Packet Tracer: Configuración de contraseñas seguras y SSH

Topología

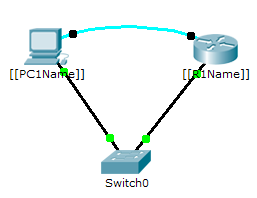


Tabla de direccionamiento

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| El administrador | Interfaces | IP Address (Dirección IP) | Subnet Mask (Máscara de subred) | Gateway predeterminado |
|  | G0/0 |  | 255.255.255.0 | N/A |
|  | NIC |  | 255.255.255.0 |  |

1. Situación

El administrador de red le solicitó que prepare **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** para la implementación. Antes de que pueda conectarse a la red, se deben habilitar las medidas de seguridad.

Requisitos

* Configure el direccionamiento IP en **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** según la tabla de direccionamiento.
* Acceda al **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** mediante el puerto de consola desde el terminal en PC-A.
* Configure el direccionamiento IP en **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** y habilite la interfaz.
* Configure el nombre del host como **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**.
* Cifre todas las contraseñas de texto.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** (config)# **service password-encryption**

* Establezca la contraseña secreta segura que desee.
* Establezca el nombre de dominio en **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** (distinguir mayúsculas de minúsculas para la puntuación de PT).

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** (config)# **ip domain-name [[R1Name]].com**

* Cree un usuario de su elección con una contraseña segura.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** (config)# **username *any\_user* password *any\_password***

* Genere claves RSA de 1024 bits.

**Nota**: en Packet Tracer, introduzca el comando **crypto key generate rsa** y presione la tecla Intro para continuar.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** (config)# **crypto key generate rsa**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Bloquee durante tres minutos a cualquier persona que no pueda iniciar sesión después de cuatro intentos en un período de dos minutos.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** (config)# **login block-for 180 attempts 4 within 120**

* Configure las líneas VTY para el acceso por SSH y solicite los perfiles de usuarios locales para la autenticación.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** (config)# **line vty 0 4**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** (config-line)# **transport input ssh**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** (config-line)# **login local**

* Guardar la configuración en la NVRAM.
* Esté preparado para demostrar al instructor que estableció el acceso por SSH de **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** a **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

ID de Isomorph: **\_\_\_\_\_\_\_ \_\_\_\_\_\_\_ \_\_\_\_\_\_\_**