09

Violação de segurança

Transcrição

[00:00] Nós tínhamos configurado essa porta fastEthernet 0/2 pra que ela atuasse naquele modo sticky, podendo assim aprender de forma dinâmica os endereços MAC dos equipamentos no qual ela vai estar conectada.

[00:11] Pegamos esse computador, o PC 1, e estabelecemos uma comunicação com esse PC 0. Então, essa porta fastEthernet 0/2 aprendeu de forma dinâmica o endereço MAC desse meu computador PC 1, e a partir desse momento essa porta fastEthernet 0/2 só vai aceitar os dados que vierem desse computador PC 1.

[00:32] Quando eu troquei e coloquei esse notebook no lugar, esse notebook tem o quê? Ele tem outro endereço MAC, então se ele tem outro endereço MAC, a partir do momento que tentarmos realizar uma comunicação com esse computador PC 0, o que vai acontecer? Essa porta aqui vai detectar que ocorreu uma violação de segurança e quando ocorre uma violação de segurança, por padrão, as portas dos switches da Cisco vão desabilitar.

[00:57] Vamos perguntar pra esse switch um pouco mais de detalhes sobre essa questão da violação de segurança que aconteceu? Vamos clicar aqui no switch e sempre que queremos pedir pra um equipamento me mostrar, temos que ir no modo privilegiado e digitar o comando "show", e depois o que nós queremos que ele me mostre.

[01:16] Colocamos o comando "enable" pra subir até o modo privilegiado. E vamos colocar o comando "show port-security" aqui. Onde que ocorreu essa violação de segurança? Foi na interface fastEthernet 0/2, então vou colocar "show port-security interface fastEthernet 0/2". E ele vai me mostrar maiores detalhes de como estão configuradas essas violações de segurança nessa interface fastEthernet 0/2.

[01:45] Logo nessa terceira linha nós temos o modo de violação que está configurado pra essa porta. Por padrão as portas dos switches da Cisco vão estar nesse modo "shutdown", que nós vimos, shutdown seria desabilitar. Isso quer dizer que quando ocorrer uma violação de segurança nessa porta desse meu switch, esse meu switch vai o quê? Ele vai desabilitar essa porta, vai ocasionar esse modo shutdown e vai desabilitar a porta.

[02:16] E olha só o que nós temos aqui embaixo. Nós temos a contagem de violação de segurança que aconteceu. Então essa interface fastEthernet 0/2 detectou o quê? Detectou uma violação de segurança. E quando ela detecta uma violação de segurança ela vai desabilitar essa porta.

[02:36] Só que essa forma que ela desabilita a porta não é uma forma natural, ela desabilitou porque ela detectou que teve uma violação de segurança. Se perguntarmos detalhes dessa interface, vamos ver que essa porta não vai aparecer somente o nome shutdown, vamos ver o nome que ela vai aparecer.

[02:58] Vou colocar o comando "show interfaces" e vou colocar "show interface fast Ethernet 0/2". Vou colocar um espaço, só para podermos ver todos os outros resultados. Ele me fala que a fastEthernet 0/2 está com um problema na camada física, porque, a porta está desabilitada. Mas olha esse nome que ele me fala aqui: essa porta está com esse nome "err", quer dizer de erro. Ela foi desabilitada porque aconteceu um erro, porque aconteceu uma violação de segurança.

[03:38] Se vermos na prova de certificação ou na nossa vida profissional esse termo "err-disable", desabilitado por erro, é porque aconteceu uma violação de segurança nessa interface e conseguimos ter essa análise também quando pedimos maiores detalhes de configuração dessa interface, não só com relação a parte de segurança. Então, veja que essa porta está nesse modo "err-disable".

[04:05] Nós, administradores de rede, vimos que essa porta, essa interface foi desabilitada porque teve um erro, porque teve uma violação de segurança e temos que fazer todo aquele processo, temos que ir no modo global de configuração, tem que entrar na interface novamente digitando "interface fastEthernet 0/2" e temos que primeiro desabilitar administrativamente essa porta.

[04:29] Pra desabilitar administrativamente essa porta colocamos o comando "shutdown" e essa porta está administrativamente desabilitada. E agora temos que o quê? Temos que habilitar essa porta administrativamente, então colocamos o comando "no shutdown". E agora essa porta voltou a estar no modo habilitada, ela mudou o status dela para up.

[04:54] Mas imagina só, toda hora temos que fazer isso por qualquer problema de violação de segurança que aconteça na nossa rede pode ser um pouco trabalhoso pro administrador, ele ter que ir, sair da mesa dele, ir lá no switch, configurar o switch pra desabilitar a porta administrativamente, depois habilitar essa porta administrativamente.

[05:12] A ideia que podemos ter é querer que essa porta continue protegendo os nossos dados, mas que não necessariamente ela desabilite a porta. Então, vamos ver quais são os outros modos de operação de segurança que essa porta vai poder operar pra nós. Então vamos lá.

[05:29] Eu vou voltar no switch e nós estamos ainda na interface fastEthernet 0/2, então ainda estamos no modo de configuração dela. Eu vou perguntar pra essa interface fastEthernet 0/2 quais são os modos de segurança que ela vai poder trabalhar. Pra isso vou colocar o comando "switchport port-security". E eu tenho que colocar o comando aqui de "violation", e uma interrogação. Eu tenho essas três opções pra configurar a minha porta, pra quando ela detectar uma violação de segurança.

[06:08] Por padrão, quando ocorre uma violação segurança, ela já vem nesse modo shutdown, que é quando ela desabilita a porta. Então vamos o quê? Vamos testar agora esses outros dois modelos, o protect e o restrict, pra ver como que eles vão se comportar.

[06:23] Vamos testar primeiro nesse modo protect. Então, vou colocar que eu quero que essa interface fastEthernet 0/2, caso ela detecte uma violação de segurança, que ela não entre nesse modo shutdown. Eu quero que ela entre nesse modo de protect.

[06:40] Pra vermos se ela está trabalhando no modo protect, eu vou colocar um Ctrl + Z e voltamos pra aquele comando "show", e pedimos com relação ao status de segurança dessa interface. Colocamos "show port-security interface fastEthernet 0/2" e ele me fala que agora essa interface está no modo protect, ou seja, se acontecer uma violação de segurança, vamos ter o quê? Essa porta vai entrar nesse modo de proteção.

[07:09] Vamos fazer o seguinte, vamos testar se esse nosso modo de operação está sendo executado com sucesso e vamos fazer esse teste com esse notebook. Lembrando que esse notebook não está configurado pra ser aceito por essa interface, então esperamos que essa porta não permita que esses dados sejam trafegados adiante na nossa rede. Vamos só ver se foi feita a configuração certa ou se foi feita alguma coisa errada.

[07:39] Vamos no Command Prompt e vamos testar a conectividade com o PC 0. Vamos colocar "ping 192.168.0.1", que é o endereço IP do PC 0 que está lá do lado esquerdo. Vamos fazer o teste e vamos ver o que nós temos aqui. Aparentemente, tivemos um request timed out, nós não estamos conseguindo estabelecer a comunicação com o nosso computador PC 0, que está do lado esquerdo. Então, vamos voltar pra nossa topologia.

[08:09] Mas, vejam só como que está a nossa porta agora. A nossa porta não está naquela cor vermelha, ela está o quê? Ela ainda está verde. Vamos ver se teve alguma violação de segurança. Vou clicar aqui, vou vir aqui e novamente vamos colocar o comando "show port-security interface fastEthernet 0/2".

[08:29] A nossa violação de segurança não foi incrementada. Será que fizemos alguma coisa errada aqui? Ou tivemos sorte que fizemos alguma coisa errada e realmente esse equipamento que não deveria se comunicar não está comunicando.

[08:46] Pra testar se foi feita alguma coisa errada, vamos voltar ao computador PC 1, porque o PC 1 deve ser aceito por essa porta, ele deve manter a comunicação com o PC 0. Vamos desconectar e vamos voltar o PC 1 pra ver se foi feita alguma coisa errada. Porque se foi feita alguma coisa errada nem o PC 1 vai conseguir se comunicar com o PC 0. Isso não pode acontecer.

[09:13] A porta fastEthernet 0/2 desse switch foi configurada em modo sticky e ela aprendeu o endereço MAC desse PC 1, então o PC 1 deve ainda estar habilitado, somente mudamos o modo de operação.

[09:25] Caso ocorresse uma violação de segurança, a porta deveria desabilitar anteriormente, quando estava no modo shutdown. Agora no modo protect ela simplesmente não passou os dados, tivemos o request timed out nosso notebook, mas o meu switch não detectou uma violação de segurança. Vamos ver se a comunicação com o PC 1 e o PC 0 está sendo feita com sucesso.

[09:50] Conectamos de novo o nosso computador, o PC 1, e vamos colocar de novo o teste de ping, "192.168.0.1". Esse computador, o PC 1, está conseguindo se comunicar com o PC 0. Então, veja só a vantagem já dessa configuração nesse modo protect.

[10:08] Esse modo protect não desabilitou a porta, ele só impediu que outro dispositivo que, no caso, não fosse o PC 1, que qualquer outro dispositivo que não seja o PC 1, ele vai impedir que esse tráfego siga adiante na nossa rede, mas ele não vai desabilitar a porta. Então se eu simplesmente desconectar esse equipamento que não pode ser utilizado nessa porta fastEthernet 0/2 e voltar o computador PC 1, que pode trafegar na porta fastEthernet 0/2, a comunicação volta a ser estabelecida normalmente.

[10:38] Não precisa o administrador ter que sair da mesa dele, ir no switch e desabilitar administrativamente a porta pra depois habilitar a porta administrativamente, simplesmente a nossa rede, essa interface do switch protege com outros equipamentos que não sejam o que nós configuramos.

[10:57] Mas olha só que curioso, não temos esse incremento de violação de segurança nesse modo protect. A violação de segurança não vai subir. Realmente é mais uma questão de fazer uma proteção, e não estamos preocupados quando colocamos no modo proteção, em ver essas informações de estatísticas que ele mostra pra mim. Então, é por isso que ele não incrementa essa violação de segurança quando colocamos o modo protect.

[11:28] Vimos que tinha o modo protect e tinha aquele outro modo, que era o modo restrict. Vamos colocar agora essa interface pra trabalhar nesse modo restrict. Vou colocar "configure terminal" pra ela entrar no modo global de configuração e vamos entrar na interface fastEthernet 0/2, e colocar que eu quero que essa porta não trabalhe mais nesse modo protect, e sim que ela trabalhe naquele segundo modo que nós vimos, que é o restrict.

[12:01] Vou colocar aqui "switchport port-security" e eu quero que a violação dessa porta, vou colocar aqui "violation", seja a restrict. Eu vou colocar enter, vamos só colocar um Ctrl + Z pra voltar no modo privilegiado e vamos ver se agora, essa porta está trabalhando nesse módulo restrict. Vou colocar "show port-security interface fastEthernet 0/2" e a nossa porta está trabalhando nesse modo restrict. Vamos ver como é que esse modo restrict vai trabalhar.

[12:35] Então, esperamos que o nosso computador PC 1 ainda consiga se comunicar, porque só mudamos o modo de violação de segurança. Esse PC 1 está permitido pra ser trafegado na fastEthernet 0/2. Vamos ver se ele ainda está comunicando com o PC 0 lá do esquerdo. Vou colocar "ping 192.168.0.1". Aparentemente a comunicação com ele está tudo ok, não tivemos nenhum problema.

[13:07] Se nós trocarmos esse meu computador, o PC 1, e voltarmos o Laptop 5 nessa porta, esperamos que esse meu laptop, ele tem lá o endereço MAC diferente do que foi configurado nessa interface fastEthernet 0/2, então esperamos que a nossa violação de segurança seja ativada. Vamos ver como é que esse modo restrict vai se comportar.

[13:33] Vamos só esperar alguns segundos pra porta carregar, porque ela demora só uns segundos e já fazemos um teste de conectividade com o PC 0, pra ver como que esse modo restrict vai trabalhar pra nós. Esperar alguns segundos aqui e a porta já está habilitada. Então, vamos lá.

[13:51] Vamos voltar no Command Prompt e vamos tentar realizar a comunicação com o PC 0. Vamos colocar "ping 192.168.0.1". E aparentemente estamos tendo uma violação de segurança da nossa porta, "Request timed out". A nossa porta está trabalhando como deveria, ela está impedindo que esse tráfego siga adiante.

[14:13] E assim, como no protect, a nossa porta continua habilitada, ela está verde aqui. Se eu for agora na violação de segurança dessa interface, lembra que quando ela estava no protect, aqui em cima, ela não teve nenhuma violação de segurança, a contagem aqui está zero. Vamos ver no restrict.

[14:38] Eu vou colocar "show port-security interface fastEthernet 0/2". Aqui tivemos um incremento dessa violação de segurança, por que 4? Porque eu mandei quatro pacotinhos. E esses quatro pacotinhos foram detectados como uma violação de segurança. Esse pacotinho aqui foi detectado como uma violação de segurança e esses também. Os quatro foram detectados como uma violação de segurança.

[15:09] E o meu modo restrict, diferentemente do modo protect, vai incrementar essa violação de segurança a cada violação que ocorrer. Essa é basicamente a única diferença que existe entre o protect e o restrict. As duas vão manter a porta habilitada, mas o protect não vai incrementar esse valor de violação de segurança, enquanto que o modo restrict vai incrementar sempre que acontecer uma violação de segurança. Vamos seguir.