

**Ejercicio integrador. “NAT, VLANs, OSPF, DHCP, DNS y ACLs”**

#### Nuestro cliente **Azupiso** ha hecho saber a los directivos de **Network Consulting** que están muy satisfechos con nuestros resultados, por lo que nos solicitan realizar la configuración del servicio **NAT**, con el fin de que su direccionamiento privado pueda ser traducido a direccionamiento público.

La topología de la red y direcciones IP están representadas en la siguiente gráfica.

A diagram of a computer network

Description automatically generated

En este escenario, la empresa **Azupiso** nos ha solicitado también configurar el protocolo de ruteo OSPF y DHCP centralizado en sus ruteadores **RA** y **RB**.

1. En el **ISP** configure una **ruta estática** hacia **RB** utilizando el rango de direcciones de la red pública asignado: **180.15.2.128 /25**
2. En el ruteador **RB:**
   * Configure una **ruta por default** hacia el **ISP**
   * Configure el protocolo de ruteo **OSPF**:
   1. Utiliza el número de proceso de tu preferencia. NOTA: Un número entre 1 y 216.
   2. Configurar las redes directamente conectadas.
   3. Configurar las interfaces pasivas.
   4. Redistribuir la ruta por default hacia los ruteadores internos de la empresa.
3. Configure manualmente la dirección IP privada (10.0.3.1), máscara de subred, default-gateway y servidor dns del servidor **azupiso.com**
4. En el ruteador **RA**

* Configure el protocolo de ruteo OSPF:
  1. Utiliza el número de proceso de tu preferencia. NOTA: Un número entre 1 y 216.
  2. Configurar las redes directamente conectadas. NOTA: No olvides configurar todas las redes de las VLANs.
  3. Configurar las interfaces pasivas.
* Configurar las subinterfaces de las VLANs (1, 20 y 30). La dirección IP de las subinterfaces será la **última dirección IP válida** de la subred correspondiente.

1. En el switch **SCompany**:

* Configurar las VLANs
  1. Crear las VLANs.
  2. Configurar los puertos troncales.
  3. Configurar la IP del switch SCompany y su default Gateway.

1. En los switches **SOeste** y **SEste**:

* Configurar las VLANs
  1. Crear las VLANs.
  2. Asignar los puertos a las VLANs y definir los puertos de acceso.
  3. Configurar los puertos troncales.
* Configurar las IPs de los switches SOeste y SEste y su default Gateway.

1. Configure **RB** como servidor de DHCP.

* Excluye la IP de los default Gateway y del servidor de Azupiso.

**NOTA:** La práctica recomendada indica que primero se deben configurar las direcciones excluidas, a fin de garantizar que no se arrienden accidentalmente a otros dispositivos.

* Configure un conjunto de direcciones DHCP para cada LAN de los ruteadores **RA** y **RB**.
* Configura la IP del servidor DNS

1. Configure **RA** como **agente de retransmisión DHCP**. Configure la dirección IP de ayuda en **RA** para que reenvíe todas las solicitudes de DHCP al servidor de DHCP en el ruteador **RB**.
2. Habilite el servicio **DHCP** en todos los equipos terminales.
3. Al terminar la configuración realiza las pruebas de conectividad necesarias para comprobar la conexión entre todos los dispositivos de la LAN. Si los pings son exitosos, tu configuración está correcta.

|  |  |  |  |
| --- | --- | --- | --- |
| **From** | **To** | **IP Address (To)** | **Ping**  (Fail / Success) |
| **Laptop0** | **Laptop2** |  |  |
| **Laptop0** | **PVenta** |  |  |
| **Laptop2** | **azupiso.com** | **10.0.3.1** |  |

1. Configure el servicio de **NAT estático** para el servidor de **azupiso**. Traduce la dirección IP privada del servidor de **azupiso** por una dirección IP pública. Utiliza la primera dirección pública disponible del POOL de direcciones IP públicas asignado: **180.15.2.128 /25**
2. Configure el servicio de **PAT**, es decir, conectar direcciones IP privadas con pocas direcciones IP públicas. Instalar el servicio de **PAT** utilizando el POOL de las siguientes direcciones IP públicas: **180.15.2.128 /25. NOTA:** Descarte la IP pública asignada al servidor de **azupiso**.
3. Especifique las **interfaces interiores y exteriores**, es decir, especifique las interfaces de la red que realizarán el nateo interno o externo en **RB**.
4. Configure el **DNSServer** con registro para el servidor de azupiso.

|  |  |
| --- | --- |
| Nombre del registro de recurso | Dirección |
| azupiso.com (dirección pública) |  |

1. Al terminar la configuración realiza las pruebas de conectividad necesarias para comprobar la conexión entre todos los dispositivos de la LAN y la conexión con el exterior.

|  |  |  |
| --- | --- | --- |
| **From** | **To** | **Web Browser**  (Fail / Success) |
| **Laptop0** | **tinder.com** |  |
| **Laptop2** | **tinder.com** |  |
| **Laptop1** | **tinder.com** |  |
| **tinder.com** | **180.15.2.128** |  |
| **tinder.com** | **azupiso.com** |  |

1. Configure una lista de acceso estándar para que la red azul del ruteador **RB** no pueda acceder a la subred de la VLAN de **Services**.

|  |  |  |  |
| --- | --- | --- | --- |
| **From** | **To** | **IP Address (To)** | **Ping**  (Fail / Success) |
| **Laptop1** | **azupiso.com** | **10.0.3.1** | Fail |
| **Laptop1** | **Laptop0** |  | Success |
| **Laptop1** | **tinder.com** | **52.84.150.54** | Success |

1. Configure una lista de acceso extendida para que la VLAN de **Users** no pueda acceder al servidor de **tinder.com** vía web.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **From** | **To** | **IP Address (To)** | **Web Browser**  (Fail / Success) | **Ping**  (Fail / Success) |
| **Laptop0** | **tinder.com** | **52.84.150.54** | Fail | Success |
| **azupiso.com** | **tinder.com** | **52.84.150.54** | Success | Success |
| **Laptop1** | **tinder.com** | **52.84.150.54** | Success | Success |

|  |  |  |  |
| --- | --- | --- | --- |
| **From** | **To** | **IP Address (To)** | **Web Browser**  (Fail / Success) |
| **Laptop0** | **dns.com** | **5.5.5.5** | Success |
| **azupiso.com** | **dns.com** | **5.5.5.5** | Success |
| **Laptop1** | **dns.com** | **5.5.5.5** | Success |