

Universidad de Costa Rica
Escuela de ciencias de la Computación e Informática
Seguridad de sistemas computacionales
I Semestre 2021

Tarea de Seguridad de Redes
Diseño de un sistema de seguridad perimetral

Estudiante:
Stephanie María Leitón Ramírez B74106
Hellen Fernández Jiménez B42525

Profesor:
Ricardo Villalón Fonseca

2 de agosto 2021

Tabla de contenidos

Introducción	3
Resumen	3
Credenciales de esxi y máquinas virtuales	4
Diagrama de componentes	4
Topología de la red	5
Red LAN	7
Configuración con el firewall	7
Red DMZ	9
Configuración con el firewall	9
Controles adicionales de seguridad	10
Vulnerabilidades y ataques de que son objeto los firewalls	12
Vulnerabilidades específicas para iptables del sistema operativo Linux.	13
Vulnerabilidades específicas para OpenVPN.	14
CVE-2018-9336 7.8 - Alto	15
Trabajo realizado y los resultados obtenidos.	16
Reglas de acceso desde la DMZ	16
Permitir el acceso hacia el servidor web a los usuarios de la LAN y a usuarios de Internet.	16
Permitir el acceso hacia el servidor de correo a usuarios de la LAN y a usuarios de Internet.	16
Permitir el envío de correos desde el servidor de correos hacia otros servidores de correo en Internet.	17
No permitir (explícitamente) el acceso desde Internet al servidor de base de datos.	17
Permitir la navegación de los servidores de la DMZ para actualizaciones de software.	17
Reglas de acceso desde la LAN	18
Permitir la navegación de usuarios solamente a través del servidor proxy.	18
Permitir el envío de información del servidor de base de datos de la LAN hacia el servidor de base de datos de la DMZ.	18
Permitir acceso desde la LAN hacia los servicios de correo y web de la DMZ.	18
• Permitir el acceso para administración por SSH hacia los servidores de la DMZ desde la LAN para el equipo del administrador.	20
• Permitir el acceso a servidores ftp en Internet al administrador de la red.	20
11.3 Pruebas de controles adicionales de seguridad	21
Referencias	24

1. Introducción

En esta tarea del curso de seguridad de sistemas computacionales consiste en el diseño de un sistema de seguridad perimetral en el cual se van a estudiar las características de un sistema de seguridad perimetral, que incluye un firewall para proteger la plataforma, así como una VPN para acceso a la administración de los servicios mediante un túnel seguro de comunicación, con el fin de atender necesidades de confidencialidad, integridad, autenticación y autorización en la línea perimetral del sistema.

2. Resumen

Primeramente se va a implementar controles de seguridad para mitigar los riesgos en una red, por medio de un firewall usando Linux con IPTables. En la cual se van a identificar vulnerabilidades en la configuración del sistema de firewall y posteriormente se va a verificar la configuración del firewall por medio de una simulación de una red usando máquinas virtuales. Además de lo anterior se va a configurar un sistema de VPN para la gestión remota de los servicios provistos por la red. resultados obtenidos.

3. Credenciales de esxi y máquinas virtuales

3.1. Esxi

Dirección IP: 172.24.131.169

Usuario: stephanie.leitonramirez

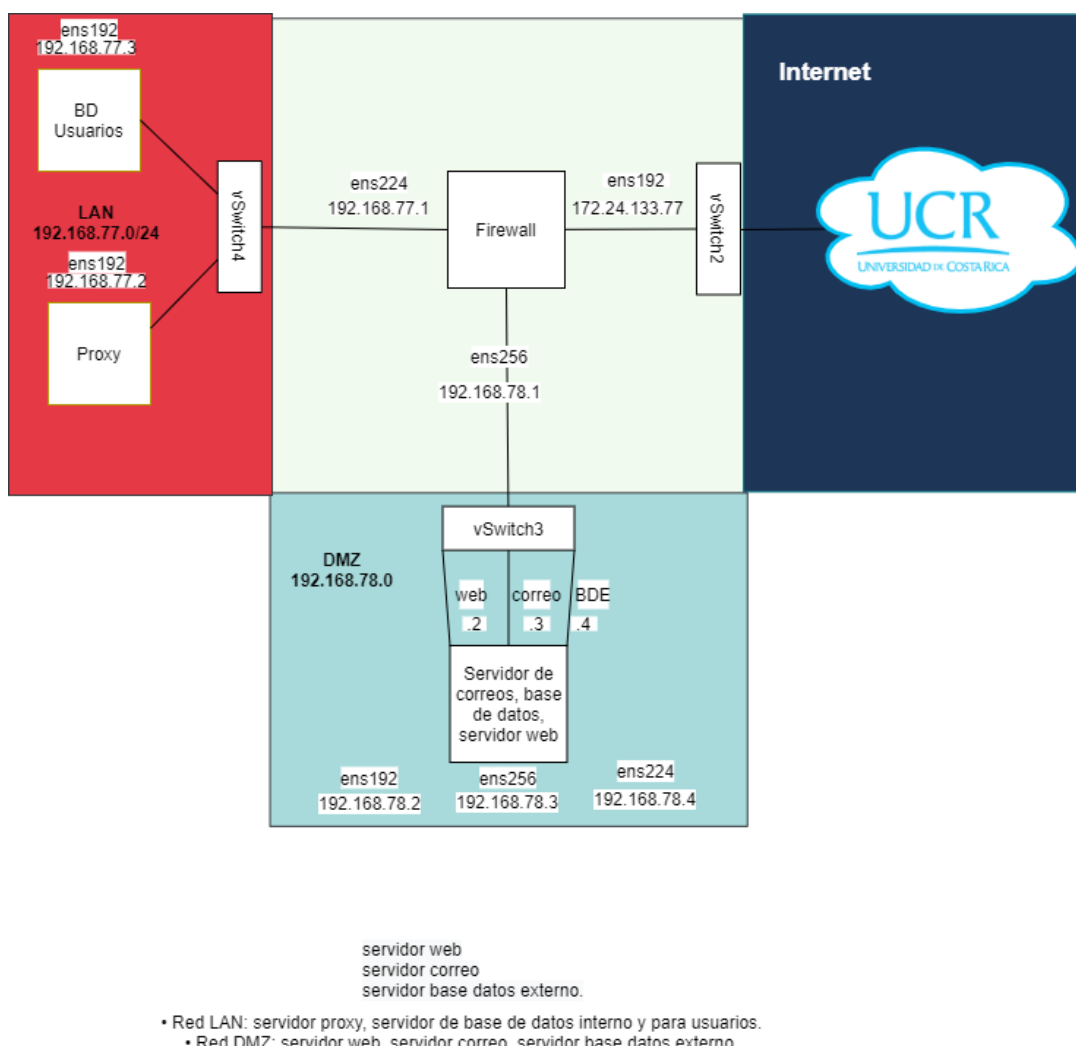
Contraseña: BNXXLvEp7kU3!

3.2. Máquinas virtuales

root = h13s01.

user1 = h02s11!

4. Diagrama de componentes



5. Topología de la red

192.168.77.0/24 - 192.168.80.0/24, 172.24.133.77-80/24

- 1) En las redes 172.24.x.y/24 el default gateway es siempre la IP 172.24.x.1.
- 2) La tercera interfaz física del hipervisor no se usa en esta tarea (vmnet2), dejarla desconectada de cualquier vswitch.
- 3) La red 172.24.133.0/24 está disponible a través de la cuarta interfaz física (vmnet3) del hipervisor y tiene salida a Internet.

Grupo de puertos	Switch	Nic de uplink	Descripción
Red - DMZ	vSwitch3	Ninguno	DMZ - firewall
Red - LAN	vSwitch4	Ninguno	BD-U -proxy- firewall
Red -Firewall	vSwitch2	vmnet3	Firewall - internet

- Red LAN: servidor proxy, servidor de base de datos interno y para usuarios.
 - IP privada: 192.168.a.0/24
 - IPs pública: 172.24.133.x para la salida de la LAN
- Red DMZ:
 - servidor web, servidor correo, servidor base datos externo.
 - IP privada: 192.168.b.0/24
 - IPs pública: 172.24.133.x la entrada a la DMZ
- IP pública: Para el servicio de VPN.

	IP	Interfaz	Gateway	Descripción	Puerto	Adaptador de Red
DMZ	192.168.78.2	ens192	192.168.77.1	Servidor web	80, 443	Red - DMZ
	192.168.78.3	ens256	Default	Servidor correo	587, 995, 25	Red - DMZ
	192.168.78.4	ens224	Default	Servidor base datos externo	3306	Red - DMZ
BD-U	192.168.77.2	ens192	Default	Servidor de base de datos interno y para usuarios	3306	Red - LAN
Proxy	192.168.77.3	ens192	Default	Proxy	3128	Red - LAN
Firewall	172.24.133.77	ens192	172.24.133.1/24	Entrada de servidor	80, 443	Red Firewall
				Entrada de servidor de Correos	587, 995, 25	Red Firewall
				Entrada base de datos	3306	Red Firewall
	192.168.77.1	ens224	192.168.77.1	Conectar LAN	3128	Red - LAN
	192.168.78.1	ens256	192.168.78.1	Conectar DMZ	-	Red - DMZ

VPN	172.24.133.80	ens192	172.24.133.1/24	VPN	3128	Red- Firewall
-----	---------------	--------	-----------------	-----	------	---------------

6. Red LAN

6.1. Configuración con el firewall

```
cat /proc/sys/net/ipv4/ip_forward
echo "net/ipv4/ip_forward=1" >> /etc/sysctl.conf
nano /etc/sysctl.conf
sysctl -p ( tiene que dar net/ipv4/ip_forward=1)
cat /proc/sys/net/ipv4/ip_forward ( tiene que dar 1)
```

Nombre	Comando	Descripción
Tablas	Input – filter – output	Tablas de iptables
Filtro	* filter : INPUT DROP [0:0] : FORWARD DROP [0:0] : OUTPUT ACCEPT [0:0]	Detiene todos los inputs Detiene todos los forward Deja pasar todas las salidas
Regla - ya establecidas	-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT	Sesión relacionada o establecida
	-A FORWARD -m state --state ESTABLISHED, RELATED -j ACCEPT	Sesión relacionada o establecida de forward
Reglas - salida	-A INPUT -i lo -j ACCEPT	icmp(se usa en ping o pong, significa internet control message protocol, protocolo para interntar salir a red)
Reglas - Traslado	-A INPUT -p icmp -j ACCEPT	Interfaz para que la maquina hable consigo misma
Reglas- Entrada	-A INPUT -s 192.168.77.2 /32 -i ens224 -j ACCEPT	Tener acceso al firewall desde la LAN
	-A POSTROUTING -s 192.168.77.2/24 -o ens192 -j MASQUERADE	• Permitir la navegación de usuarios solamente a través del servidor proxy.
	-A FORWARD -s 192.168.77.3/32 -d 192.168.78.4/32 -p tcp -m tcp --dport 3306 -j ACCEPT	• Permitir envío de información del servidor de base de datos de la LAN hacia el servidor de base de datos de la DMZ.

	-A FORWARD -s 192.168.77.0/24 -d 192.168.78.2/32 -p tcp -m tcp --dport 80 -j ACCEPT -A FORWARD -s 192.168.77.0/24 -d 192.168.78.2/32 -p tcp -m tcp --dport 443 -j ACCEPT	<ul style="list-style-type: none"> • Permitir acceso desde la LAN hacia los servicios de correo y web de la DMZ. 80, 443
	-A FORWARD -s 192.168.77.0/24 -d 192.168.78.3/32 -p tcp -m tcp --dport 587 -j ACCEPT -A FORWARD -s 192.168.77.0/24 -d 192.168.78.3/32 -p tcp -m tcp --dport 995 -j ACCEPT -A FORWARD -s 192.168.77.0/24 -d 192.168.78.3/32 -p tcp -m tcp --dport 25 -j ACCEPT	 587, 995, 25
	-A FORWARD -s 192.168.77.3/24 -d 192.168.78.2/32 -p tcp -m tcp --dport 22 -j ACCEPT -A FORWARD -s 192.168.77.3/24 -d 192.168.78.3/32 -p tcp -m tcp --dport 22 -j ACCEPT -A FORWARD -s 192.168.77.3/24 -d 192.168.78.4/32 -p tcp -m tcp --dport 22 -j ACCEPT	<ul style="list-style-type: none"> • Permitir el acceso para administración por SSH hacia los servidores de la DMZ desde la LAN para el equipo del administrador.
	-A POSTROUTING -s 192.168.77.2/24 -o ens192 -p tcp --dport 21 -j SNAT --to 172.24.133.77:21 -A FORWARD -s 192.168.77.2/32 -p tcp -m tcp --dport 21 -j ACCEPT -A FORWARD -m state --state RELATED,ESTABLISHED -p tcp --dport 20 -j ACCEPT	<ul style="list-style-type: none"> • Permitir el acceso a servidores ftp en Internet al administrador de la red 20, 21, mayor a 1024

Este comando es útil para la visualización de los paquetes
watch 'iptables -vL'

7. Red DMZ

7.1. Configuración con el firewall

Nombre	Comando	Descripción
Reglas- Entrada	<pre>-A PREROUTING -d 172.24.133.77 -p tcp --dport 80 -j DNAT --to 192.168.78.2:80 -A PREROUTING -d 172.24.133.77 -p tcp --dport 443 -j DNAT --to 192.168.78.2:443 -A FORWARD -d 192.168.78.2 -p tcp --dport 80 -j ACCEPT -A FORWARD -d 192.168.78.2 -p tcp --dport 443 -j ACCEPT</pre>	<ul style="list-style-type: none"> • Permitir el acceso hacia el servidor web a usuarios desde Internet. <p>Realizando prerouting 80 443</p>
	<pre>-A PREROUTING -d 172.24.133.77 -p tcp --dport 587 -j DNAT --to 192.168.78.3:587 -A PREROUTING -d 172.24.133.77 -p tcp --dport 995 -j DNAT --to 192.168.78.3:995 -A PREROUTING -d 172.24.133.77 -p tcp --dport 25 -j DNAT --to 192.168.78.3:25 -A FORWARD -d 192.168.78.3 -p tcp --dport 587 -j ACCEPT -A FORWARD -d 192.168.78.3 -p tcp --dport 995 -j ACCEPT -A FORWARD -d 192.168.78.3 -p tcp --dport 25 -j ACCEPT</pre>	<ul style="list-style-type: none"> • Permitir el acceso hacia el servidor de correo a usuarios de Internet. <p>587, 995, 25</p>
	<pre>-A POSTROUTING -s 192.168.78.3/24 -o ens192 -p tcp --dport 25 -j SNAT --to 172.24.133.77:25 -A FORWARD -s 192.168.78.3/32 -p tcp -m tcp --dport 25 -j ACCEPT</pre>	<ul style="list-style-type: none"> • Permitir el envío de correos desde el servidor de correos hacia otros servidores de correo en Internet. <p>Puertos para enviar 20,587</p>

	<pre>-A POSTROUTING -s 192.168.78.3/24 -o ens192 -p tcp --dport 587 -j SNAT --to 172.24.133.77:587</pre> <pre>-A FORWARD -s 192.168.78.3/32 -p tcp -m tcp --dport 587 -j ACCEPT</pre>	SE PONE INTERFAZ DE SALIDA, Y SE AFINAN LOS PUERTOS
	<pre>-A FORWARD -i ens192 -d 192.168.77.4/32 -p tcp -m tcp --dport 3306 -j DROP</pre>	<ul style="list-style-type: none"> • No permitir (explícitamente) el acceso desde Internet al servidor de base de datos.
	<pre>-A POSTROUTING -s 192.168.78.2/24 -o ens192 -j MASQUERADE</pre> <p>O esta otra</p> <pre>-A POSTROUTING -s 192.168.78.0/24 -o ens192 -p tcp --dport 80 -j SNAT --to 172.24.133.77:80</pre> <pre>-A FORWARD -s 192.168.78.0/32 -p tcp -m tcp --dport 80 -j ACCEPT</pre>	<ul style="list-style-type: none"> • Permitir la navegación de los servidores de la DMZ para actualizaciones de software.

Este comando es útil para la visualización de los paquetes
 watch 'iptables -vL' .

Controles adicionales de seguridad

Adicionalmente a los filtros de paquetes a través del firewall, implemente políticas que permitan determinar y controlar los siguientes problemas en la red:

- Implemente un sistema de VPN con OpenVPN para establecer la gestión remota de los servidores y equipos de la LAN y la DMZ.
- Monitoree, controle y reporte excesos en la cantidad de sesiones de red, para las estaciones cliente en la LAN, cuando las conexiones estén dirigidas al puerto 25 de servidores de correo, incluyendo en dicho monitoreo el servidor

de correo propio de la red. El objetivo de esta regla es poder detectar equipos infectados con algún tipo de malware que esté generando correo basura (spam). Establezca su propia estrategia y parámetros para implementar este control.

- Monitoree, controle y reporte la cantidad de intentos de conexión en un periodo de tiempo, hacia el servicio SSH de los servidores de la DMZ y del firewall. Establezca una lista de las direcciones IP que sobrepasen el límite y bloquee las por un periodo definido de tiempo.
- Opcional: implemente el servidor proxy con el software open source squid-cache. Los controles descritos en esta sección pueden ser implementados de diversas formas, usted debe implementarlos en el equipo que funciona como firewall.

Nombre	Comando	Descripción
Reglas-entrada	-A POSTROUTING -s 192.168.77.1/24 -o ens192 -j MASQUERADE -A FORWARD -s 192.168.77.1/24 -d 172.24.131.0/24 --sport 1194 -j ACCEPT -A FORWARD -s 172.24.131.0/24 -d 192.168.77.1/24 -dport 1194 -j ACCEPT	Implemente un sistema de VPN con OpenVPN para establecer la gestión remota de los servidores y equipos de la LAN. 172.24.131.0/24 = NAC interna UDP 1194
	-A POSTROUTING -s 192.168.78.1/24 -o ens192 -j MASQUERADE -A FORWARD -s 192.168.78.1/24 -d 172.24.131.0/24 --sport 1194 -j ACCEPT -A FORWARD -s 172.24.131.0/24 -d 192.168.78.1/24 --dport 1194 -j ACCEPT	Implemente un sistema de VPN con OpenVPN para establecer la gestión remota de los servidores y equipos de la DMZ 172.24.131.0/24 = NAC interna UDP 1194
	-A PREROUTING -d 172.24.133.77 -p tcp --dport 25 -j DNAT --to 192.168.78.3:25 -A FORWARD -d 192.168.78.3 -p tcp --dport 25 -j ACCEPT -A INPUT -p tcp --dport 25 -i ens256 -m state --state NEW -m recent --update --seconds 120 -m limit --limit 2/min --hitcount 4 -j LOGDROP --log-prefix "IPTables-Dropped: Intentos 4 intentos fallidos en puerto 25"	Monitoree, controle y reporte excesos en la cantidad de sesiones de red, para las estaciones cliente en la LAN, cuando las conexiones estén dirigidas al puerto 25 de servidores de correo, incluyendo en dicho monitoreo el servidor de correo propio de la red.

	<pre>iptables -A INPUT -p tcp --syn --dport 25 -i ens256 -m connlimit --connlimit-above 3 - -j REJECT --reject-with tcp-reset --log-prefix "IPTables-Reject: Se superó el límite de conexiones"</pre>	
	<pre>-A FORWARD -s 192.168.77.3/32 -d 192.168.78.2/32 -p tcp -m tcp --dport 22 -j ACCEPT -A FORWARD -s 192.168.77.3/32 -d 192.168.78.3/32 -p tcp -m tcp --dport 22 -j ACCEPT -A FORWARD -s 192.168.77.3/32 -d 192.168.78.4/32 -p tcp -m tcp --dport 22 -j ACCEPT -A INPUT -s 192.168.77.3/32 -d 192.168.78.2/32 -p tcp --dport 22 -i eth0 -m state --state NEW -m recent --update --seconds 120 --hitcount 4 -j LOGDROP</pre>	<p>Monitoree, controle y reporte la cantidad de intentos de conexión en un periodo de tiempo, hacia el servicio SSH de los servidores de la DMZ y del firewall. Establezca una lista de las direcciones IP que sobrepasen el límite y bloquee las por un periodo definido de tiempo.</p>
	COMMIT	

8. Vulnerabilidades y ataques de que son objeto los firewalls

Existen Firewalls menos avanzados los cuales son vulnerables a ataques de alto nivel ya que no utilizan herramientas para examinar los paquetes por completo, aunque existen algunas herramientas que lo pueden hacer estas aún se enfrentan desafíos y son vulnerables a las amenazas en evolución. Por esto, las organizaciones deben emparejarlos con otros componentes de seguridad, como sistemas de detección de intrusos y sistemas de prevención de intrusos.[7]

Ejemplos de amenazas modernas a las que un firewall puede ser vulnerable son:

1. **Ataques internos** : las organizaciones pueden utilizar firewalls internos sobre un firewall perimetral para segmentar la red y proporcionar protección interna. Si se sospecha de un ataque, las organizaciones pueden realizar auditorías sensibles mediante las funciones de NGFW.

2. **Ataques distribuidos de denegación de servicio (DDoS):** un ataque DDoS es un intento malicioso con el objetivo de interrumpir el tráfico normal de una red objetivo abrumando el objetivo o la infraestructura circundante con una avalancha de tráfico. Utiliza múltiples sistemas informáticos comprometidos como fuentes de tráfico de ataque. La preocupación principal para mitigar un ataque DDoS es diferenciar entre ataque y tráfico normal. Muchas veces, puede provenir de fuentes aparentemente legítimas y requiere verificación cruzada y auditoría de varios componentes de seguridad.
3. **Malware:** las amenazas de malware son variadas, complejas y en constante evolución junto con la tecnología de seguridad y las redes que protege. A medida que las redes se vuelven más complejas y dinámicas con el auge de IoT, a los firewalls les resulta más difícil defenderlas.

Otra vulnerabilidad es que un firewall mal configurado o una actualización pérdida del proveedor pueden ser demasiado perjudiciales para la seguridad de una red.

Un firewall generalmente no protege las capas superiores del modelo OSI

1. Al actuar de defensa perimetral, no defiende a hosts de ataques o errores provenientes de la intranet.
2. Tampoco ofrece protección una vez que el intruso lo traspasa.
3. Sus capacidades de auditoria son limitadas.
4. Su capacidad de registro de actividades es limitada.
5. No soportan políticas de seguridad complejas tales como:
 - a. Autenticación de usuarios.
 - b. Control de accesos con horarios prefijados.
6. El firewall no puede proteger contra los ataques de ingeniería social
7. El firewall no puede proteger contra los ataques de virus informáticos o software malicioso.

Es muy importante recordar que los firewalls no son sistemas inteligentes, ellos actúan de acuerdo a parámetros introducidos por quien los diseña, por eso, si un paquete de información no se encuentra dentro de estos parámetros como una amenaza de peligro simplemente lo deja pasar. [2]

9. Vulnerabilidades específicas para iptables del sistema operativo Linux.

● iptables: --syn flag bypass

CVE-2012-6638 Alta

Una vulnerabilidad encontrada es en el archivo en `extensions/libxt_tcp.c` en iptables hasta 1.4.21 no hace coincidir paquetes TCP SYN+FIN en reglas `--syn`, lo que podría permitir que a atacantes remotos eludir las restricciones de firewall a través de paquetes manipulados.

Se encontró como realizar la mitigación para esta vulnerabilidad ya que en lugar de --syn, use --tcp-flags SYN, RST, ACK SYN en sus conjuntos de reglas en caso de que también desee hacer coincidir paquetes con ambos indicadores SYN + FIN establecidos [4] La solución de CVE-2012-6638 hace que este problema sea menos relevante.[3]

- CVE-2004-0986

Iptables anterior a 1.2.11, bajo ciertas condiciones, no carga correctamente los módulos requeridos al inicio del sistema, lo que hace que las reglas del firewall no carguen y protejan el sistema de atacantes remotos [9].

7.5

CVSSV2

CVE-2004-0986

Published: 01/03/2005 Updated: 11/07/2017

CVSS v2 Base Score: 7.5 | Impact Score: 6.4 | Exploitability Score: 10

VMscore: 668

Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

[Subscribe to Suse](#)

10. Vulnerabilidades específicas para OpenVPN.

Principales vulnerabilidades y ataques de que son objeto los firewalls mejoras correspondientes a su firewall o describa los mecanismos de control requeridos cuando no sea posible implementarlas pero ubicando vulnerabilidades específicas para OpenVPN.

Algunas vulnerabilidades específicas más recientes de OpenVPN son:

- **OpenVPN 3 Core Library version 3.6 and 3.6.1**

CVE-2021-3547 7.4 - Alto

Esto permite que se realice un ataque de “man in the middle” en el que se omite la autenticación del certificado mediante la emisión de un certificado de un servidor no relacionado con el mismo nombre de host que se encuentra en la configuración del cliente.

- **OpenVPN Connect 3.2.0 a 3.3.0**

CVE-2021-3613 7.8 - Alto

Permite a usuarios locales cargar bibliotecas dinámicas arbitrarias a través de un archivo de configuración OpenSSL si está persistente, lo que permite al usuario

ejecutar código arbitrario con los mismos privilegios que posee el proceso principal de OpenVPN.

- **Servidor de acceso OpenVPN 2.7.3 a 2.8.7**

CVE-2020-36382 7.5 - Alto

Un servidor de OpenVPN Access Server 2.7.3 a 2.8.7 tiene una vulnerabilidad que permite a atacantes remotos activar una afirmación en la fase de autenticación del usuario. Esto se realiza a través de incorrectos datos de token de autenticación en una fase temprana de la autenticación del usuario. El que los atacantes aprovechen esta vulnerabilidad resulta en una denegación del servicio.

- **OpenVPN 2.5.1 y versiones anteriores**

CVE-2020-15078 7.5 - Alto

Permiten a los atacantes remotos evitar la autenticación y los datos del canal de control de acceso en servidores con configuración de autenticación diferida, lo que podría desencadenar en fugas de información.

- **OpenVPN Access Server anterior a la versión 2.8.4 genera nuevos tokens de autenticación de usuario en lugar de reutilizar los tokens existentes al volver a conectarse, lo que permite eludir la marca de tiempo de vencimiento del token inicial.**

CVE-2020-15074 7.5 - Alto

Otra vulnerabilidad de OpenVPN Access Server anterior a la versión 2.8.4 se da ya que genera nuevos tokens de autenticación de usuario en vez de reutilizar los tokens que ya existen cuando se vuelve a conectar, esto da como resultado el eludir del token inicial, la marca de tiempo de vencimiento.

- **Se descubrió un problema en OpenVPN Access Server antes de 2.7.0 y 2.8.x antes de 2.8.3**

CVE-2020-11462 7.5 - Alto

Con estas versiones de OpenVPN y con la interfaz RCP2 con todas las funciones habilitadas, es posible lograr un estado de denegación de servicio temporal de la interfaz de administración al enviar una carga útil XML XEE.

- **Servidor de acceso OpenVPN 2.8.x antes de 2.8.1**

CVE-2020-8953 9.8 - Crítico

Con la versión de OpenVPN Access Server 2.8.x y anterior a 2.8.1 existe una vulnerabilidad que permite la omisión de autenticación LDAP (exceptuando cuando un usuario está inscrito con autenticación de dos factores) Es muy importante ya que es a nivel de autenticación y por ende es crítico.

- **openvpnserv.exe (también conocido como el asistente de servicio interactivo) en OpenVPN 2.4.x antes de 2.4.6**

CVE-2018-9336 7.8 - Alto

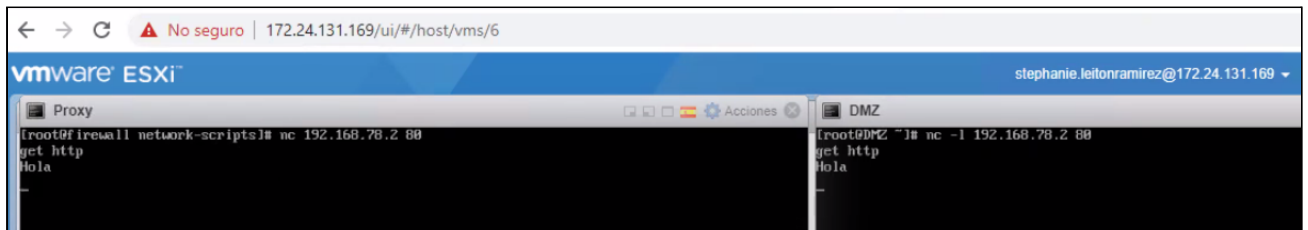
openvpnserv.exe en las versiones de 2.4.x anteriores de 2.4.6 permite que un atacante local provoque una doble liberación de memoria enviando una solicitud con formato incorrecto al servicio interactivo. Esto podría ocasionar una denegación de servicio debido a la corrupción de la memoria.

11. Trabajo realizado y los resultados obtenidos.

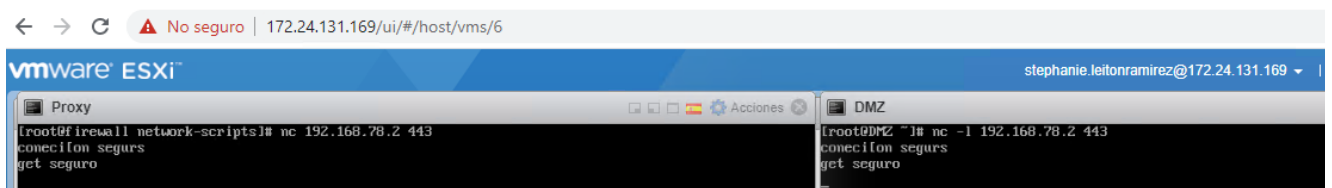
11.1. Reglas de acceso desde la DMZ

- Permitir el acceso hacia el servidor web a los usuarios de la LAN y a usuarios de Internet.

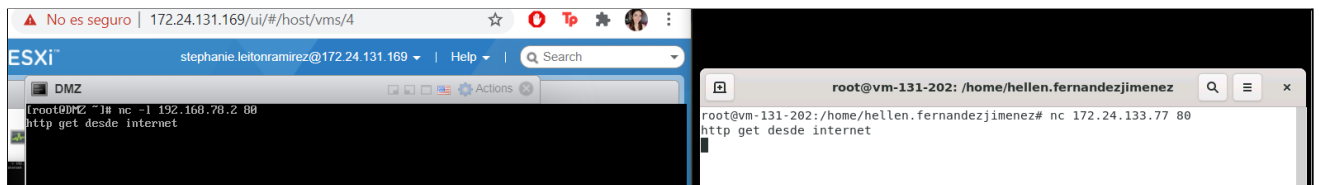
Desde usuarios de la LAN al servidor web con el puerto 80:



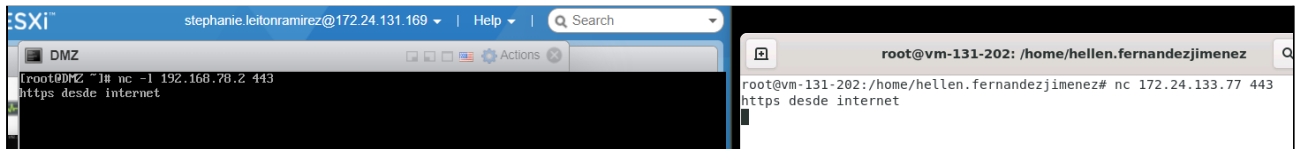
Desde usuarios de la LAN al servidor web con el puerto 443:



Desde usuarios de internet al servidor web con el puerto 80:

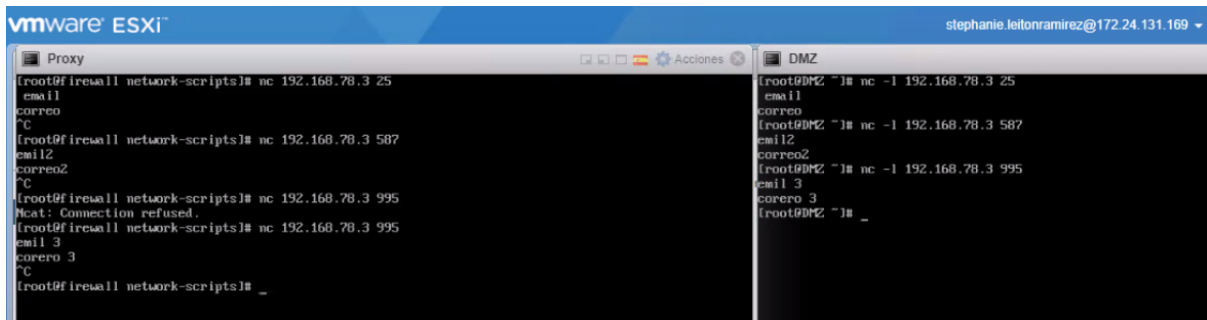


Desde usuarios de internet al servidor web con el puerto 80:

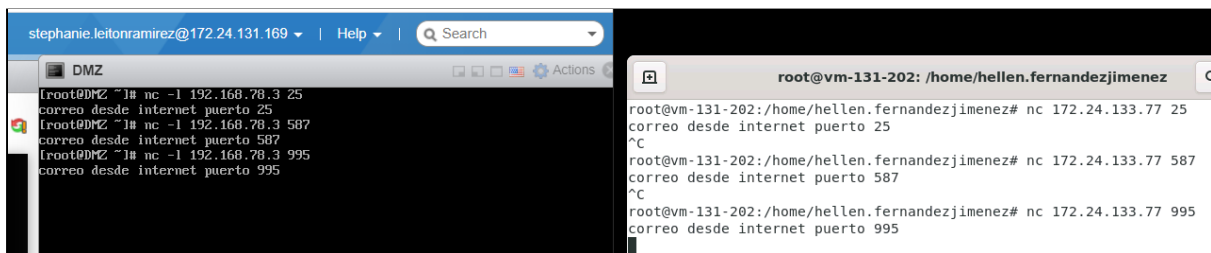


- Permitir el acceso hacia el servidor de correo a usuarios de la LAN y a usuarios de Internet.

Desde usuarios de la LAN al servidor de correo:



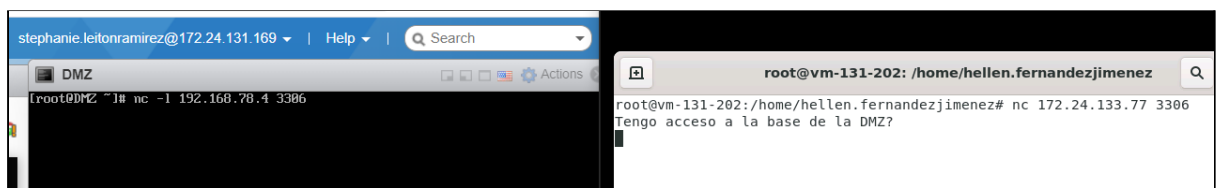
Desde usuarios de internet al servidor correo:



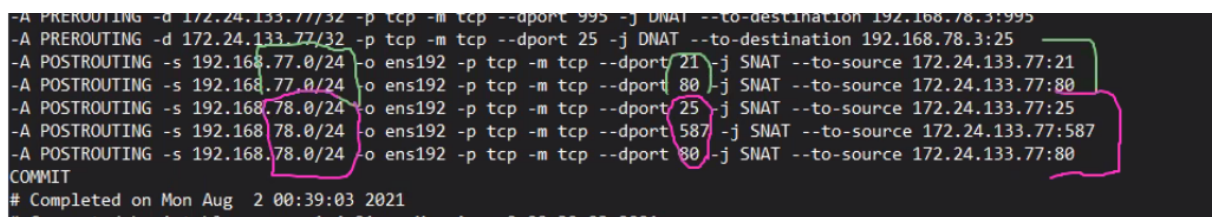
Permitir el envío de correos desde el servidor de correos hacia otros servidores de correo en Internet.

Es casi la misma regla que la del proxy para navegar solo cambia el puerto pero no funciona y la misma maquina

No permitir (explícitamente) el acceso desde Internet al servidor de base de datos.



Permitir la navegación de los servidores de la DMZ para actualizaciones de software.



```

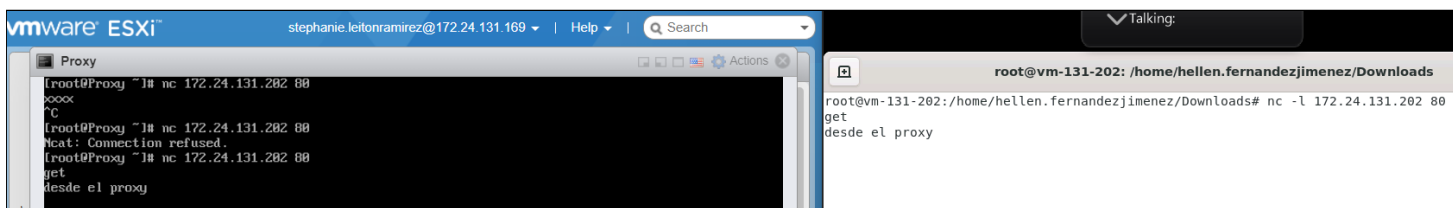
-A FORWARD -s 192.168.77.0/24 -d 192.168.78.3/32 -p tcp -m tcp --dport 25 -j ACCEPT
-A FORWARD -d 192.168.78.2/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A FORWARD -d 192.168.78.2/32 -p tcp -m tcp --dport 443 -j ACCEPT
-A FORWARD -d 192.168.78.3/32 -p tcp -m tcp --dport 587 -j ACCEPT
-A FORWARD -d 192.168.78.3/32 -p tcp -m tcp --dport 995 -j ACCEPT
-A FORWARD -d 192.168.78.3/32 -p tcp -m tcp --dport 25 -j ACCEPT
-A FORWARD -s 192.168.78.3/32 -p tcp -m tcp --dport 25 -j ACCEPT
-A FORWARD -s 192.168.78.3/32 -p tcp -m tcp --dport 587 -j ACCEPT
-A FORWARD -s 192.168.77.2/32 -p tcp -m tcp --dport 3128 -j ACCEPT
-A FORWARD -s 192.168.77.2/32 -p tcp -m tcp --dport 21 -j ACCEPT
-A FORWARD -s 192.168.77.2/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A FORWARD -s 192.168.78.3/32 -p tcp -m tcp --dport 25 -j ACCEPT
-A FORWARD -s 192.168.78.3/32 -p tcp -m tcp --dport 587 -j ACCEPT
-A FORWARD -s 192.168.78.0/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A FORWARD -d 192.168.77.4/32 -i ens192 -p tcp -m tcp --dport 3306 -j DROP
COMMIT

```

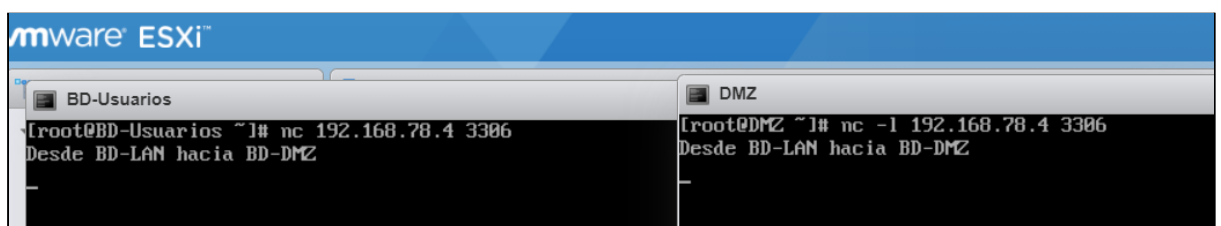
Es casi la misma regla que la del proxy para navegar solo cambia el puerto pero no funciona

11.2. Reglas de acceso desde la LAN

Permitir la navegación de usuarios solamente a través del servidor proxy.



Permitir el envío de información del servidor de base de datos de la LAN hacia el servidor de base de datos de la DMZ.



Permitir acceso desde la LAN hacia los servicios de correo y web de la DMZ.

Web:

```

vmware ESXi™

BD-Usuarios
[root@BD-Usuarios ~]# nc 192.168.78.2 80
Desde la LAN al servidor web 80
^C
[root@BD-Usuarios ~]# nc 192.168.78.2 443
Desde la LAN al servidor web 443

DMZ
[root@DMZ ~]# nc -l 192.168.78.2 80
Desde la LAN al servidor web 80
[root@DMZ ~]# nc -l 192.168.78.2 443
Desde la LAN al servidor web 443

```

```

Proxy
[root@firewall network-scripts]# nc 192.168.78.2 80
Desde proxy a servidor web
^C
[root@firewall network-scripts]# nc 192.168.78.2 443
Desde proxy a servidor web 443

DMZ
[root@DMZ ~]# nc -l 192.168.78.2 80
Desde proxy a servidor web
[root@DMZ ~]# nc -l 192.168.78.2 443
Desde proxy a servidor web 443

```

Correo:

```

vmware ESXi™

BD-Usuarios
[root@BD-Usuarios ~]# nc 192.168.78.3 25
Correo puerto 25
^C
[root@BD-Usuarios ~]# nc 192.168.78.3 587
Correo puerto 587
^C
[root@BD-Usuarios ~]# nc 192.168.78.3 995
Correo puerto 995

DMZ
[root@DMZ ~]# nc -l 192.168.78.3 25
Correo puerto 25
[root@DMZ ~]# nc -l 192.168.78.3 587
Correo puerto 587
[root@DMZ ~]# nc -l 192.168.78.3 995
Correo puerto 995

```

```

vmware ESXi™

Proxy
[root@firewall network-scripts]# nc 192.168.78.3 25
Correo desde proxy hacia DMZ 25
^C
[root@firewall network-scripts]# nc 192.168.78.3 587
Ncat: Connection refused.
[root@firewall network-scripts]# nc 192.168.78.3 587
Correo desde proxy a DMZ 587
^C
[root@firewall network-scripts]# nc 192.168.78.3 995
Ncat: Connection refused.
[root@firewall network-scripts]# nc 192.168.78.3 995
Correo desde proxy a DMZ 995

DMZ
[root@DMZ ~]# nc -l 192.168.78.3 25
Correo desde proxy hacia DMZ 25
[root@DMZ ~]# nc -l 192.168.78.3 587
Correo desde proxy a DMZ 587
[root@DMZ ~]# nc -l 192.168.78.3 995
Correo desde proxy a DMZ 995

```

- Permitir el acceso para administración por SSH hacia los servidores de la DMZ desde la LAN para el equipo del administrador.

```

[root@firewall network-scripts]# nc 192.168.78.2 22
SSH hacia servidor web
^C
[root@firewall network-scripts]# nc 192.168.78.3 22
SSH hacia servidor de correos
^C
[root@firewall network-scripts]# nc 192.168.78.4 22
SSH hacia Base Datos
  
```

- Permitir el acceso a servidores ftp en Internet al administrador de la red.

```

[root@firewall network-scripts]# nc 172.24.131.202 21
ftp inicio de conexion
  
```

11.3 Pruebas de controles adicionales de seguridad

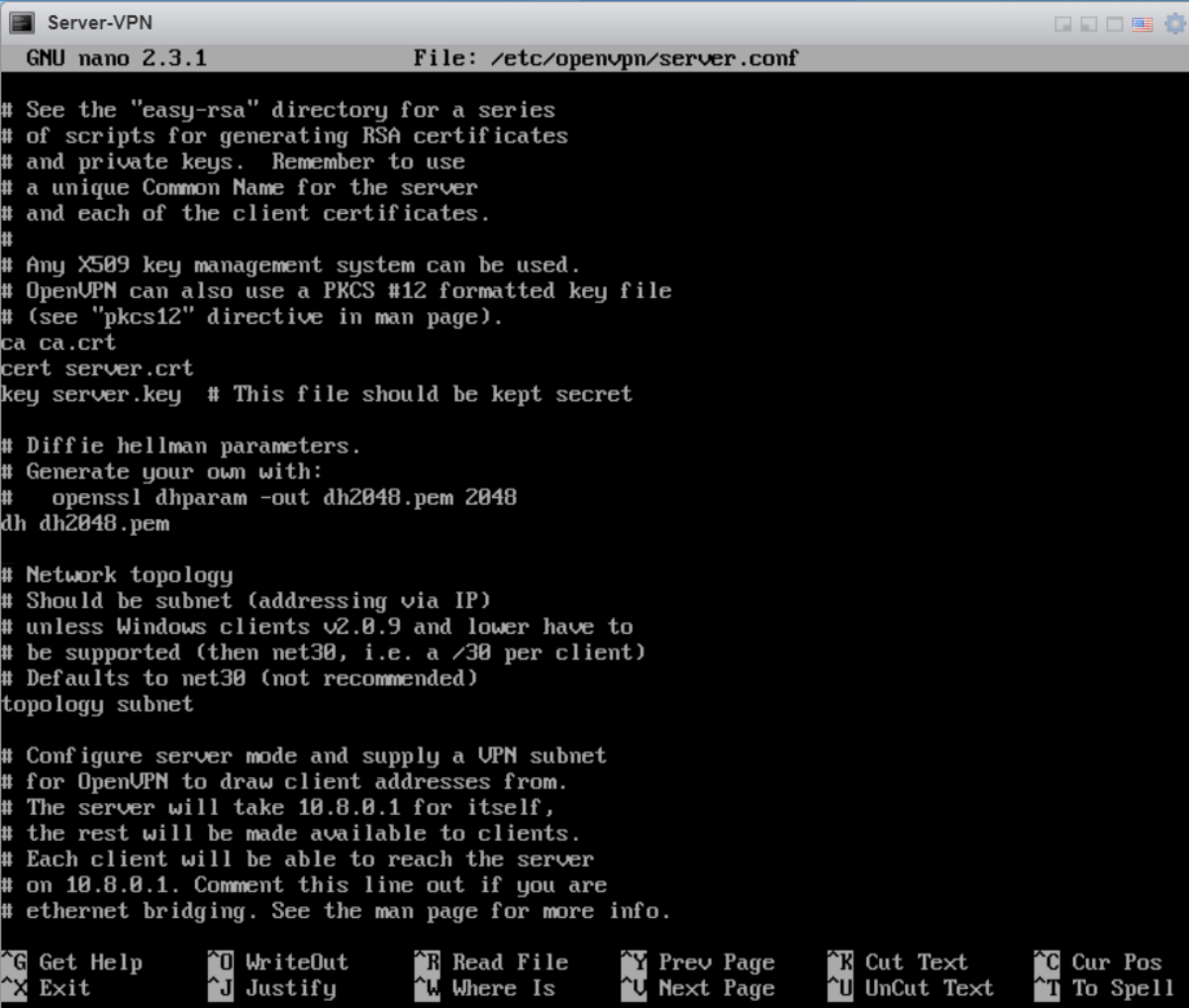
Adicionalmente a los filtros de paquetes a través del firewall, implemente políticas que permitan determinar y controlar los siguientes problemas en la red:

- Implemente un sistema de VPN con OpenVPN para establecer la gestión remota de los servidores y equipos de la LAN y la DMZ.

Para la configuración del VPN se siguió el tutorial que se encuentra en el siguiente enlace:

<https://www.digitalocean.com/community/tutorials/how-to-set-up-and-configure-an-openvpn-server-on-centos-7>

En este se instaló y configuró OpenVpn. Se generaron las llaves y certificados tanto para el servidor de openvpn como para el cliente. Se activó el bit de forward.



```
Server-VPN
GNU nano 2.3.1      File: /etc/openvpn/server.conf

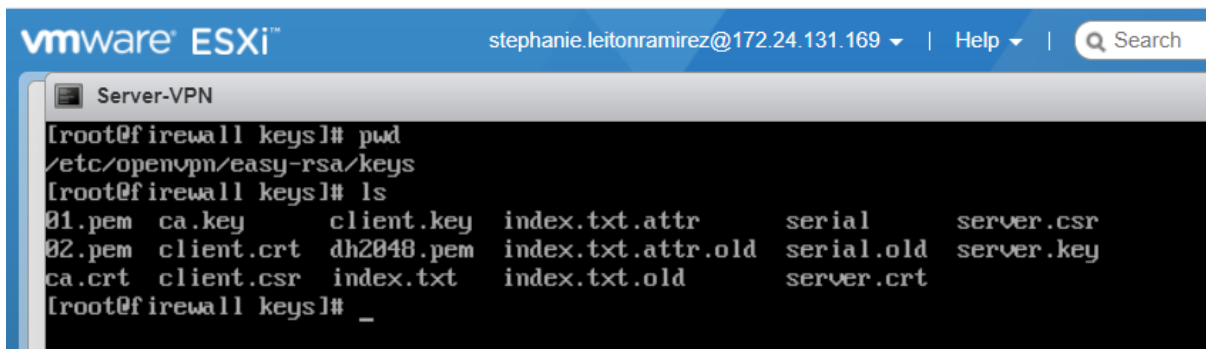
# See the "easy-rsa" directory for a series
# of scripts for generating RSA certificates
# and private keys. Remember to use
# a unique Common Name for the server
# and each of the client certificates.
#
# Any X509 key management system can be used.
# OpenVPN can also use a PKCS #12 formatted key file
# (see "pkcs12" directive in man page).
ca ca.crt
cert server.crt
key server.key # This file should be kept secret

# Diffie hellman parameters.
# Generate your own with:
#   openssl dhparam -out dh2048.pem 2048
dh dh2048.pem

# Network topology
# Should be subnet (addressing via IP)
# unless Windows clients v2.0.9 and lower have to
# be supported (then net30, i.e. a /30 per client)
# Defaults to net30 (not recommended)
topology subnet

# Configure server mode and supply a VPN subnet
# for OpenVPN to draw client addresses from.
# The server will take 10.8.0.1 for itself,
# the rest will be made available to clients.
# Each client will be able to reach the server
# on 10.8.0.1. Comment this line out if you are
# ethernet bridging. See the man page for more info.

^G Get Help      ^O WriteOut      ^R Read File     ^Y Prev Page     ^K Cut Text      ^C Cur Pos
^X Exit          ^J Justify       ^W Where Is      ^U Next Page     ^U UnCut Text   ^T To Spell
```



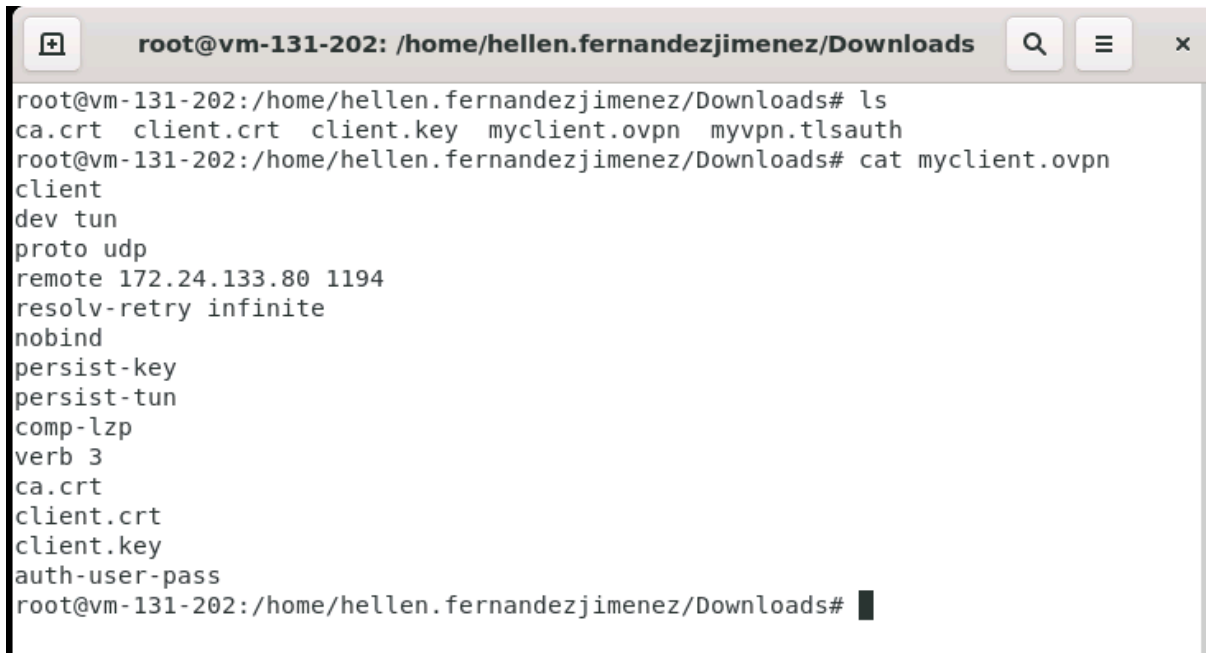
The screenshot shows a VMware ESXi interface with a terminal window titled "Server-VPN". The terminal is running commands to generate OpenVPN keys. The user is at the prompt [root@firewall keys]# and has executed 'pwd' and 'ls'. The 'ls' command shows a directory listing of generated files.

```
vmware ESXi™
stephanie.leitonramirez@172.24.131.169 | Help | Search

Server-VPN

[root@firewall keys]# pwd
/etc/openvpn/easy-rsa/keys
[root@firewall keys]# ls
01.pem  ca.key      client.key  index.txt.attr  serial  server.csr
02.pem  client.crt  dh2048.pem  index.txt.attr.old  serial.old  server.key
ca.crt  client.csr  index.txt   index.txt.old    server.crt
[root@firewall keys]# _
```

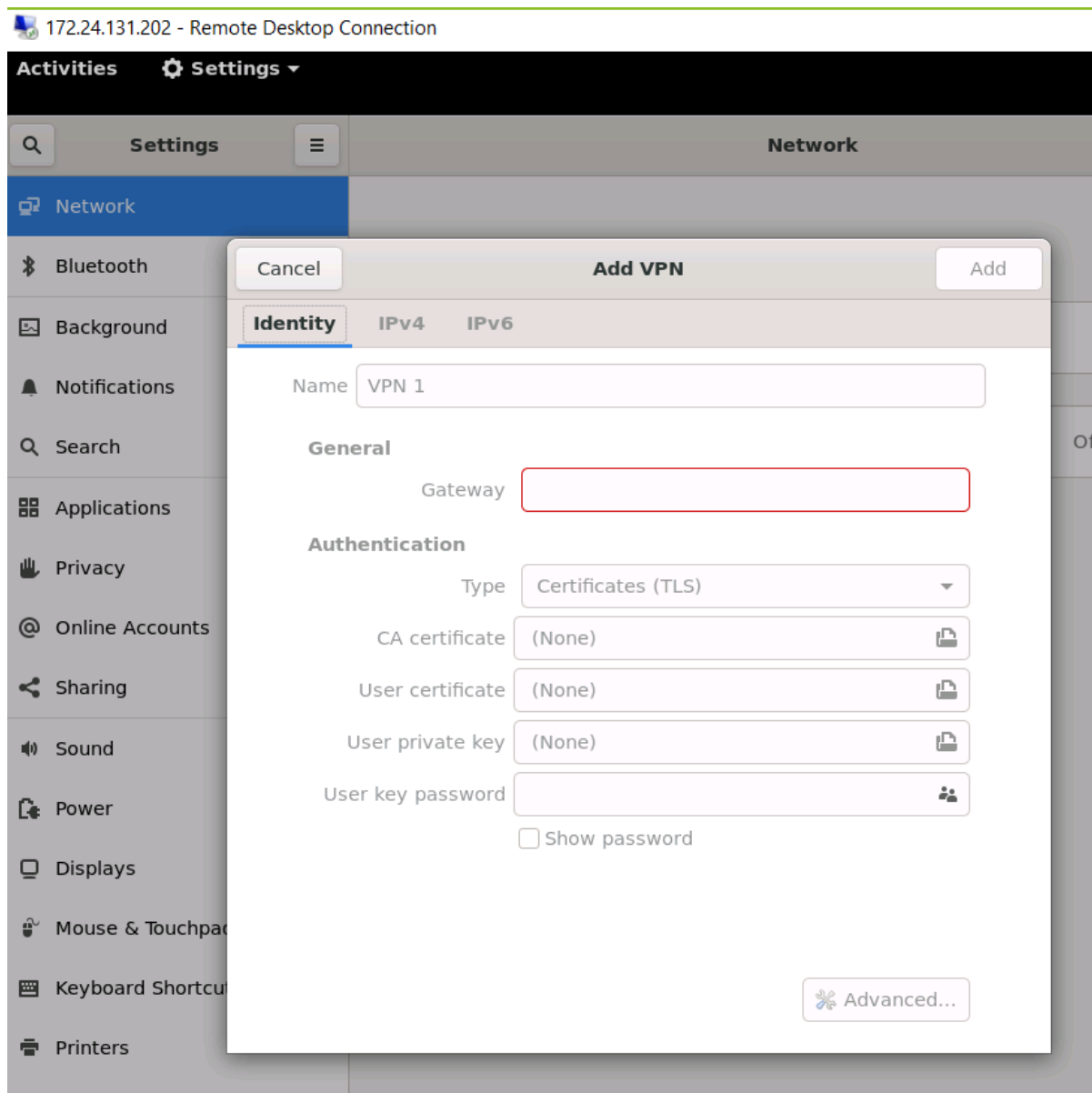
Además, se realizó la configuración correspondiente para el cliente:



The screenshot shows a VMware terminal window titled "root@vm-131-202: /home/hellen.fernandezjimenez/Downloads". The terminal is running commands to list files and display the contents of a client configuration file.

```
root@vm-131-202: /home/hellen.fernandezjimenez/Downloads
root@vm-131-202: /home/hellen.fernandezjimenez/Downloads# ls
ca.crt  client.crt  client.key  myclient.ovpn  myvpn.tlsauth
root@vm-131-202: /home/hellen.fernandezjimenez/Downloads# cat myclient.ovpn
client
dev tun
proto udp
remote 172.24.133.80 1194
resolv-retry infinite
nobind
persist-key
persist-tun
comp-lzo
verb 3
ca.crt
client.crt
client.key
auth-user-pass
root@vm-131-202: /home/hellen.fernandezjimenez/Downloads#
```

Y no funcionó, de la misma forma, no se tenía permitido modificar la siguiente ventana en la máquina cliente:



- Monitoree, controle y reporte excesos en la cantidad de sesiones de red, para las estaciones cliente en la LAN, cuando las conexiones estén dirigidas al puerto 25 de servidores de correo, incluyendo en dicho monitoreo el servidor de correo propio de la red. El objetivo de esta regla es poder detectar equipos infectados con algún tipo de malware que esté generando correo basura (spam). Establezca su propia estrategia y parámetros para implementar este control.
- Monitoree, controle y reporte la cantidad de intentos de conexión en un periodo de tiempo, hacia el servicio SSH de los servidores de la DMZ y del firewall. Establezca una lista de las direcciones IP que sobrepasen el límite y bloquee las por un periodo definido de tiempo.

12. Referencias

1. <https://unix.stackexchange.com/questions/126595/iptables-forward-all-traffic-to-interface>
2. <https://silo.tips/download/firewalls-iptables-y-netfilter>
3. <https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2012-2663>
4. https://bugzilla.redhat.com/show_bug.cgi?id=826702
5. <http://redesdecomputadores.umh.es/iptables.htm>
6. <https://rm-rf.es/iptables-ftp-y-passive-mode/>
7. <https://www.cs.purdue.edu/homes/fahmy/papers/firewall-analysis.pdf>
8. <https://stack.watch/product/openvpn/>
9. <https://www.vulmon.com/searchpage?q=iptables&sortby=byriskscore>