03

Habilitando segurança da porta

Transcrição

[00:00] Nós conseguimos desabilitar todas as outras portas que não estamos utilizando para evitar que algum usuário venha em alguma outra porta desse switch, conecte o seu computador e comece a fazer alguns testes na nossa rede.

[00:13] Só que nós temos ainda essas duas portas, a porta fastEthernet 0/1 e a porta fastEthernet 0/2, que somente as duas estão habilitadas, mas nada me impede que algum usuário desconecte esses computadores, o PC 0 e o PC 1, e faça algum cenário que eles estão imaginando na nossa rede pra fazer alguns testes.

[00:35] Qual é esse primeiro cenário que enfrentamos? Esse cenário aqui, o nosso funcionário está estudando para a prova do CCNA da Cisco e ele decide desconectar esse cabo do fastEthernet 0/1, e ele quer montar como se fosse uma mini rede de testes. Então, ele quer desconectar esse cabo, o fastEthernet 0/1, e ele quer conectar nessa porta fastEthernet 0/1 um outro switch com outro computador, pra poder fazer alguns testes, ver como é que os switches conseguem se comunicar, aqueles protocolos todos que já vimos.

[01:12] Então, temos um problema aqui, porque essa porta fastEthernet 0/1 no momento não está habilitada com nenhuma forma de segurança, ela só está habilitada e, teoricamente, tudo o que fizemos nessa porta, essa porta vai aceitar, ela não tem nenhuma política de segurança.

[01:31] Como uma primeira regra que esse nosso cliente passou pra nós, é que queremos evitar que essa porta fastEthernet 0/1 aceite mais do que um dispositivo. Só queremos que ela aceite um único dispositivo, evitando que esse nosso funcionário traga os switches e os hubs da casa dele e conecte nessa porta fastEthernet 0/1 pra fazer alguns testes. Não queremos isso. Só queremos que ele tenha a possibilidade de conectar um único dispositivo.

[01:59] Pra fazer isso vamos configurar o nosso switch, essa porta fastEthernet 0/1 desse switch, pra aceitar somente um dispositivo. Evitando assim que ele traga os switches da casa dele, os hubs da casa dele, e fique aqui montando uma mini rede de testes nessa porta fastEthernet 0/1.

[02:15] Entramos no nosso switch, estamos no modo user exec. E temos que subir os níveis pra chegar até esse nível de configuração da interface fastEthernet 0/1. Colocamos "enable" pra entrar no modo privilegiado. Colocamos "configure terminal" pra entrar no modo global de configuração. E agora entramos na interface, colocamos "interface fastEthernet 0/1". E agora já estou no último nível, que é a configuração da interface.

[02:45] Como primeiro passo, temos que falar como que vai ser o modo de operação dessa porta. Se lembrarmos daquele modelo hierárquico da Cisco, quando um equipamento, no caso, o switch, está conectado a um dispositivo final, essa camada da nossa rede chamamos de "camada de acesso".

[03:05] Eu tenho que falar que essa porta fastEthernet 0/1 é uma porta que vai trabalhar no modo de acesso. Tenho que colocar "switchport mode access" e agora sim. Uma vez que eu especifiquei que essa porta vai trabalhar nesse mundo de acesso, eu posso vir aqui e configurar uma segurança nessa porta. Pra eu configurar essa segurança, o primeiro passo é habilitar a segurança nessa porta, eu tenho que dizer que eu vou habilitar a segurança.

[03:33] Para eu habilitar a segurança eu venho e coloco o comando "switchport port-security". É um comando novo, ainda não vimos o "switchport port-security". Com esse comando eu estou habilitando essa porta, para que ela trabalhe com mais segurança. Só que eu tenho que especificar como que eu quero que essa segurança seja feita.

[03:56] Pela requisição do nosso cliente, queremos evitar que esses funcionários, no caso é o nosso funcionário que está estudando pro CCNA, queremos evitar que ele fique conectando vários equipamentos nessa porta. Somente queremos que essa porta fastEthernet 0/1 aceite somente um único dispositivo. Então, diz aqui que queremos que essa porta aceite somente um dispositivo.

[04:18] Para isso vamos colocar um comando bem parecido com a linha anterior, que é "switchport port-security". E agora eu tenho que falar o quê? Eu quero que o máximo da quantidade de dispositivos, então eu venho e coloco "maximum", seja igual a um dispositivo, então eu coloco enter. E a partir de agora essa porta, fastEthernet 0/1, só vai aceitar um único dispositivo. Se eu tiver mais do que um dispositivo, vamos ver como é que essa rede vai se comportar.

[04:45] Nesse nosso cenário nós configuramos que essa porta fastEthernet 0/1 desse switch aceite somente um dispositivo conectado nela. Vamos fazer um teste inicial e verificar se esses computadores estão conseguindo se comunicar. Porque, teoricamente, aqui somente temos esse PC 0 conectado nessa porta, então não tem nenhuma violação de segurança, estamos dentro do que nós especificamos como uma norma de segurança dessa porta. Só temos um dispositivo conectado, que é esse computador PC 0.

[05:19] Vamos só configurar os endereços IPs desses computadores pra fazer o teste do ping pra ver a conectividade, se ela está acontecendo. Vou colocar nesse computador, o PC 0 da esquerda, o endereço IP 192.168.0.1. E nesse computador aqui, o PC 1 da direita, colocar o endereço IP 192.168.0.2. Vamos tentar realizar o teste de conectividade entre eles.

[05:47] Voltamos pro PC 0 e vamos aqui e digita "ping 192.168.0.2", que é o endereço IP do computador da direita, que é o PC 1, e a nossa comunicação foi estabelecida com sucesso. Então, a nossa porta aparentemente está funcionando normalmente.

[06:06] Esse nosso funcionário, no dia seguinte, como nós suspeitávamos que ele está estudando pro CCNA, decide trazer o switch da casa dele pra fazer um teste nessa nossa rede de produção. Então ele vem aqui, desconecta esse cabo e traz o switch da casa dele, e ele vai o quê? Ele vai conectar esse switch na única porta que está habilitada, que é a fastEthernet 0/1, porque todas as outras nós havíamos desabilitado.

[06:37] Então, ele vem aqui e conecta na porta que está disponível, que é a porta fastEthernet 0/1 que está habilitada, conecta o switch dele. E ele vem aqui e conecta o computador nesse switch que ele trouxe da casa dele. Ele vem aqui e conecta esse computador nesse switch.

[06:55] Agora, nós temos o quê? Nessa porta fastEthernet 0/1 somente tínhamos configurado pra ela aceitar um único dispositivo, mas agora essa porta fastEthernet 0/1 vai ter o endereço MAC que seria vinculado a esse switch e vamos ter também o endereço MAC que seria vinculado a esse meu computador. Então nessa porta fastEthernet 0/1 eu não estou tendo mais um dispositivo como eu especifiquei na minha norma de segurança, eu tenho dois dispositivos conectados.

[07:29] Vamos ver o que vai acontecer nessa porta se tentarmos realizar a comunicação. Teoricamente, esperamos que tenha alguma proteção, porque não estamos seguindo a norma de segurança dessa porta. Então, o que eu vou fazer? Pra verificar se essa segurança está sendo feita, eu vou clicar nesse computador, no PC 0, eu venho no Command Prompt. Veja que ainda temos os resultados na tela do teste anterior, somente tínhamos um computador conectado.

[07:56] Eu venho aqui e digito novamente □ping 192.168.0.2□ e vamos ver o resultado agora. Olha só o que tivemos aqui: "Request timed out". E vamos ver como que a nossa porta ficou? A porta aqui está vermelha. Quando tem essa cor vermelha quer dizer que a porta está desabilitada. Por que ela desabilitou? Porque tivemos uma violação de segurança.

[08:21] Essa porta fastEthernet 0/1 só estava habilitada pra aceitar um dispositivo e a partir do momento que ela detectou que tem mais do que um dispositivo nessa porta, como padrão, as portas da Cisco, quando detectam uma violação de segurança, elas vão desabilitar essa porta prevenindo que a comunicação siga adiante.

[08:45] O que vai acontecer? Essa porta desabilitou. Esperamos que esse funcionário que fez o teste, que não sabia que não podia, esperamos que ele entre em contato conosco, porque nós somos os administradores da rede, dizendo o que aconteceu. e explicamos pra ele que: "não podemos conectar mais do que um dispositivo nessa porta fastEthernet 0/1, somente podemos conectar um único dispositivo". Então, vamos voltar e habilitar novamente essa porta.

[09:15] Vamos no nosso switch e explicamos pro nosso funcionário que ele não pode ficar conectando mais do que um equipamento. Agora, nós, administradores de rede, temos que voltar essa porta e recuperar o modo dela pra que ela trabalha normalmente. Para podermos recuperar essa porta precisamos fazer um comando um pouco diferente do fizemos aqui. Essa porta desabilitou porque teve uma violação de segurança.

[09:42] Pra eu poder habilitá-la novamente, eu tenho que fazer o quê antes? Eu tenho que desabilitar essa porta administrativamente. Tenho que colocar aqui "shutdown". Eu sei que é um pouco estranho, mas pelo fato de ter tido uma violação de segurança, eu tenho que desabilitar essa porta agora administrativamente. Eu tenho que colocar "shutdown". E uma vez que essa porta está desabilitada administrativamente, eu tenho que habilitá-la administrativamente colocando o comando "no shutdown".

[10:11] E essa porta agora, perceba que ela voltou o status para "up". Essa porta agora vai voltar a ficar ativa. Somente explicamos para o nosso funcionário que ele não pode fazer essa conexão. Então, ele vem aqui e retira o switch da rede dele, da rede de produção e ele volta a conectar o computador, o PC 0, de volta na porta fastEthernet 0/1.

[10:37] Perceba que agora a porta está só esperando aqueles segundos iniciais de conexão, pra que ela fique habilitada e temos a nossa porta voltando a funcionar normalmente.

[10:53] Essa questão de quando acontecem essas violações de segurança, não podemos esquecer que pra voltá-la ao normal, temos que primeiro desabilitá-la administrativamente, colocando o comando "shutdown" e depois habilitá-la administrativamente, colocando comando "no shutdown".

[11:11] Vamos só confirmar se agora a porta voltou e está a conexão estabelecida, como estava antes de colocarmos o switch? Vou voltar no meu computador, o PC 0, e vamos fazer o teste novamente. Colocamos o switch e vimos que teve a violação de segurança, então habilitamos a porta novamente e vamos fazer o teste colocando "ping 192.168.0.2". E veja lá que a nossa porta voltou a funcionar normalmente como antes. Vamos analisar mais alguns cenários.