Laboratório - Implementação de Segurança de VLAN

Topologia

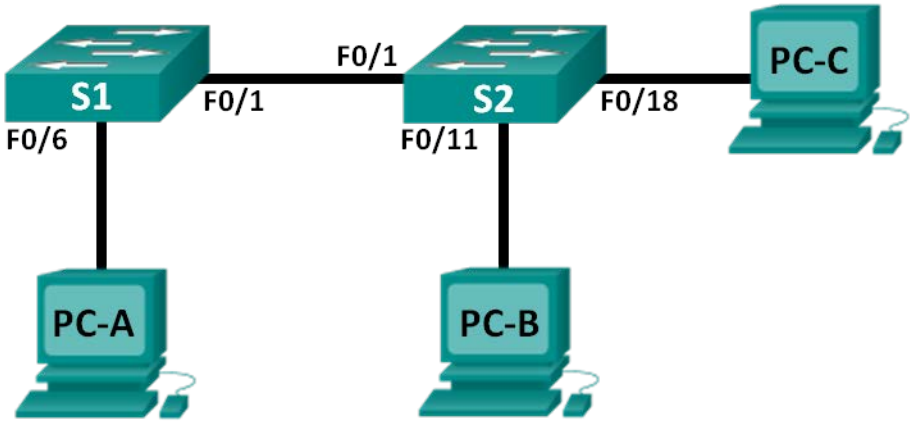

Tabela de Endereçamento

Dispositivo	Interface	Endereço IP	Máscara de Sub-rede	Gateway Padrão
S1	VLAN 99	172.17.99.11	255.255.255.0	172.17.99.1
S2	VLAN 99	172.17.99.12	255.255.255.0	172.17.99.1
PC-A	NIC	172.17.99.3	255.255.255.0	172.17.99.1
PC-B	NIC	172.17.10.3	255.255.255.0	172.17.10.1
PC-C	NIC	172.17.99.4	255.255.255.0	172.17.99.1

Atribuições de VLAN

VLAN	Nome
10	Dados
99	Gerenciamento&Nativa
999	BuracoNegro

Objetivos

Parte 1: Construir a rede e definir as configurações básicas do dispositivo

Parte 2: Implementar Segurança com VLANs nos switches

Histórico/cenário

A prática recomendada determina definir algumas configurações básicas de segurança para ambas as portas de acesso e de tronco nos switches. Isso ajudará a proteger contra ataques à VLAN e impedirá que sniffers detectem o tráfego na rede.

Neste laboratório, você configurará os dispositivos de rede na topologia com algumas configurações básicas, verificará a conectividade e, em seguida, aplicará medidas de segurança mais rigorosas nos switches. Você examinará como os switches Cisco se comportam usando vários comandos **show**. Em seguida, você aplicará medidas de segurança.

Observação: os switches usados neste laboratório são Cisco Catalyst 2960s com software IOS Cisco versão 15.0(2) (imagem lanbasek9). Outros switches e versões do IOS Cisco podem ser usados. Dependendo do modelo e da versão do IOS Cisco, os comandos disponíveis e a saída produzida podem diferir dos mostrados nos laboratórios.

Observação: certifique-se de que os switches tenham sido apagados e que não haja configurações de inicialização. Se estiver em dúvida, entre em contato com o instrutor.

Recursos necessários

- 2 Switches (Cisco 2960 com IOS Cisco versão 15.0(2), imagem lanbasek9 ou semelhante)
- 3 PCs (Windows 7, Vista ou XP com um programa de emulação de terminal, como o Tera Term)
- Cabos de console para configurar os dispositivos IOS Cisco através das portas de console
- Cabos Ethernet conforme mostrado na topologia

Parte 1: Construir a rede e definir as configurações básicas do dispositivo

Na Parte 1, você definirá configurações básicas nos switches e nos PCs. Consulte a Tabela de Endereçamento para obter os nomes de dispositivos e as informações de endereço.

Etapa 1: Instale os cabos da rede conforme mostrado na topologia.

Etapa 2: Inicialize e recarregue os switches.

Etapa 3: Configure os endereços IP nos PC-A, PC-B e PC-C.

Consulte a Tabela de Endereçamento para obter informações de endereço do PC.

Etapa 4: Defina as configurações básicas de cada switch.

a. Desative a pesquisa DNS.

b. Configure os nomes de dispositivos conforme mostrado na topologia.

c. Atribua **class** como a senha do modo EXEC privilegiado.

d. Atribua **cisco** como senha de console e VTY e habilite o login para as linhas do console e vty.

e. Configure **synchronous logging** para as linhas do console e vty.

Etapa 5: Configure VLANs em cada switch.

a. Crie e nomeie as VLANs de acordo com a tabela de atribuições de VLAN.

b. Configure o endereço IP listado na Tabela de Endereçamento para VLAN 99 em ambos os switches.

c. Configure a interface F0/6 em S1 como uma porta de acesso e a atribua à VLAN 99.

d. Configure F0/11 em S2 como uma porta de acesso e a atribua à VLAN 10.

e. Configure F0/18 em S2 como uma porta de acesso e a atribua à VLAN 99.

f. Emita o comando **show vlan brief** para verificar a VLAN e as atribuições de porta.

À qual VLAN pertenceria uma porta não atribuída, como F0/8 em S2?

Etapa 6: Configure a segurança básica do switch.

a. Configure um banner MOTD para avisar aos usuários que o acesso não autorizado é proibido.

b. Criptografe todas as senhas.

c. Desative todas as portas físicas não utilizadas.

d. Desative o serviço básico de web em execução.

```
S1(config)# no ip http server
S2(config)# no ip http server
```

e. Copie a configuração em execução para a configuração de inicialização.

Etapa 7: Verifique a conectividade entre dispositivos e informações de VLAN.

a. Do prompt de comando no PC-A, faça ping no endereço de gerenciamento do S1. Os pings foram bem-sucedidos? Por quê?

b. A partir do S1, faça ping no endereço de gerenciamento de S2. Os pings foram bem-sucedidos? Por quê?

c. A partir do prompt de comando do PC-B, faça ping nos endereços de gerenciamento em S1 e S2 e no endereço IP do PC-A e do PC-C. Os pings foram bem-sucedidos? Por quê?

d. De um prompt de comando no PC-C, faça ping nos endereços de gerenciamento em S1 e S2. Você obteve êxito? Por quê?

Observação: talvez seja necessário desativar o firewall do PC para fazer ping entre os PCs.

Parte 2: Implemente a segurança de VLAN nos switches

Etapa 1: Configure as portas de tronco em S1 e S2.

a. Configure a porta F0/1 em S1 como uma porta de tronco.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
```

b. Configure a porta F0/1 em S2 como uma porta de tronco.

```
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
```

c. Verifique o entroncamento em S1 e S2. Emita o comando **show interface trunk** em ambos os switches.


```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,99,999
```

Etapa 2: Altere a VLAN nativa para as portas de tronco em S1 e S2.

Alterar a VLAN nativa das portas de tronco de VLAN 1 para outra VLAN constitui uma boa prática de segurança.

a. Qual é a VLAN nativa atual das interfaces F0/1 de S1 e S2?

b. Configure a VLAN nativa na interface de tronco F0/1 de S1 para Gerenciamento&Nativa VLAN 99.

```
S1# config t
S1(config)# interface f0/1
S1(config-if)# switchport trunk native vlan 99
```

c. Aguarde alguns segundos. Você deve começar a receber mensagens de erro na sessão de console do S1. O que significa a mensagem %CDP-4-NATIVE_VLAN_MISMATCH:?

d. Configure a VLAN nativa na interface de tronco F0/1 de S2 para a VLAN 99.

```
S2(config)# interface f0/1
S2(config-if)# switchport trunk native vlan 99
```

e. Verifique se a VLAN nativa é, agora, 99 em ambos os switches. O resultado de S1 é mostrado abaixo.

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99,999

Port         Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,999
```


Etapa 3: Verifique se o tráfego pode atravessar com sucesso o link de tronco.

a. Do prompt de comando no PC-A, faça ping no endereço de gerenciamento do S1. Os pings foram bem-sucedidos? Por quê?

b. A partir da sessão de console no S1, faça ping no endereço de gerenciamento do S2. Os pings foram bem-sucedidos? Por quê?

c. A partir do prompt de comando do PC-B, faça ping nos endereços de gerenciamento em S1 e S2 e no endereço IP do PC-A e do PC-C. Os pings foram bem-sucedidos? Por quê?

d. A partir do prompt de comando do PC-C, faça ping nos endereços de gerenciamento do S1 e S2 e no endereço IP do PC-A. Você obteve êxito? Por quê?

Etapa 4: Impeça o uso do DTP em S1 e S2.

A Cisco usa um protocolo proprietário conhecido como DTP (Dynamic Trunking Protocol) em seus switches. Algumas portas negociam automaticamente o entroncamento. Uma boa prática é desativar a negociação. Para ver esse comportamento padrão, emita o seguinte comando:

```
S1# show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
<saída omitida>
```

a. Desative a negociação em S1.

```
S1(config)# interface f0/1
S1(config-if)# switchport nonegotiate
```

b. Desative a negociação em S2.

```
S2(config)# interface f0/1
S2(config-if)# switchport nonegotiate
```

c. Para verificar se a negociação está desativada, emita o comando **show interface f0/1 switchport** em S1 e S2.

```
S1# show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
```



```
<saída omitida>
```

Etapa 5: Garanta portas de acesso em S1 e S2.

Apesar de você ter desativado as portas não utilizadas nos switches, se um dispositivo estiver conectado a uma daqueles portas e a interface estiver ativada, o entroncamento ainda poderia acontecer. Além disso, por padrão, todas as portas estão na VLAN 1. Uma boa prática consiste em colocar todas as portas não utilizadas em uma VLAN "buraco negro". Nesta Etapa, você desabilitará o entroncamento em todas as portas não utilizadas. Você também atribuirá portas não utilizadas à VLAN 999. Para este laboratório, somente as portas de 2 a 5 serão configuradas em ambos os switches.

a. Emita o comando **show interface f0/2 switchport** em S1. Observe o estado e o modo administrativo da negociação de entroncamento.

```
S1# show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
<saída omitida>
```

b. Desative o entroncamento nas portas de acesso de S1.

```
S1(config)# interface range f0/2 – 5
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 999
```

c. Desative o entroncamento nas portas de acesso de S2.

d. Verifique se a porta F0/2 está configurada para acesso no S1.

```
S1# show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 999 (BlackHole)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
<saída omitida>
```

e. Verifique se as atribuições da porta VLAN em ambos os switches estão corretas. S1 é exibido abaixo como um exemplo.

```
S1# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
```



```
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gi0/1, Gi0/2
10   Data                             active
99   Management&Native                active    Fa0/6
999  BlackHole                        active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
1002 fddi-default                       act/unsup
1003 token-ring-default                 act/unsup
1004 fddinet-default                    act/unsup
1005 trnet-default                      act/unsup
Restrict VLANs allowed on trunk ports.
```

Por padrão, todas as VLANs podem ser transportadas em portas de tronco. Por motivo de segurança, é uma boa prática permitir que apenas VLANs desejadas específicas cruzem os links de tronco em sua rede.

f. Restrinja a porta de tronco F0/1 em S1 para permitir somente VLANs 10 e 99.

```
S1(config)# interface f0/1
S1(config-if)# switchport trunk allowed vlan 10,99
```

g. Restrinja a porta de tronco F0/1 em S2 para permitir somente VLANs 10 e 99.

h. Verifique as VLAN permitidas. Emita um comando **show interface trunk** no modo EXEC privilegiado em S1 e S2.

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       10,99

Port        Vlans allowed and active in management domain
Fa0/1       10,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,99
```

Qual é o resultado?

Reflexão

Quais são os problemas de segurança, se houver, da configuração padrão de um switch Cisco?

