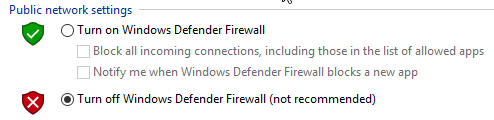
Laud Mills

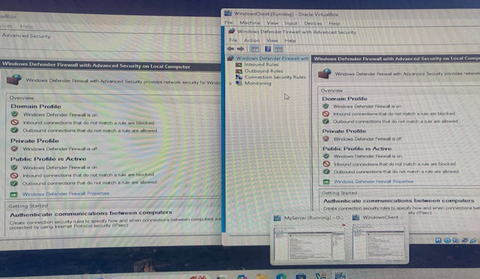
Prepare two virtual machines, one with Windows 10 Home and another with Windows Server 2019 Standard (Desktop Experience). You can download them from Microsoft, [here](https://www.microsoft.com/en-ca/software-download/windows10ISO) for Windows 10 and [here](https://www.microsoft.com/en-us/evalcenter/download-windows-server-2019) for Windows Server. Make sure both VM have interfaces in internal mode and with manual IP addresses of the same network.

Execute wf.msc in both. You might need to temporarily disable the firewall on the public networks for pings to work. Once you have both VMs communicating, enable it again before proceeding with the questions.

Reply to the questions below and **provide a screenshot** of the specific configuration or message:

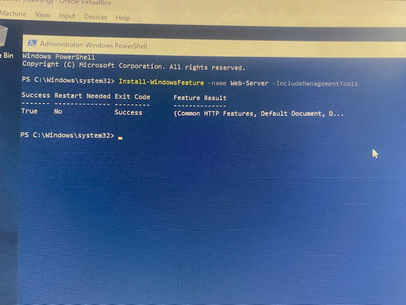
1. What is the default policy for inbound connections that do not match a rule? Would you say this is strict or loose from a security point of view?

The Policy for inbound connections that do not match a rule are BLOCKED. From a security point of view this is strict, and it helps to reduce the attack surface.



1. In the Windows Server, open PowerShell as administrator (right click to do it). Then, execute the cmdlet below:

Install-WindowsFeature -name Web-Server -IncludeManagementTools



1. Refresh the firewall rules if necessary. What is the local port for the “World Wide Web” inbound rule in Windows Server? What server is mentioned in the description?

The local port is TCP 80 and the server is Internet Information Services (IIS) -HTTP traffic.

A screenshot of a computer

AI-generated content may be incorrect.

1. Check that the Windows client can access the web server using its IP address from a web browser. Capture a screenshot showing the communication works.

A computer screen with blue squares

AI-generated content may be incorrect.

1. Set the “Action” to “Block the connection”. What happens when trying again? Do you get any message?

A screenshot of a computer

AI-generated content may be incorrect.A computer screen with a message

AI-generated content may be incorrect.

1. Open “\\IP\_of\_client” from the server. You will not be allowed because the firewall on Windows 10 has all File and Printer Sharing rules disabled. Make this work by enabling the right rule. Explain what rule you chose and what exact change was necessary.

In File and Printer Sharing I turned that on then under private I enabled turn on Network discovery, I also selected use 128-bit encryption to help protect file sharing connection. There is an option to enable password protected sharing but for this assignment I did not use that though it add another layer of security in the real world.

1. Show proof that it worked.

A computer screen shot

AI-generated content may be incorrect.

1. Modify the rule so that only the server is allowed to access the shared resources. What tab did you use? What information did you provide?

Under Inbound rules I went to the New Inbound Rule wizard, then custom rule,

Under Program-all programs ignored Protocol and Ports. Under Scope I selected These IP addresses and added the Server IP 192.168.1.10. selected customize for Interfaces and selected Local Area Network. Under action-Allow Connection and applied this to all the Profiles then gave the rule a name.

A screenshot of a computer

AI-generated content may be incorrect.

1. Where in the Windows Server is located the firewall log file? What is its maximum size? What would happen if this size is reached?

C:\Windows\System32\LogFiles\Firewall\pfirewall.log

It has a default size of 4 MB and when the maximum size is exhausted, old logs are deleted for new logs.

1. Change the firewall’s configuration in the Windows Server so that the firewall will log dropped packets for all three domains (private, public and domain). What options did you click on? What tabs? Explain.

A screenshot of a computer screen

AI-generated content may be incorrect.

Went to Windows Defender Firewall with Advanced Security, selected properties to display Tabs for each profile (Domain, Private, Public), then selected Customize under the Logging section. Then selected Yes for Log dropped packets. Then clicked ok to save configurations.

1. Add a new rule to block all inbound traffic to the port 80 and try the server’s IP from a browser in the client. Show the rule and the browser’s message.

A screenshot of a computer

AI-generated content may be incorrect.A computer screen with a message

AI-generated content may be incorrect.

1. Looking at the information available in the server’s firewall log, determine how would you know the communication failed and what systems were communicating.

It indicated DROP TCP and the server IP it also shows DROP TCP and the Client’s IP.

The communication between the Sever and the Client IPS as source and destination respectively as well as the ports with tcp and icmp at various steps in the syn and ack process.

1. What would happen with the log file if you enabled logging for successful communications? Explain a situation in which that could be useful.

Because the default storage for the log file is 4MB any subsequent logs will automatically take the storage space and earlier will be archived. Therefore, the log for the successful communication will be the latest file.