

Acceso Corporativo a Internet

Guillermo Pérez Trabado ©2016-2024

Diseño de Infraestructuras de Redes

Depto. de Arquitectura de Computadores - Universidad de Málaga

Introducción al escenario

Recuerda que el funcionamiento normal en una empresa es que los puestos de trabajo en los departamentos solo puedan acceder a servicios internos de la propia empresa y que los servicios sean accedidos solamente por los puestos de los departamentos. Por tanto, el acceso desde/a internet es considerado una **excepción a la política de seguridad normal y un riesgo de seguridad inevitable**.

La conexión a Internet de la red de un site de la empresa tiene dos finalidades posibles claramente delimitadas. La conectividad con Internet no es un fin en sí mismo, sino que debe ser una herramienta para cumplir los prerequisites contenidos en la política de funcionamiento de la empresa **definida por la dirección de la misma**. Los requisitos que necesitan dicha conexión son:

- Ofrecer al público de Internet acceso a un servicio web ubicado en el site de la empresa.
- Dar a ciertos puestos de trabajo de la empresa (en departamentos concretos) acceso a ciertos servicios web de otras empresas a través de Internet.

Ambos objetivos son totalmente independientes y puede haber muchas instancias distintas de cada uno de ellos (distintos servicios a ofrecer a Internet y distintos departamentos que necesitan acceso a servicios en Internet).

En esta práctica vamos a diseñar la infraestructura de conexión de nuestro site a Internet. Dicha infraestructura permitirá inicialmente dar acceso a **todos** los puestos de trabajo a **cualquier servicio** de Internet, y dar acceso desde **todos** los usuarios de Internet a **todos** los servicios de nuestro Data Center. Como hemos explicado anteriormente, esta infraestructura es solo una herramienta para implementar la política de acceso definida, que tan solo permite conectar a aquello que hayan sido autorizados por la dirección. En este paso nos centraremos en hacer que funcione la conectividad con Internet, y en una fase posterior de la práctica nos centraremos en restringir el acceso mediante reglas de seguridad (ACLs).

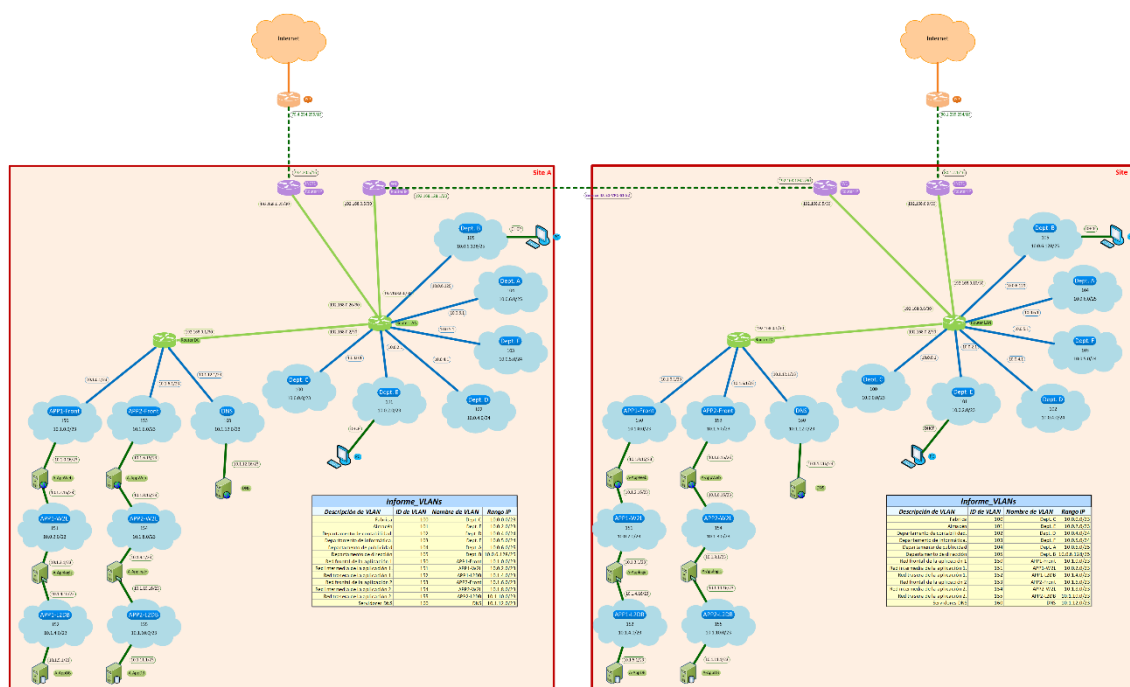
1. Esquema lógico del acceso a Internet

El esquema lógico es muy sencillo porque el **acceso corporativo a Internet** consiste en conectar nuestros router LAN con el router del operador de telecomunicaciones (Internet Service Provider o ISP) a través de un enlace WAN punto a punto. Como dicho enlace WAN también pertenece al operador, es bastante usual que el operador nos ofrezca en alquiler un router en alquiler que termina el enlace en nuestras instalaciones (router WAN o router de acceso a Internet). Por tanto, el **punto de presencia** (PoP) del ISP en nuestras instalaciones es el puerto Ethernet interno de dicho router.

En el esquema lógico de la figura siguiente podemos ver que en cada site se ha añadido el router WAN adicional (router INET) que conecta con el router del ISP a través de un enlace WAN punto a punto. Si observas las direcciones IP de los enlaces punto a punto añadidos:

- El enlace Router-LAN↔Router INET tiene direcciones privadas ya que se considera que este enlace está dentro de la Intranet.
- El enlace Router INET↔Router ISP tiene direcciones públicas, ya que se considera que el enlace WAN ya forma parte de Internet.

Por tanto, **el router INET constituye la frontera entre Internet y la Intranet de nuestro site.** Tiene un puerto con una dirección IP de Intranet y otro puerto con una dirección IP de Internet.



Como ya pasó anteriormente con los enlaces privados WAN entre sites, los routers WAN diferenciados del router LAN permiten separar funciones en distintos equipos y facilitar así la división de tareas de administración.

Otro detalle importante a resaltar es que cada site tiene su propio acceso a Internet. Analizando las consecuencias de este diseño podemos sacar las siguientes observaciones:

- Cada site puede establecer su propia política de acceso a Internet. Es decir, definir distintas reglas de seguridad.
- La calidad de servicio del enlace WAN que va hasta el router del ISP puede ser contratada para adaptarse a las **necesidades concretas de cada site**. Si en un site solo hay oficinas, las garantías de BW mínimo y de latencia máxima podrían ser menos exigentes que en un site donde existe un *data center* que ofrece servicios a Internet con miles de clientes simultáneos.
- Por otro lado, la presencia de un enlace a Internet en cada sede nos permitiría que una sede pudiera usar el acceso a Internet de otra en caso de fallo de su enlace local por medio de los enlaces WAN entre sedes y gracias al routing dinámico. En caso de fallo del

acceso a Internet local, el routing dinámico elegirá automáticamente la siguiente ruta a 0.0.0.0/0 más barata.

- Internet no es una abstracción única. No hay una sola Internet sino regiones de Internet. Si un site está ubicado en una región del mundo, requiere un acceso a la región de Internet de dicha zona del mundo para que los servicios disponibles sean los que nos interesan. Por ejemplo, si una sucursal de una empresa ubicada en España accede a Internet a través del enlace de una sucursal en EEUU, un empleado que tratara de acceder a la web de un banco con presencia internacional sería redirigido automáticamente a la página de la organización en EEUU basándose en su **IP pública** de origen.

Conexión al ISP en Packet Tracer

Para simular la conexión al ISP en tu implementación usaremos una nube Multiuser Connection que nos proveerá con un enlace WAN (Ethernet óptica a 1Gbps) a la red de transporte del operador de telecomunicaciones. Dicho enlace nos da acceso a una VLAN en la que nuestro router de Internet (INET) y el router del ISP pueden verse al formar parte del mismo rango IP.

En el campus virtual encontrarás una tabla con todos los datos de la conexión al ISP, incluyendo los parámetros para conectar la nube:

- Servidor: isp.ho.ac.uma.es (conéctate a la VPN antes).
- Puerto: 38001 (atención que es diferente al puerto para los circuitos WAN).
- Network name: Ex-SITEy-ISP, donde x es el número de empresa, e y es el número del site. Tu profesor te ha asignado en clase un número de empresa y site.
- Password: Es siempre vc0910\$\$.

Una vez establecida la conexión (la nube se pone en color azul al pasar el ratón por encima y podemos ver los datos de la conexión) podemos conectar los cables entre puertos de cualquier equipo local y el puerto remoto que aparezca en la nube. Al pinchar en una nube ya conectada para conectar un cable, nos listará el puerto disponible para conectar.

No pongas los cables con las nubes desconectadas y nunca elijas la opción **create new link**. No sirve de nada ya que conecta el cable a la nube remota pero requiere que alguien lo conecte posteriormente al equipo remoto en el otro diseño, por lo que tu cable quedará desconectado. Cuando conectas un cable en una nube **conectada** se muestran los puertos remotos disponibles. Si conectas correctamente un cable a una nube remota, las conexiones de los cables son preservadas aunque cierres Packet Tracer o la conexión a la nube remota.

Parámetros del enlace al ISP

La conexión a Internet requiere que nuestro ISP nos proporcione una serie de datos que necesitaremos para hacer diversas configuraciones. Si quieres encontrar los parámetros para tu site, encontrarás una tabla publicada en este mismo apartado del campus virtual.

- Parámetros IP:
 - **El número de direcciones IP públicas que hemos solicitado para nuestra empresa (Req. IPs):** Este número lo hemos especificado nosotros al solicitar a nuestro operador el acceso a Internet. Las necesidades dependen del número de desktops que requieren acceso simultáneo a Internet, aunque el uso de PAT

- (en lugar de NAT) reduce mucho el número de direcciones necesarias ya que cada IP está multiplexada entre miles de conexiones TCP/UDP hacia fuera.
- **Las direcciones IP públicas de nuestra empresa (Public IP range):** Estas direcciones no forman un rango IP completo con un tamaño que sea potencia de dos, sino que es un conjunto de direcciones consecutivas que pueden empezar y terminar en cualquier número.
- **La máscara a usar en el Interfaz del router para las IP públicas (Mask):** Nuestras direcciones públicas forman parte de la VLAN que compartimos con el router del ISP y, por tanto, requieren una máscara para el Interfaz Ethernet externo del router INET. Esta máscara no coincide con el número de IPs públicas asignadas sino con el tamaño de la VLAN del operador. Por tanto, hay otras empresas que poseen direcciones IP dentro de la misma VLAN a la que pertenecen las nuestras. Por eso, la máscara que nos indica el operador puede ser mucho mayor que lo que corresponde al número de IPs asignadas.
- **La dirección del router del ISP:** Es la dirección del router del ISP. Como todo el tráfico a Internet pasa a través de dicho router, esa será la dirección del default router (0.0.0.0/0) para el router INET de nuestra sede.

Una pregunta importante que surge al leer la lista anterior es *¿cuál es la dirección IP del interfaz del Router de Internet de mi site si el operador me ha dado un listado de direcciones?* La respuesta no es sencilla, pero tampoco imposible de entender. Nuestro router usará todo el bloque de direcciones IP públicas para traducir las direcciones de las máquinas que están dentro de la empresa cuando accedan o sean accedidas desde Internet. Usas direcciones no se configuran en el interfaz sino en la configuración de NAT (*Network Address Translation*). Sin embargo, el router necesita una dirección IP en el interfaz, que usará solo cuando su propio sistema operativo tenga que comunicarse con el router del ISP. Por ejemplo, si realizamos un *ping* o una conexión *ssh* desde el Router de Internet hacia una IP de Internet, nuestro router usará la dirección asignada al interfaz como origen de los paquetes que envía.

¿Qué dirección elijo entonces para el interfaz del router? Cualquiera del bloque de IP públicas que nos ha dado el operador. Obviamente, por razones de administración y documentación, es recomendable que sea la primera.

Configuración del enlace al ISP

Para conectar a Internet, necesitamos un nuevo router WAN que en este caso estará dedicado exclusivamente a la conexión a internet. En el ejemplo de esquema lógico que puedes ver más arriba, puedes ver la conexión del router de internet. Dicho router tendrá dos enlaces:

- Una conexión punto a punto con el router LAN (se usarán direcciones locales).
- Una conexión punto a punto con el router del ISP (se usarán las direcciones proporcionadas por el operador).

Los pasos para configurar la conexión serán los siguientes:

- Crea una conexión Multiuser para la conexión al ISP. Conéctala con los parámetros que puedes encontrar en la tabla de servicios WAN.
- Añade un nuevo router de acceso a Internet con puertos ópticos de 1Gbps y UTP (puede ser una copia del router WAN, pero ten cuidado de editar su configuración).

- Si la nube está ya conectada pon la fibra óptica del router a la nube.
- Activa los interfaces del router (**no shutdown**). Si el cable está conectado correctamente, el diodo debe pasar a color verde en ambos routers.
- Documenta los enlaces punto a punto en tu tabla de enlaces antes de configurarlos.
- Configura el enlace Router INT ↔ Router LAN con las direcciones locales asignadas en el paso anterior.
- Configura el **interfaz** de tu Router INT hacia el Router ISP con la primera de las direcciones públicas.
- Verifica que el nuevo router pueda hacer ping tanto al router LAN como al router del ISP cuya dirección viene en la tabla.

En este momento este router puede acceder a cualquier dirección de internet. Puedes probar también a hacer ping a cualquiera de las siguientes direcciones de Internet como test (pueden tardar bastante en responder):

- 80.0.255.253 (www.potafone.com)
- 81.0.255.253 (www.potafone.com)
- 199.9.14.202 (www.ripe.org)
- 198.41.0.5 (www.icann.org)

También puedes intentar hacer ping a la dirección pública del router de internet de otros sites de tu empresa cuando estén operativos.

2. Difusión de la ruta a internet

Nuestro Router INT va a usar EIGRP para formar parte del routing dinámico de nuestro site. Sin embargo, su conexión con el router ISP no debe tener ningún tipo de negociación. De hecho, la ruta a internet será estática porque *sabemos que esa conexión lleva a Internet por diseño*.

Para incorporar la ruta estática usaremos el comando:

```
ip route 0.0.0.0 0.0.0.0 <IP_router_ISP>
```

A partir de este momento, este router ya sabe cómo acceder a cualquier dirección de Internet. Ahora hace falta configurar EIGRP para que este router participe en el Autonomous System de tu empresa y propague la ruta. Una vez configurado EIGRP, hay que:

- Habilitar al Router de Internet para negociar en el enlace punto a punto con el router LAN.
- Habilitar al router LAN para negociar en el enlace con el router de Internet.
- Habilitar a EIGRP en el router de Internet para propagar la ruta estática a internet con el comando:

```
router eigrp <AutSysNum>
 redistribute static
```

Ahora la ruta estática debe aparecer en el resto de routers. Sin embargo, nadie podrá acceder a Internet porque los paquetes enviados hacia el router ISP tienen direcciones locales a las que nadie puede responder. Por tanto, es necesario configurar NAT para poder probar el acceso a Internet desde cualquier otro equipo que no sea el router de Internet.