

Real-World Scenario 8-2: Configuring a Firewall's Rule Set

Scenario: You are the security administrator for a company with 200 computers, five of which are servers. Your company wants you to devise a firewall rule set for a specific client computer and allow it specific access to a server.

Details:

Server IP: 10.18.255.101

Client IP: 10.18.255.16

Access needed to server: HTTPS

In the following table, fill out the required information given the previous details.

Source IP	Destination IP	Port Number	TCP/UDP	Allow/Deny

Real-World Scenario 8-2 Solution

In this scenario you created a basic rule allowing HTTPS access from a client computer to a server. The following table has the solution for the proper configuration.

Source IP	Destination IP	Port Number	TCP/UDP	Allow/Deny
10.18.255.16	10.18.255.101	443	TCP	Allow

The client is the source IP and the server is the destination IP because it is the device that runs the service. The port number is 443, the one used by HTTPS. Like HTTP, HTTPS uses TCP as its transport mechanism; it is a guaranteed packet delivery system, otherwise known as connection-oriented. Finally, the rule is that connections are allowed.

Consider practicing with hardware- and software-based firewalls. If you can't get access to a Cisco, Check Point, or similar device, try working with Windows or Linux in the command-line. For Windows, configure the Windows Firewall with Advanced Security using the Command Prompt and netsh.exe. For more information on how to add rules with netsh.exe, see the following link:

[http://technet.microsoft.com/en-us/library/dd734783\(v=ws.10\).aspx#BKMK_3_add](http://technet.microsoft.com/en-us/library/dd734783(v=ws.10).aspx#BKMK_3_add)

For Linux, use `iptables` or `nftables` in the command-line. For more information on `iptables`, see the following MAN page link:

<http://ipset.netfilter.org/iptables.man.html>

Try to practice working with firewall rules. You are bound to get questions on this topic when you take the exam. Plus, it is a necessary skill for the security administrator.

Simulation: Complete the simulation "8-2: Configuring a Firewall's Rule Set."