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 prerrequisitos 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.

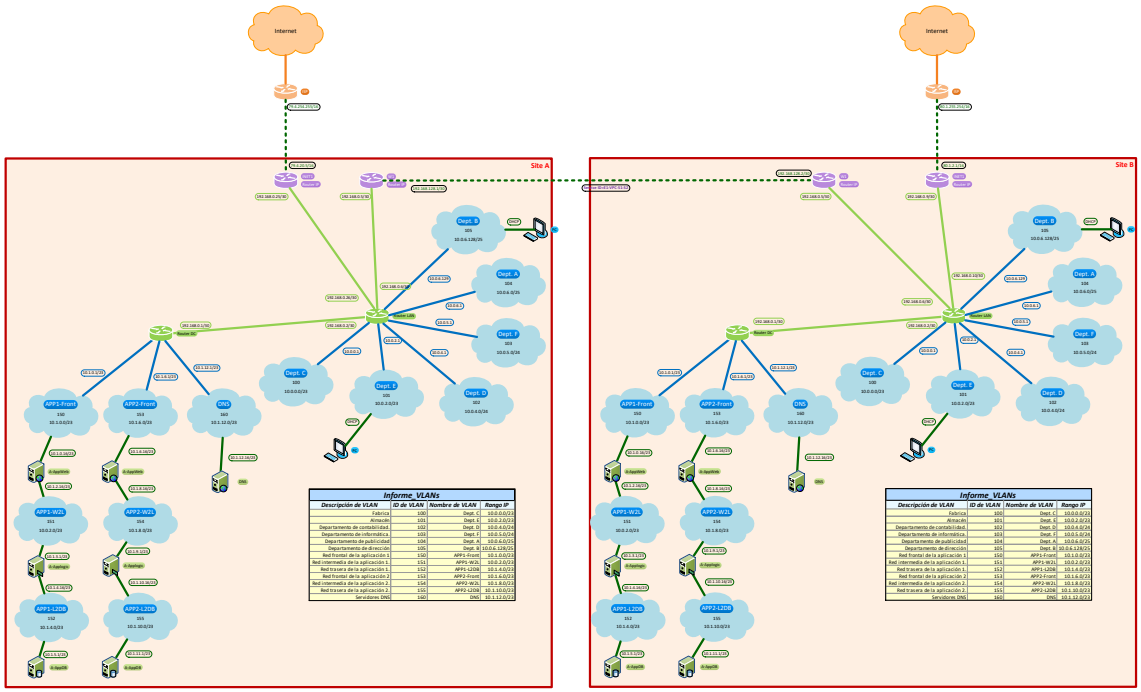

Figura 1: Esquema lógico de la conexión al ISP de varios sites.

En el esquema lógico de la Figura 1, 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** ya que 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 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.

Direcciones públicas y privadas

Anteriormente hemos usado para el site direcciones privadas pertenecientes a los rangos 10.0.0.0/8, 192.168.0.0/16 y 172.16.0.0/20. El estándar que permite el uso de dicha direcciones recuerda que no se pueden usar en Internet ya que serán usadas en casi todas las empresas en incluso domicilios particulares, por lo que el destinatario no podrá responder correctamente. Además, los ISP suelen filtrar dichas direcciones para evitar problemas.

Por tanto, nuestra empresa está obligada a adquirir o alquilar algunas direcciones públicas para los servicios que se ofrezcan a Internet, y también para que los desktops de la Intranet puedan acceder a Internet. La estrategia para esto está en usar NAT (Network Address Translation) en el router que hace de frontera entre la empresa e Internet. Esta estrategia consiste en traducir la dirección privada del paquete (la del interior de la empresa) por una dirección pública.

La traducción NAT será implementada por nuestro router de Internet, no por el router del ISP. Esto nos permite controlar la dirección pública con la que nuestros servicios serán vistos por el resto de usuarios de Internet.

Algunos operadores hacen NAT de forma transparente para sus usuarios. Esto se conoce como NAT de operador, y hace imposible al usuario tener el control de cómo sus servicios son vistos por el resto de Internet, ya que no sabe qué dirección pública es asignada por el operador en cada momento.

Direcciones públicas estáticas

Los servidores de Internet de una empresa son referenciados por el nombre completo (Full Qualified Domain Name) de la URL de sus servicios. El FQDN incluye el nombre de máquina y el dominio de la empresa, por ejemplo www.acme.com. El FQDN se traduce mediante el servicio DNS a una dirección IPv4 o IPv6 alcanzable desde cualquier ISP en Internet. Esto quiere decir que los routers de cualquier ISP de Internet tienen una ruta que lleva a esta IP.

Las empresas usan para sus servicios siempre direcciones IP estáticas, que son alquiladas por los ISP pagando el uso de dicha dirección como un servicio adicional. No es posible usar direcciones IP dinámicas (asignadas por DHCP) para ningún servicio **serio** que tenga que estar presente continuamente en Internet incluso si nos planteamos la posibilidad de actualizar la entrada DNS cada vez que nuestro servicio cambia de IP. La causa es que los servidores DNS en Internet hacen caching agresivo de las traducciones que realizan incluso durante días. Por eso, un cambio de IP

puede suponer incluso días durante los cuales los clientes reciben la dirección IP antigua, por lo que no podrán encontrar el servicio en la IP antigua.

El caching de DNS es una piedra angular para la eficiencia de los servicios de Internet que no puede ser suprimida. Cualquier página web con AJAX o servicios REST hace decenas de conexiones por segundo que requieren que la latencia de conexión de TCP sea muy baja. Para ello, las traducciones de nombres a direcciones deben ser almacenadas en caches incluso en cada desktop cliente.

Aunque sería posible invalidar las entradas obsoletas para acelerar el proceso de actualización de las direcciones IP, este sería un vector de ataque usado por los hackers para lograr ataques DoS o phishing, razón por la cual, una vez que el administrador del dominio establece el TTL máximo (Time To Live) de cada entrada, la entrada solo es invalidada en un cliente cuando expira dicho TTL.

Por tanto, nunca usaremos DHCP para la conexión de nuestro router de Internet al ISP.

2. 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 operatdor. 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, el Router de Internet solo puede llegar hasta el router del ISP y el router LAN porque se le ha añadido ninguna ruta adicional. En el apartado siguiente nos encargaremos de configurarlo para que tenga las tablas de rutas correctas.

3. Configuración de las tablas de rutas

En este apartado necesitamos configurar dos aspectos del encaminamiento del nuevo router:

- El encaminamiento desde este router hacia Internet.
- El encaminamiento desde este router hacia la intranet de la empresa (nuestro site y los otros sites). Este apartado también incluye configurar el resto de routers de la empresa para que aprendan la ruta hacia Internet.

Encaminamiento hacia Internet

Aunque nuestro Router de Internet usará (más adelante) 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 ya que pertenece a una empresa ajena a la nuestra. De hecho, la ruta a internet será estática porque sabemos que esa conexión lleva a Internet ***por diseño***.

Para incorporar de forma estática la **ruta por defecto** usaremos el comando siguiente en nuestro router de Internet:

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

En este momento **este router** puede acceder a cualquier dirección de internet que sea alcanzable por el router del ISP. 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.

Encaminamiento hacia el interior de la empresa

Ahora hace falta configurar EIGRP para que el router de Internet participe en el Autonomous System de tu empresa y propague la ruta. Una vez configurado EIGRP, hay que:

- Habilitar en el router de Internet el mismo AS de EIGRP que en el resto de la empresa.
- 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 está tica a internet con el comando:

```
router eigrp <ASNum>
 redistribute static
```

Después de estos pasos debemos verificar que:

- El router de Internet conoce las rutas del router LAN.
- Cualquier otro router conoce la ruta por defecto a Internet (0.0.0.0/0).

En este punto, las rutas ya son correctas. Sin embargo, nadie puede aun acceder a Internet porque los paquetes enviados hacia el router ISP tienen **direcciones locales** a las que nadie puede responder desde Internet. Por tanto, es necesario configurar NAT en el router de Internet para poder probar el acceso a Internet desde cualquier otro equipo que no sea el router de Internet.

4. Configuración del NAT de entrada

En la configuración vamos a distinguir dos partes. Primero configuraremos la traducción de las conexiones que se hagan desde Intranet hacia Internet, lo que llamaremos NAT de salida. Dicha traducción es dinámica. Es decir, no hay una dirección ni puerto fijo asignado a cada equipo, sino que se asigna de forma paulatina conforme se producen las conexiones.

En la segunda parte vamos a configurar el NAT de entrada, que permite traducir las conexiones entrantes desde Internet a los servicios ofrecidos por nuestra empresa a Internet. Esta traducción tiene que ser estática, ya que nuestro servicio debe ser encontrado siempre en la misma IP y puerto TCP o UDP públicos por los clientes (la URL pública). Por tanto, en esta parte haremos asignaciones estáticas de puertos externos a puertos internos. Es similar al proceso que se conoce como *abrir un puerto* en un router doméstico.

Configuración de NAT/PAT dinámico de salida en el router WAN

1. Identifica en el router de Internet cuál es el interfaz interno y cuál el externo para la traducción NAT. Tienes que añadir a cada interfaz los subcomandos **`ip nat inside`** e **`ip nat outside`** para identificar respectivamente el interfaz de Intranet y el de Internet. Por ejemplo:

```
# Este es el interfaz de Intranet
interface GigabitEthernet0/0
  ip nat inside
# Este es el interfaz de Internet
interface GigabitEthernet0/1
  ip nat outside
```

2. Para la traducción NAT dinámica tenemos que definir un pool de direcciones IP públicas que van a ser asignadas cuando se traduzcan accesos desde las direcciones privadas hacia Internet. El nombre del pool en el ejemplo siguiente es la etiqueta **isp-pool.** Las direcciones IP del pool son las que nos ha dado el ISP. Para ello usa el comando:

   ```
   ip nat pool isp-pool <ip-inicial> <ip-final> netmask <máscara>
   ```

3. Por otro lado necesitamos una entrada que indique exactamente qué direcciones IP internas están autorizadas a ser traducidas mediante NAT. Para esto se usa una ACL igual a las que se usan para filtrar el tráfico. Dicha ACL identifica un patrón de direcciones y/o protocolos y puertos. Posteriormente será asociada al pool anterior con otro comando. En este ejemplo, 10 es la etiqueta que identifica esta ACL.

   ```
   access-list 10 permit 10.0.0.0 0.255.255.255
   ```

4. Por último, asocia la ACL están asociadas a las direcciones externas del pool **isp-pool**. Si no se especificara la palabra clave `overload`, usaríamos NAT, por lo que se asignaría una dirección IP externa a cada IP interna que intente acceder hasta que se agotaran las IPs externas. Al usar `overload` se indica que queremos usar PAT (Port Address Translation), con el cual se asignan puertos TCP o UDP de las direcciones internas a puertos de las IPs externas del pool. Una sola IP externa puede estar traduciendo puertos de múltiples direcciones internas.

   ```
   ip nat inside source list 10 pool isp-pool overload
   ```

Como puedes observar, en este momento el router Internet tiene una dirección externa en el interfaz con el router del ISP que usa cuando se comunica como router con direcciones externas, y a la vez tiene asignadas varias direcciones IP externas para la traducción NAT de direcciones internas, y solamente para dicho fin.

Esta configuración permite traducir la dirección de cualquier IP interna que inicie una conexión **hacia fuera**. La traducción es dinámica porque los puertos TCP/UDP externos se asignan y liberan conforme se abren y cierran conexiones (existe un temporizador de expiración para liberarlas pasado un tiempo).

Ahora deberías testear que los PCs de tu empresa son capaces de navegar por internet usando diversos protocolos (ICMP ping y HTTP) y las direcciones siguientes:

- 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)

Configuración de NAT estático para puertos de servidores internos en el router WAN

Necesitamos ahora definir traducciones estáticas de entrada para que se pueda acceder a los servidores WWW y DNS de la empresa desde internet (**hacia dentro**). En este caso vamos asignar puertos TCP de cualquier dirección del pool de IPs externas a un puerto TCP o UDP de una dirección IP interna.

1. En el router de Internet establece la asociación entre el puerto TCP:80 del un servidor HTTP público (por ejemplo 10.0.1.253:80) y el puerto 80 de una dirección pública (por

ejemplo 80.0.0.136:80). Recuerda también añadir el puerto 443 para los servicios HTTPS.

```
ip nat inside source static tcp 10.0.1.253 80 80.0.0.136 80
```

2. En este ejemplo asociamos el puerto UDP:53 del servidor DNS público (10.0.1.249:53) y el puerto UDP:53 la misma dirección pública de antes (80.0.0.136:53).

   ```
   ip nat inside source static udp 10.0.1.249 53 80.0.0.136 53
   ```

3. Verifica que cualquier usando una conexión doméstica a Internet que los clientes pueden ver los servicios que has publicado. Para ello, usa el PacketTracer con una conexión doméstica que puedes encontrar en el campus.
   En dicho esquema hay un User Cloud que debes conectar a la etiqueta HOME*e-s* (donde *e* es el número de tu empresa y *s* el número de tu site). Conecta la nube a isp.ho.ac.uma.es:38001 y luego conecta un **cable telefónico** entre el módem ADSL y el puerto de la central del operador. Una vez conectado, el PC doméstico debería poder obtener una dirección pública mediante DHCP.
   Cuando el PC tenga un dirección pública, prueba a acceder a tu propia empresa y acceder a los servicios publicados mediante HTTP, HTTPS.

Observa que en con el NAT de entrada no estamos protegiendo el interior de la empresa de accesos desde Internet mediante ACLs que restrinjan el tráfico, sino que estamos confiando en que la propia traducción de direcciones NAT por defecto prohíbe cualquier acceso hacia dentro ya que no hay traducción excepto para los accesos definidos explícitamente.

De todas formas, más adelante deberíamos establecer ACLs en el router LAN para para controlar cualquier conexión adicional debida a un error de administración de NAT o una intrusión en el router WAN.