ICSI MODULE 3:

What is a Firewall

3.1 What is a Firewall

A firewall is a fence between your computer or your internal network and the outside world or the Internet. A particular fire wall implementation might use one or more of the methods listed here to provide that barrier.

- Packet filtering
- Stateful packet filtering
- User authentication
- Client application authentication

At a minimum, a firewall will filter incoming packets based on parameters such as packet size, source IP address, protocol, a nd destination port.

As you may already know, both Linux and Windows (this includes every Windows version since XP through the Windows 10 and the server editions) ship with a simple firewall built into the operating system. Norton and McAfee both offer personal firew all solutions for individual PCs. These firewalls are meant for individual machines.

There are more advanced solutions available for networks. In an organisational setting, you will want a dedicated firewall be tween your network and the outside world. This might be a router that also has built-in firewall capabilities. (Cisco Systems is one company that is well-known for high quality routers and firewalls.) Alternatively, it might be a server that is dedicated to run firewall software. There are a number of firewall solutions that you can examine. Selecting a firewall is an important decisi on.

Firewall Types

3.2 Firewall Types

Packet filtering firewalls are the simplest and often the least expensive type of firewalls. Several other types of firewalls offer their own distinct advantages and disadvantages. The basic types of firewalls are:

- Packet filtering
- Application gateway
- Circuit level gateway
- Stateful packet inspection

3.2.1 Packet Filtering Firewall

The packet filtering firewall is the most basic type of firewall. In a packet filtering firewall, each incoming packet is exa mined. Only those packets that match the criteria you set are allowed through. Many operating systems, such as Windows clients (such as Windows 8 and 10) and many Linux distributions, include basic packet filtering software with the operating system.

Packet filtering firewalls are also referred to as screening firewalls. They can filter packets based on packet size, protoco l used, source IP address, and many other parameters. Some routers offer this type of firewall protection in addition to their normal routing functions.

Packet filtering firewalls work by examining a packet's source address, destination address, source port, destination port, a nd protocol type. Based on these factors and the rules that the firewall has been configured to use, they either allow or deny p assage to the packet. These firewalls are very easy to configure and inexpensive. Some operating systems, such as Windows 10 and Linux, include built-in packet filtering capabilities.

There are a few disadvantages of packet filtering firewalls. One disadvantage is that they do not actually examine the packet or compare it to previous packets; therefore, they are quite susceptible to either a ping flood or SYN flood. They also do not o ffer any user authentication. Because this type of firewall looks only at the packet header for information, it has no information abo ut the packet contents.

It also does not track packets, so it has no information about the preceding packets. Therefore, if thousands of packets came from the same IP address in a short period of time, a host would not notice that this pattern is unusual. Such a pattern often indicat es that the IP address in question is attempting to perform a DoS attack on the network.

To configure a packet filtering firewall, simply establish appropriate filtering rules. A set of rules for a given firewall w ould need to cover the following:

- What types of protocols to allow (FTP, SMTP, POP3, etc.)
- What source ports to allow
- What destination ports to allow
- What source IP addresses to allow (you can block certain IP addresses if you wish)

These rules will allow the firewall to determine what traffic to allow in and what traffic to block. Because this sort of fir ewall uses only very limited system resources, is relatively easy to configure, and can be obtained inexpensively or even for free. Alth ough it is not the most secure type of firewall, you are likely to encounter it frequently.

3.2.2 Stateful Packet Inspection

The stateful packet inspection (SPI) firewall is an improvement on basic packet filtering. This type of firewall will examine each packet, denying or permitting access based not only on the examination of the current packet, but also on data derived from previous packets in the conversation.

This means that the firewall is aware of the context in which a specific packet was sent. This makes these firewalls far less susceptible to ping floods and SYN floods, as well as being less susceptible to spoofing. SPI firewalls are less susceptible to these attacks for the following reasons:

- They can tell whether the packet is part of an abnormally large stream of packets from a particular IP address, thus indicating a possible DoS attack in progress.
- They can tell whether the packet has a source IP address that appears to come from inside the firewall, thus indicating IP spoofing is in progress.
- They can also look at the actual contents of the packet, allowing for some very advanced filtering capabilities.

Most quality firewalls today use the stateful packet inspection method; when possible, this is the recommended type of firewall for most systems. In fact, most home routers have the option of using stateful packet inspection.

The name stateful packet inspection derives from the fact that in addition to examining the packet, the firewall is examining the packet's state in relationship to the entire IP conversation. This means the firewall can refer to the preceding packets as well as those packets' contents, source, and destination. As you might suspect, SPI firewalls are becoming quite common.

3.2.3 Application Gateway

An application gateway (also known as application proxy or application-level proxy) is a program that runs on a firewall. This type of firewall derives its name from the fact that it works by negotiating with various types of applications to allow their traffic to pass the firewall. In networking terminology, negotiation is a term used to refer to the process of authentication and verification. In other words, rather than looking at the protocol and port the packet is using, an application gateway will examine the client application and the server-side application to which it is trying to connect.

It will then determine if that particular client application's traffic is permitted through the firewall. This is significantly different from a packet filtering firewall, which examines the packets and has no knowledge of what sort of application sent them.

Application gateways enable the administrator to allow access only to certain specified types of applications, such as web browsers or FTP clients.

When a client program, such as a web browser, establishes a connection to a destination service, such as a web server, it connects to an application gateway, or proxy. The client then negotiates with the proxy server in order to gain access to the destination service. In effect, the proxy establishes the connection with the destination behind the firewall and acts on behalf of the client, hiding and protecting individual computers on the network behind the firewall. This process actually creates two connections. There is one connection between the client and the proxy server and another connection between the proxy server and the destination.

Once a connection is established, the application gateway makes all decisions about which packets to forward. Since all communication is conducted through the proxy server, computers behind the firewall are protected.

With an application gateway, each supported client program requires a unique program to accept client application data. This sort of firewall allows for individual user authentication, which makes them quite effective at blocking unwanted traffic. However, a disadvantage is that these firewalls use a lot of system resources. The process of authenticating client applications uses more memory and CPU time than simple packet filtering.

Application gateways are also susceptible to various flooding attacks (SYN flood, ping flood, etc.) for two reasons. The first potential cause of a flooding attack may be the additional time it takes for an application to negotiate authenticating a request. Remember that both the client application and the user may need to be authenticated. This takes more time than simply filtering packets based on certain parameters.

For this reason, a flood of connection requests can overwhelm the firewall, preventing it from responding to legitimate requests. Application gateways may also be more susceptible to flooding attacks because once a connection is made, packets are not checked. If a connection is established, then that connection can be used to send a flooding attack to the server it has connected to, such as a web server or e-mail server.

This vulnerability is mitigated somewhat by authenticating users. Provided the user logon method is secure (appropriate passwords, encrypted transmission, etc.), the likelihood that someone can use a legitimate connection through an application gateway for a flooding attack is reduced.

3.2.4 Circuit Level Gateway

Circuit level gateway firewalls are similar to application gateways but are more secure and generally implemented on high-end equipment. These types of firewalls also employ user authentication, but they do so earlier in the process.

With an application gateway, first the client application is checked to see if access should be granted, and then the user is authenticated. With circuit level gateways, authenticating the user is the first step. The user's logon ID and password are checked, and the user is granted access before the connection to the router is established. This means that each individual, either by username or IP address, must be verified before any further communication can take place.

Once this verification takes place and the connection between the source and destination is established, the firewall simply passes bytes between the systems. A virtual "circuit" exists between the internal client and the proxy server. Internet requests go through this circuit to the proxy server, and the proxy server delivers those requests to the Internet after changing the IP address. External users only see the IP address of the proxy server.

Responses are then received by the proxy server and sent back through the circuit to the client. It is this virtual circuit that makes the circuit level gateway secure. The private secure connection between the client application and the firewall is a more secure solution than some other options, such as the simple packet filtering firewall and the application gateway.

While traffic is allowed through, external systems never see the internal systems.

Firewall Implementation

3.3 Firewall Implementation

Administrators must be able to evaluate implementation issues to achieve a successful security solution for their systems. Understanding the type of firewall means knowing how the firewall will evaluate traffic and decide what to allow and what not to allow. Understanding the firewall's implementation means understanding how that firewall is set up in relation to the network it is protecting. The most widely used configurations include:

- Network host-based
- Dual-homed host
- Router-based firewall
- Screened host

3.3.1 Host Based

In the host-based (sometimes-called network host-based) scenario the firewall is a software solution installed on an existing machine with an existing operating system. The most significant concern in this scenario is that, no matter how good the firewall solution is, it is contingent upon the underlying operating system. In such a scenario, it is critical that the machine hosting the firewall have a hardened operating system. Hardening the operating system refers to taking several security precautions including:

- Ensuring all patches are updated
- Uninstalling unneeded applications or utilities
- Closing unused ports
- Turning off all unused services

In the network host-based implementation, you install the firewall software onto an existing server. Sometimes, the server's operating system may come with such software. It is not at all uncommon for administrators to use a machine running Linux, configure its built-in firewall, and use that server as a firewall. The primary advantage to this option is cost. It is much cheaper to simply install firewall software onto an existing machine, and use that machine as your firewall.

3.3.2 Dual-Homed Hosts

A dual-homed host is a firewall running on a server with at least two network interfaces. This is an older methodology. Most firewalls today are implemented in actual routers, rather than servers. The server acts as a router between the network and the interfaces to which it is attached.

To make this work, the automatic routing function is disabled, meaning that an IP packet from the Internet is not routed directly to the network. The administrator can choose what packets to route and how to route them. Systems inside and outside the firewall can communicate with the dual-homed host, but cannot communicate directly with each other.

The dual-homed host configuration is simply an expanded version of the network host firewall implementation. That means it is also dependent on the security of the underlying operating system. Any time a firewall is running on a server of any kind, the security of that server's operating system becomes even more critical than normal.

This option has the advantage of being relatively simple and inexpensive. The primary disadvantage is its dependency on the underlying operating system.

3.3.3 Router-Based Firewall

Administrators can implement firewall protection on a router. In fact, even the simplest, low-end routers today have some type of firewall included. In larger networks with multiple layers of protection, this is often the first layer of protection. Although various types of firewalls can be implemented on a router, the most common type uses packet filtering. Users of a broadband connection in a home or small office can get a packet filtering firewall router to replace the basic router provided by the broadband company.

In many cases, this solution is also ideal for the firewall novice. A number of vendors supply router-based firewalls that can be preconfigured by the vendor based on the customer's needs. The customer can then install it between the network and external Internet connection. In addition, most of the widely known brands (Cisco, 3Com, etc.) offer vendor-specific training and certifications in their hardware, making it relatively easy to find qualified administrators or to train current staff.

Another valuable way to implement router-based firewalls is between subsections of a network. If a network is divided into segments, each segment needs to use a router to connect to the other segments. Using a router that also includes a firewall significantly increases security. If the security of one segment of the network is compromised, the rest of the network is not necessarily breached.

Perhaps the best advantage of router-based firewalls is the ease of setup. In many cases, the vendor will even configure the firewall for you, and you simply plug it in. Most home-based routers today, such as those from Linksys, Belkin, or Netgear, have a built-in firewall. And in fact virtually all higher-end routers include firewall capability.

3.3.4 Screened Hosts

A screened host is really a combination of firewalls. In this configuration, a combination of a bastion host and a screening router is used. The combination creates a dual firewall solution that is effective at filtering traffic. The two firewalls can be different types. The bastion host might be an application gateway and the router packet screener (or vice versa). This approach gives the advantages of both types of firewalls and is similar in concept to the dual-homed host.

The screened host has some distinct advantages over the dual-homed firewall. Unlike the dual-homed firewall, the screened host needs only one network interface and does not require a separate subnet between the application gateway and the router. This makes the firewall more flexible but perhaps less secure because its reliance on only one network interface card means that it might be configured to pass certain trusted services to the application gateway portion of the firewall and directly to servers within the network.

The most significant concern when using the screened host is that it essentially combines two firewalls into one. Therefore, any security flaw or misconfiguration affects both firewalls. When you use a DMZ there are physically two separate firewalls, and the likelihood of any security flaw being propagated to both is low.

Proxy Servers

3.4 Proxy Servers

A proxy server is often used with a firewall to hide the internal network's IP address and present a single IP address (its own) to the outside world. A proxy server is a server that sits between a client application, such as a web browser, and a real server. Proxy servers prevent hackers from seeing the IP addresses of internal machines, knowing how many machines are behind the proxy server, or learning anything about the network configuration.

Proxy servers also provide a valuable control mechanism because most proxy servers log all outgoing traffic. This enables network administrators to see where employees go on the Internet. A proxy server normally runs as software on the same machine as your firewall.

The proxy server is configured to redirect certain traffic. For example, incoming traffic using the HTTP protocol is usually allowed through the proxy server but is redirected to the web server. That means that all outgoing and incoming HTTP traffic first goes through the proxy server. A proxy server can be configured to redirect any traffic you want. If an e-mail server or FTP server is on the network, all incoming and outgoing traffic for that network will run through the proxy server.

Using a proxy server means that when a machine inside the network visits a website, the website will only detect that the proxy server visited it. In fact, if dozens of different machines on the network visit a site that logs the IP addresses of incoming connections, they will all be logged with the same IP address—that of the proxy server.

For the most part this sort of proxy server has been supplanted by network address translation. However, the term proxy server is still used, but with a different application. Now proxy servers work with the firewall to filter things such as web content. They allow a network administrator to block certain sites and to record all the websites a given user visits.

This hiding of the network is a very valuable service because knowledge of internal IP addresses can be used to execute certain forms of attack. For example, IP spoofing is contingent upon knowing the IP address of some internal server. Hiding those IP addresses is an important step in network security. It can also be very useful to know where employees go on the Internet.

Proxy servers track such information, and many network administrators use this to restrict employees from using the company Internet connection for illicit purposes. This can also be a useful tool for stopping attacks. An employee who visits hacker websites might be a potential security risk. They may elect to try some of the techniques they read about on the network. Administrators can also detect potential industrial espionage. An employee who spends a lot of time on a competitor's website might be considering a job change and might consider taking valuable data with him.

3.4.1 NAT (Network Address Translation)

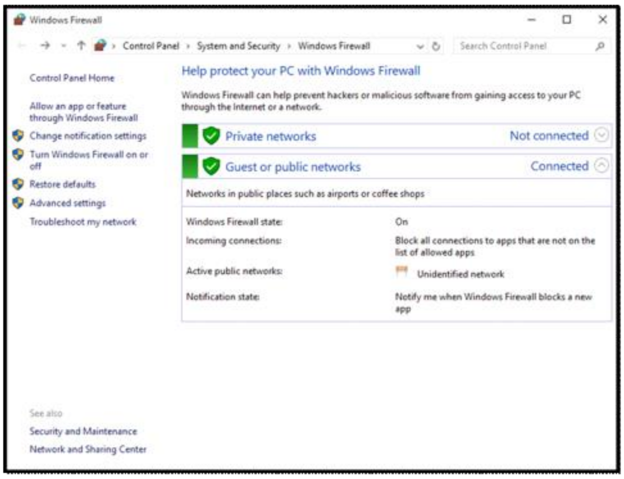
For many organisations, proxy servers have been superseded by a newer technology known as network address translation (NAT). Today what we call proxy servers don't do what proxy servers originally did (i.e., translate a private IP address into a public IP address). Primarily, NAT translates internal addresses and external addresses to allow communication between network computers and outside computers. The outside sees only the address of the machine running NAT (often the firewall). From this perspective, it is functioning exactly like a proxy server.

NAT also provides significant security because, by default, it allows only connections that are originated on the inside network. This means that a computer inside the network can connect to an outside web server, but an outside computer cannot connect to a web server inside the network. You can make some internal servers available to the outside world via inbound mapping, which maps certain well-known TCP ports (80 for HTTP, 21 for FTP, etc.) to specific internal addresses, thus making services such as FTP or websites available to the outside world. However, this inbound mapping must be done explicitly; it is not present by default.

Windows Firewalls

3.5 Windows Firewalls

Windows first started shipping a primitive firewall, called Internet Connection Firewall (ICF), with Windows 2000. It was very simple. Each version of Windows since then has expanded upon this idea. Windows 10 ships with a fully functioning firewall. This firewall can block inbound and outbound packets. To access the Windows 10 firewall, click the Start button and type Firewall.


Windows Firewall
Control Panel › System and Security › Windows Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Center

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or coffee shops

Windows Firewall state: On

Incoming connections: Block all connections to apps that are not on the list of allowed apps

Active public networks: Unidentified network

Notification state: Notify me when Windows Firewall blocks a new app

Beginning with Windows Server 2008 and all versions after that, Windows Firewalls are stateful packet inspection firewalls. With the Windows 10 Firewall, you can set different rules for outbound and inbound traffic. For example, your standard workstation will probably allow outbound HTTP traffic on port 80, but you might not want to allow inbound traffic (unless you are running a web server on that workstation).

You can also set up rules for a port, a program, a custom rule, or one of the many predefined rules that Microsoft has for you to select from. You can also choose not only to allow or block the connection, but to allow it only if it is secured by IPSec. That provides you with three options for any connection.

Rules allow or block a given application or port. You can also have different rules for inbound and outbound traffic. The rules allow you to decide whether a particular type of communication is blocked or allowed. You can have different settings for inbound and outbound traffic. You can set rules for individual ports (all 65,535 available network ports) and for applications. The rules in the Windows firewall give you a lot of flexibility.

More importantly, you can apply rules differently depending on where the traffic comes from. You can set up rules for three areas or profiles:

- **Domain:** For those computers authenticated on your domain.
- **Public:** For computers from outside your network. You would treat outside traffic more carefully than traffic coming from another machine in your domain.
- **Private:** Private refers to traffic from your own computer, thus the term private.

Administrators should always follow these rules with all packet filtering firewalls:

- If you do not explicitly need a port, then block it. For example, if you are not running a web server on that machine, then block all inbound port 80 traffic. With home machines, you can usually block all ports. With individual workstations on a network, you may need to keep some ports open in order to allow various network utilities to access the machine.
- Unless you have a compelling reason not to, always block ICMP traffic because many utilities such as ping, tracert, and many port scanners use ICMP packets. If you block ICMP traffic, you will prevent many port scanners from scanning your system for vulnerabilities.
- Occasionally, I would suggest continuing to write out acronyms such as ICMP just to make sure this is reinforced.

The Windows Firewall also has a logging feature, but it is disabled by default. Turn this feature on (when you configure the firewall you will see a place to turn on logging). Check this log periodically. You can find more details on the Windows 10 Firewall at https://docs.microsoft.com/en-us/windows/access-protection/windows-firewall/windows-firewall-with-advanced-security.

Guided Exercise: Configuring Windows Firewall

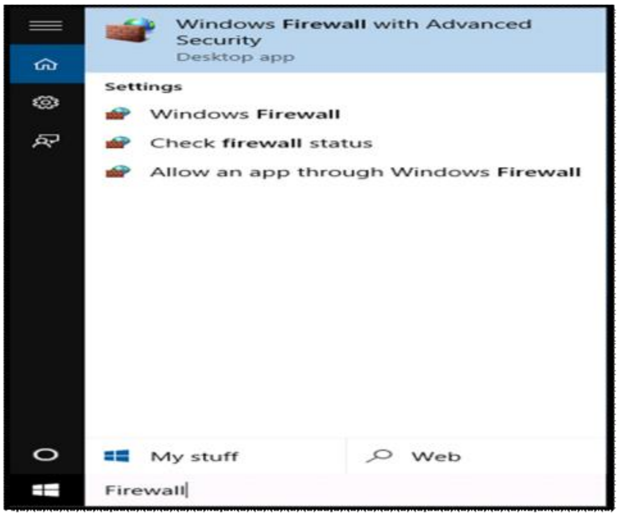
3.6 Guided Exercise: Configuring Windows Firewall

Resources	
Files	None
Machines	Windows 10, Windows Server 2012

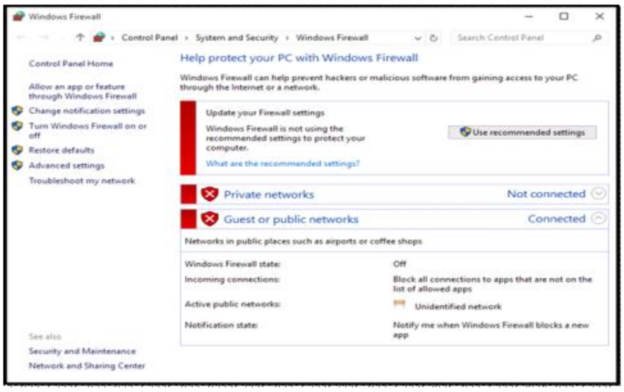
In this exercise, you are required to configure the firewall on the Windows machines.

Login to Windows 10 and enable the Firewall.

Click on the Start button and then write on the search box Firewall.


Windows Firewall with Advanced Security
Desktop app
Settings
Windows Firewall
Check firewall status
Allow an app through Windows Firewall
My stuff
Web
Firewall

The select the Windows Firewall. Once the Windows Firewall window opens click on **“Turn Windows Firewall on or off”.**


Windows Firewall
Control Panel › System and Security › Windows Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Center
Use recommended settings

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Update your Firewall settings

Windows Firewall is not using the recommended settings to protect your computer.

What are the recommended settings?

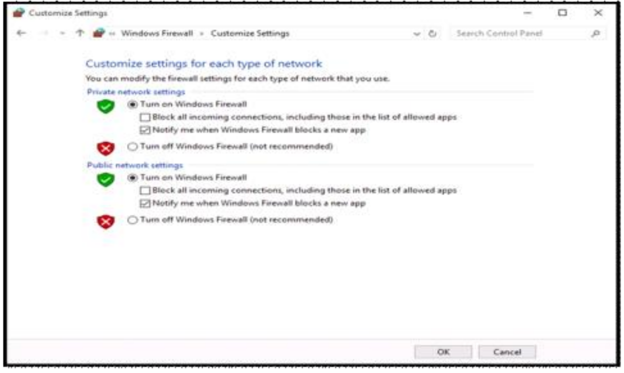
Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or coffee shops

Windows Firewall state:	Off
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	Unidentified network
Notification state:	Notify me when Windows Firewall blocks a new app

On the Customize Settings window of Firewall select both radio buttons **“Turn on Windows Firewall”** for Private and Public network settings and then click OK.



Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

● Turn on Windows Firewall

☐ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Firewall blocks a new app

○ Turn off Windows Firewall (not recommended)

Public network settings

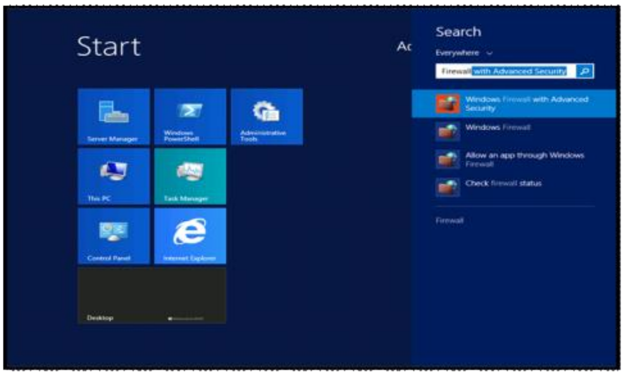
● Turn on Windows Firewall

☐ Block all incoming connections, including those in the list of allowed apps

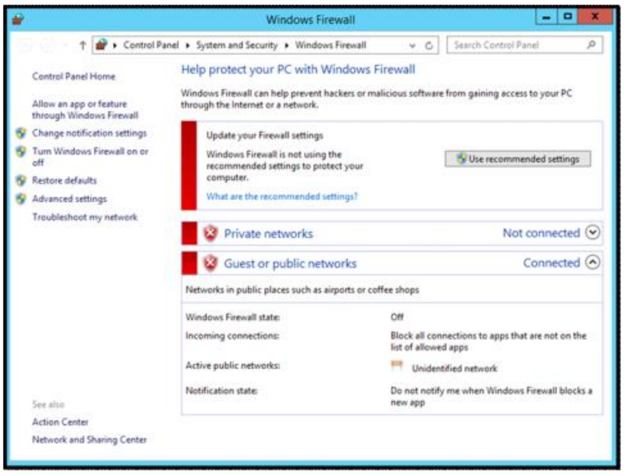
☑ Notify me when Windows Firewall blocks a new app

○ Turn off Windows Firewall (not recommended)

Login to Windows Server and enable the Firewall.
Click on the Start button and write Firewall.



Click on Windows Firewall and the Windows Firewall window will be revealed.


Windows Firewall
Control Panel ▸ System and Security ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center
Use recommended settings

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Update your Firewall settings

Windows Firewall is not using the recommended settings to protect your computer.

What are the recommended settings?

Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or coffee shops

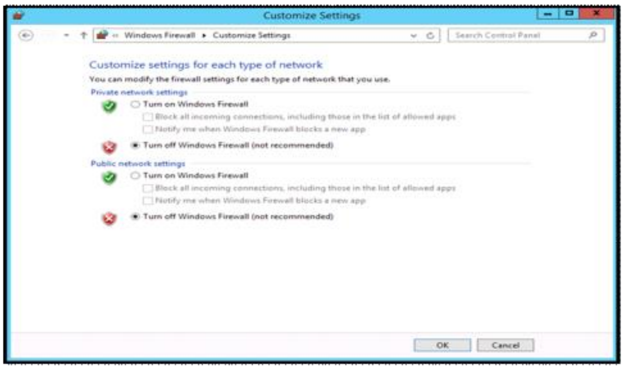
Windows Firewall state: Off

Incoming connections: Block all connections to apps that are not on the list of allowed apps

Active public networks: Unidentified network

Notification state: Do not notify me when Windows Firewall blocks a new app

From the Windows Firewall window click on **“Turn Windows Firewall on or off”** and the Customize Settings window will be shown.



Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

○ Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed apps

□ Notify me when Windows Firewall blocks a new app

● Turn off Windows Firewall (not recommended)

Public network settings

○ Turn on Windows Firewall

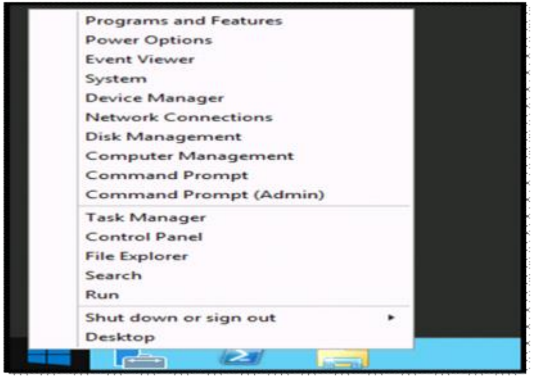
□ Block all incoming connections, including those in the list of allowed apps

□ Notify me when Windows Firewall blocks a new app

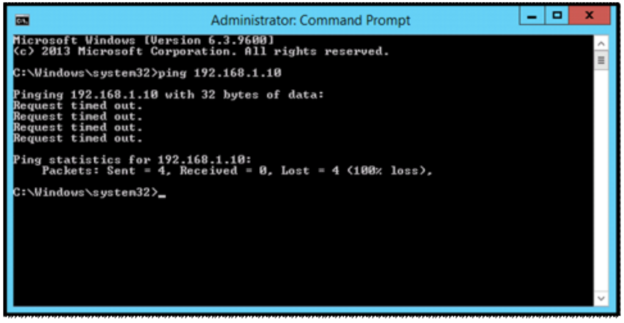
● Turn off Windows Firewall (not recommended)

On the Customize Settings window of Firewall select both radio buttons **“Turn on Windows Firewall”** for Private and Public network settings and then click OK.

Right click on the Windows Server Start button and select Command Prompt (Admin).



On the command prompt run the command ping 192.168.1.10.

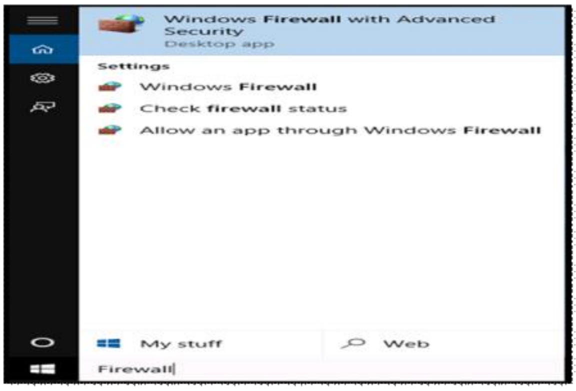


```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Windows\system32>_
```

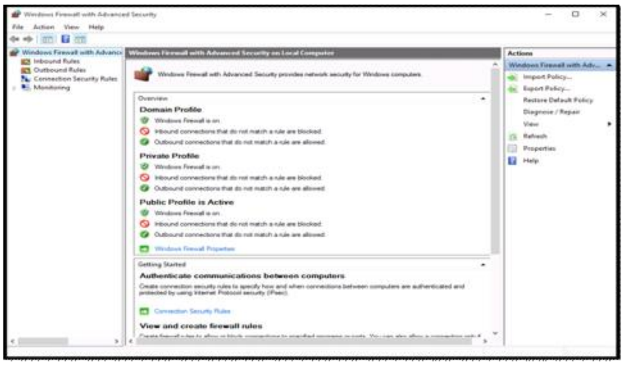
Because we have enabled the firewall, it blocks ICMP packets.

In Windows 10 Firewall enable the Inbound rule titled “File and Printer Sharing (Echo Request – ICMPv4-In)”

Click on the Start button and then write on the search box Firewall.


Windows Firewall with Advanced Security
Desktop app
Settings
Windows Firewall
Check firewall status
Allow an app through Windows Firewall
My stuff
Web
Firewall

From the Windows Firewall window click on Advanced Settings and the Windows Firewall with Advanced Security will open.


Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Firewall with Advanced Security on Local Computer
Actions
Windows Firewall with Adv...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help

Windows Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile

- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Public Profile is Active

- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Windows Firewall Properties

Getting Started

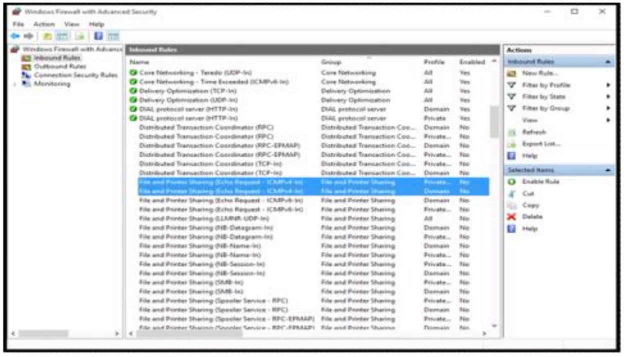
Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

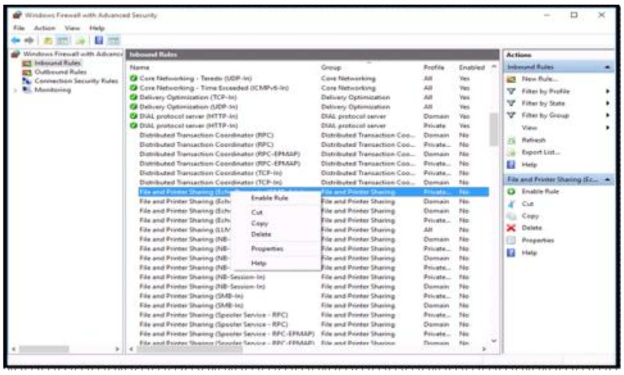
Connection Security Rules

View and create firewall rules

Click on Inbound Rules and enable the rules File and Print Sharing (Echo Request – ICMPv4-In) for both profiles Private and Domain. Enable them by right clicking on each rule and select Enable Rule.

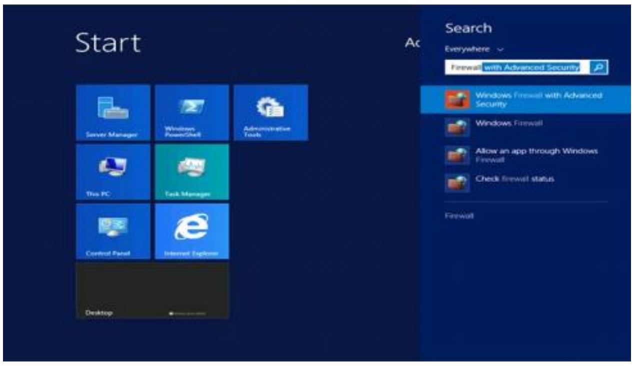


Name	Group	Profile	Enabled
Core Networking - Teredo (UDP-In)	Core Networking	All	Yes
Core Networking - Time Exceeded (ICMPv6-In)	Core Networking	All	Yes
Delivery Optimization (TCP-In)	Delivery Optimization	All	Yes
Delivery Optimization (UDP-In)	Delivery Optimization	All	Yes
DIAL protocol server (HTTP-In)	DIAL protocol server	Domain	Yes
DIAL protocol server (HTTP-In)	DIAL protocol server	Private	Yes
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...	Domain	No
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...	Private...	No
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coo...	Domain	No
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coo...	Private...	No
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...	Private...	No
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...	Domain	No
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Private...	No
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Private...	No
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All	No
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	Private...	No
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	Private...	No
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Private...	No
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (SMB-In)	File and Printer Sharing	Private...	No
File and Printer Sharing (SMB-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	Private...	No
File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	Domain	No
File and Printer Sharing (Spooler Service - RPC-EPMAP)	File and Printer Sharing	Private...	No
File and Printer Sharing (Spooler Service - RPC-EPMAP)	File and Printer Sharing	Domain	No

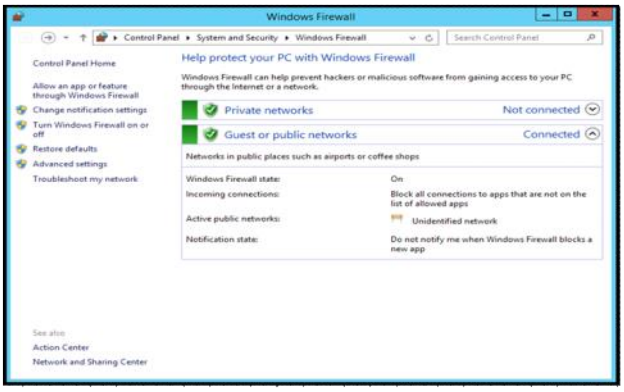


Name	Group	Profile	Enabled
Core Networking - Teredo (UDP-In)	Core Networking	All	Yes
Core Networking - Time Exceeded (ICMPv6-In)	Core Networking	All	Yes
Delivery Optimization (TCP-In)	Delivery Optimization	All	Yes
Delivery Optimization (UDP-In)	Delivery Optimization	All	Yes
DIAL protocol server (HTTP-In)	DIAL protocol server	Domain	Yes
DIAL protocol server (HTTP-In)	DIAL protocol server	Private	Yes
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...	Domain	No
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...	Private...	No
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coo...	Domain	No
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coo...	Private...	No
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...	Private...	No
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...	Domain	No
File and Printer Sharing (Ech	File and Printer Sharing	Private...	No
File and Printer Sharing (Ech	File and Printer Sharing	Domain	No
File and Printer Sharing (Ech	File and Printer Sharing	Domain	No
File and Printer Sharing (Ech	File and Printer Sharing	Private...	No
File and Printer Sharing (LLM	File and Printer Sharing	All	No
File and Printer Sharing (NB-	File and Printer Sharing	Domain	No
File and Printer Sharing (NB-	File and Printer Sharing	Private...	No
File and Printer Sharing (NB-	File and Printer Sharing	Domain	No
File and Printer Sharing (NB-	File and Printer Sharing	Private...	No
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Private...	No
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (SMB-In)	File and Printer Sharing	Private...	No
File and Printer Sharing (SMB-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	Private...	No
File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	Domain	No
File and Printer Sharing (Spooler Service - RPC-EPMAP)	File and Printer Sharing	Private...	No
File and Printer Sharing (Spooler Service - RPC-EPMAP)	File and Printer Sharing	Domain	No

In Windows Server enable the Inbound rule titled “File and Printer Sharing (Echo Request – ICMPv4-In)”.
Click on the Start button and write Firewall.



Click on Windows Firewall and the Windows Firewall window will be revealed.


Windows Firewall
Control Panel ▸ System and Security ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

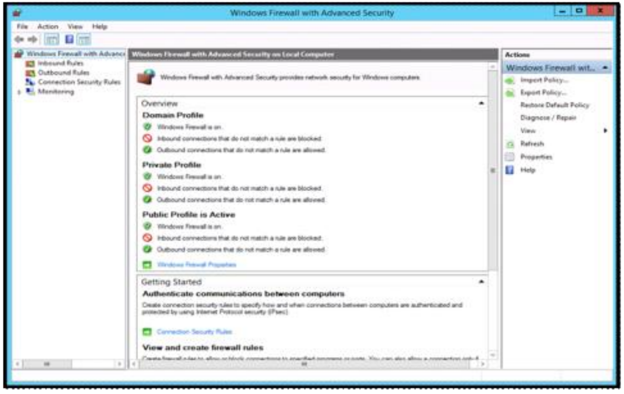
Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or coffee shops

Windows Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	Unidentified network
Notification state:	Do not notify me when Windows Firewall blocks a new app

Click on the Advanced Settings and the Windows Firewall with Advanced Security window will open.



Windows Firewall with Advanced Security on Local Computer

Windows Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile

- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Public Profile is Active

- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Windows Firewall Properties

Getting Started

Authenticate communications between computers

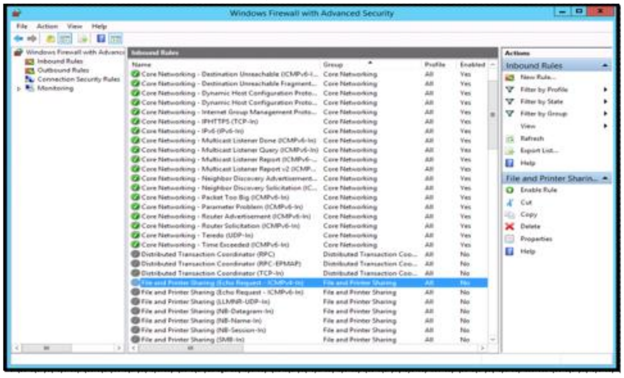
Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

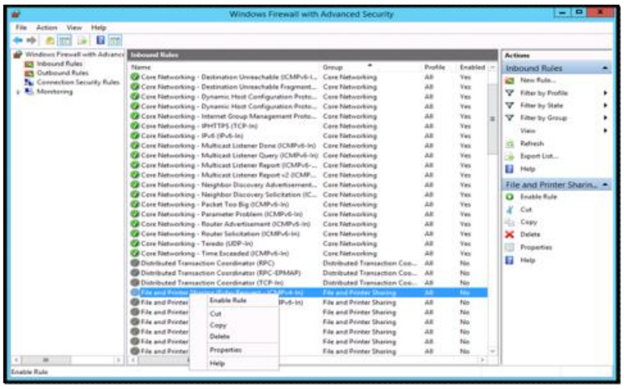
Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if

Click on Inbound Rules, select the rule “File and Printer Sharing (Echo Request – ICMPv4-In)” and enable it.



Inbound Rules

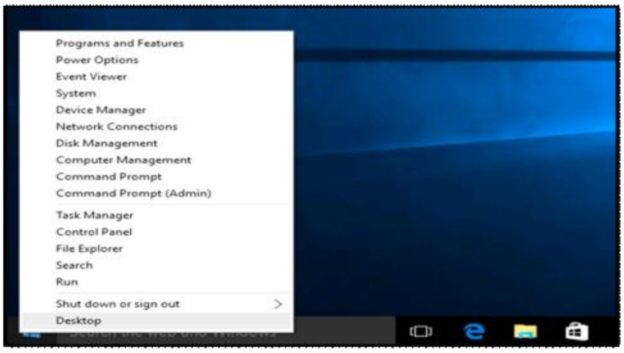
Name	Group	Profile	Enabled
Core Networking - Destination Unreachable (ICMPv6-I...	Core Networking	All	Yes
Core Networking - Destination Unreachable Fragment...	Core Networking	All	Yes
Core Networking - Dynamic Host Configuration Proto...	Core Networking	All	Yes
Core Networking - Dynamic Host Configuration Proto...	Core Networking	All	Yes
Core Networking - Internet Group Management Proto...	Core Networking	All	Yes
Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes
Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes
Core Networking - Multicast Listener Done (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Multicast Listener Query (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Multicast Listener Report (ICMPv6-...	Core Networking	All	Yes
Core Networking - Multicast Listener Report v2 (ICMP...	Core Networking	All	Yes
Core Networking - Neighbor Discovery Advertisement...	Core Networking	All	Yes
Core Networking - Neighbor Discovery Solicitation (IC...	Core Networking	All	Yes
Core Networking - Packet Too Big (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Parameter Problem (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Router Advertisement (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Router Solicitation (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Teredo (UDP-In)	Core Networking	All	Yes
Core Networking - Time Exceeded (ICMPv6-In)	Core Networking	All	Yes
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...	All	No
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coo...	All	No
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...	All	No
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	All	No
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	All	No
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All	No
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	All	No
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	All	No
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	All	No
File and Printer Sharing (SMB-In)	File and Printer Sharing	All	No



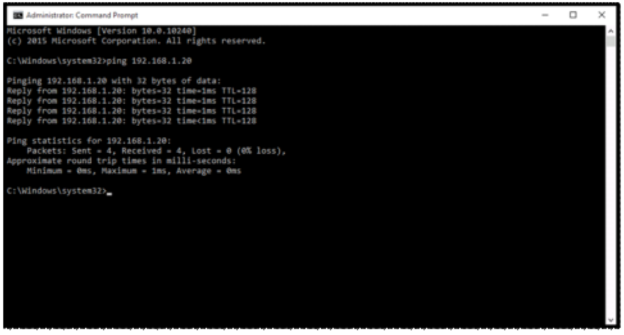
Inbound Rules

Name	Group	Profile	Enabled
Core Networking - Destination Unreachable (ICMPv6-I...	Core Networking	All	Yes
Core Networking - Destination Unreachable Fragment...	Core Networking	All	Yes
Core Networking - Dynamic Host Configuration Proto...	Core Networking	All	Yes
Core Networking - Dynamic Host Configuration Proto...	Core Networking	All	Yes
Core Networking - Internet Group Management Proto...	Core Networking	All	Yes
Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes
Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes
Core Networking - Multicast Listener Done (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Multicast Listener Query (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Multicast Listener Report (ICMPv6-...	Core Networking	All	Yes
Core Networking - Multicast Listener Report v2 (ICMP...	Core Networking	All	Yes
Core Networking - Neighbor Discovery Advertisement...	Core Networking	All	Yes
Core Networking - Neighbor Discovery Solicitation (IC...	Core Networking	All	Yes
Core Networking - Packet Too Big (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Parameter Problem (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Router Advertisement (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Router Solicitation (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Teredo (UDP-In)	Core Networking	All	Yes
Core Networking - Time Exceeded (ICMPv6-In)	Core Networking	All	Yes
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...	All	No
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coo...	All	No
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...	All	No
File and Printer ... ICMPv4-In)	File and Printer Sharing	All	No
File and Printer ... Pv6-In)	File and Printer Sharing	All	No
File and Printer	File and Printer Sharing	All	No
File and Printer	File and Printer Sharing	All	No
File and Printer	File and Printer Sharing	All	No
File and Printer	File and Printer Sharing	All	No
File and Printer	File and Printer Sharing	All	No

In Windows 10 use the ping command to ping Windows Server (192.168.1.20)
Right click on the Start button and click on “Command Prompt (Admin)” and then Yes on the pop up window.



On the Command Prompt window write the command “ping 192.168.1.20”.



```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping 192.168.1.20

Pinging 192.168.1.20 with 32 bytes of data:
Reply from 192.168.1.20: bytes=32 time=1ms TTL=128
Reply from 192.168.1.20: bytes=32 time=1ms TTL=128
Reply from 192.168.1.20: bytes=32 time=1ms TTL=128
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Windows\system32>_
```

The server replies to the ICMP pings because we have enabled the rule on the Firewall.

Linux Firewalls

3.7 Linux Firewalls

Linux has firewall capabilities built into the operating system. This has been a part of the Linux operating system for many years, with occasional improvements in the technology.

3.7.1 Iptables

The first widely used Linux firewall was called ipchains. It was essentially a chain of rules for filtering traffic. It was first introduced in version 2.2 of the Linux kernel and superseded the previous ipfwadm (which was not widely used). The more modern iptables replaced ipchains and is the primary firewall for Linux. The iptables service was first introduced in Linux kernel 2.4.

On most Linux systems, iptables is installed as /usr/sbin/iptables. However, if it was not included in your particular Linux installation, you can add it later.

An iptables firewall is made up of three different kinds of objects: tables, chains, and rules. Basically, the tables contain chains of rules. Put another way, iptables is an expansion on the concept of ipchains. Each chain has a series of rules that define how to filter packets. There are actually three tables and each has some standard rule chains in it. You can, of course, add your own custom rules.

The three tables and their standard chains are as follow:

- **Packet filtering:** This table is the essential part of the firewall. It is a packet filtering firewall and it contains three standard chains: INPUT, OUTPUT, and Forward. The INPUT chain processes incoming packets, and the OUTPUT chain processes traffic sent out from the machine. If the firewall system is also acting as a router, only the FORWARD chain applies to routed packets.
- **Network address translation:** This table is used for performing network address translation on outbound traffic that initiates a new connection. This is used only if your machine is serving as a gateway or proxy server.
- **Packet alteration:** This table is used only for specialized packet alteration. It is often called the mangle table because it alters, or mangles, packets. It contains two standard chains. This table might not even be needed for many standard firewalls.

3.7.2 Iptables Configuration

Iptables requires some configuration. You can do it through the GUI (KDE, GNOME, etc.) but the shell commands are common to most distributions. Let’s take a look at some common basic configuration.

To cause iptables to function as a basic packet filtering firewall, you need these commands:

- iptables -F
- iptables -N block
- iptables -A block -m state --state ESTABLISHED,RELATED -j ACCEPT

Obviously, that is the most basic and essential iptables configuration. However, here are some others.

To list the current iptables rules use:

- iptables –L

To allow communication on a specific port, SSH port 22 and HTTP port 80 for example use:

- iptables –A INPUT –p tcp –dport ssh –j ACCEPT
- iptables –A INPUT –p tcp –dport 80 –j ACCEPT

Also there are several flags that can be passed to the iptables command. Below are listed the most common flags and what they do. Several other flags exist but are not listed.
A: Append this rule to a rule chain
-L: List the current filter rules
-p: The connection protocol used
--dport: The destination port required for the rule. A single port can be given or a range.
-i: Only match if the packet is coming in on the specified interface.
-v: Verbose output
-s, --source: address source specification
-d, --destination: address destination specification

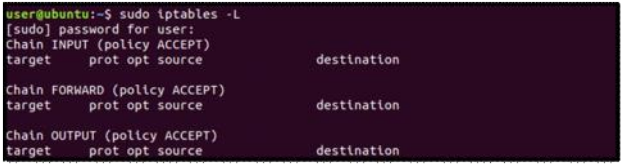
Guided Exercise: Configuring iptables Rules

3.8 Guided Exercise: Configuring iptables Rules

Resources	
Files	None
Machines	Ubuntu Server

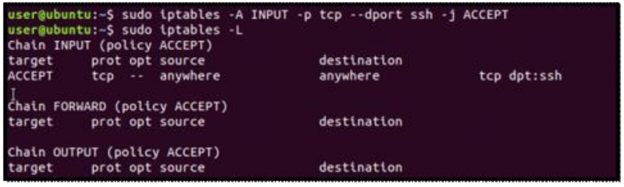
In this exercise, you are required to write custom iptables rules.

Login to Ubuntu Server and then run the command “sudo iptables -L”. It will ask for the user password. Enter the user password which is “Pa$$w0rd”, press enter and then it will show the current iptables rules.



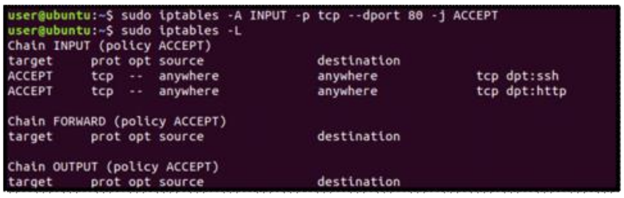
```
user@ubuntu:~$ sudo iptables -L
[sudo] password for user:
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Write the command “sudo iptables –A INPUT –p tcp --dport ssh –j ACCEPT” and if sudo asks for the user password enter “Pa $$w0rd”. Then run the command sudo iptables –L to list the iptables rules.



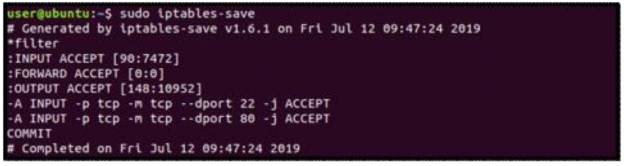
```
user@ubuntu:~$ sudo iptables -A INPUT -p tcp --dport ssh -j ACCEPT
user@ubuntu:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Write the command “sudo iptables –A INPUT –p tcp --dport 80 –j ACCEPT” and if sudo asks for the user password enter “Pa $$w0rd”. Then run the command sudo iptables –L to list the iptables rules.



```
user@ubuntu:~$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
user@ubuntu:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

To save the iptables rules run the command “sudo iptables-save”.



```
user@ubuntu:~$ sudo iptables-save
# Generated by iptables-save v1.6.1 on Fri Jul 12 09:47:24 2019
*filter
:INPUT ACCEPT [90:7472]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [148:10952]
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
COMMIT
# Completed on Fri Jul 12 09:47:24 2019
```

QUIZ:

- 1. Why a stateful packet inspection firewall is less susceptible to spoofing attacks?
- 2. Which of the following is a combination of firewalls?
- 3. Which of the following can be shipped preconfigured?
- 4. Which type of firewall is considered the most secure?
- 5. Which of the following is an advantage of the network host based configuration?
- 6. What is the most important security advantage to NAT
- 7. Which of the following are four basic types of Firewalls?
- 8. Why might a proxy gateway be susceptible to a flood attack?
- 9. What type of firewall requires client applications to be authorised to connect?
- 10.A device that hides its internal IP addresses is called?