SoftEther VPN

¿Que es una VPN?

- VPN (Virtual Private Network) es una tecnología de red que permite conectar uno o más ordenadores en una red privada virtual, a través de una red pública como Internet.

  De esta forma, dos dispositivos o más pueden conectarse e intercambiar datos de forma segura y privada a través de un usuario y contraseña.

¿Que es Softether VPN?

- SoftEther VPN es un software VPN multiprotocolo que podemos utilizar en sistemas operativos como Windows, Linux o macOS, entre otros.

- Cuenta con un protocolo propio: SSL-VPN que está optimizado totalmente para esta herramienta, por lo que ofrece un rendimiento muy rápido, baja latencia y resistencia al firewall.

Características de Softether

- Es gratuito y de código abierto.
- Fácil de establecer VPN site to site y de acceso remoto (en windows).
- Tunelación SSL-VPN en HTTPS para atravesar tanto NAT como Firewalls.
- Funciones de VPN sobre ICMP y DNS.
- Puentes Ethernet y enrutamientos ip a través de VPN.
- DNS dinámico y NAT transversal integrados para que no se requiera una dirección IP fija o estática.
- Rendimiento de alta velocidad (1GBps) haciendo uso de bajo consumo de memoria y CPU.

- Admite gran variedad de sistemas operativos: Windows, Linux, Android, MAC, IPHONE, IPAD.
- Permite clonar Openvpn y permite clientes heredados.
- Varias formas de autentificación.
- SSL-VPN (HTTPS) es compatible con los principales protocolos VPN: OpenVPN, Ipsec, L2TP, MS-SSTP, ETHERIP, etc.
- Compatible con Azure Cloud.

DNS Integrado

- La función DDNS registra la dirección IP de su servidor VPN en el registro DNS de ".softether.net", que es el sufijo de dominio operado por SoftEther Corporation y la Universidad de Tsukuba, de forma gratuita.

- Se asignará un DDNS FQDN a su servidor VPN SoftEther. Puede decirle el nombre de host DDNS a los usuarios de su servidor VPN. Un usuario de su servidor VPN ahora puede especificar el nombre de host DDNS como destino.

NAT Transversal

Al utilizar los sistemas VPN existentes, se debe pedir al admin del firewall de la empresa que abra un punto final (puerto TCP o UDP) en el firewall / NAT en la frontera entre la empresa e Internet.

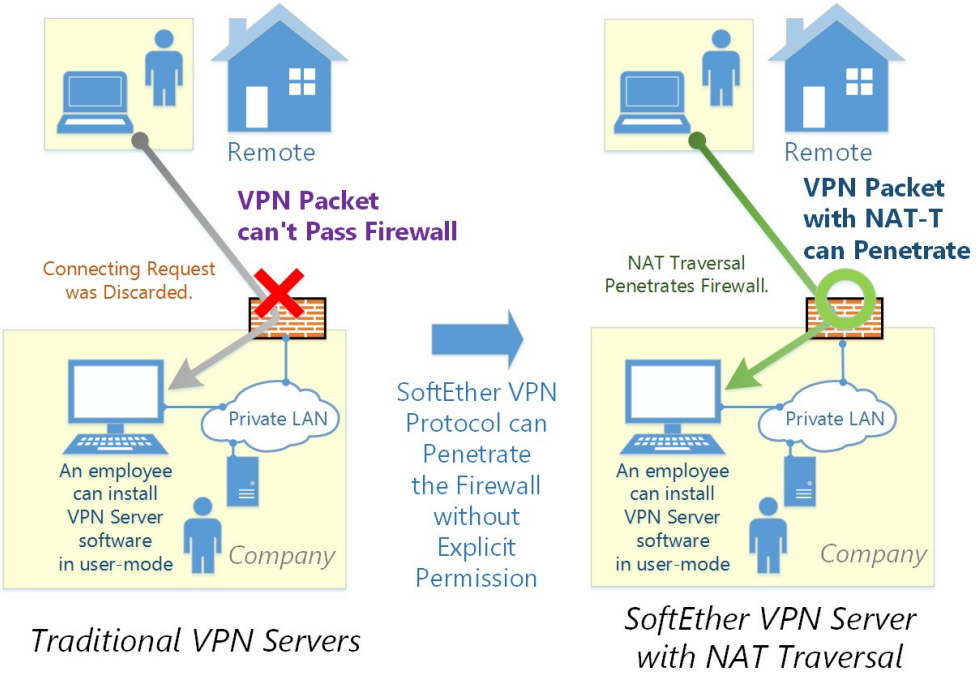
NAT Traversal está habilitado de forma predeterminada. Mientras está habilitado, las maquinas del Cliente VPN SoftEther pueden conectarse a su Servidor VPN detrás del firewall / NAT.

Compatibilidad OpenVPN

- Softether permite una fácil sustitución de openvpn tanto en Linux como en Windows.

  En Linux usando el comando OpenVpnEnable de forma que se clonara la configuración del servidor openvpn en el caso de existir.

  En Windows es aun mas fácil todavía, ya que al iniciar el servidor nos da la opción de cargar un fichero de configuración openvpn para usarlo.



Traditional VPN Servers

SoftEther VPN Server with NAT Traversal

Protocolos que usa Softether

- L2TP/IPsec - Internet Protocol security - Esta función es para aceptar conexiones VPN desde iPhone, iPad, Android, Windows y Mac OS X.
- MS-SSTP - Microsoft Secure Socket Tunneling Protocol - Implementa PPP sobre HTTPS (SSL). Encapsula todos los paquetes de usuario en TCP. Para que pueda pasar el cortafuegos fácilmente.
- L2TPv3 - puede establecer un túnel cifrado con IPsec entre el enrutador Cisco del sitio remoto y el servidor VPN SoftEther.
- EtherIP - protocolo de tunelacion ethernet.
- SSL-VPN - para segurizar las conexiones.

Comparativa con OpenVPN y Wireguard

	OpenVPN	Wireguard	SoftetherVPN
Rendimiento (velocidad de conexión)	100 mbps	900 mbps (aprox)	1 Gbps
Configuración	sencilla	sencilla	sencilla
Seguridad	baja	media-alta	alta
Estabilidad	buena	buena	buena
Transmisión de contenido	medio	alto	alto

Formas de autentificación

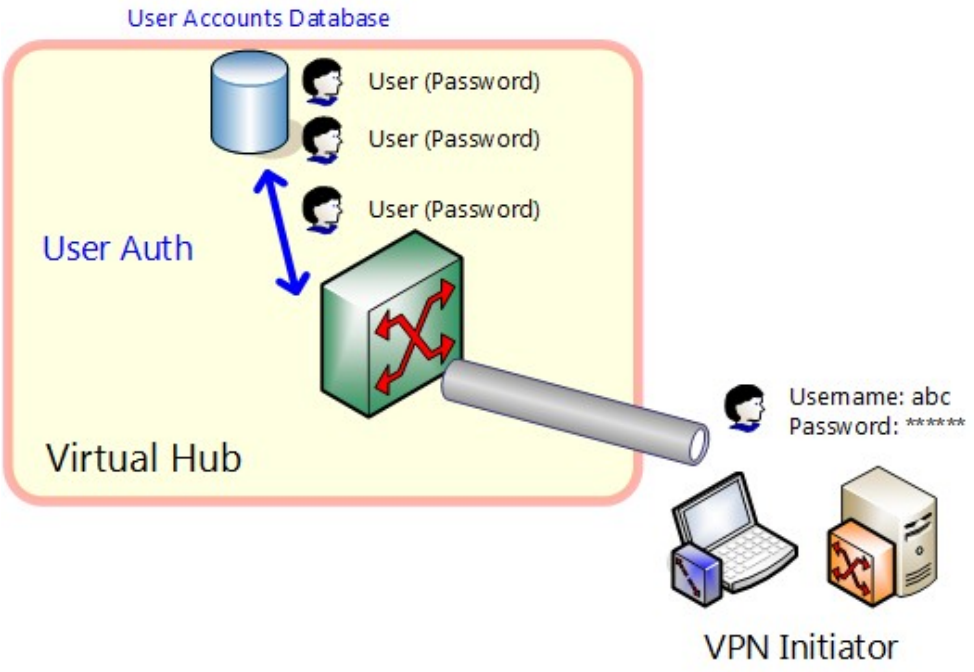
Anónima

- Es el tipo más simple de autenticación de usuario. Si existe un usuario configurado mediante autenticación anónima para Virtual Hub, cualquier persona que conozca el nombre de usuario puede conectarse a Virtual Hub y realizar una comunicación VPN.

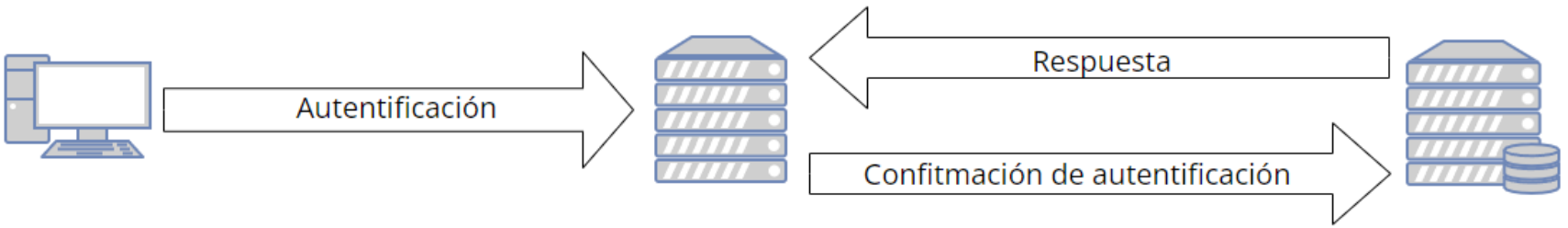
Este tipo de autentificación es la usada en los servidores públicos

https://www.vpngate.net/en/

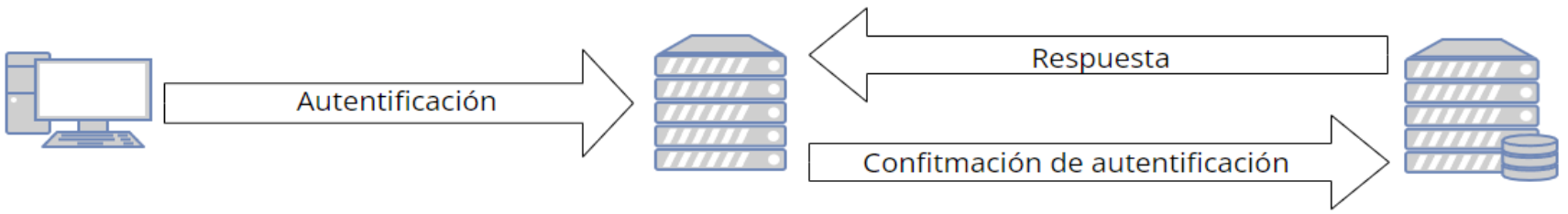
Por contraseña



RADIUS

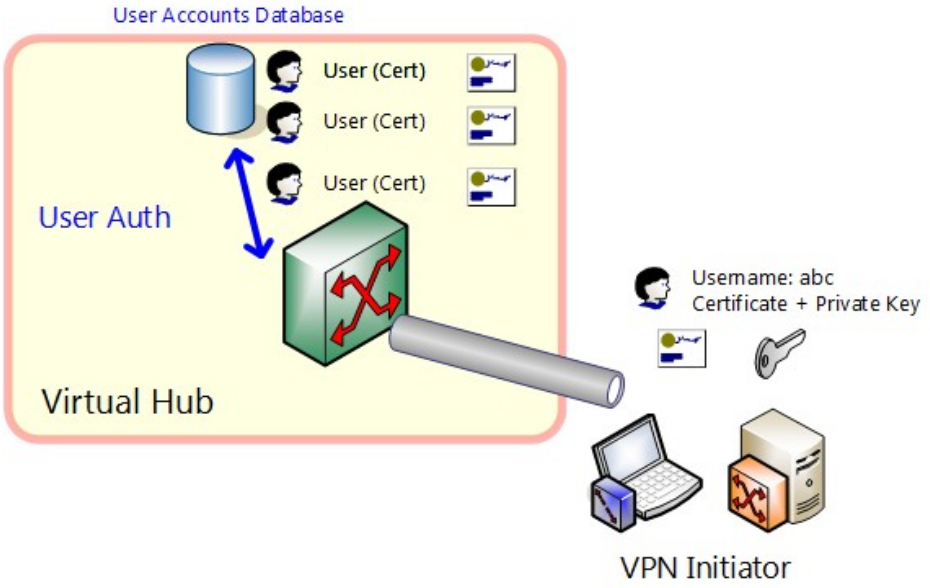

Autentificación
Respuesta
Confitmación de autentificación

NT Domine



Este caso es muy parecido al anterior, salvo que esta vez la confirmación del usuario la hace un servidor Windows NT que confirma los usuarios a través de AD.

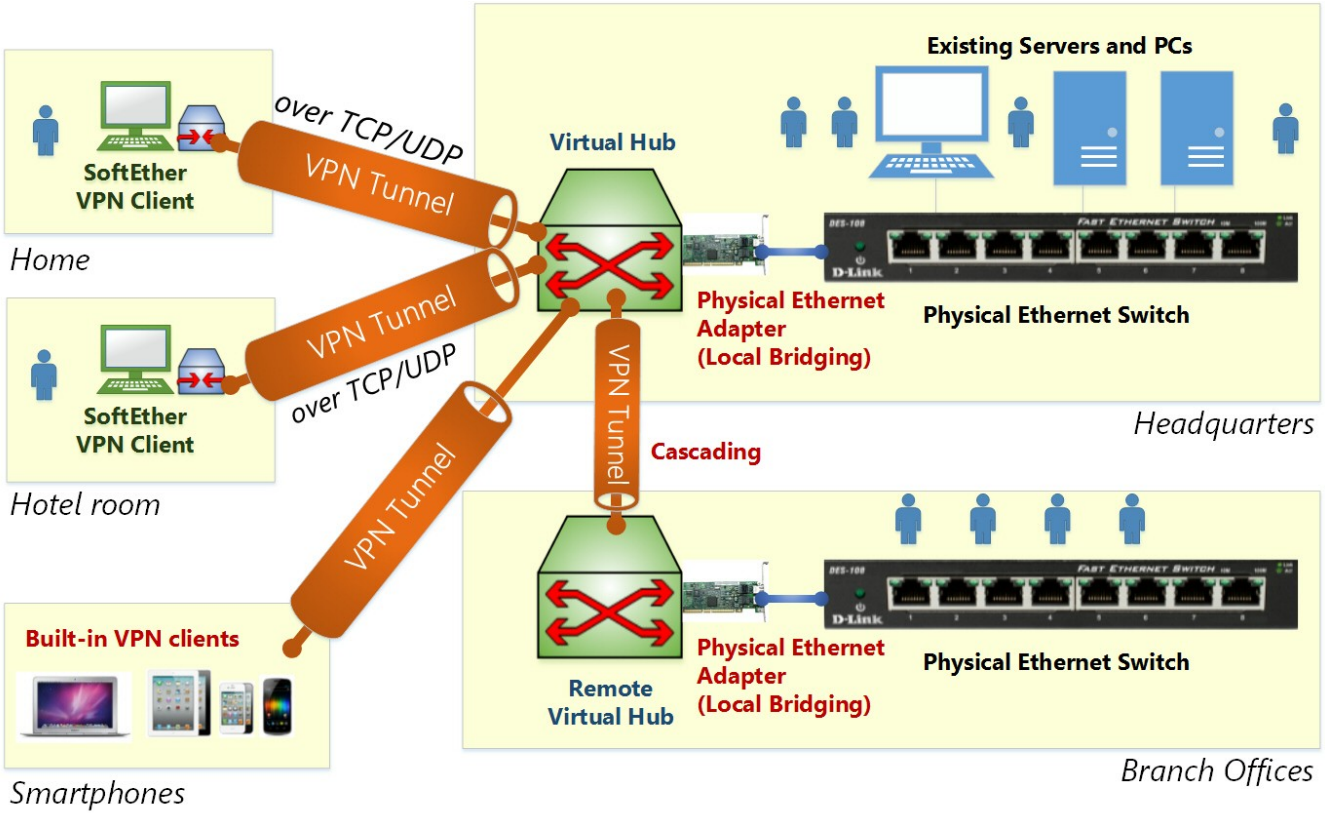
Certificado



En este caso podemos crear un certificado a través del propio servidor y mandarlo a los clientes para poder acceder o incluso usar let´s encript para crear los certificados y firmarlos.

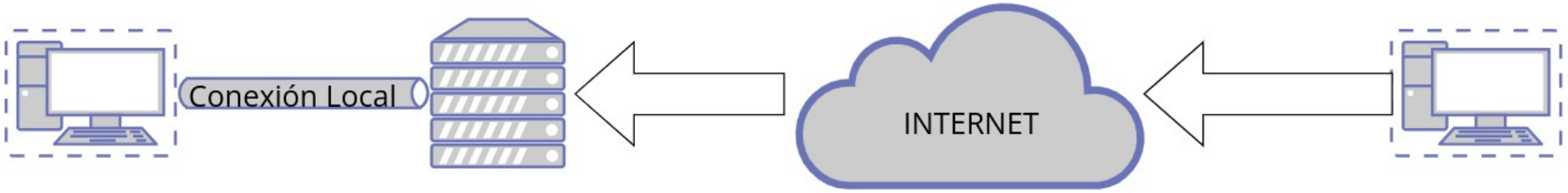
Arquitectura Softether

- Por parte del cliente creamos un adaptador de red virtual (una tarjeta de red virtual).
- Por parte del server/bridge creamos los virtual hubs (son el equivalente fisico a un switch).
- Los usuarios clientes se conectan mediante su adaptador creado al Hub, ya sea del server o del Bridge.


Existing Servers and PCs
Virtual Hub
over TCP/UDP
VPN Tunnel
SoftEther
VPN Client
Home
VPN Tunnel
over TCP/UDP
SoftEther
VPN Client
Hotel room
VPN Tunnel
Built-in VPN clients
Smartphones
Physical Ethernet
Adapter
(Local Bridging)
Physical Ethernet Switch
VPN Tunnel
Cascading
Headquarters
Remote
Virtual Hub
Physical Ethernet
Adapter
(Local Bridging)
Physical Ethernet Switch
Branch Offices

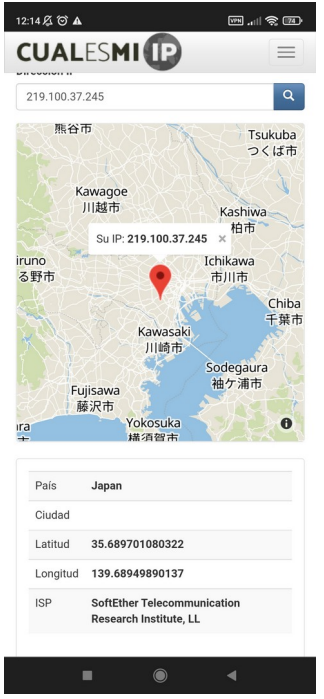
USOS

Acceso Remoto a LAN

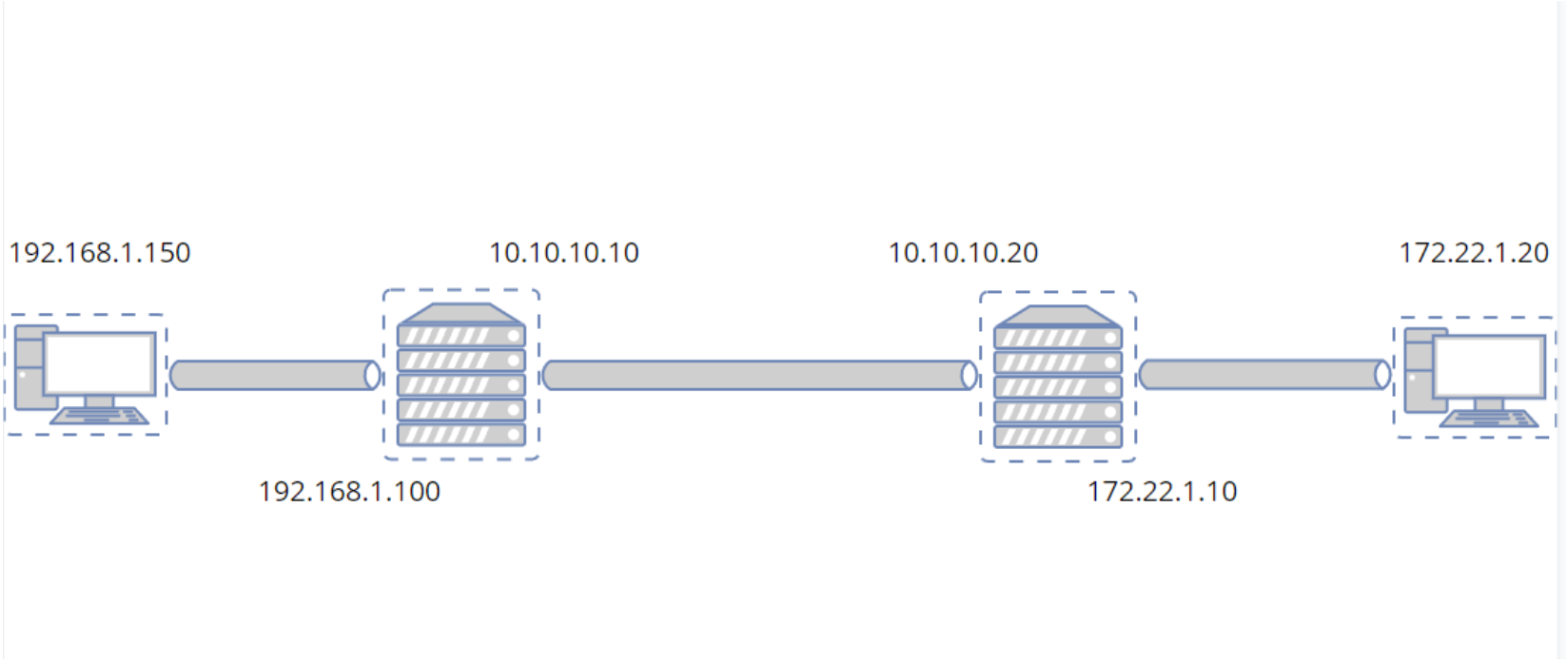


Practica android Remoto

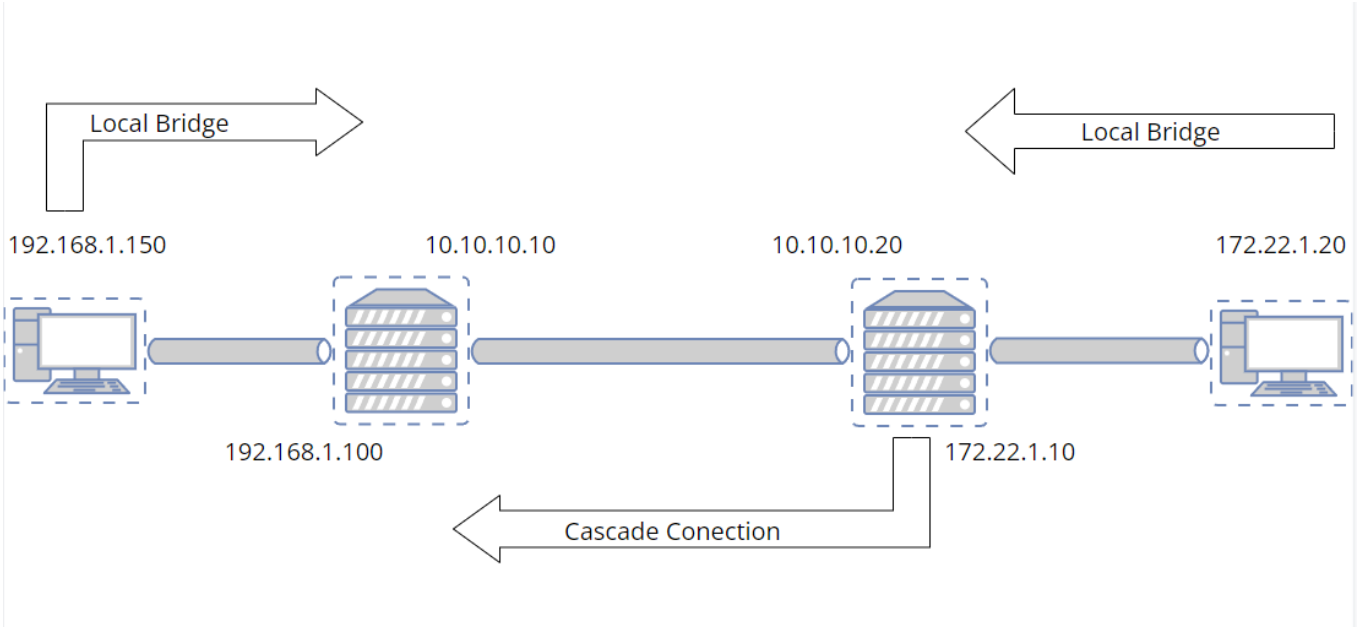

12:14
cual-es-mi-ip.net
CUALESMI IP
¿Qué diferencia hay entre dirección IP pública y privada?
La dirección IP puede ser pública o privada:
La dirección IP pública es un número único que identifica nuestra red desde el exterior.
La dirección IP privada es un número único que identifica a un dispositivo conectado en nuestra red interna.
Tu dirección IP es
219.100.37.245
Geolocalizar IP
Proveedor de Internet
Pais
Proxy
SoftEther Telecommunication Research Institute, LL
Japan
no


12:14
CUALESMI IP
219.100.37.245
Su IP: 219.100.37.245
Tsukuba
つくば市
Kawagoe
川越市
Kashiwa
柏市
Ichikawa
市川市
Chiba
千葉市
Kawasaki
川崎市
Sodegaura
袖ケ浦市
Fujisawa
藤沢市
Yokosuka
País
Japan
Ciudad
Latitud
35.689701080322
Longitud
139.68949890137
ISP
SoftEther Telecommunication Research Institute, LL

Escenario práctico local



Configuración site to site



En este caso el cliente de la red2 (172.22.1.20) no puede conectarse al puente por lo que por ahora el cliente2 no tiene acceso a la red1, el puente si llega al cliente1.