

Real-World Scenario 8-4: Configuring an Inbound Filter

Scenario: Your boss is concerned with the repeated intrusion attempts from a group of IP addresses on the Internet. They are all part of a single IP network and range between 12.46.14.66 and 12.46.14.100. The main concern is that they are trying to insert unwanted packets into the network. Your public IP address is 65.13.82.14.

Your job is to block these IP addresses at the firewall. What can you implement that will filter out the unwanted IP addresses? How would this work from a logical standpoint?

Real-World Scenario 8-4 Solution

Intrusion attempts on a network are extremely common. A public IP address can expect to be scanned and have intrusion attempts multiple times every day because of the plethora of bots and automatic scanning systems on the Internet.

The first and most obvious defense is to make sure the firewall is on, and test it by scanning it with an online program or with a command-line program such as Nmap. If at all possible, make sure all ports are closed and shielded.

Next, recommend creating an inbound filter for the IP addresses in question. This firewall rule will block all attempts by those IP addresses to access the network. This is often done graphically, but it can also be done in the command-line. In essence, what you are trying to accomplish can be represented as the following:

```
deny TCP/UDP 12.46.14.66 - 12.46.14.100 65.13.82.14 all ports
```

In this example, you are denying all TCP and UDP port connections for computers with the IP range of 12.46.14.66 to 12.46.14.100. Again, this is just a representation. The actual syntax for how this is implemented will vary from one system to the next. Or it might simply be done within the GUI of the firewall. That will depend on a variety of factors, including the level of complexity of your hardware and software.

Whatever the case, keep track of your firewall rules. Having too many rules can end up blocking access to known good IP addresses. Finally, if you are worried that external attackers are trying to insert unwanted packets on your network, you should strongly consider a NIDS or NIPS solution, and possibly a honeypot. These might be implemented as individual technologies or as part of the overall UTM solution.

Video Solution: Watch the video solution "8-4: Configuring an Inbound Filter."