

Unit – 4 Protection of Computing Resources

Protection refers to a mechanism which controls the access of programs, processes, or users to the resources defined by a computer system. We can take protection as a helper to multi programming operating system, so that many users might safely share a common logical name space such as directory or files.

Computer Science MCA Operating System Protection and security requires that computer resources such as CPU, softwares, memory etc. are protected. This extends to the operating system as well as the data in the system. This can be done by ensuring integrity, confidentiality and availability in the operating system.

We can take protection as a helper to multi programming operating system, so that many users might safely share a common logical name space such as directory or files. To ensure that each active programs or processes in the system uses resources only as the stated policy, To improve reliability by detecting latent errors.

Need of Protection: 1 To prevent the access of unauthorized users and 2 To ensure that each active programs or processes in the system uses resources only as the stated policy, 3 To improve reliability by detecting latent errors.

Protection and security require that computer resources such as CPU, softwares, memory etc. are protected. This extends to the operating system as well as the data in the system. This can be done by ensuring integrity, confidentiality and availability in the operating system. The system must be protected against unauthorized access, viruses, worms etc.

Threats to Protection and Security

A threat is a program that is malicious in nature and leads to harmful effects for the system. Some of the common threats that occur in a system are –

Virus

Viruses are generally small snippets of code embedded in a system. They are very dangerous and can corrupt files, destroy data, crash systems etc. They can also spread further by replicating themselves as required.

Trojan Horse

A trojan horse can secretly access the login details of a system. Then a malicious user can use these to enter the system as a harmless being and wreak havoc.

Trap Door

A trap door is a security breach that may be present in a system without the knowledge of the users. It can be exploited to harm the data or files in a system by malicious people.

Worm

A worm can destroy a system by using its resources to extreme levels. It can generate multiple copies which claim all the resources and don't allow any other processes to access them. A worm can shut down a whole network in this way.

Denial of Service

These type of attacks do not allow the legitimate users to access a system. It overwhelms the system with requests so it is overwhelmed and cannot work properly for other user.

Protection and Security Methods

The different methods that may provide protect and security for different computer systems are –

Authentication

This deals with identifying each user in the system and making sure they are who they claim to be. The operating system makes sure that all the users are authenticated before they access the system. The different ways to make sure that the users are authentic are:

- **Username/ Password**

Each user has a distinct username and password combination and they need to enter it correctly before they can access the system.

- **User Key/ User Card**

The users need to punch a card into the card slot or use they individual key on a keypad to access the system.

- **User Attribute Identification**

Different user attribute identifications that can be used are fingerprint, eye retina etc. These are unique for each user and are compared with the existing samples in the database. The user can only access the system if there is a match.

One Time Password

These passwords provide a lot of security for authentication purposes. A one time password can be generated exclusively for a login every time a user wants to enter the system. It cannot be used more than once. The various ways a one time password can be implemented are –

- **Random Numbers**

The system can ask for numbers that correspond to alphabets that are pre arranged. This combination can be changed each time a login is required.

- **Secret Key**

A hardware device can create a secret key related to the user id for login. This key can change each time.

Secure Programs:

"Top 10" List of Secure Computing Tips

Tip #1 - You are a target to hackers

Don't ever say, "It won't happen to me." We are all at risk and the stakes are high - both for your personal and financial well-being and for the university's standing and reputation.

- Cybersecurity is everyone's responsibility.
- By following the tips below and remaining vigilant, you are doing your part to protect yourself and others.

Tip #2 - Keep software up-to-date

Installing software updates for your operating system and programs is critical. Always install the latest security updates for your devices:

- Turn on Automatic Updates for your operating system.
- Use web browsers such as Chrome or Firefox that receive frequent, automatic security updates.
- Make sure to keep browser plug-ins (Flash, Java, etc.) up-to-date.

Tip #3 - Avoid Phishing scams - beware of suspicious emails and phone calls

Phishing scams are a constant threat - using various social engineering (link is external) ploys, cyber-criminals will attempt to trick you into divulging personal information such as your login ID and password, banking or credit card information.

- Phishing scams can be carried out by phone, text, or through social networking sites - but most commonly by email.
- Be suspicious of any official-looking email message or phone call that asks for personal or financial information.

Tip #4 - Practice good password management

We all have too many passwords to manage - and it's easy to take short-cuts, like reusing the same password. A password manager can help you to maintain strong unique passwords for all of your accounts. These programs can generate strong passwords for you, enter credentials automatically, and remind you to update your passwords periodically.

Tip #5 - Be careful what you click

Avoid visiting unknown websites or downloading software from untrusted sources. These sites often host malware that will automatically install (often silently) and compromise your computer.

If attachments or links in the email are unexpected or suspicious for any reason, don't click on it.

Tip #6 - Never leave devices unattended

The physical security of your devices is just as important as their technical security.

- If you need to leave your laptop, phone, or tablet for any length of time - lock it up so no one else can use it.
- If you keep protected data on a flash drive or external hard drive, make sure their encrypted and locked up as well.
- For desktop computers, lock your screen or shut-down the system when not in use.

Tip #7 - Safeguard Protected Data

Be aware of Protected Data that you come into contact with and its associated restrictions. Review the UCB [Data Classification Standard](#) to understand data protection level requirements. In general:

- Keep high-level Protected Data (e.g., SSN's, credit card information, student records, health information, etc.) off of your workstation, laptop, or mobile devices.
- Securely remove sensitive data files from your system when they are no longer needed.
- Always use encryption when storing or transmitting sensitive data.

Tip #8 - Use mobile devices safely

Considering how much we rely on our mobile devices and how susceptible they are to attack, you'll want to make sure you are protected:

- Lock your device with a PIN or password - and never leave it unprotected in public.
- Only install apps from trusted sources (Apple AppStore, Google Play).
- Keep the device's operating system up-to-date.
- Don't click on links or attachments from unsolicited emails or texts.
- Avoid transmitting or storing personal information on the device.
- Most handheld devices are capable of employing data encryption - consult your device's documentation for available options.

Tip #9 - Install antivirus/anti-malware protection

Only install these programs from a known and trusted source. Keep virus definitions, engines and software up-to-date to ensure your programs remains effective.

Tip #10 - Back up your data

Back up regularly - if you are a victim of a security incident, the only guaranteed way to repair your computer is to erase and re-install the system.

NON-MALICIOUS PROGRAM ERRORS

- Buffer Overflows. ...
- Definition. ...
- Security Implication. ...
- Incomplete Mediation. ...
- Definition. ...
- Security Implication. ...
- Time-of-Check to Time-of-Use Errors. ...
- Definition. ...
- Security Implication. ...
- Combinations of Non-malicious Program Flaws.

Being human, programmers and other developers make many mistakes, most of which are unintentional and non-malicious. Many such errors cause program malfunctions but do not lead to more serious security vulnerabilities. However, a few classes of errors have plagued programmers and security professionals for decades, and there is no reason to believe they will disappear. In this section we consider three classic error types that have enabled many recent security breaches. We explain each type, why it is relevant to security, and how it can be prevented or mitigated.

Viruses and Other Malicious Code:

Types of Malicious Code

Code Type	Characteristics
Virus	Attaches itself to program and propagates copies of itself to other programs
Trojan horse	Contains unexpected, additional functionality
Logic bomb	Triggers action when condition occurs
Time bomb	Triggers action when specified time occurs
Trapdoor	Allows unauthorized access to functionality
Worm	Propagates copies of itself through a network
Rabbit	Replicates itself without limit to exhaust resource

Because "virus" is the popular name given to all forms of malicious code and because fuzzy lines exist between different kinds of malicious code, we will not be too restrictive in the following discussion. We want to look at how malicious code spreads, how it is activated, and what effect it can have. A virus is a convenient term for mobile malicious code, and so in the following sections we use the term "virus" almost exclusively. The points made apply also to other forms of malicious code.

How Viruses Attach

A printed copy of a virus does nothing and threatens no one. Even executable virus code sitting on a disk does nothing. What triggers a virus to start replicating? For a virus to do its malicious work and spread itself, it must be activated by being executed. Fortunately for virus writers, but unfortunately for the rest of us, there are many ways to ensure that programs will be executed on a running computer.

Targeted Malicious Code:

Targeted malicious code is **written for a particular system**. To do so the attacker or the code writer studies the system carefully identifying its weaknesses. The different types are: i. Brain: The Brain virus placed itself in the boot sector and other places on the system.

Targeted malicious code

- Targeted malicious code is written for a particular system. To do so the attacker or the code writer studies the system carefully identifying its weaknesses. The different types are:

i. Brain:

The Brain virus placed itself in the boot sector and other places on the system. It then screened all disk access so as to avoid detection and to maintain its infection. Each time the disk was read, Brain would check the boot sector to see if it was infected. If not, it would reinstall itself in the boot sector and elsewhere. This made it difficult to completely remove the virus.

ii. Morris Worm:

The Morris worm obtains a remote access to machines on the network by guessing the user account passwords. If that failed, it tried to exploit a buffer overflow and also tried to exploit a trapdoor in send-mail. Once access had been obtained to a machine, the worm sent a bootstrap loader to the victim. The bootstrap loader then fetched the rest of the worm. In this process, the victim machine even authenticated the sender. The Morris worm went to great lengths to remain undetected. If the transmission of the worm was interrupted, all of the code that had been transmitted was deleted. The code was also encrypted when it was downloaded, and the downloaded source code was deleted after it was decrypted and compiled. When the worm was running on a system, it periodically changed its name and process identifier (PID), so that a system administrator would be less likely to notice anything unusual.

iii. Code Red:

To gain access to a system, the Code Red worm exploited a buffer overflow in Microsoft IIS server software. It then monitored traffic on port 80, looking for other potential targets. The action of Code Red depended on the day of the month. From day 1 to 19, it

tried to spread its infection, then from day 20 to 27 it attempted a distributed denial of service (DDoS) attack .

iv. SQL Slammer:

The Slammer infected sites by randomly generating IP addresses. A more efficient search strategy could have made it more effective use of the available bandwidth. Slammer spreads too fast and effectively burns out the available bandwidth on the Internet. If Slammer had been able to throttle itself slightly, it could have ultimately infected more systems and it might have caused significantly more damage.

v. Time Bomb:

This is a code that it will take effect at a particular time or date. The virus is stored in the memory till it is time to burst. Y2K is a good example of time bomb.

vi. Logic Bomb:

It is a malicious code initiated when a specific condition occurs. Logic can be with respect to some event. The logic can be a condition or a count which remains in the memory for the condition to occur and affect the system.

Methods of Control:

The following are the main control measures are used to provide security of data in databases: 1. Authentication 2. Access control 3. Inference control 4. Flow control 5. Database Security applying Statistical Method 6. Encryption These are explained as following below.

These are explained as following below.

1. Authentication :

Authentication is the process of confirmation that whether the user log in only according to the rights provided to him to perform the activities of data base. A particular user can login only up to his privilege but he can't access the other sensitive data. The privilege of accessing sensitive data is restricted by using Authentication.

By using these authentication tools for biometrics such as retina and figure prints can prevent the data base from unauthorized/malicious users.

2. Access Control :

The security mechanism of DBMS must include some provisions for restricting access to the data base by unauthorized users. Access control is

done by creating user accounts and to control login process by the DBMS. So, that database access of sensitive data is possible only to those people (database users) who are allowed to access such data and to restrict access to unauthorized persons.

The database system must also keep the track of all operations performed by certain user throughout the entire login time.

3. Inference Control :

This method is known as the countermeasures to statistical database security problem. It is used to prevent the user from completing any inference channel. This method protect sensitive information from indirect disclosure.

Inferences are of two types, identity disclosure or attribute disclosure.

4. Flow Control :

This prevents information from flowing in a way that it reaches unauthorized users. Channels are the pathways for information to flow implicitly in ways that violate the privacy policy of a company are called covert channels.

5. Database Security applying Statistical Method :

Statistical database security focuses on the protection of confidential individual values stored in and used for statistical purposes and used to retrieve the summaries of values based on categories. They do not permit to retrieve the individual information.

This allows to access the database to get statistical information about the number of employees in the company but not to access the detailed confidential/personal information about the specific individual employee.

6. Encryption :

This method is mainly used to protect sensitive data (such as credit card numbers, OTP numbers) and other sensitive numbers. The data is encoded using some encoding algorithms.

An unauthorized user who tries to access this encoded data will face difficulty in decoding it, but authorized users are given decoding keys to decode data.

Firewalls:

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

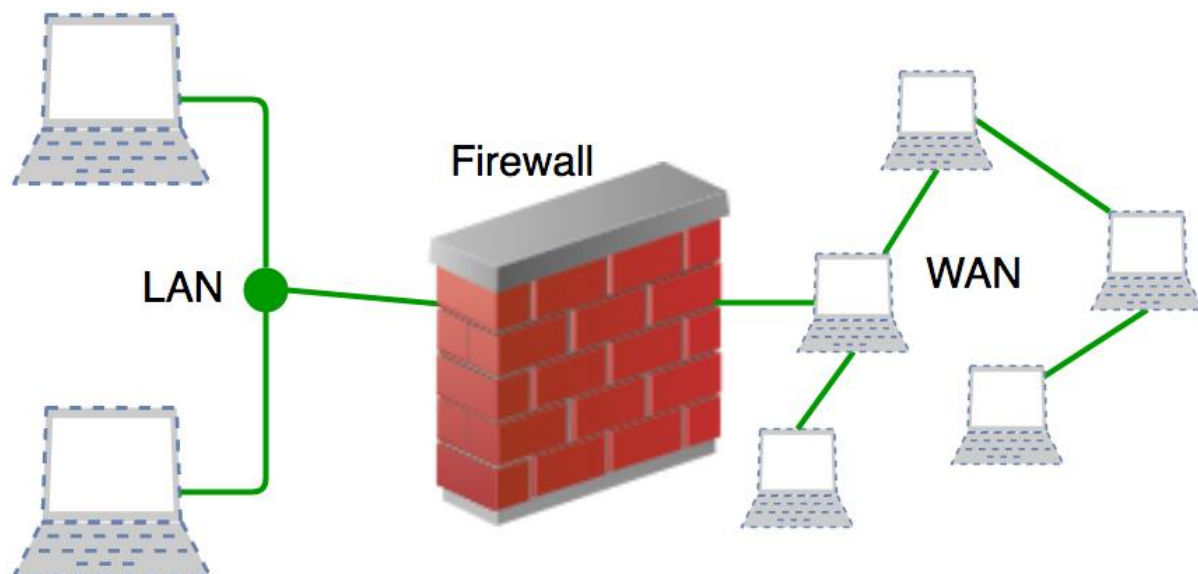
Accept : allow the traffic

Reject : block the traffic but reply with an “unreachable error”

Drop : block the traffic with no reply

A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. ... An early type of firewall device, a proxy firewall serves as the gateway from one network to another for a specific application.



Types of Firewalls:

- Software Firewalls. A software firewall is installed on the host device. Accordingly, this type of firewall is also known as a Host Firewall.
- Hardware Firewalls. As the name suggests, hardware firewalls are security devices that represent a separate piece of hardware placed between an internal and external network (the Internet).

- Packet-Filtering Firewalls. When it comes to types of firewalls based on their method of operation, the most basic type is the packet-filtering firewall.
- Circuit-Level Gateways. Circuit-level gateways are a type of firewall that work at the session layer of the OSI model, observing TCP (Transmission Control Protocol) connections and sessions.

Comparison of Firewall Types:

Different Types Of Firewalls And Architectures

Did you know that there are eight different types of firewalls? Firewalls have different uses, and it depends on why you are using one to decide which type you should have for your business. Let's go over the different types of firewall:

Packet-Filtering Firewalls

This is the oldest firewall type out there. They are designed to create checkpoints at individual routers or switches. The packet-filtering firewalls will check the data packets that try to come through, without inspecting the contents. If the information trying to come through looks suspicious, it cannot get through the network. This is a simple firewall that does not impact network performance too much.

Circuit-Level Gateways

Circuit-level gateways are much like packet-filtering firewalls in that they quickly and easily check and approve or deny traffic. They do it without being heavy on resources, too. Circuit-level gateways work by verifying the transmission control protocol handshake. It doesn't check the packet directly, so there is a risk of malware getting through. These are not the best ones to protect your business.

Stateful Inspection Firewalls

A combination of the two firewalls above, the stateful inspection firewalls offer a higher level of protection for your business. The problem with these is that they take up more resources, which can slow down the legitimate packet transfer.

Proxy Firewalls (Application-Level Gateways/Cloud Firewalls)

If you want firewalls that operate at the application layer to filter traffic, proxy firewalls do the job. These are cloud-based most of the time, and they establish traffic connections and examine data packets coming through. The difference between these and the stateful inspection firewalls is that the proxy firewalls can also do a more in-depth inspection to check the packet contents.

Next-Generation Firewalls

There's no real insight into what makes a firewall today "next-generation" besides the time it was created. There are commonalities between these firewalls and the originals, and those include TCP handshakes and packet inspections. Next-generation firewalls also use IPS – intrusion prevention systems – to stop network attacks.

Software Firewalls

These are any firewalls installed on local devices. The biggest draw for these is that they can create a useful, in-depth defense path. Maintaining these on more than one device is not easy, though, so you may need more than one for each asset.

Hardware Firewalls

Hardware firewalls use physical appliances, and they act like a traffic router. They intercept data packets before they are connected to a network server. The weakness here is that they can be easily bypassed, which goes against your need for a firewall.

Cloud Firewalls

Cloud solutions are also called FaaS – firewalls as a service. They often go hand in hand with proxy firewalls, and the most significant benefit to these is that they grow with your business. They work to filter large amounts of traffic away from your company, where it's malicious.

Firewall Configurations:


Checking Firewall Settings on a PC

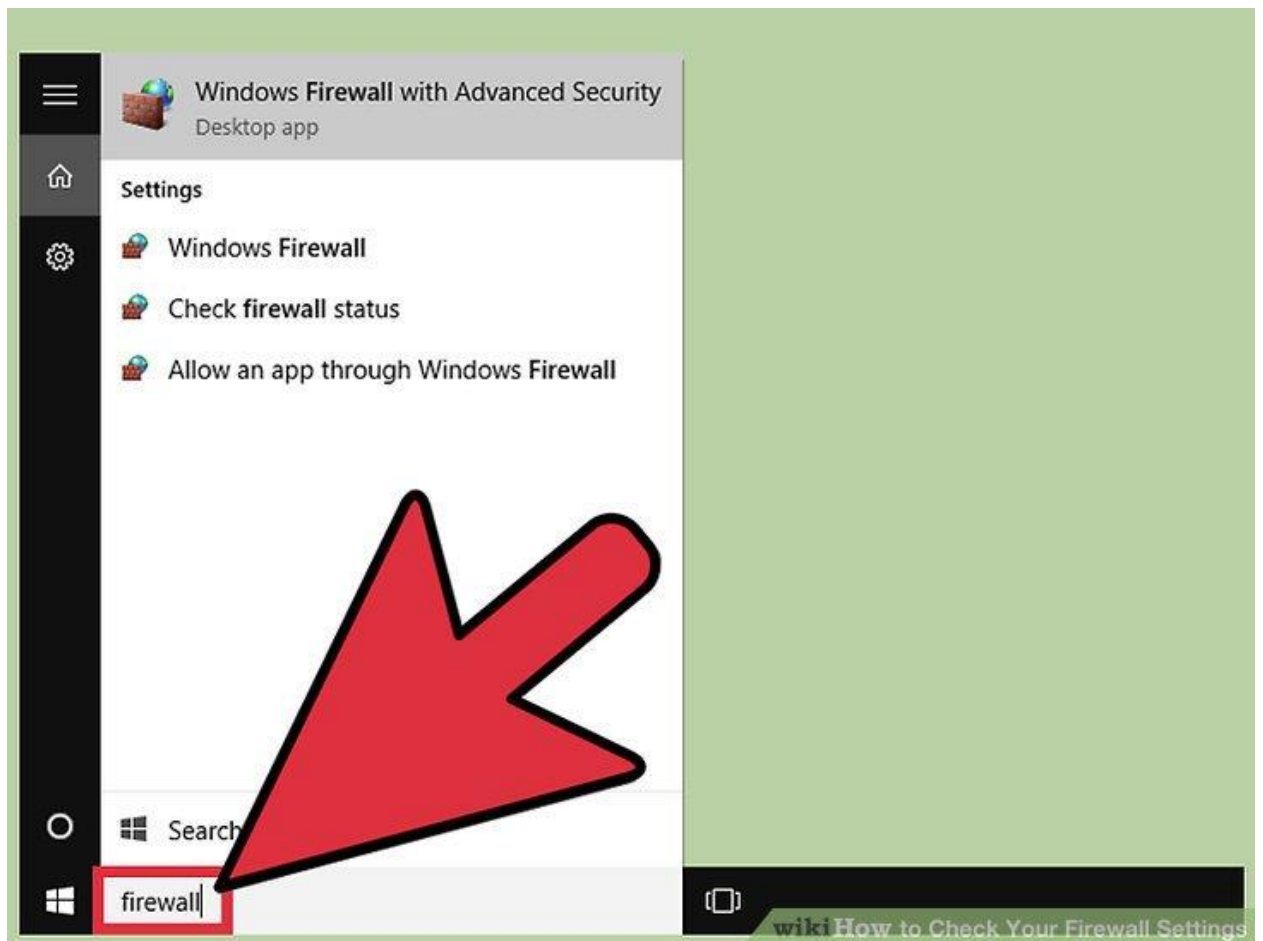
1. Open your Start menu. Windows' default firewall program is located in the "System and Security" folder of the Control Panel app, but you can easily access your firewall's settings ...
2. Type "firewall" into the search bar. Doing so will automatically search your computer for applications matching your typing.
3. Click the "Windows Firewall" option.

Your computer's firewall is largely responsible for blocking incoming connections that could potentially harm your computer. You can view and alter your firewall settings on any computer, but keep in mind that the firewall application is best applied to PCs; Mac users usually need not enable or use the built-in firewall program.



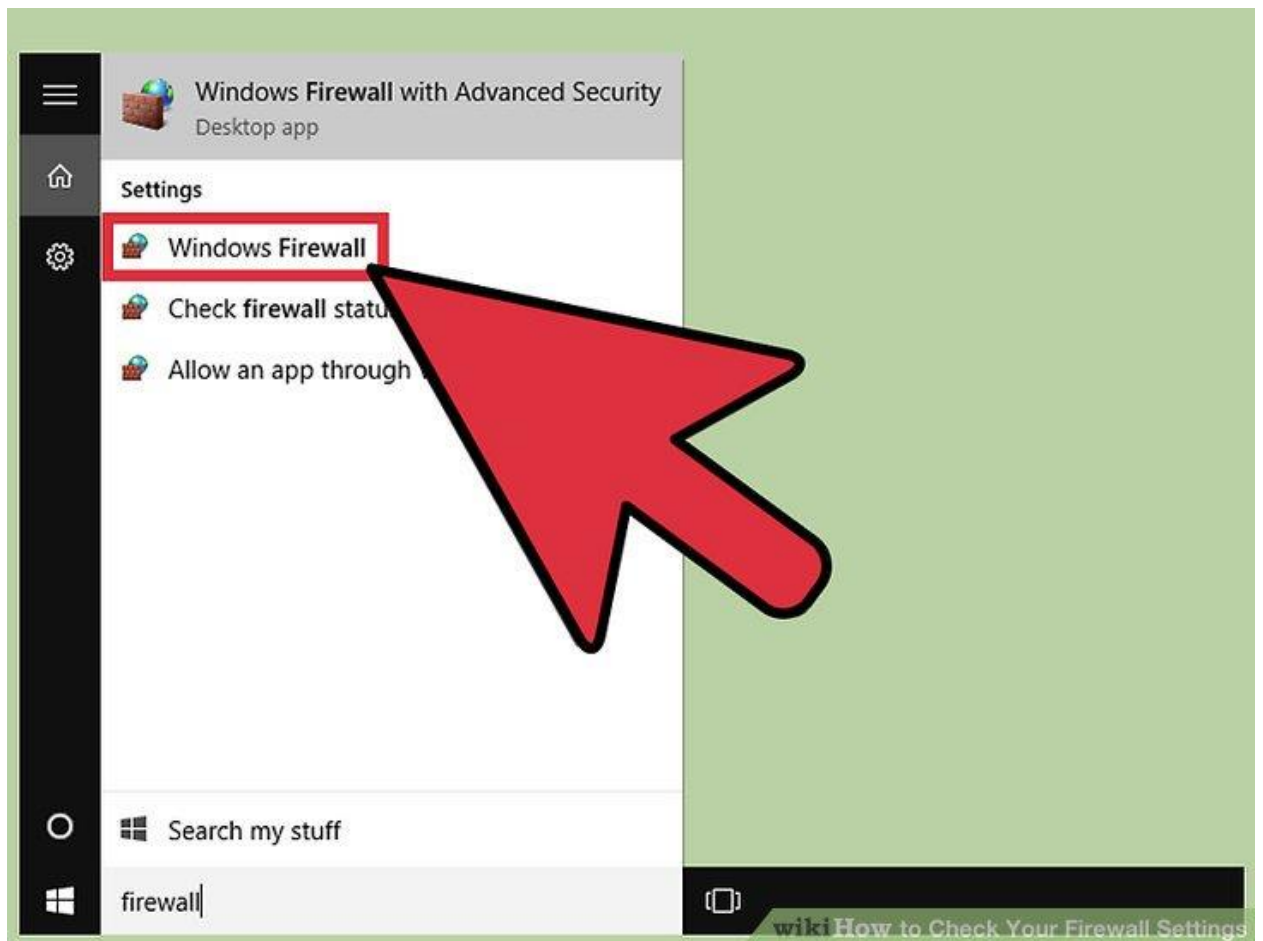
Open your Start menu. Windows' default firewall program is located in the "System and Security" folder of the Control Panel app, but you can easily access your firewall's settings by using the Start menu's search bar.

- You can also tap the  Win key to do this.



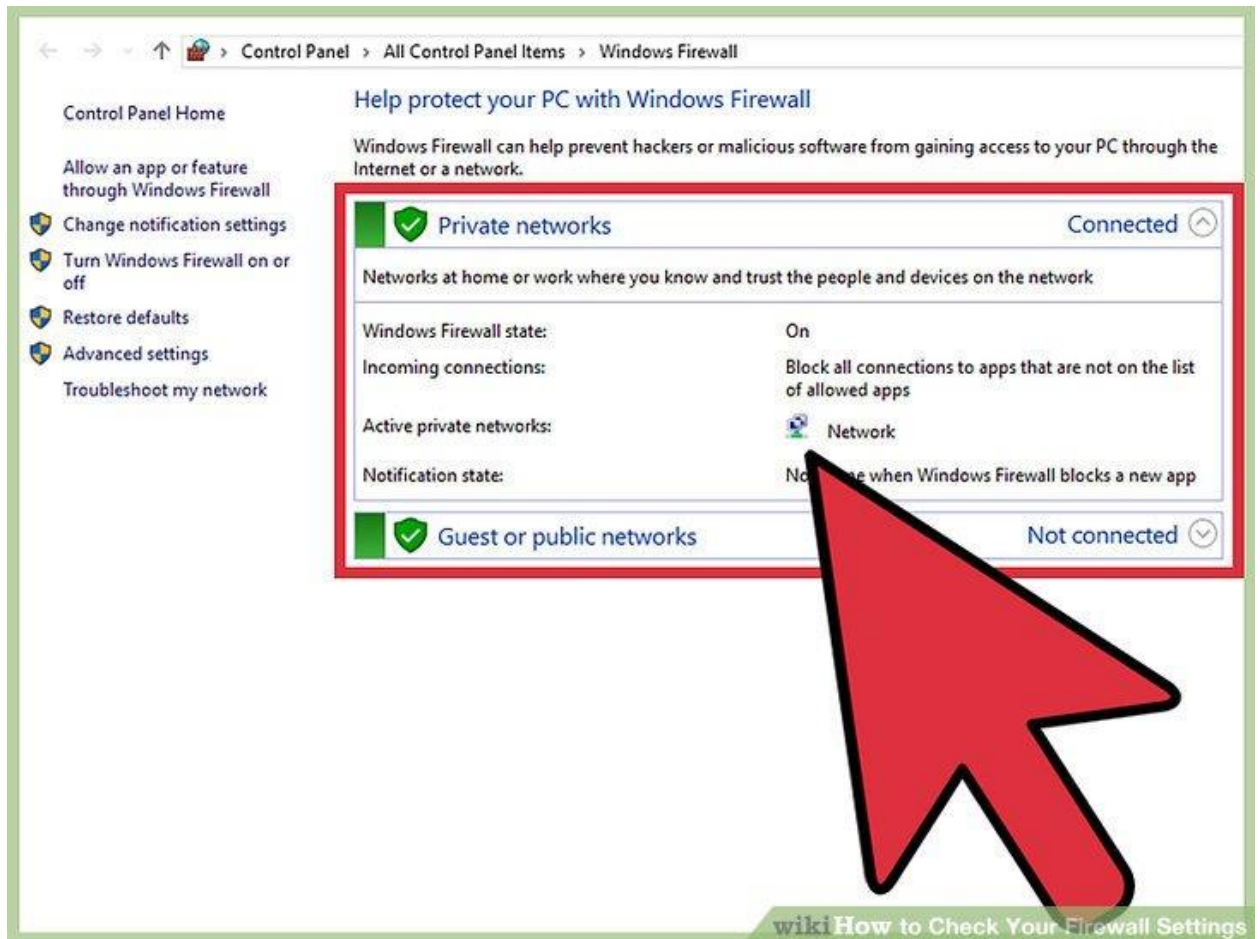
2

Type "firewall" into the search bar. Doing so will automatically search your computer for applications matching your typing.



3

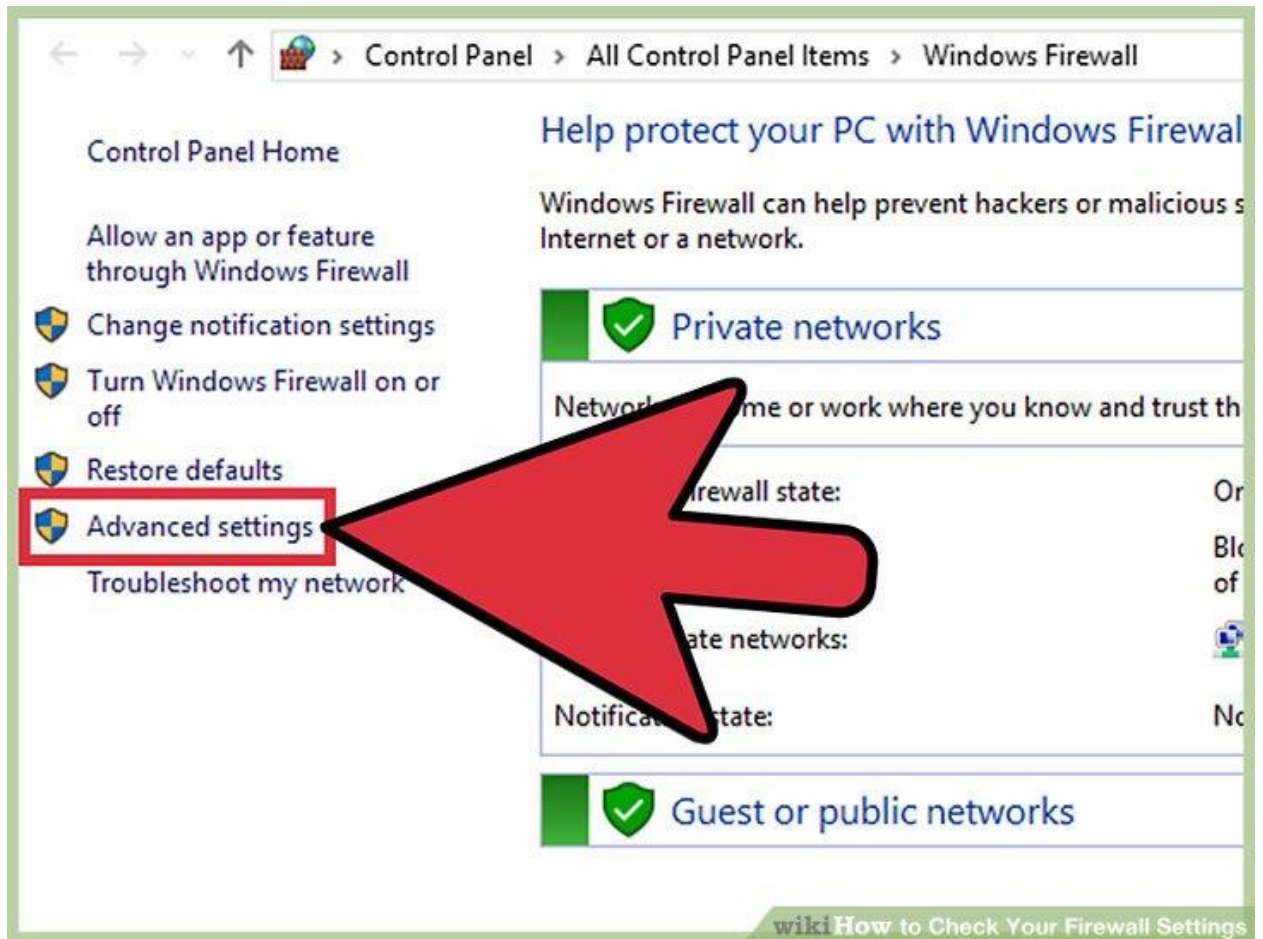
Click the "Windows Firewall" option. You should see this at the top of the search window.



4

Review your firewall settings. You should see two sections entitled "Private networks" and "Guest or public networks" with green shields to the left of them, signifying that your firewall is active.

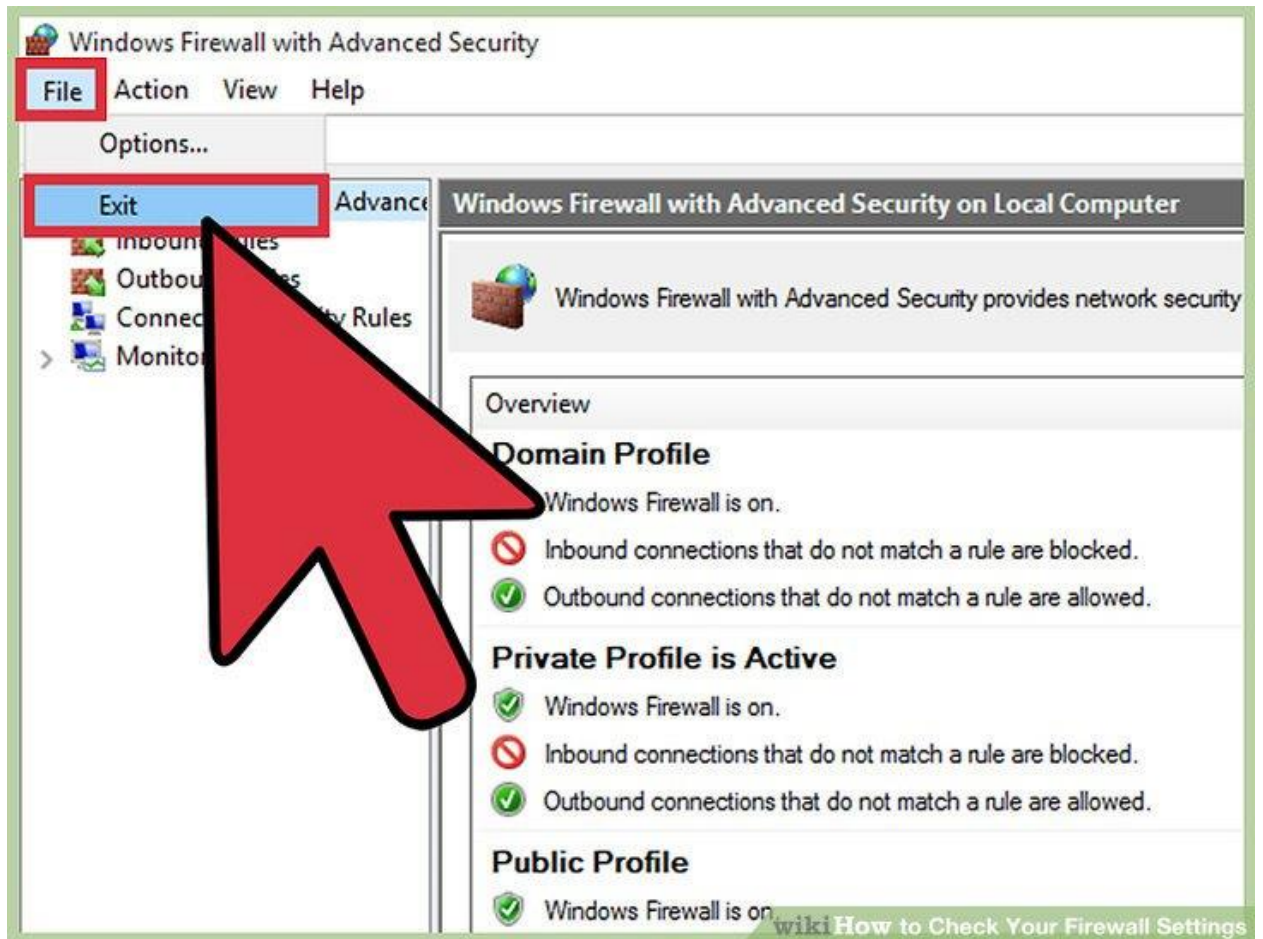
- Clicking on either of these sections will prompt a drop-down menu with details about your current private or public networks.



5

Click the "Advanced Settings" option. This is to the left of the main menu; clicking it will open your firewall's advanced settings menu, from which you can view or alter the following:

- "Inbound Rules" - Which incoming connections are automatically allowed.
- "Outbound Rules" - Which outgoing connections are automatically allowed.
- "Connection Security Rules" - Baselines for which connections your computer will allow and which ones it will block.
- "Monitoring" - An overview of your firewall's basic monitoring guidelines.



6

Exit the Advanced Settings menu when you're finished. You have successfully checked your PC's firewall settings!

- Note that you can also click the "Turn Windows Firewall on or off" in the same option menu in which you found Advanced Settings. Be wary of disabling your firewall, especially when connected to a public network.