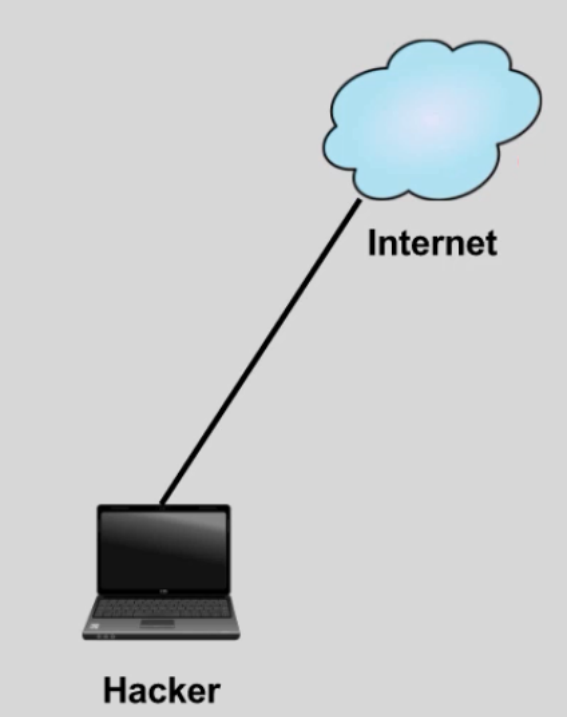
04

# Espelhando o tráfego com o IDS e prevenindo com IPS

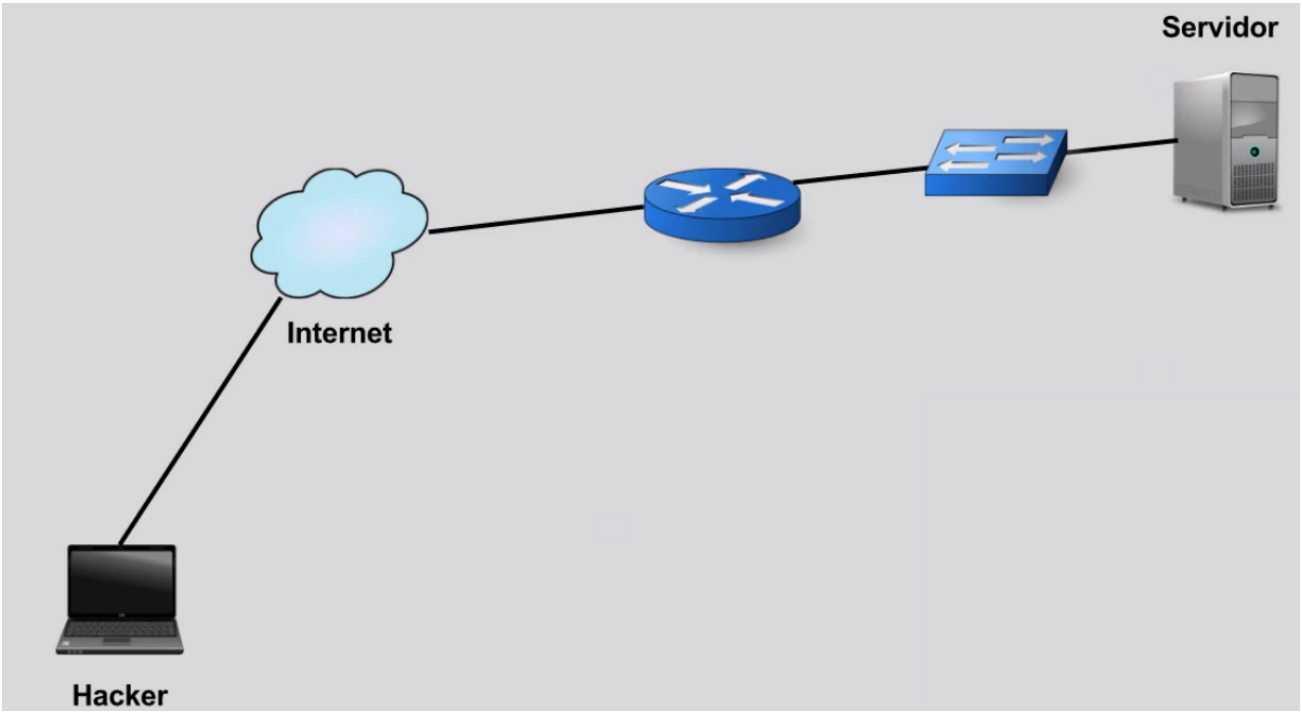
### Transcrição

Veremos como ataques DOS podem ser evitados em redes corporativas. Sairemos do ambiente em que estávamos fazendo as demonstrações e iremos para um cenário mais amplo.

Temos o hacker, que está trabalhando de sua casa, e que consegue acessar a página da Multillidae. Ele está necessariamente conectado à internet.

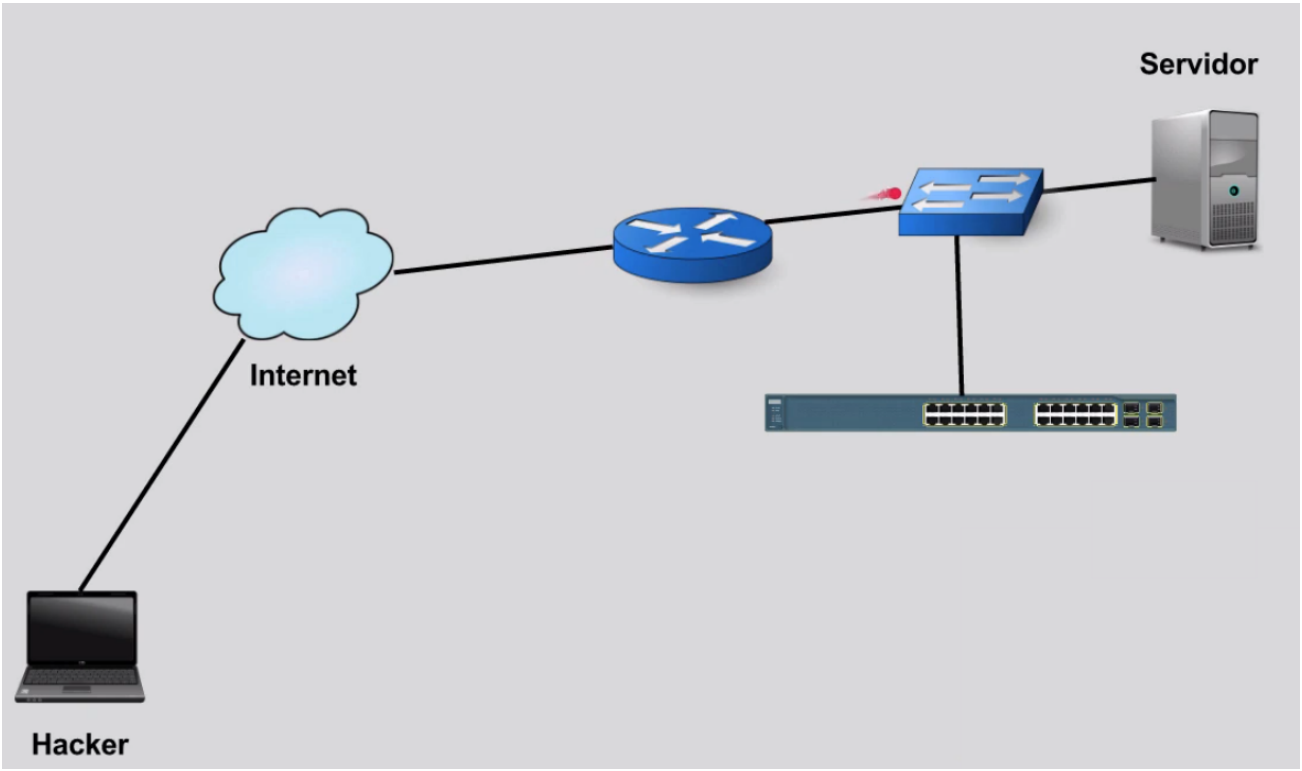



A internet encontrará uma rota para finalmente chegar ao roteador da Multillidae. Como já conversamos no curso de redes (https://cursos.alura.com.br/course/redes-introducao), o roteador segmenta a rede em rede externa, que está vindo do provedor de serviços, e rede interna da Multillidae, conectada a um switch.



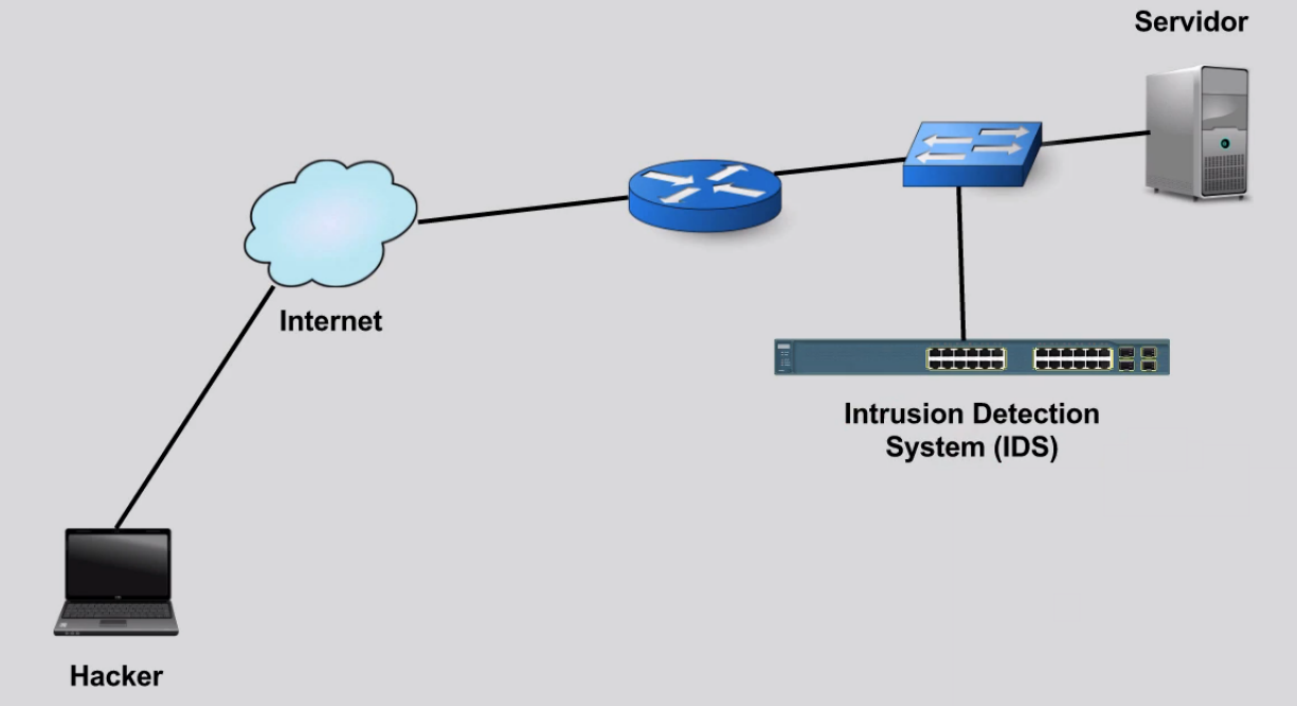

Do jeito que está aqui, não conseguimos verificar o tipo de tráfico que está passando pelo link entre o roteador e o servidor. Isso é um pouco perigoso, pois não sabemos como será feito esse acesso. Por exemplo, o hacker conseguiu abrir uma série de portas de conexões com o servidor, e acabou comprometendo o serviço para outros usuários que queriam acessar o serviço da Multillidae. É um pouco perigoso não termos nenhum tipo de verificação do tráfego que passa pela rede interna.

Precisamos de alguns equipamentos que nos ajudarão nessa análise. O primeiro que veremos se conecta a uma das portas do switch.




O switch copiará o tráfego dos usuários e passar pela porta para o equipamento, que fará a detecção de possíveis anomalias nesse tráfego. A cópia do tráfego de uma porta para a outra é chamada de espelhamento. Se alguma anomalia for detectada, o equipamento manda alarmes para o administrador da rede avisando que há um comportamento incomum ou que não deveria acontecer na rede, e que é preciso verificar e tomar uma providência.

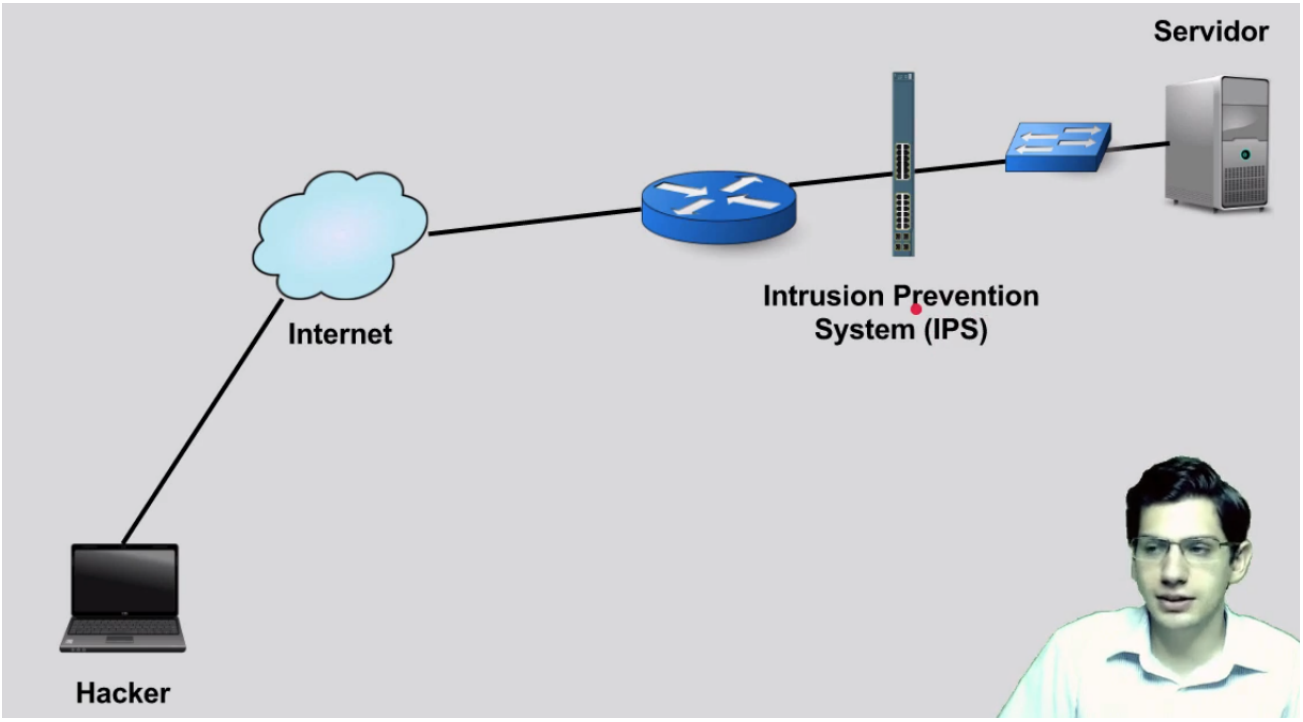
Como o equipamento está recebendo apenas cópias, ele não consegue tomar impedir que um ataque seja propagado por outros pontos da rede. O ataque virá via internet pelo roteador, e chegará ao link entre o switch e o equipamento, que vê apenas cópias do tráfego. Pelo fato de o equipamento apenas detectar um ataque e não conseguir fazer nada a respeito, é conhecido como *Intrusion Detection System* ou IDS.




Sua aparência na vida real é a seguinte:

Como já dissemos, esse é um equipamento que vai detectar um ataque, sem poder impedi-lo de acontecer.

Há outro equipamento que poderá nos ajudar nessa análise, que virá conectado ao link entre o roteador e o switch, entrando diretamente na rede interna. A grande diferença entre ele e o IDS é que ele consegue prevenir que esse ataque seja propagado a outros pontos da rede. Assim que ele percebe que há algo de errado no tráfego, não permite que ele passe adiante. Pelo fato de prevenir o ataque, esse equipamento é chamado de *Intrusion Prevention System*, ou IPS.




O hardware é bem parecido com o do IDS, mas ele tem essa significativa diferença de funcionalidade.

Ele é diretamente conectado à rede, e consegue prevenir as anomalias que aparecerem.

Teoricamente, poderíamos pensar em um primeiro momento que um IPS é melhor que um IDS. Mas isso deve ser avaliado de acordo com o cenário de cada cliente. Não há como dizer que um equipamento é melhor que o outro, pois isso dependerá do que cada cliente precisa. Por exemplo, podemos ter um cliente cujo link nunca possa ficar indisponível. Se ele tiver um IPS e o equipamento tiver uma falha, teremos um problema com o cliente. Na substituição precisaríamos fazer uma interrupção do link. Para esse caso, o IPS não seria a melhor solução, talvez o IDS satisfizesse melhor as necessidades do cliente.

Assim, para determinar o uso de um ou de outro equipamento, é preciso conhecer o cenário e a necessidade de cada equipamento. Até logo!