipsec-01.
- Como plantilla, no vamos a utilizar ninguna, sino que será una configuración manual.

En el siguiente menú tendremos en cuenta que:

- No habrá un “Gateway remoto” sino que será bajo la petición de los usuarios.
- La interfaz por donde van acceder esos usuarios será por la interfaz “WAN1”.

- Tendremos que habilitar el “Modo de Configuración” para poder definir el rango de direcciones IP que asignará el equipo Fortigate a los usuarios que se conecten por VPN. En el caso del Fortigate-01 será de la IP 10.11.11.10 a la 10.11.11.20 y en el Fortigate-02 de la IP 10.22.22.10 a la 10.22.22.20.
- Dejaremos habilitado el NAT Transversal ya que puede haber elementos que hagan una traducción de nombres de red.
- El método de autenticación deberá ser contraseña compartida y ésta será “icslab2025$”
- El modo será “Agresivo”.
- El “grupo de usuarios” será el que hemos creado anteriormente y al que pertenecen vpn01y vpn02.
- En la Fase 1 como algoritmo de cifrado emplearemos AES256 y como autenticación SHA512. El resto los vamos a eliminar.
- Como Grupo Diffie-Hellman elegiremos sólo el 14.
- En el apartado de “XAuth” deberemos indicar que el firewall hará de servidor, por así decirlo, automático, y que emplee el grupo de usuarios que hemos elegido antes.
- En la Fase 2 habrá que indicar que tanto las redes locales como remotas incluyan todas las posibles redes.
- Como algoritmos aquí emplearemos como cifrado AES192 y de autenticación SHA 256. El grupo Diffie-Hellman será el mismo.
- Finalmente le damos a “OK” y lo guardamos.

Luego deberemos ir a nuestro equipo cliente, el PC con Forticlient instalado y crear una nueva conexión VPN. Vamos a crear dos conexiones VPN, una para el Fortigate-01 y otra para el Fortigate-02.

La misma deberá tener las siguientes características.

- Será del tipo VPN IPSec.
- El nombre de la conexión deberá ser VPN-FGT-01 y VPN-FGT-02.
- El Gateway Remoto (Cortafuegos) será la dirección IP de la interfaz “WAN1” de cada uno de los Fortigate.
- Método de autenticación será clave pre-compartida y será la que hemos asignado en el proceso de configuración de la VPN en el Fortigate.
- En “Ajustes Avanzados” deberemos de indicar los mismos parámetros que el proceso de configuración en el equipo Fortigate.

Luego nos conectaremos a la red inalámbrica la red 192.168.100.0/24 u otra disponible.

Dejaremos un “ping” continuo al PLC que tendremos simulado para cada una de las máquinas 10.2.201.10 y 10.2.202.10, respectivamente.

¿Qué ocurre? ¿Responde? ¿Si? ¿No? ¿Porqué?
¿Es necesario realizar alguna configuración adicional? Si es necesario, ¿Cuál?

Cada grupo deberá conectarse a cada uno de los respectivos Fortigate y establecer el túnel VPN.

Para visualizar el tráfico generado por la VPN podrán conectarse a los respectivos cortafuegos en la dirección IP 10.2.1.1 y 10.2.2.1 en el apartado “Log and Report” y “Fortiview”. Las credenciales deber admin21/admin21.

¿La conexión es satisfactoria? ¿Responde a “ping”?
¿Es necesario realizar alguna configuración adicional? Si es necesario, ¿Cuál?

3. ACTIVIDADES ADICIONALES:

    a. Limitar los accesos exclusivamente a las IPs de los equipos 10.2.201.10 y 10.2.202.10 para que podamos conectarnos empleando S7 e ICMP.
    b. Permitir que el usuario vpn01 y vpn02 puedan conectarse por RDP a un equipo con IP 10.2.201.20 y 10.2.202.20.
    c. Permitir “ping” al servidor DNS de Google, 8.8.8.8.