**O que é SSH?**

**SSH** significa **Secure Shell** (Shell Seguro). É um protocolo de rede que permite acesso remoto seguro a dispositivos de rede, como switches Cisco, através de uma conexão criptografada.

**Analogia:**

* **Telnet** = Cartão postal (texto visível para qualquer um)
* **SSH** = Carta em envelope seguro (conteúdo criptografado)

**Para que serve a configuração do SSH em switches Cisco?**

**1. Acesso Remoto Seguro**

Permite que administradores configurem e monitorem o switch remotamente de forma segura, sem risco de interceptação de senhas ou comandos.

**2. Criptografia de Dados**

* **Senhas** são transmitidas de forma criptografada
* **Comandos** são protegidos contra espionagem
* **Configurações** trafegam de forma segura na rede

3. Autenticação Forte

Suporta diferentes métodos de autenticação:

Usuário/Senha local

Servidores AAA (TACACS+, RADIUS)

Chaves públicas/privadas

**4. Substituição do Telnet**

O Telnet envia tudo em **texto puro**, tornando-o inseguro para ambientes de produção.

**5. Conformidade com Políticas de Segurança**

Atende requisitos de segurança corporativa e normas de compliance.

**Configuração Completa do SSH em Switch Cisco**

**Pré-requisitos Obrigatórios:**

Switch> enable

Switch# configure terminal

! 1. Configurar hostname (obrigatório)

Switch(config)# hostname SW-Seguro-01

! 2. Configurar domínio (obrigatório para gerar chaves)

SW-Seguro-01(config)# ip domain-name empresa.com

! 3. Gerar chaves criptográficas RSA (obrigatório)

SW-Seguro-01(config)# crypto key generate rsa modulus 2048

The name for the keys will be: SW-Seguro-01.empresa.com

% Generating 2048 bit RSA keys, keys will be non-exportable...

[OK]

Configuração Principal do SSH:

! 4. Configurar versão do SSH (recomendado versão 2)

SW-Seguro-01(config)# ip ssh version 2

! 5. Configurar parâmetros de tempo e tentativas

SW-Seguro-01(config)# ip ssh time-out 60

SW-Seguro-01(config)# ip ssh authentication-retries 3

! 6. Criar usuários para autenticação

SW-Seguro-01(config)# username admin privilege 15 secret SenhaAdmin123!

SW-Seguro-01(config)# username suporte privilege 5 secret SenhaSuporte456!

! 7. Configurar linhas VTY para usar SSH

SW-Seguro-01(config)# line vty 0 15

SW-Seguro-01(config-line)# transport input ssh ! ACEITA APENAS SSH

SW-Seguro-01(config-line)# login local ! Autenticação local

SW-Seguro-01(config-line)# exec-timeout 10 0

SW-Seguro-01(config-line)# end

**Configurações Avançadas de Segurança:**

SW-Seguro-01# configure terminal

! 8. Desativar completamente o Telnet

SW-Seguro-01(config)# line vty 0 15

SW-Seguro-01(config-line)# no transport input telnet

SW-Seguro-01(config-line)# no transport input all

SW-Seguro-01(config-line)# transport input ssh ! Somente SSH

! 9. Configurar ACL para restringir acesso SSH

SW-Seguro-01(config)# ip access-list standard ACL-SSH

SW-Seguro-01(config-std-nacl)# permit 192.168.10.0 0.0.0.255

SW-Seguro-01(config-std-nacl)# permit 10.1.1.100

SW-Seguro-01(config-std-nacl)# deny any

SW-Seguro-01(config-std-nacl)# exit

! Aplicar ACL nas linhas VTY

SW-Seguro-01(config)# line vty 0 15

SW-Seguro-01(config-line)# access-class ACL-SSH in

SW-Seguro-01(config-line)# end

**Salvar Configuração:**

SW-Seguro-01# copy running-config startup-config

**Como Testar e Usar o SSH**

**Testar Conexão SSH do Próprio Switch:**

! Testar conectividade SSH para outro dispositivo

SW-Seguro-01# ssh -l admin 192.168.10.20

**Conectar do Cliente para o Switch:**

**No Linux/macOS:**

ssh [admin@192.168.10.10](mailto:admin@192.168.10.10)

**No Windows (PowerShell):**

ssh [admin@192.168.10.10](mailto:admin@192.168.10.10)

**Verificar Status do SSH:**

SW-Seguro-01# show ip ssh

SSH Enabled - version 2.0

Authentication timeout: 60 secs; Authentication retries: 3

**Verificar Sessões SSH Ativas:**

SW-Seguro-01# show ssh

Connection Version Mode Encryption Hmac State Username

0 2.0 IN aes128-ctr hmac-sha1 Session started admin

1 2.0 OUT aes128-ctr hmac-sha1 Session started suporte

**Verificar Chaves RSA:**

SW-Seguro-01# show crypto key mypubkey rsa

**Testar Conectividade:**

SW-Seguro-01# ping 192.168.10.1

! Verificar se o switch tem reachability para a rede

**Comparação: SSH vs Telnet**

| Característica | SSH | Telnet |
| --- | --- | --- |
| **Segurança** | ✅ Criptografado | ❌ Texto puro |
| **Autenticação** | ✅ Múltiplos métodos | ❌ Senha em texto |
| **Porta** | TCP 22 | TCP 23 |
| **Performance** | ⚠️ Leve overhead | ✅ Mais rápido |
| **Recomendação** | ✅ Produção | ❌ Apenas lab |

**Solução de Problemas Comuns**

**SSH Não Funciona? Verifique:**

! 1. Chaves RSA foram geradas?

show crypto key mypubkey rsa

! 2. SSH está habilitado?

show ip ssh

! 3. Linhas VTY configuradas para SSH?

show running-config | section line vty

! 4. Usuários locais criados?

show running-config | include username

! 5. Domínio configurado?

show running-config | include domain-name

! 6. ACL bloqueando?

show ip access-list ACL-SSH

**Regenerar Chaves SSH (se necessário):**

SW-Seguro-01(config)# crypto key zeroize rsa

SW-Seguro-01(config)# crypto key generate rsa modulus 2048

**Resumo da Importância do SSH**

**Por que usar SSH?**

* 🔒 **Segurança**: Dados criptografados
* 👥 **Autenticação**: Múltiplos usuários com diferentes privilégios
* 📋 **Auditoria**: Logs de quem acessou e quando
* 🚀 **Conformidade**: Atende políticas de segurança corporativa
* ⚡ **Produtividade**: Acesso remoto seguro de qualquer lugar

Quando configurar SSH?

✅ SEMPRE em ambientes de produção

✅ SEMPRE quando o acesso for através de redes não confiáveis

✅ SEMPRE para compliance com normas de segurança

❌ NUNCA depender apenas do Telnet

Conclusão: Configurar SSH não é opcional em redes modernas - é uma necessidade de segurança básica para qualquer switch Cisco em ambiente corporativo! 🛡️