Entrada estática NAPT R1

Protocolo	Socket Local	Socket Remoto
TCP	80.10.20.2:80	10.1.1.30:80

Estática

Una dirección IP privada se traduce siempre en una misma dirección IP pública. Este modo de funcionamiento permitiría a un host dentro de la red ser visible desde Internet. (Ver imagen anterior)

Dinámica

El router tiene asignadas varias direcciones IP públicas, de modo que cada dirección IP privada se mapea usando una de las direcciones IP públicas que el router tiene asignadas, de modo que a cada dirección IP privada le corresponde al menos una dirección IP pública.

Cada vez que un host requiera una conexión a Internet, el router le asignará una dirección IP pública que no esté siendo utilizada. En esta ocasión se aumenta la seguridad ya que dificulta que un host externo ingrese a la red ya que las direcciones IP públicas van cambiando.

Cuando te preguntan si se puede meter un servidor web, en el caso de que se pueda, tienes que añadir al router una entrada NAPT estática. Siempre se puede añadir, a menos que haya un conflicto en ese mismo puerto con otro servidor que estuviera de antes, si son servidores que usan puertos distintos, por ejemplo, correo (puerto 25) y web (puerto 80), no habría problema.

Fijarse si una TCP_PDU va al puerto 80, dentro de la red privada, porque entonces habrá un servidor web, y por tanto habrá que añadir una entrada estática.

Entrada estática --> PC a servidor web o viceversa

Entrada dinámica --> PC a PC

DHCP

- MAC_PDUs de gestión:
  - Sirven para gestionar el enlace inalámbrico.
    - Beacon. La envía subnivel MAC periódicamente para informar de la existencia de una red inalámbrica.
      - Intervalo es un parámetro configurable
    - Probe request. Sirve para que el subnivel MAC escanee un área en buscando redes inalámbricas.
      - Se informa de las velocidades soportadas.
    - Probe response. Enviado por el subnivel MAC en respuesta a un Probe request.
    - Association request. Sirve para que el subnivel MAC solicite "conectarse" a una red inalámbrica.
    - Association response. Confirmación de la "conexión" a una red inalámbrica.
    - Otras…

DHCPDISCOVER → Sirve para que el cliente "pida" una dirección IP. Es un broadcast, debe incluirse la MAC del cliente (chaddr), el cliente puede sugerir tanto opciones adicionales como su propia IP.

DHCPOFFER → Cada servidor DHCP envía una "oferta" de dirección (yiaddr) y opciones adicionales de configuración (DNS, gateway, etc). Los servidores comprobarán (ej: PING) que la dirección que ofrecen no está en uso.

DHCPREQUEST → El cliente elige una de las ofertas y responde con una IP_PDU de broadcast en la que indica la IP que le ofrecían. Debe enviar además en las opciones el identificador del servidor, de esta forma todos los demás servidores saben que el cliente no usará la dirección que le ofrecieron.

DHCPPACK → Se confirma finalmente la asignación de esa IP. El servidor DHCP marcará la IP como "en uso" y el cliente tiene que, en ese momento, comprobar que la IP no esté en uso (por ejemplo, con ARP) y rechazar esa IP si está en uso (DHCPDECLINE).

DHCPRELEASE → En caso de parada ordenada de un ordenador, este puede liberar la IP asignada.

c) Describa cómo funciona el mecanismo de reserva del medio previsto en IEEE802.11

Para reservar el medio, un cliente debe enviar una MAC_PDU de control llamada RTS, de esta forma evitará que otros clientes colisionen con él. También se especificará la duración de la reserva. El punto de acceso de su BSS responderá con una MAC_PDU de control llamada CTS, indicando qué puede enviar y la duración de la reserva.

La IP de autoconfiguración es cualquiera del tipo 169.254.X.X

HolePunching

Consiste en el establecimiento de comunicaciones entre dos partes en organizaciones separadas que están deras de firewalls. Se utiliza para aplicaciones como juegos, P2P y VoIP.

Para que sea una dirección IPV6 pública, debe empezar por 001 de izquierda a derecha.

Si no se fragmenta el mensaje, no hace falta usar el protocolo ARP.

DNS

Para saber el FQDN del servidor principal de una zona, hay que fijarse en los NS que tengamos en la caché. Si tenemos más de uno, no podemos saber cuál es el principal ya que eso viene en el SOA, y no ahí; sin embargo, si tenemos un solo NS, quiere decir que ese es el principal.

TTL SOA → TTL para las entradas de los servidores.

TTL/entrada→ Nos indica el tiempo de vida durante el cual esa entrada puede ser considerada válida, entrada tipo A.

Correo

MIME
Caracteres extendidos en cabeceras

- Las cabeceras, a no ser que el MTA soporte 8bits, siguen transmitiéndose con 7bits. ¿Qué ocurre con los caracteres ASCII extendidos en las cabeceras?
- Puede ser necesario que en el asunto, el From o el To aparezcan estos caracteres.
- SOLUCIÓN. Se codifican, si es necesario, determinadas partes de las cabeceras con este esquema:
  - encoded-word = "=?" charset "?" encoding "?" encoded-text "?="
  - charset es el juego de caracteres, encoding: q=quoted-printable, b=Base64.
  - Los espacios se sustituyen por "_", los "_" por su codificación. Restricciones con otros.

Subject: Elaboración de guías ECTS
Subject: =?iso-8859-1?Q?Elaboraci=F3n_de_gu=EDas_ECTS?=

Subject: Abierto el plazo de petición de libros
Subject: Abierto el plazo de =?ISO-8859-1?Q?petici=F3n_de_libros?=

Subject: Este_es_un_texto_extraño
Subject: =?ISO-8859-1?Q?Este=5Fes=5Fun=5Ftexto=5Fextra=F1o?=

Subject: No_necesariamente_se_codifica.
Subject: No_necesariamente_se_codifica.

10 Q → quoted printable

B → Base64

f) Con los datos que se muestran, ¿es posible saber si se han usado caracteres ASCII extendidos en el cuerpo del correo?

Content-Transfer-Encoding: 7bit
Subject: =?iso-8859-1?**B**?UmVwb3J0

El Subject nos dice que tiene iso-8859-1 y que tiene de enconding base 64 (la B, quoted-printable es Q). Base 64 permite caracteres de la "A" a la "Z", de la "a" a la "z", del "0" al "9" y "+" y "/", así pues **NO permite caracteres extendidos, puesto que no se pueden poner acentos, ni la ñ.** Si tuviera Q sí que permitiría caracteres extendidos.

Ataques man in the middle

1. El atacante captura la conexión.

2. El atacante envía su clave pública (que él ha generado) y negocia una conexión segura.

3. El atacante se conecta al servidor real, negociando una conexión segura.

4. El atacante gestiona esas dos conexiones y, por tanto, tiene acceso a los datos de la conexión.

Para que todo funcione bien, es necesario garantizar la propiedad de la clave pública (garantizar que es de quien dice ser), la manera que te preguntarán en el examen es mediante certificados, aunque también podría ser de manera offline.

CRL Distribution Point: Lista de certificados revocados.