Packet Tracer - Configure contraseñas seguras y SSH

# Tabla de asignación de direcciones

| Dispositivo | Interfaz | Dirección IP | Máscara de subred | Gateway predeterminado |
| --- | --- | --- | --- | --- |
| RTA | G0/0 | 172.16.1.1 | 255.255.255.0 | N/D |
| PCA | NIC | 172.16.1.10 | 255.255.255.0 | 172.16.1.1 |
| SW1 | VLAN 1 | 172.16.1.2 | 255.255.255.0 | 172.16.1.1 |

# Situación

El administrador de red le ha pedido que prepare **RTA** y **SW1** para la implementación. Antes de que puedan conectarse a la red, se deben habilitar las medidas de seguridad.

# Instrucciones

## Configure la seguridad básica en el enrutador

Abra un símbolo del sistema.

* + 1. Configure el direccionamiento IP en **PCA** de acuerdo con la tabla de direccionamiento.

Cierre símbolo del sistema

Abrir la ventana de configuración

* + 1. Consola en RTA desde la Terminal en PCA.
    2. Configure el nombre de host como **RTA**.
    3. Configure el direccionamiento IP en **RTA** y habilite la interfaz.
    4. Cifre todas las contraseñas no cifradas.

RTA(config)# **service password-encryption**

* + 1. Establezca la longitud mínima de la contraseña en 10.

RTA(config)# **security password min-length 10**

* + 1. Establezca la contraseña secreta segura que desee. **Nota**: Elija una contraseña que recuerde, o tendrá que restablecer la actividad si está bloqueado fuera del dispositivo.
    2. Desactive la búsqueda de DNS.

RTA(config)# **no ip domain-lookup**

* + 1. Establezca el nombre de dominio en **CCNA.com** (distingue entre mayúsculas y minúsculas para la puntuación en PT).

RTA(config)# **ip domain-name CCNA.com**

* + 1. Cree un usuario de su elección con una contraseña cifrada segura.

RTA(config)# **username *any\_user* secret *any\_password***

* + 1. Genere claves RSA de 1024bits.

**Nota**: En Packet Tracer, ingrese la clave criptográfica generar el comando rsa y presione Entrar para continuar.

RTA(config)# **crypto key generate rsa**

El nombre de las claves será:**RTA.CCNA.com**

Elija el tamaño del módulo clave en el rango de 360 a 2048 para su

llaves de uso general. Elegir un módulo clave mayor que 512 puede tomar

unos minutos.

How many bits in the modulus [512]: **1024**

* + 1. Bloquee durante tres minutos a cualquier persona que no pueda iniciar sesión después de cuatro intentos en un período de dos minutos.

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

* + 1. Configure todas las líneas VTY para el acceso SSH y use los perfiles de usuario locales para la autenticación.

RTA (config) # **línea vty 0 4**

RTA(config-line)# **transport input ssh**

RTA(config-line)# **login local**

* + 1. Establezca el tiempo de espera del modo EXEC en 6 minutos en las líneas VTY.

RTA(config-line)# **exec-timeout 6**

* + 1. Guarde la configuración en la NVRAM.

Cerrar la ventana de configuración

* + 1. Acceda al símbolo del sistema en el escritorio de **PCA** para establecer una conexión SSH a **RTA** .

Abra un símbolo del sistema.

C:\ > **ssh/?**

Packet Tracer PC SSH

Uso: **SSH -l username target**

C:\ >

Cierre símbolo del sistema

## Configure la seguridad básica en el Switch

Configure el conmutador **SW1** con las medidas de seguridad correspondientes. Consulte los pasos de configuración del router si necesita ayuda adicional.

* + 1. Haga clic en **SW1** y seleccione la pestaña **CLI** .

Abra una ventana de configuración

* + 1. Configure el nombre de host como **SW1**.
    2. Configure el direccionamiento IP en SW1 **VLAN1** y habilite la interfaz.
    3. Configure la dirección de gateway predeterminado.
    4. Deshabilite todos los puertos de conmutador no utilizados.

**Nota**: En un switch, es una buena práctica de seguridad deshabilitar los puertos no utilizados. Un método para hacer esto es simplemente apagar cada puerto con el comando '**shutdown**'. Esto requeriría acceder a cada puerto individualmente. Existe un método de acceso directo para realizar modificaciones en varios puertos a la vez mediante el **comando** interface range. En **SW1,** todos los puertos excepto Fastethernet0/1 y GigabiteThernet0/1 se pueden apagar con el siguiente comando:

SW1 (config) # **interface range F0/2-24, G0/2**

SW1 (config-if-range) # **shutdown**

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down

<Output omitted>

%LINK-5-CAMBIADO: Interfaz FastEthernet0/24,cambióel estadoa administrativamente inactivo

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down

El comando utilizó el rango de puertos de 2-24 para los puertos FastEthernet y, a continuación, un rango de puertos único de GigabiteThernet0/2.

* + 1. Cifre todas las contraseñas de texto.
    2. Establezca la contraseña secreta segura que desee.
    3. Desactive la búsqueda de DNS.
    4. Establezca el nombre de dominio en **CCNA.com** (distingue entre mayúsculas y minúsculas para la puntuación en PT).
    5. Cree un usuario de su elección con una contraseña cifrada segura.
    6. Genere claves RSA de 1024 bits.
    7. Configure todas las líneas VTY para el acceso SSH y use los perfiles de usuario locales para la autenticación.
    8. Establezca el tiempo de espera del modo EXEC en 6 minutos en todas las líneas VTY.
    9. Guarde la configuración en la NVRAM.

Cierre la ventana de configuración

Fin del documento