

Real-World Scenario 8-3: Configuring Packet Filtering and NAT

Scenario: You are consulting for a small company that has seven computers connected to an all-in-one SOHO router (also known as a multi-function network device). The owner is concerned about whether data passing through the device is being inspected and/or filtered properly. The owner is also not sure whether the internal IP addresses of his computers are being protected from the Internet properly. Your tasks are to make sure packet filtering is functioning and explain to the owner how NAT works on this device.

Consider your options when it comes to packet filtering for a device such as this. Make a recommendation based on today's SOHO routers. If the owner wanted to take packet filtering further, what could you suggest?

In your own words, explain to the owner (as if you were actually speaking to the person) how NAT functions within a SOHO router.

Real-World Scenario 8-3 Solution

First, you should make sure that stateful packet inspection (SPI) is being implemented. SPI keeps track of the individual sessions running through the router. It can differentiate between good and bad packets to a small extent. Small office/home office (SOHO) routers usually can run SPI, at least at a basic level; however, you should test this capability. How much does it slow down communications? For example, VPN or remote connectivity connections. If the difference in communication speed between SPI being enabled and being disabled is great, you might recommend a newer SOHO router.

If the owner requires a greater level of packet filtering, you can suggest a NIDS/NIPS solution that sits inline on the network, and perhaps a proxy server of sorts.

Your explanation of NAT to the owner should include a description of how it translates the private internal IP addresses of the network to the public external IP address. This, you can tell the owner, protects the internal IP addresses from discovery. The public IP address is connected to the Internet, but if firewalled properly, it should be virtually invisible.

Most small four- and eight-port SOHO routers also offer NAT filtering that can filter out TCP and UDP traffic in a variety of ways depending on the IP address and port in question. This is something you should also examine, and see if the filtering capability can be increased without undue slowdown of the network.

Video Solution: Watch the video solution "8-3: Configuring Packet Filtering and NAT."