-	TALLER SR – PRÁCTICA 64 – VPN + Dynamic DNS + Con	ROUTER WiFI 4G LTE nprobación CGNAT
NÚMERO DE GRUPO	FUNCIÓNS	Apelidos, Nome
	Coordinador/a:	
	Responsable Limpeza:	
	Responsable Documentación:	
ESCENARIO: Router WiFi 4G L	TE - VPN + Dynamic DNS	\sim
Router WiFi 4G LTE Configuración VPN Prerrequisitos: 1. Hora sincronizada con Internet (2. IP fixa na WAN do Router (Cont Portátil:	(NTP) ratada ou Dynamic DNS) USB	ocal no-ip→grupo7tallersrvpn.ddns.net 192.168.1.0/24
SSID + Contrasinal (etiqueta trase Ethernet Rede Aula \rightarrow VPN \rightarrow grupo	era router) Live Kali amd64 o7tallersrvpn.ddns.net	192.168.1.1/24
Conectar ao router		ISP → IP dinimics ← X1Y1Z1W1/P
www.no-ip.com (ou IP estática W Dynamic dns → grupo7tallersrvpn.c	VPN grupo7tallersrvpn.čtdns.net	Etiqueta trasera router 192.168.1.0/24
		KALI LINUX® KALI LINUX® do proconto documonto doclina colguero

LIMITACIÓN DE RESPONSABILIDADE O autor do presente documento declina calquera responsabilidade asociada ao uso incorrecto e/ou malicioso que puidese realizarse coa información exposta no mesmo. Por tanto, non se fai responsable en ningún caso, nin pode ser considerado legalmente responsable en ningún caso, das consecuencias que poidan derivarse da información contida nel ou que esté enlazada dende ou hacia el, incluíndo os posibles erros e información incorrecta existentes, información difamatoria, así como das consecuencias que se poidan derivar sobre a súa aplicación en sistemas de información reais e/ou virtuais. Este documento foi xerado para uso didáctico e debe ser empregado en contornas privadas e virtuais controladas co permiso correspondente do administrador desas contornas.

Material necesario	Práctica: ROUTER WiFI 4G LTE VPN + Dynamic DNS + Comprobación CGNAT
■ Portátil	(1) Prerrequisito: Realizar a <u>Práctica 61</u> [1]
∎ Regleta	(2) Entrega/Revisión material necesario para a
■ [1] <u>Práctica 61</u>	práctica: Figuras 1,2,3,4,5 e 6
■ USB Live amd64 Kali	(3) NON conectar o portátil á roseta da aula.
■ Móbiles alumnado	(4) Portátil:
[2] tp-link 4G LTE Router TR-ML6400	a) Arrancar co USB Live amd64 Kali
■ [3] <u>Cómo encontrar la versión de hardware en un</u>	b) Configurar a rede WiFi según escenario
<u>dispositivo de TP-Link</u>	(router).
■ [4] <u>TR-MR6400 Soporte</u>	c) Configurar VPN (OpenVPN) no Router WiFi
[5] TL-MR6400(EU)_V5.3_Quick Installation Guide	4G LTE
[6] tp-link: <u>Vídeo de configuración</u>	d) Comprobar CGNAT
■ [7] <u>Vídeo techdroy - Análisis TP-Link TL-MR6400 </u>	(5) Comprobar conexión clientes VPN:
TODO lo que DEBES saber de este ROUTER 4G	a) Portátil : deshabilitar WiFi e conectar á
LTE	roseta da aula.
[8] www.no-in.com (Dynamic DNS)	h) Móbiles alumnado

Procedemento:

- 1. Prerrequisito: Realizar esta práctica unha vez rematada e validada a Práctica 61 [1]
- 2. Entrega/Revisión material necesario para a práctica:





Figura 2: Lateral dereita

Figura 4: Trasera



Figura 5: Unboxing 1

- - Figura 6: Unboxing 2
- a) Avisar ao docente para a revisión.
- 3. Conectar os dispositivos móbiles do alumnado ao router e cubrir a Táboa 1. Móbiles alumnado

4. Portátil:

a) Acceder mediante o navegador firefox á URL <u>http://192.168.1.1</u> e Iniciar sesión:

$\leftarrow \ \ \rightarrow \ \ G$	◊ Å 192.168.1.1		☆	⊚ ≡
	P tp-link	Espa	añol 💙	
	ی Se te olvidó tu contraseña?			
	Iniciar sesión Iniciar sesión con ID de TP-			
	Link			
	TL-MR6400 300Mbps Wireless N 4G	LTE Router	Aplicación	

b) Dirixirse a Avanzado → VPN → OpenVPN

$\leftarrow \rightarrow C$	0 8	192.168.1.1						90% 5	3
	P	tp-link	Configuració rápida	ⁿ BÁSICO	Avanzado	Español 💙	Cerrar sesión	X Reiniciar	
	Q Bu	scar	OpenVP	N				0	
	¢	Controles parentales	Nota: No h	ay certificado actualmente,	por favor, Generar uno antes de	e habilitar el servidor VPN.		_	
	ţ↑	QoS	Tipo de se	rvicio:	Habilitar servidor VPN UDP				
	۲	Seguridad	Puerto de	servicio:	1194				
	ø	VPN	VPN Subn	et / Netmask: clientes:	10 · 8 · 0 · 0	255 · 255 · 255 · 0			
		- OpenVPN					Guardar		
		- PPTP VPN	Certifica	do					
		- VPN IPSec	Generar e	certificado.		_			
		- Conexiones VPN					Generar		
	٢	Herramientas de sistema	Archivo Exportar la	de configuración				_	
	Versió	n de firmware:1.4.0 0.9.1 v0001.	0 Build 220506 Rel.5	555n Versión del har	dware:TL-MR6400 v5.3 000000	2 IMEI:861436064254737	Backup	Aplicación	



c) Este router mediante la configuración de OpenVPN permite 2 tipos de conexiones VPN a los clientes: Sólo red doméstica e Internet y red doméstica

Acceso de clientes

Seleccione el tipo de acceso para el cliente OpenVPN.

Sólo red doméstica - El cliente solo puede acceder a la red doméstica. La ruta por defecto del cliente no se cambiará. Internet y red doméstica - El cliente puede acceder a la red doméstica y a los sitios o servicios de Internet con una limitación geográfica cuando se encuentre fuera del país. La ruta por defecto del cliente será alterada.

d) Pero antes de Habilitar servidor VPN debemos:

(1) Comprobar que a configuración da data é hora do router son as que corresponden á nosa zona horaria(+1): Avanzado → Herramientas de sistema → Ajustes de hora

$\leftarrow \rightarrow C$	🔿 웥 192.168.1.1		ជ	⊗ ≡
	Ptp-link	Configuración BÁSICO Avanzado Español 💙	오 米 Cerrar sesión Reiniciar	
	Q Buscar Herramientas de sistema	Hora del sistema		
	- Ajustes de hora	Hora actual: 14/07/2023 12:55:10 Zona horaria: (GMT + 01: 00) Ámsterdam, Berlín, Roma, Estocolmo, París, Praga, Bratisi	ava 👻	
	- Control de LEDs - Diagnósticos	Fecha: 14/7/2023 (DD / MM / YY) Hora: 12 * : 54 * : 42 *		
	- Actualización de firmware	Servidor NTP II: 0.0.0.0 (Opcional) Servidor NTP II: 0.0.0.0 (Opcional)		
	- Copia de segundad y Restauracion - Reiniciar	Obtener la hora del PC Obtener la hora de internet	Guardar	
	- Administración	Horario de verano		
	- Registro del sistema Versión de firmware:1.4.0 0.9.1 v0001.0	Habilitar el horario de verano Build 220506 Rel.57555n Versión del hardware:TL-MR6400 v5.3 00000002 IMEI:861436064254737	Backup Aplicación	

(2) Xerar un certificado: Certificado → Generar el certificado → Generar

Generar el certificado.	
	Generar
ertificado	
nerar el certificado.	
	Generar
Exitoso	

(3) De non dispoñer de IP estática en Internet, é dicir, se non temos contratada co ISP unha IP estática de saída a Internet, debemos xerar/configurar unha conta DDNS (DNS Dinámico). Así, imos configurar no router unha conta DNS Dinámico para que aínda que a IP que empreguemos para saír a Internet non sexa sempre a

NOT

mesma poidamos acceder á noso router sempre co mesmo nome DNS. Se non fose así, de cada vez que un cliente se quixera conectar por VPN ao noso router debería saber a IP que o router ten concedido nese momento polo ISP.

$\leftarrow \rightarrow C$	🔿 웥 192.168.1.1		90%	☆ ♡ ≡
	Ptp-link	Configuración BÁSICO Avanzado Español 🌱 cerrar ses	sión Reiniciar	
	Q Buscar		0	
	🜐 Red	Configuración Dinámico de DNS		
		Proveedor de servicio:		
	- Internet	DDNS no disponible		
	- Actualización ISP	Para usar nuestro servicio superior de TP-Link DDNS, Log in con su cuenta TP-Link Cloud, o elija otro proveedor d	ie	
	- Gestión del PIN	servicios.		
	- Configuraciones de datos	Nombre de dominio actual:		
	- Configuración de LAN	Lista de nombres de dominio		
	- DNS Dinámico	Nombre de dominio La fecha registrada Estado Operación I	Modificar	
	- Enrutamiento estatico		-	
	- Túnel IPv6			
	- USSD			
	Versión de firmware:1.4.0 0.9.1 v0001.	Build 220506 Rel.57555n Versión del hardware:TL-MR6400 v5.3 00000002 IMEI:861436064254737 Bac	kup <u>Aplicación</u>	

Como podemos observar podemos configurar DNS Dinámico con: TP-Link, Dyndns e NO-IP. Imos xerar unha conta en NO-IP:

(a) Seguimos os pasos indicados na axuda:

Ricardo Feijoo 00

Proveedor de servicio:	⊖ TP-Link ⊖	Dyndns NO-IP Ir	al registro	
Nombre de usuario:				
Código secreto:		ø		
Iniciar sesión ⁿ Cerrar se	esión			
	Desconectado			
				Guardar
figuración Dinámico de DNS				
45 (Sistema de nombres de dominio dinâmico) le p isombre de dominio y host fijo a una dirección IP de imico. Es útil cuando está alojando su propio sitio v u otro servidor detrás del router. Para empezar, de un proveedor de servicios de DNS dinâmico como	ermite asignar Internet veb, servidor ebe registrarse			
v.dyndns.com -				
<u>v.dyndns.com</u> - a configurar un DNS dinámico				
<u>v.dyndns.com</u> a configurar un DNS dinámico ieleccione el proveedor de servicios de DNS dinámi	ico.			
<u>v.dyndns.com</u> . a configurar un DNS dinámico eleccione el proveedor de servicios de DNS dinâmi atroduzca el nombre de usuarlo y la contraseña de l NS dinámico.	ico. la cuenta de			
<u>volyndins.com</u> . a configurar un DNS dinámico eleccione el proveedor de servicios de DNS dinámi atroduzca el nombre de usuario y la contraseña de l NS dinámico. atroduzca el nombre de dominio que recibió del pro- ervicios de DNS dinámico.	ico. la cuenta de veedor de			
v.dyndns.com a configurar un DNS dinámico eleccione el proveedor de servicios de DNS dinámi troduzca el nombre de usuario y la contraseña de l NS dinámico. troduzca el nombre de dominio que recibió del pro- ervicios de DNS dinámico. laga clic en Iniciar sesión y haga clic en Guardar.	lco. la cuenta de veedor de			
<u>volyndins.com</u> . a configurar un DNS dinámico eleccione el proveedor de servicios de DNS dinámi atroduzca el nombre de usuario y la contraseña de l NS dinámico. atroduzca el nombre de dominio que recibió del pro- ervicios de DNS dinámico. laga clic en Iniciar sesión y haga clic en Guardar. a:	ico. la cuenta de veedor de			
<u>exityndins.com</u> . a configurar un DNS dinámico eleccione el proveedor de servicios de DNS dinámi troduzca el nombre de usuario y la contraseña de l NS dinámico. troduzca el nombre de dominio que recibió del pro- ervicios de DNS dinámico. laga clic en Iniciar sesión y haga clic en Guardar. a: esea usar una nueva cuenta DDNS, primero clerre jo inicie sesión con la nueva cuenta.	ico. la cuenta de veedor de la sesión y			

(b) Configuración Dinámico de DNS

DDNS (Sistema de nombres de dominio dinámico) le permite asignar un nombre de dominio y host fijo a una dirección IP de Internet Dinámico. Es útil cuando está alojando su propio sitio web, servidor FTP u otro servidor detrás del router. Para empezar, debe registrarse con un proveedor de servicios de DNS dinámico como <u>www.dyndns.com</u>.

I. Acceder a <u>www.no-ip.com</u> e xerar o dominio grupontallersrvpn.ddns.net, onde o primeiro *n* toma o valor do número do grupo de prácticas.



II. Clic en *Inscribirse* e cubrir os campos do formulario solicitado. Modificar no correo electrónico o carácter *n* polo número do grupo que corresponda e os números *2223* polos correspondentes ao curso académico actual.

NOTA₂: No caso que non teñades xerado o correo electrónico de gmail debedes crealo.

grupontallersr2223@gmail.com	
Contraseña	Show password
Password strength: Strongest.	
Hostname	
grupontallersrvpn	.ddns.net 🗸
Crear mi nombre de host después	
Termino del Servicio y Política de Privaci	idad
Termino del Servicio y Política de Privaci → By checking this box, I agree to the Te agree that I will only create one free a	idad erms of Service and Privacy Policy. I also account.
Termino del Servicio y Política de Privaci ✓ By checking this box, l agree to the Te agree that I will only create one free a Optar en Correo Electrónico	idad erms of Service and Privacy Policy. I also account.
 Termino del Servicio y Política de Privaci By checking this box, I agree to the Te agree that I will only create one free a Optar en Correo Electrónico Desbloquee ofertas exclusivas e infor interno de No-IP ahora! 	idad erms of Service and Privacy Policy. I also account. rmación de vanguardia. ¡Únase al círculo

III. Clic en Free Sign Up

IV. Automaticamente accederemos á conta recén xerada na interface de no-ip indicándonos que temos que acceder ao correo electrónico que configuramos no formulario e activar a conta no-ip. Polo tanto accedemos á conta do correo electrónico e activamos a conta no-ip abrindo o correo recibido e facendo clic en *Confirm Account*:

🔲 🕁 Ď No-IP Notices

Confirm Your No-IP Account - Confirm Your No-IP Account Thanks for creating a N...

Confirm Account

V. Conta activada:



Así, Paso 2 → https://www.noip.com/es-MX/download

Pero non é necesario, xa que o *Paso 2* e o *Paso 3* conseguímolo configurando a conta de no-ip no router. Así, tiñamos a seguinte información na axuda:

Para configurar un DNS dinámico

1. Seleccione el proveedor de servicios de DNS dinámico.

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

- 2. Introduzca el nombre de usuario y la contraseña de la cuenta de DNS dinámico.
- 3. Introduzca el nombre de dominio que recibió del proveedor de servicios de DNS dinámico.
- 4. Haga clic en Iniciar sesión y haga clic en Guardar.

Nota:

Si desea usar una nueva cuenta DDNS, primero cierre la sesión y luego inicie sesión con la nueva cuenta.

Polo cal, agora introducimos usuario e contrasinal de no-ip na configuración Dynamic DNS. Pero primeiro debemos xerar un Nombre de usuario na nosa conta no-ip, co cal dirixirse a URL <u>https://my.noip.com/account</u> e configuralo:

configuralo:				
Información básica Correo electrónico	Contraseña		Nombre de usuario	
grupo7tallersr@gmail.com				
Cambiar correo electrónico	Cambiar contraseña		Agregar nombre de usuario	
Facer clic en Agregar nombre d	e usuario einse r	tar o voso nome de	e usuario:	
O Actualizar nombre de	usuario			
Nota : Actualizar su contraseña puede afec excepto Windows DUC v3.0 y versiones pos Nuevo nombre de usuario grupontallersr2223	tar a todos los clientes de act teriores. Para crear contrasei	ualización dinámica (DUC d ìas de cuentas y credencia Can	de No-IP o dispositivos integrados), les DDNS individuales, cree un grupo . celar Guardar	
Facer clic en <i>Guardar</i> Tamén é necesario actualizar o <i>Huse</i>	o Horario na conf	iguración da conta]	
Información do bora o idioma		.8		
Idioma	а	Huso horario		
Espanol	~	GMT+01:00 - Brussels, Coj	penhagen, Madrid, Paris	~
				Guardar
Agora si cubrir no router os campos o	do formulario Dynar	nic DNS \rightarrow Inic	ciar sesión → Guard	ar
Configuración Dinámico de D	ONS		(?

Proveedor de servicio:	○ TP-Link ○ Dyndns
Nombre de usuario:	grupontallersr2223@gmail.com
Código secreto:	Ø
Nombre de dominio:	grupontallersrvpn.ddns.net
Iniciar sesión Cerrar sesión	Desconectado
	Guardar

- e) Avisar ao docente para revisión 2
- f) Agora que xa temos todos os prerrequisitos realizados xa podemos configurar a conta VPN. Así:

$\leftarrow \rightarrow C$	08	o - 192.168.1.1						90%	☆	⊚ ≡
	P	tp-link	Configuración rápida	BÁSICO	Avanzado	Español 💙	Cerrar sesión	兴 Reiniciar		
	Q Bu	scar	OpenVPN					?		
	¢	Controles parentales			 Habilitar servidor VPN 			-		
	î↓	QoS	Tipo de servici	D:	● UDP ○ TCP					
	٢	Seguridad	Puerto de serv VPN Subnet / I	icio: Netmask:	1194	0 255 · 255 · 255 · 0				
	ø	VPN	Acceso de clie	ntes:	 Sólo red doméstica 	Internet y red doméstica				
		- OpenVPN					Guardar			
		- PPTP VPN	Certificado							
		- VPN IPSec	Generar el cer	ificado.			Generar			
		- Conexiones VPN	Archivo de o	configuración						
	٢	Herramientas de sistema	Exportar la cor	figuración.			Exportar			
	Versió	n de firmware:1.4.0 0.9.1 v0001.	0 Build 220506 Rel.57555	n Versión del ha	rdware:TL-MR6400 v5.3 000000	002 IMEI:861436064254737	Backup A	plicación		

g) Falta exportar o certificado para que o poidan empregar os clientes na súa conexión VPN:

Archivo de configuración	
Exportar la configuración.	Exportar
单 Abriendo client.ovpn	~ □ X
Ha elegido abrir:	
🔲 client.ovpn	
que es: documento de texto sencillo (2,6 KB) de: http://192.168.1.1	
¿Qué debería hacer Firefox con este archivo?	
Abrir c <u>o</u> n Mousepad (predeterminada)	~
💽 G <u>u</u> ardar archivo	
Hacer esto automáticamente para estos archivos a	a partir de ahora.
Cancel	ar Aceptar

5. Clientes VPN: Podemos proceder como se indica na axuda do router:

Guía de instalación de cliente VPN

Antes de configurar el servidor OpenVPN, configure el Servicio DNS Dinámico (recomendado) o asigne una dirección IP estática para el puerto WAN. Y asegúrese de que el puerto externo de configuración de NAT no sea el puerto de servicio y que la Hora del sistema esté sincronizada con Internet.

Para conectar los dispositivos cliente al servidor OpenVPN:

- 1. Seleccione Activar servidor VPN.
- 2. Configure los parámetros del servidor OpenVPN (Tipo de servicio, Puerto de servicio, Acceso de cliente y Máscara de red / máscara de VPN) y haga clic en Guardar.
- 3. Haga clic en Exportar para guardar el archivo de configuración.
- 4. En los dispositivos cliente, descargue e instale la utilidad de cliente OpenVPN desde el sitio web openvpn.net. Las plataformas oficiales compatibles incluyen Windows, Mac OSX y Linux.
- 5. Inicie la utilidad de cliente OpenVPN y agregue una nueva conexión VPN utilizando el archivo de configuración guardado para conectar el dispositivo cliente al servidor VPN.

Nota: para obtener más información sobre los clientes OpenVPN, visite el sitio web openvpn.net.

Pero imos empregar outros clientes gráficos para poder establecer a conexión vpn mediante openvpn.

6. CGNAT Activado?

Definición CGNAT:

CGNAT (Carrier-Grade Network Address Translation)(Tradución de Direccións de Rede de Nivel de Portador) é unha técnica que se utiliza nos provedores de servizos de Internet (ISP) para conservar e compartir direccións IP públicas entre varios clientes. En resumo, CGNAT é unha solución para enfrontar a escaseza de direccións IP públicas IPv4.

Á medida que a demanda de direccións IP públicas IPv4 aumentou exponencialmente debido ao crecemento de Internet e a proliferación de dispositivos conectados, a cantidade de direccións IPv4 dispoñibles tórnase limitada. Para solucionar este problema, os ISP implementan CGNAT para compartir un conxunto limitado de direccións IP públicas entre varios clientes.

Funcionamento CGNAT:

1. Os clientes dun ISP reciben direccións IP privadas dentro dun rango específico (por exemplo, 10.0.0.0/8 ou 192.168.0.0/16) nas súas redes locais.

2. Cando un dispositivo na rede local dun cliente desexa comunicarse coa Internet, o router ou gateway do ISP realiza unha tradución da dirección de rede, convertendo a dirección IP privada do cliente nunha dirección IP pública compartida.

3. Os paquetes de datos enviados desde o dispositivo do cliente a través da dirección IP pública compartida pasan polo CGNAT do ISP. O CGNAT mantén unha táboa de tradución que asocia a dirección IP pública compartida coa dirección IP privada orixinal do cliente.

4. Cando os paquetes de datos de resposta regresan desde a Internet á dirección IP pública compartida, o CGNAT redirixeos ao cliente correcto segundo a táboa de tradución.

Esta técnica permite que varios clientes compartan a mesma dirección IP pública, o que estende o uso de direccións IPv4 e atrasa a necesidade de migrar a IPv6, que ofrece un espazo de direccións moito máis amplo.

Non obstante, CGNAT tamén pode ter algunhas limitacións, como dificultar o acceso a servizos de rede desde o exterior (como servidores VPN, web ou xogos en liña) debido á tradución de direccións e á falta dunha dirección IP pública dedicada para cada cliente.

En resumo, CGNAT é unha solución temporal para a escaseza de direccións IPv4 e permite aos ISP seguir proporcionando servizos de Internet a un gran número de clientes mentres se planifica e se migra gradualmente a IPv6, que ofrece un espazo de direccións IP moito máis grande e evita a necesidade de CGNAT.

Para determinar se o router TL-MR6400 está detrás dunha conexión CGNAT, segue estes pasos:

1. Accede á configuración do router TL-MR6400 a través dun navegador web ingresando a dirección IP do router na barra de direccións. A dirección IP predeterminada do router TP-Link é tipicamente 192.168.0.1 ou 192.168.1.1. Se cambiaches a dirección IP do router, utiliza a nova dirección que configuraches.

2. Unha vez dentro da configuración do router, busca a sección de "BÁSICO" \rightarrow "Mapa de red" \rightarrow "Internet" \rightarrow "Dirección IP". Deberías atopar alí a dirección IP pública que o router está a recibir do provedor de servizos de Internet (ISP). Esta dirección IP é a que o ISP asigna ao router para identificalo en Internet.

$\leftarrow \ \ \rightarrow \ \ {\tt G}$	◊ 👌 192.168.1.1		90% ☆ ♡ ≡
	Ptp-link	Configuración BÁSICO Avanzado Español Y Cerrar sesión	** Renicar
	Q Buscar	46 1111 2.46Hz	0
	🐴 Mapa de red	Internet TL-MR6400	
	Internet		
	Red inalámbrica		
	Red de invitados	Clientes inalámbricos Clientes Cableados Mensaje	
	Controles parentales		
	C TP-Link Cloud	Internet	
		Nombre de la interfaz WAN: LTE	-
		Estado de Internet: Conectado	
-		Dirección IP: 10.3.28.14 / ::	
		Servidores DNS: 217.168.13.34 46.6.113.34 / :: ::	
	Versión de firmware:1.4.0 0.9.1 v0001.0	Build 220506 Rel.57555n Versión del hardware:TL-MR6400 v5.3 00000002 IMEI:861436064254737 Backup	Aplicación

Tamén pódese atopar esa información en:

"Avanzado" → "Herramientas del sistema" → "Administración" → "Gestión Remota"

$\leftarrow \rightarrow C$	🔿 웥 192.168.1.1	90% ☆ ♡ ≡	
	Ptp-link	Configuración BÁSICO Avanzado Español Y	Cerrar sesión Reiniciar
	Q Buscar	Gestión remota	0
	Herramientas de sistema	Gestión remota:	
	- Ajustes de hora	Gestión remota a través de HTTPS: Habilitado	
	- Control de LEDs	Puerto: 80 Administre este router a través de la dirección:	
	- Diagnósticos	http://10.3.28.14 o	
	- Actualización de firmware	http://grupontallersrvpn.ddns.net	
	- Copia de seguridad y Restauracion	Dispositivo cliente permitido para la administración remota:	
	- Reiniciar		
	- Administración	TODOS	Guardar
	- Registro del sistema	Certificado	
	- Configuraciones CWMP	La gestión local a través de HTTPS y la gestión remota a través de HTTPS están deshabilitadas.	
	Versión de firmware:1.4.0 0,9.1 v000	Decentrati cettiliceti Build 220506 Rel.57555n Versión del hardware:TL-MR6400 v5.3 00000002 IMEI:861436064254737	Backup Aplicación

3. Anota a dirección IP pública que se mostra na configuración do router na Táboa3. CGNAT

4. Logo, abre un navegador web e accede a un sitio web que te mostre a túa dirección IP pública actual, como "https://www.whatismyip.com/" ou "https://www.whatismyip.net/" e anota a dirección IP pública que se mostra na configuración do router na *Táboa3*. CGNAT

5. Compara a dirección IP pública obtida no paso 3 coa dirección IP pública mostrada no sitio web, no paso 4. Se ambas as direccións IP son diferentes, isto indica que o router TL-MR6400 está detrás dunha conexión CGNAT.

Se as direccións IP públicas son diferentes, o router TL-MR6400 está detrás dun CGNAT implementado polo ISP. Isto pode afectar a configuración de certos servizos ou aplicacións que requiren acceso externo a dispositivos na túa rede local, como servidores VPN ou servidores web.

E se as direccións IP públicas son iguais, o router TL-MR6400 non está detrás dun CGNAT implementado polo ISP, sendo posible o acceso externo de clientes a dispositivos na túa rede local, como servidores VPN ou servidores web.

En calquera caso, seguiremos coa práctica tendo en conta que se se está detrás dun CGNAT non será posible a conexión de clientes VPN co noso router.

7. Avisar ao docente para revisión 3

8. Clientes VPN

a) Cliente gráfico GNU/Linux → NetworkManager OpenVPN

Portátil: Empregar o portátil como cliente VPN GNU/Linux

Existen varios clientes gráficos de OpenVPN dispoñibles para distribucións GNU/Linux como Debian. Un dos clientes máis populares e amplamente utilizado é "NetworkManager-openvpn". A continuación, proporciónase un procedemento xeral para utilizar NetworkManager-openvpn en Debian (ou en sistemas baseados en Debian):

- 1. Nunha consola executar:
 - \$ setxkbmap es
 - \$ sudo apt update && sudo apt-get install network-manager
- 2. Engadir unha nova conexión VPN no cliente gráfico NetworkManager:

NetworkManager \rightarrow Conexiones VPN \rightarrow Añadir una conexión VPN

E.	^ _ X
	Elegir un tipo de conexión VPN
	Seleccione el tipo de VPN que quiere usar para la nueva conexión. Si el tipo de conexión VPN que quiere crear no aparece en la lista, puede que no tenga instalado el complemento de VPN correcto.
	Cancelar Crear

- 3. É preciso ter instalado o paquete "network-manager-openvpn" para habilitar o soporte de OpenVPN en NetworkManager:
 - \$ sudo apt-get install network-manager-openvpn

- 4. Reinicia o servizo NetworkManager para asegurarte de que os cambios se aplican correctamente:
 - \$ sudo systemctl restart NetworkManager
- 5. Agora, deberíades poder atopar unha nova opción de conexión VPN no menú de rede do voso entorno de escritorio (ver paso 2.)

E	^ _ X		
	Elegir un tipo de conexión VPN		
Seleccione el tipo de VPN que quiere usar para la nueva conexió tipo de conexión VPN que quiere crear no aparece en la lista, pue que no tenga instalado el complemento de VPN correcto.			
	OpenVPN 👻		
	Compatible con el servidor OpenVPN.		
	Cancelar Crear		

6. Na configuración de VPN, selecciona a opción para engadir unha nova conexión e escolle "Importar una configuración VPN guardada..."

<u>R</u>	^ _ X		
	Elegir un tipo de conexión VPN		
	Seleccione el tipo de VPN que quiere usar para la nueva conexión. Si el tipo de conexión VPN que quiere crear no aparece en la lista, puede		
	OpenVPN		
	Importar una configuración VPN guardada		
	Cancelar Crear		

7. Localiza e selecciona o arquivo de configuración de OpenVPN que exportáchedes dende o router TP-Link TL-MR6400.

Cancelar	Seleccione el archivo que importar Introducir ubicación	٩	Abrir
⊘ Recientes	client.ovpn		

8. Completa calquera campo adicional necesario, como as credenciais de autenticación, segundo a configuración da túa conexión VPN.

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

E.		Editando clier	ıt-tp-link	^ _ O X
Nombre de	la conexión	client-tp-link		
General	Proxy	Ajustes de IPv4	Ajustes de IPv6	
Método	Automático	o (VPN)		•
Direccio	nes estátic	as adicionales		
Direco	:ión №	láscara de red	Puerta de enlace	Añadir Eliminar
5	Servidores D	NS adicionales		
Dominic	os de búsque	da adicionales		
				Rutas
Exportar			Cance	elar 🗸 Guardar

- 9. Garda a configuración e intenta establecer a conexión VPN seleccionando a nova conexión no menú de rede.
- 10. Avisar ao docente para revisión 🗌

NOTA₃: Ten en conta que os pasos específicos poden variar lixeiramente segundo o entorno de escritorio que estás a utilizar na túa distribución Debian. Asegúrate de consultar a documentación do entorno de escritorio ou os recursos específicos da túa distribución para obter instrucións máis detalladas.

b) Cliente gráficoAndroid → OpenVPN Connect

Móbiles Android

Existen varios clientes gráficos de OpenVPN dispoñibles para dispositivos móbiles Android que che permiten conectarte a unha conexión OpenVPN. Un dos clientes máis populares e amplamente utilizado é "OpenVPN Connect". A continuación, proporciónase un procedemento xeral para utilizar OpenVPN Connect nun teléfono móbil Android:

- 1. Instalar a aplicación "OpenVPN Connect" dende Google Play Store e seguir o proceso de instalación normal.
- 2. Unha vez instalado, abrir a aplicación "OpenVPN Connect" no teléfono móbil Android.
- Transferir o certificado de cliente necesario e o arquivo de configuración que exportaches dende o router TP-Link TL-MR6400 ao teléfono móbil. Pódese facer mediante correo electrónico, almacenamento na nube ou outra forma de transferencia de arquivos.

- 4. No teléfono móbil, abrir a aplicación "OpenVPN Connect" e seleccionar a opción de importar a configuración ou o arquivo de configuración.
- 5. Localizar e seleccionar o arquivo de configuración de OpenVPN que se transferiu ao teléfono móbil.
- 6. A aplicación importará automaticamente a configuración e mostrará unha lista de perfís VPN dispoñibles.
- 7. Seleccionar o perfil VPN correspondente á conexión OpenVPN configurada no router TP-Link TL-MR6400.
- 8. Introducir as credenciais de autenticación se é necesario.
- 9. Tocar o botón de conexión para establecer a conexión VPN.
- 10. Unha vez completados estes pasos, OpenVPN Connect intentará establecer a conexión utilizando a configuración proporcionada. Se a conexión é exitosa, verase unha mensaxe indicando que se está conectado ao router TP-Link TL-MR6400 a través de OpenVPN.
- 11. Cubrir a Táboa2. VPN: Móbiles alumnado

12. Avisar ao docente para revisión 🗌 5

NOTA₄: Recorda que os pasos específicos poden variar lixeiramente dependendo da versión da aplicación "OpenVPN Connect" e da configuración exacta da túa conexión OpenVPN.

9. Razoa. Contesta brevemente:

- a) Definir NTP. Por que é necesario para que funcionen as conexións VPN?
- b) Definir IP Estática ofrecida polo ISP.
- c) Definir IP Dinámica ofrecida polo ISP.

d) Se o noso ISP ofrecenos unha IP Dinámica, por que e para que configurar Dynamic DNS no router do noso domicilio?

- e) Definir VPN.
- f) Pódese acceder mediante unha conexión VPN a servidores configurados nun domicilio?

g) Pódese mediante unha conexión VPN acceder a un domicilio e saír a Internet como se estivésemos "in situ" no domicilio?

h) Imaxinemos que unha páxina web soamente deixa acceder dende unha localización dentro de Galicia. Poderiades fóra de Galicia acceder a esa páxina web? Como?

- i) Para que serve o comando GNU/Linux traceroute
- j) Existen diferencias ao executar o comando seguinte nunha consola nun cliente GNU/Linux (Portátil):
- \$ traceroute www.google.es

Nunha conexión VPN e nunha conexión a Internet non VPN(WiFi ou ethernet)?

- k) CGNAT: Executa e explica o que fan os seguintes comandos:
 - \$ wget -q0- https://ipinfo.io/ip
 - \$ host grupontallersrvpn.ddns.net
 - \$ dig grupontallersrvpn.ddns.net
 - \$ nslookup grupontallersrvpn.ddns.net

Compara a saída coa Táboa3. CGNAT. Que acontece? Que podes concluír con respecto a CGNAT?

- I) CGNAT: Executa e explica o que fan os seguintes comandos:
 - \$ wget -qO- https://ipinfo.io/ip
 - \$ host grupontallersrvpn.ddns.net 8.8.8.8
 - \$ dig @8.8.8.8 grupontallersrvpn.ddns.net
 - \$ nslookup grupontallersrvpn.ddns.net 8.8.8.8

Compara a saída coa Táboa3. CGNAT. Que acontece? Que podes concluír con respecto a CGNAT?

Que ten de diferente este apartado co anterior?

m) Se o noso ISP ten activado CGNAT e configuramos VPN no router, é posible que os clientes externos á nosa rede poidan acceder coa nosa conexión VPN configurada? Fai un diagrama que explique a túa resposta.

n) Se o noso ISP ten activado CGNAT e configuramos NAT Forwarding(redirección de portos) no router, é posible que os clientes externos á nosa rede poidan acceder a un servidor web que temos configurado nun equipo pertencente á nosa rede? Fai un diagrama que explique a túa resposta.

10. Avisar ao docente para a entrega e revisión da práctica.

Táboa 1: Móbiles alumnado

Móbil alumnado	MAC-Address
1	
2	
3	

Táboa 2: VPN: Móbiles alumnado

Móbil alumnado	MAC-Address
1	
2	
3	

Táboa 3: CGNAT

Fonte	IP Pública
Router TL-MR6400	
https://www.whatismyip.com/	
https://www.whatismyip.net/	

Revisión:



Ricardo Feijoo Costa