DHCP

Abril 2017

Con respecto a DHCP, indique un caso de ejemplo en el que sea importante que la configuración del servicio tenga la característica indicada:

a) Dirección IP fija: Servidores de red.

En entornos donde se necesite acceder de manera consistente a un dispositivo específico mediante una dirección IP conocida, como servidores de red, impresoras de red o dispositivos de seguridad, es importante asignar direcciones IP fijas.

b) Dirección IP dinámica: No se conoce la MAC de antemano

. En entornos donde la movilidad de los dispositivos es frecuente, como en una red Wi-Fi pública o en una red de conferencias, asignar direcciones IP dinámicas es importante. Esto permite que los dispositivos obtengan automáticamente una dirección IP disponible cuando se conectan a la red, sin necesidad de configuración manual.

c) Tiempo de concesión breve: Lugar con mucha rotación de clientes.

En redes donde los dispositivos se conectan y desconectan con frecuencia, como en una red Wi-Fi pública o en una red de invitados en una empresa, es importante configurar un tiempo de concesión breve.

Esto asegura que las direcciones IP se liberen rápidamente cuando los dispositivos se desconectan, permitiendo que otros dispositivos puedan utilizar esas direcciones IP disponibles.

d) Uso de repetidor de DHCP: Redes de ámbito diferente.

Un caso de ejemplo en el que es importante utilizar un repetidor de DHCP es en redes que abarcan múltiples subredes separadas por routers. En tales casos, los repetidores de DHCP, también conocidos como servidores relay de DHCP, retransmiten los mensajes DHCP entre los clientes y los servidores DHCP que pueden estar en diferentes subredes.

Esto permite que los dispositivos en subredes remotas obtengan direcciones IP y

otros parámetros de configuración de red del servidor DHCP central, incluso si el servidor DHCP no está en la misma subred que los dispositivos que solicitan la configuración.

Marzo 2018

En el protocolo DHCP, y su implementación isc-dhcp:

a) Si dos servidores DHCP reciben la solicitud que un cliente envía, indique cómo se comportan tanto servidores como el cliente.

Ambos servidores envían su OFFER. El cliente acepta uno de los OFFER e ignora los demás. El servidor no elegido reutiliza su IP pues no recibe aceptación.

b) ¿Cómo se debe configurar un servidor isc-dchp para que considere conocido a un cliente determinado?

Para que un servidor isc-dhcp considere conocido a un cliente determinado, se puede configurar una asignación estática de dirección IP para la dirección MAC del cliente en el archivo de configuración dhcpd.conf. Esto se realiza mediante la siguiente sintaxis:

```
host nombre_del_cliente {
hardware ethernet dirección_MAC_del_cliente;
f
 ixed-address dirección_IP_asignada_al_cliente;
}
```

c) Indique un caso en el que el uso de asignación dinámica de direcciones IP sea conveniente respecto al uso de asignación estática. En el caso que elija, indique cómo afecta establecer un mayor o menor tiempo de licencia

Un caso en el que el uso de asignación dinámica de direcciones IP sea conveniente respecto al uso de asignación estática es en entornos donde hay dispositivos que se conectan y desconectan frecuentemente de la red, como en una red Wi-Fi pública o en una red de oficina donde los empleados utilizan dispositivos personales.

Con la asignación dinámica, los dispositivos pueden obtener automáticamente una dirección IP disponible sin necesidad de intervención manual.
Un mayor tiempo de licencia puede ser beneficioso en entornos donde los dispositivos permanecen conectados durante períodos prolongados, reduciendo la frecuencia de renovación de direcciones IP y la carga en el servidor DHCP.
Sin embargo, un tiempo de licencia más corto puede ser preferible en entornos donde los dispositivos se conectan y desconectan con frecuencia, asegurando que las direcciones IP se liberen rápidamente y estén disponibles para otros dispositivos. Sin embargo, un tiempo de licencia demasiado corto puede generar una sobrecarga en el servidor DHCP debido a la frecuencia de renovación de las concesiones.

Marzo 2023

En el protocolo DHCP, y su implementación isc-dhcp:

a) Indique un caso de ejemplo en el que sea importante que la configuración del servicio tenga un tiempo de concesión breve. Justifique brevemente el motivo.
Un caso de ejemplo en el que es importante que la configuración del servicio DHCP tenga un tiempo de concesión breve es en entornos donde los dispositivos se conectan y desconectan con frecuencia, como en una red Wi-Fi pública o en una red de invitados en una empresa.

Un tiempo de concesión breve asegura que las direcciones IP se liberen rápidamente cuando los dispositivos se desconectan, permitiendo que otros dispositivos puedan utilizar esas direcciones IP disponibles. Esto es importante para evitar el agotamiento del pool de direcciones IP disponibles y garantizar una asignación eficiente de direcciones IP a los dispositivos que se conectan temporalmente.

b) Si un cliente DHCP solicita una dirección IP en una subred donde, por disponibilidad, existen dos servidores DHCP, indique qué ocurriría si ambos servidores ofrecieran IP diferentes: ¿el cliente acepta ninguna, una o ambas direcciones IP? ¿qué direcciones IP , ninguna, una o ambas, quedarían registradas en los servidores como asignadas para no ofertarlas ya a otros clientes?

Si un cliente DHCP solicita una dirección IP en una subred donde existen dos servidores DHCP, y ambos servidores ofrecen direcciones IP diferentes, el cliente aceptará solo una

de las direcciones IP ofrecidas.

Ambos servidores registrarán la dirección IP ofrecida al cliente en sus tablas de asignación DHCP para evitar ofrecerlas nuevamente a otros clientes hasta que expire el tiempo de concesión o se liberen manualmente.

c) ¿Cuándo se necesita utilizar un repetidor DHCP?

Un repetidor de DHCP se necesita utilizar cuando se tienen múltiples subredes separadas por routers y se desea ofrecer servicios DHCP a dispositivos en esas subredes. Los repetidores de DHCP, también conocidos como servidores relay de DHCP, retransmiten los mensajes DHCP entre los clientes y los servidores DHCP que pueden estar en subredes diferentes.

Esto permite que los dispositivos en subredes remotas obtengan direcciones IP y otros parámetros de configuración de red del servidor DHCP central, incluso si el servidor DHCP no está en la misma subred que los dispositivos que solicitan la configuración.

NAT y FIREWALL

NAT

Sobre NAPT:

a) ¿Debe tener lugar en la interfaz de salida, de entrada, o en ambas? (NOTA: esta se anuló debido a cierta ambigüedad: aunque generalmente lo denominamos “salida” a Internet --desde el punto de vista de la organización--, sería más adecuado indicar interfaz externa, interna o ambas. Toda la puntuación va a la cuestión 2, pues incluye en cierta forma ésta.)

b) En el tráfico saliente, ¿afecta a las direcciones y puertos origen, destino o ambos?
Direcciones y puertos origen.

a) ¿Debe tener lugar en la interfaz externa, interna o en ambas?
En el contexto de NAPT, la traducción de direcciones y puertos generalmente ocurre en la interfaz externa del firewall o del dispositivo que realiza la traducción. Esto significa que las direcciones IP y los puertos de los dispositivos en la red interna se traducen a una dirección IP y puerto únicos en la interfaz externa cuando se comunican con recursos en Internet. Por lo tanto, la traducción de direcciones y puertos debe tener lugar en la interfaz externa.

b) En el tráfico entrante (procedente de la red Internet), ¿afecta a las direcciones y puertos origen, destino o ambos?
En el tráfico entrante desde Internet, la traducción de direcciones y puertos afecta a las direcciones y puertos de destino. Cuando un paquete entra desde Internet hacia la red interna, la dirección IP y el puerto de destino del paquete se traducen de la dirección IP pública y el puerto asignado a una dirección IP privada y puerto correspondiente en la red interna. Esto permite que múltiples dispositivos internos compartan una única dirección IP pública. Por lo tanto, la traducción de direcciones y puertos en el tráfico entrante afecta al destino del paquete.

Cortafuegos

Sea un cortafuegos como el que se ha configurado en el laboratorio. Indique si las siguientes afirmaciones son ciertas o falsas, justificando la respuesta.

1. Todos los paquetes que no sean de la interfaz local pasan por el proceso de NAT

Falso. Los paquetes que van al cortafuegos por la interfaz interna no pasan por NAT.

2. Cuando un paquete no es aceptado por el cortafuegos (deny), se envía un rechazo al remitente.

Falso. Se descarta sin más.

3. No todas las reglas que aceptan un paquete (allow) generan una regla dinámica.

Cierto. Por ejemplo, las de ICMP.

4. Si un paquete viaja de una red a otra, pasa dos veces por el cortafuegos ipfw.

Cierto. Pasa una vez por cada interfaz

Sea un cortafuegos como el que se ha configurado en el laboratorio. Indique si las siguientes afirmaciones son ciertas o falsas. Imprescindible justificar la respuesta

a): ¿Todos los datagramas IP que no sean de la interfaz local son analizados por el proceso de NAPT?

Falsa: No todos los datagramas IP que no son de la interfaz local son analizados por el proceso de NAPT. En la configuración del laboratorio, se aplica NAPT solo al tráfico saliente, es decir, el tráfico que sale de la red interna hacia la red externa. Los datagramas IP que no son de la interfaz local pueden ser filtrados por otras reglas del firewall antes de que se realice la traducción de direcciones y puertos por el proceso de NAPT.

b): ¿Cuándo un datagrama IP no es aceptado por el cortafuegos (deny), este genera y envía un datagrama IP al remitente para informar de dicho rechazo?

Falsa: El cortafuegos IPFW en FreeBSD, como se ha configurado en el laboratorio, no genera y envía un datagrama IP al remitente para informar de un rechazo. Cuando un datagrama IP es denegado (deny) por una regla del cortafuegos, simplemente se descarta

y no se envía ningún mensaje de rechazo al remitente.

c): ¿Todas las reglas que aceptan un paquete (allow) generan una regla dinámica (estado)?
Falsa: En el cortafuegos IPFW, solo las reglas que utilizan la opción keep-state o established generan reglas dinámicas de estado. Estas reglas se utilizan para realizar un seguimiento del estado de las conexiones y permitir el tráfico de retorno asociado con esas conexiones.

d): ¿Si un datagrama IP viaja de una red a otra (p.ej. desde la red externa a la interna), ambas conectadas directamente al cortafuegos ipfw y activado el cortafuegos como rúter IP, se procesarán dos veces todas las reglas del cortafuegos ipfw?
Falsa: Las reglas del cortafuegos IPFW no se procesarán dos veces. El procesamiento de las reglas del cortafuegos ocurre una sola vez, ya sea que el paquete entre o salga de la red interna o externa. El cortafuegos examina los paquetes basándose en las reglas definidas y decide si permitir o denegar el paso del paquete según corresponda, independientemente de si el paquete entra o sale de la red interna o externa.