A – This country allows patients to access their own medical records. To implement this online, a database system is needed to store medical records, and it is connected to the Internet.

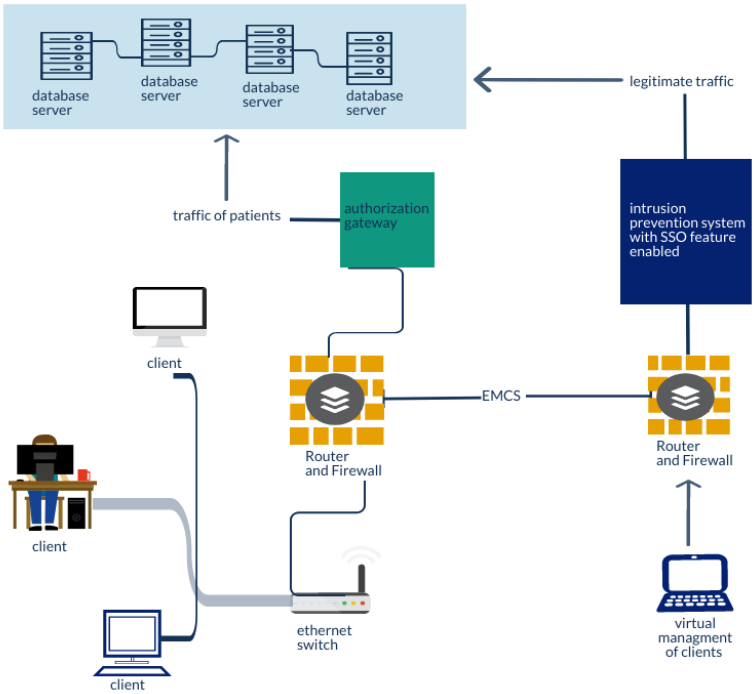
1. Design a solution to allow the system to securely send a large medical record to

   its associated patient (e.g. by email) upon his/her request.

2. The record should be sent efficiently with the assurance of message secrecy,

   integrity and authenticity.

The screenshot below depicts the network topology for solution of this problem :



Software Country

Sending Patient information in secure manner :

Nowadays, Electronic Medical Records a typical technique instead of using paper records, it is leading to saving time, lowering costs, and enhancing the quality of medical treatment.
And in nowadays, using of E-mail is a ubiquitous means of contact in most of fields.
E-mail makes transmitting and exchanging medical information or patient reports convenient for all parties.
But regrettably, so many violations of security have confirmed that this is not a protected way of data sharing.
Public sites and email communications with patients have already begun to be used for physicians' offices.
These options are good, but they also put patients at greater risk of theft of medical identification.
So, Special countermeasures must also be taken to securely relay patient records .

Mail Encryption and Protected health information :

Before viewing of medical records, patients should certain that their used end-devices are encrypted .
So, it also must to encrypt internet sites that provide medical data.
Patients must be made aware that if their local end-systems are no longer secure, then they have positioned their data at risk .

Different Types of Email :

When it comes to efficiently send information to patients, there are many forms of addresses. Doctors' offices and patients alike need to use accounts with HTTPS protection for web-based email application .
The only way by which web-based email is safe is through this process.
You can also encrypt the email that is sent to a patient using either PGP encryption methods or applying wireless access policy such as Symantec Wireless IDs, and any email comes with encryption in all of these ways.

Patient's ID hash :

Usage of the message digest-5 (MD5) and secure hashing algorithm (SHA) as methods for encrypting electronic medical data.
The studies show that the composite message can be used to create a unique one-way encrypted ID per patient record that can be used for data sharing.
So, we can share patient EMRs between practitioners without revealing patient's identifiable data.

Digital Document Signing:

Digital transformation has made this process considerably easier.
The document can be signed digitally on any device, and secure cloud storage can automate the storage, retrieval and disposal process.
So, we can achieve all of these benefits when the document is digitally signed :

- Saving Time and Money.
- Secure Access to Medical Data.
- Elimination of Bottlenecks
- Legal Compliance

Cloud providers' services:

Regulations explain statements on how data from the office and therefore the customer are often moved on.

For emails, one among the tools to use for this correspondence depends on cloud providers.

There are their own firewalls and security filtering systems for these cloud providers, and that they make sure the data only goes to a specific location.

A virtual private network (VPN) access code could also be used.

Using of physical characteristics technologies (Biometric Identification):

Authentication through biometric is growing in use when it comes to accessing secret information, as passcodes become weak and dangerous for healthcare information protection.

The chance for data breaches, even with the precisely designed codes, comes with passcodes.

It is almost difficult for identity theft to occur with the use of fingerprint, eye scans, and facial recognition applications, and retina scan, because these characteristics cannot easily be imitated.

Result:

Depends on this problem, the cryptography algorithm to be used can be RSA (public key encryption) where the private key will be private by EMCS while the patient program will maintain a public key to be used to decrypt the health data sent from the EMCS systems.

The main reason for preferring RSA encryption is that it is known as the most reliable encryption algorithm.

Instead of keeping two keys, one for encryption and the other for decryption, for each client patient, EMCS should have a private key and the same situation as the public key.

A strong way of exchanging these keys with the client patient should also be introduced by EMCS.

The keys may also have a validity feature where they need to be used to use the facilities after which they have been revoked.

D - E-mail is a critical Internet application. However, as more people join the Internet, concerns over privacy are mounting. PGP (Pretty Good Privacy) tries to combat these concerns.

1. Explain how PGP can achieve the confidentiality, integrity and authenticity of an e-mail message.

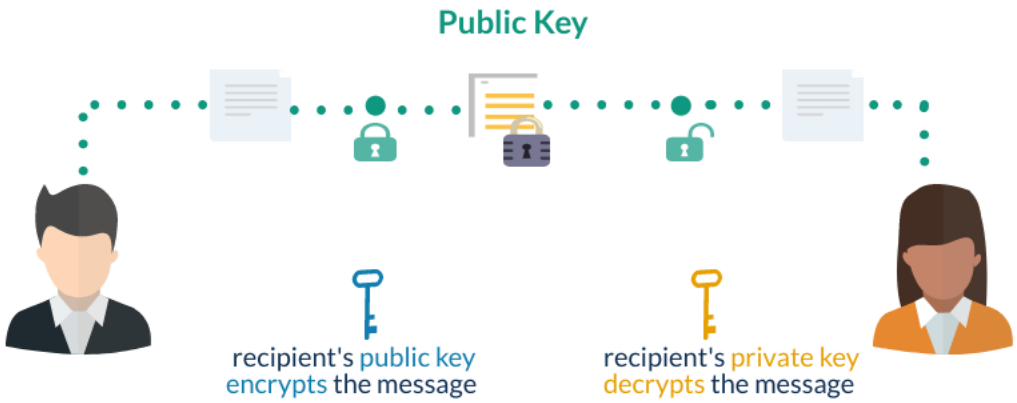
2. Discuss why trust management is essential to PGP public-key rings, and what relationships exist among the four fields of a public-key ring: Owner Trust, Key Legitimacy, Signature(s), and Signature Trust(s).

Frist one what is PGP ?

PGP is a program that uses encryption to guard the privacy of your email
And files that you simply store on your computer.
As well as a digital signature verification system, which allows you to verify those files or e-mail
Messages haven't been modified. it's also one among the
foremost prominent encryption standards that provide end-to-end encryption for email messages and other information exchange.

PGP is a popular encryption protocol used to encrypt emails, texts, files, directories, and even disk partitions. The concept of PGP is predicated on asymmetric public key cipher for user identification,

it can only be decoded by Someone knows the file that encrypts the password.
After creating your private and public keys. Keys to encrypt the file. By employing a public and personal key for encryption and decryption, recipients are often confident that the info is what the sender says. The recipient assures the confidentiality, integrity, and authenticity of the data.



Confidentiality

is guaranteed because the content protected with the general public key can only be decrypted with the private key. This ensures that only the intended recipient can review the contents

Integrity

is guaranteed because a part of the decryption process requires verification that the message received matches the message sent. This ensures that the message doesn't change between them.

Authenticity

is guaranteed because every message Alice sends to Bob is additionally signed by Alice's private key. the sole thanks to decrypt Alice's private key's to use her public key, which Bob can access. By signing the message together with her private key, Alice guarantees the authenticity of the message and shows that it actually came from it.

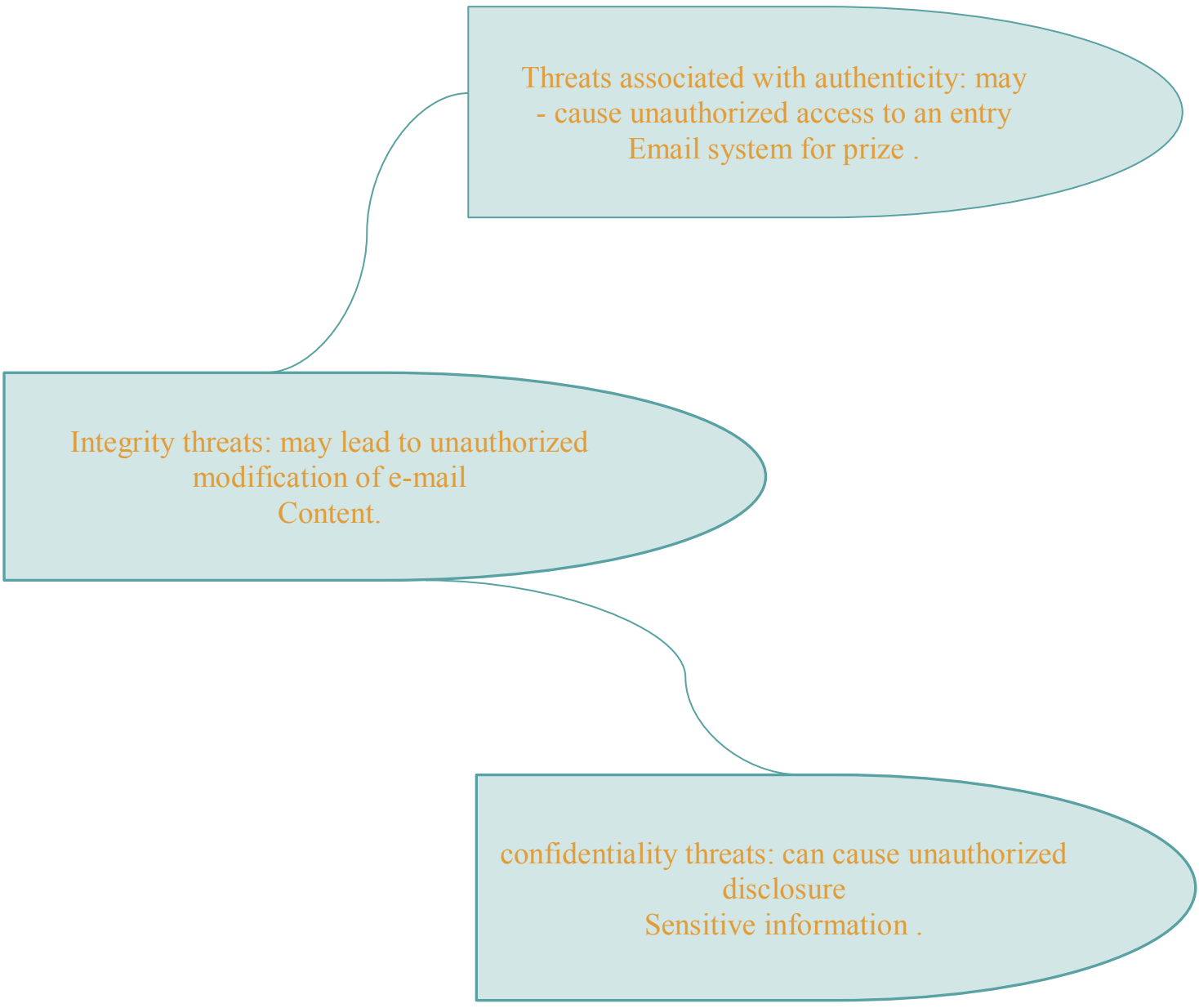
PGP provides the conceivable confidentiality and authentication service for email applications

Authentication

On the sender side, SHA-1 is employed to get a 160-bit hash code for the sent message. The hash code is encrypted with the sender's private key and therefore the result's appended to the message. The receiver decrypts the hash code using the sender's public key. The receiver generates a replacement hash code for the message and compares it to the hash code that was decrypted. If both hash symbols are an equivalent , the message is original

Confidentiality

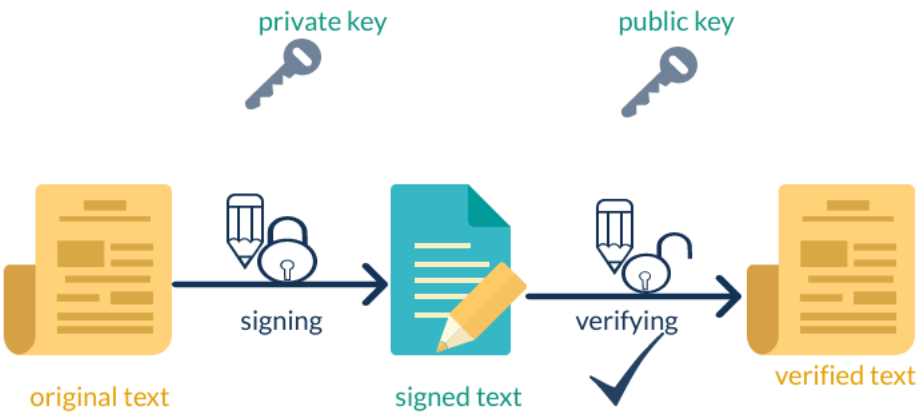
The sender creates a message which will be sent and therefore the 128-bit number to use because the secret session key for the sent message. The message is encrypted using 3DES with the session secret key. The session secret key's again encrypted with the recipient's public key and appended to the sent message. The receiver used its private key to decrypt and restore the session's secret key, then a session's secret key's wont to decrypt the sent message.


Threats associated with authenticity: may
- cause unauthorized access to an entry
Email system for prize .
Integrity threats: may lead to unauthorized
modification of e-mail
Content.
confidentiality threats: can cause unauthorized
disclosure
Sensitive information .

Second why do you need PGP and encryption ?

The size of the internet doubles per annum . Email is one among the most reasons For this excellent growth. Email is extremely fast and almost empty, with over 100 million emails crossing the world's computer networks a day . Most of this email is vulnerable.
It may be much easier to intercept and replica email without know the sender or recipient. In fact, the transmission itself did an email message from one person to a different includes making a replica of these messages .
Also what happens when a message makes its way from the sender to the recipient .

Public key digital signatures provide authentication and data integrity. The digital signature also provides non-repudiation, which suggests it prevents the sender from claiming that they didn't actually send the knowledge . These features are as fundamental to encryption as privacy,
The primary way digital signatures are created. rather than encrypting information with someone else's public key, you're encrypting it together with your private key. If the knowledge might be decrypted using your public key,



PGP confidence levels

The highest level of trust during a key, implicit trust, is trust in your key pair. PGP assumes that if you own the private key, you want to trust the actions of the general public key related to it. Any keys signed together with your implicitly trusted key are valid.

Example

Assume your keyring contains the Alice key. I even have verified Alice's key and indicated it by signing it. you recognize Alice may be a powerful tool to validate other people's keys. So you set her key with complete confidence. This makes Alice a certification authority. If Alice falls to a different key, it appears as a legitimate hoop .

Associated with each public key within the user's public key loop may be a valid primary field indicating how confident the PGP is that this is often a legitimate public key for that user.
Legitimacy is decided from the certificates, and therefore the user's assessment of the trust which will be assigned to the key.

Key Legitimacy

It is computed by PGP. This field specifies the amount of PGP's trust about the validity of user's public key. supported the extent of trust, the user ID is sure to the key. A KEYLEGIT field can hold the subsequent information:

1. unknown or undefined trust
2. key ownership not trusted
3. marginal trust in key ownership
4. complete trust in key ownership

A WARNONLY bit is set if user wants only to be warned when key that's not fully validated is employed for encryption

Owner's trust

Domain of the owner's trust
Each entry within the public hoop represents a public key related to a selected owner, along side the owner trust field. This field defines how reliable the general public key's , so it are often wont to sign other public key certificates.
The OWNERTRUST field can contain values like:

1. Unspecified confidence
2. Unknown user
3. Usually don't trust other keys to sign
4. Usually authenticated to sign other keys
5. Always believe to sign other keys
6. This key's within the secret keyring (absolute trust).

It also features a BUCKSTOP bit that adjusts automatically, if the key's present within the secret hoop .

Signature field

The owner of the hoop collects all the signatures associated with the entries. Each signature features a signature's trust field that defines the extent of trust a PGP user has toward the signer, in order that all of their public keys are often approved. SIGTRUST FIELD can contain values such as:

1. Unspecified confidence
2. Unknown user
3. Usually don't trust other keys to sign
4. Usually authenticated to sign other keys
5. Always believe to sign other keys
6. This key's within the secret keyring (absolute trust).

It also contains the CONTIG bit that's set if the signature tends to a contiguous trusted certificate path that ultimately reaches the owner of the trusted keyring.

E - The Firewall function of a Router is made up of rules. By using Firewall Rules, form the below rules:

1. Block a website IP address from accessing your Wifi.
2. Block your browser from sending or receiving network traffic from your device.
3. For both rules:

- Present the steps and explain your choices.
- Test the rule and display the output to support your rule.

What is the firewall on windows ?

Firewall has become crucial elements in network security, and are widely deployed in most businesses and institutions for securing private networks. The function of a firewall is to look at each packet that passes through it and choose whether to letting them pass or halting them supported preconfigured rules and policies, so firewall now's the primary defense line against cyber attacks. However most of individuals doesn't knowledge firewall works, and therefore the most users of windows OS doesn't knowledge to use the windows embedded firewall.

Typically, a personal firewall may be a software unit on a PC. at Home environment with multiple computers connected to the web , a firewall

The function also can be placed during a router that connects all home computers

To DSL, cable modem, or other internet interface.

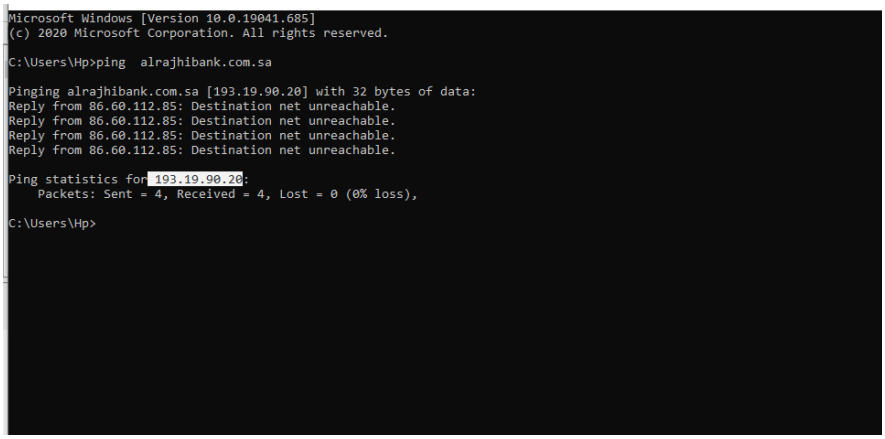
Firewalls or standalone firewalls. the first role of a private firewall is Deny unauthorized remote access to the pc . Firewall also can monitor Outbound activity in an attempt to detect and block worms and other malware.

For additional protection, advanced firewall features could also be configured.

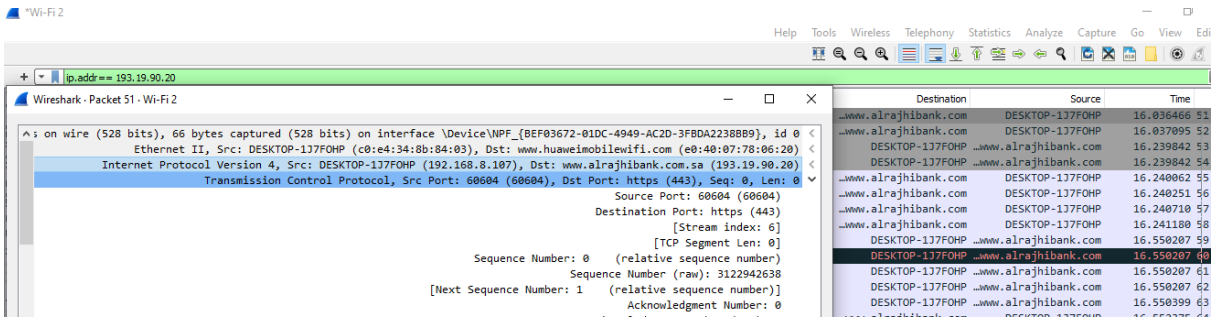
For example, stealth mode hides the system on the web by dropping it unwanted
Connection packets, which makes it appear as if the
system doesn't exist.
UDP packets are often blocked, which limits network traffic to only TCP packets for
Ports are open. The firewall also supports logging, which is a crucial verification tool
Unwanted activity. Other sorts of personal firewall allow the user to specify this
Only selected applications, or applications signed by a
legitimate certification authority,
It may provide services to access it from the network

The screenshot below depicts the Block a website IP address from accessing your Wifi

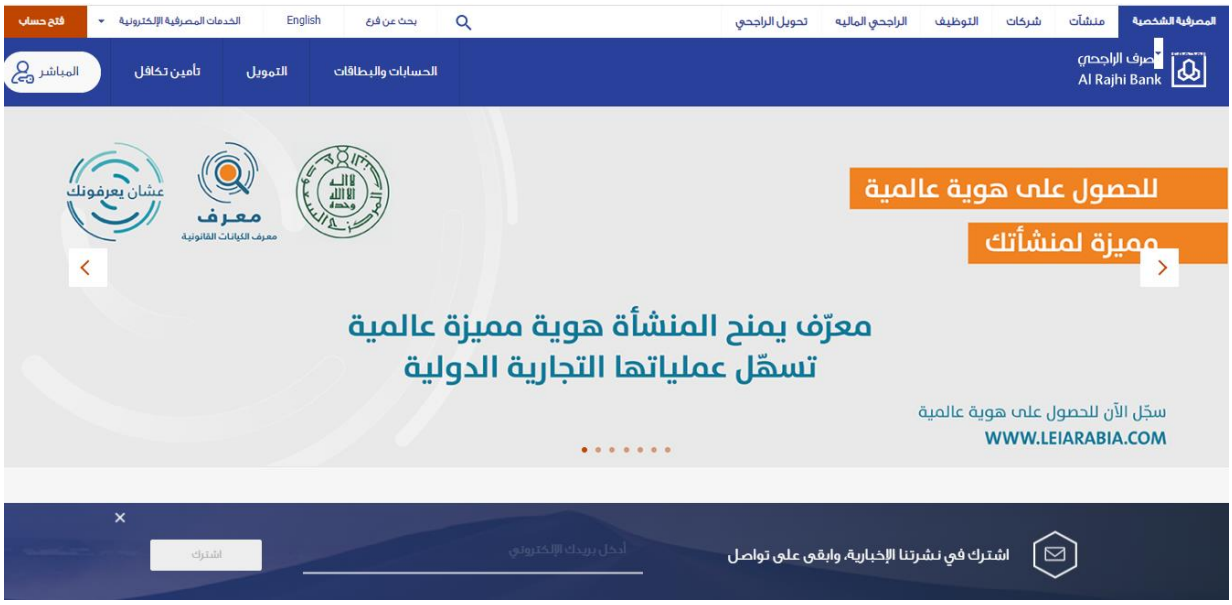
The website has been chosen is https://www.alrajhibank.com.sa



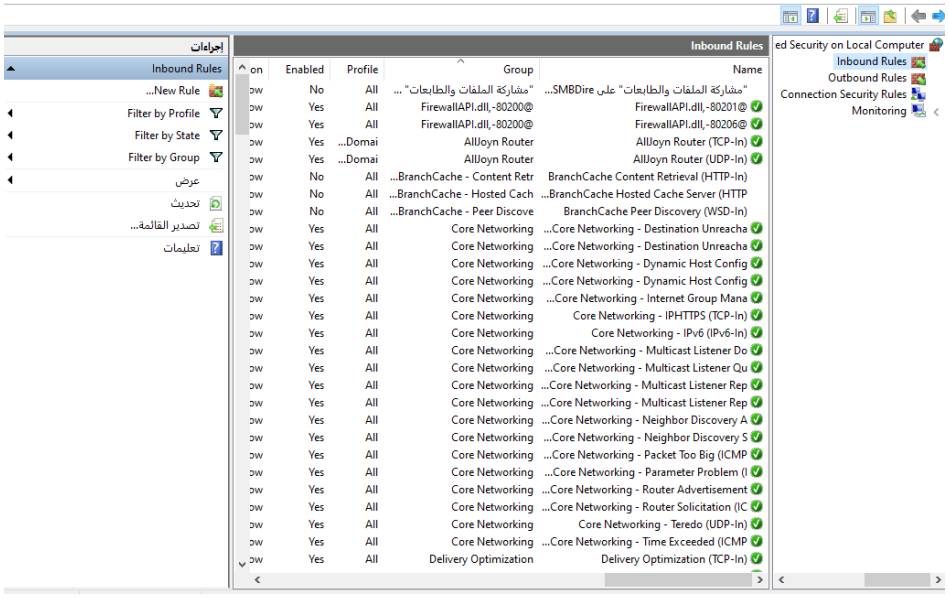
The website IP address that will be blocked from the Wi-Fi network has been determined.



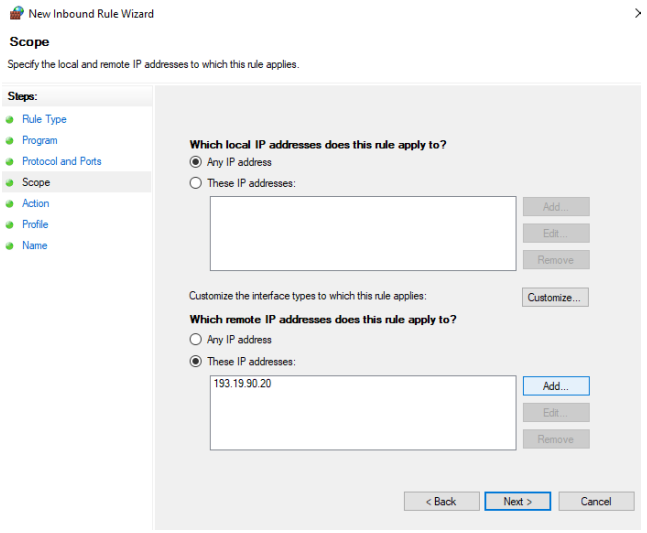
Also the website IP address that will be blocked from the Wi-Fi network has been determined from Wireshark .



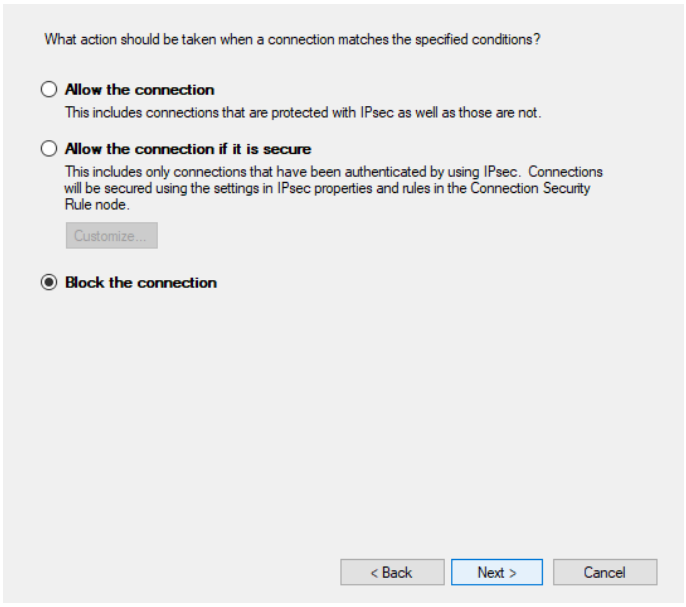
This is the interface of the website before the block



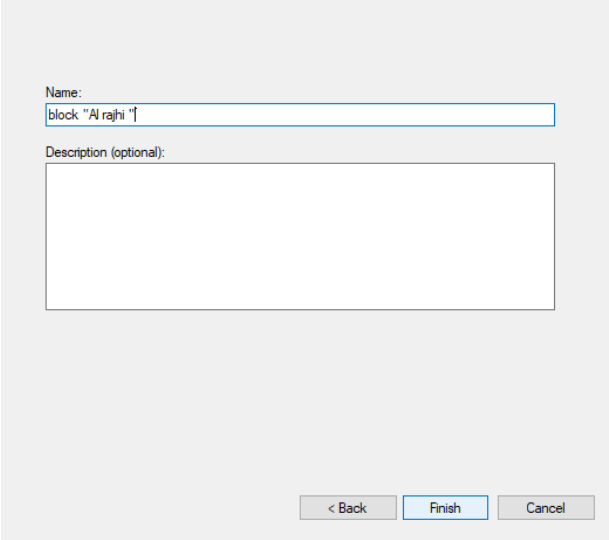
Now we go to the steps to block a website with a Windows firewall



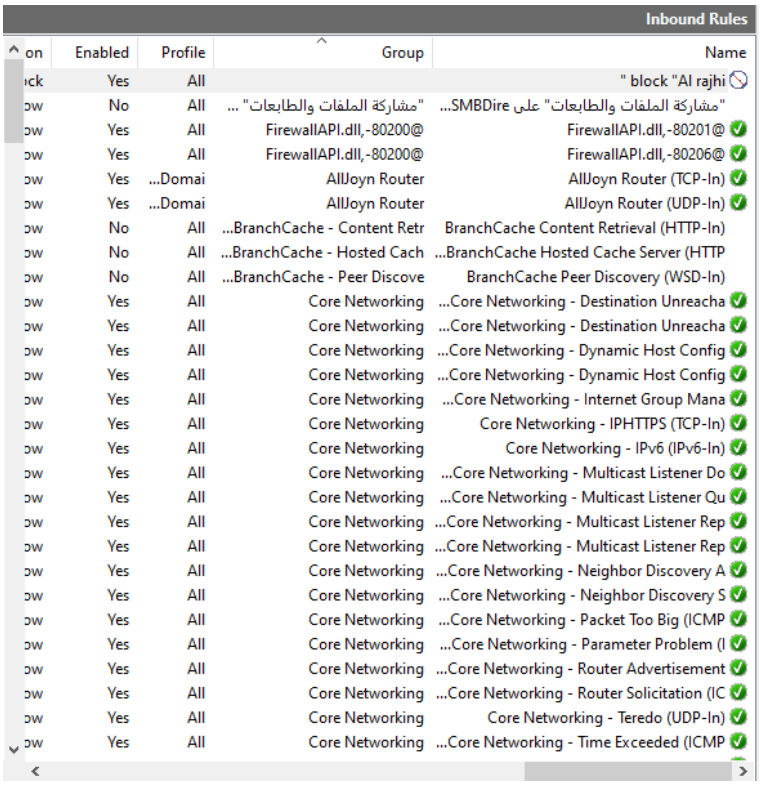
From the list, go to the option "inbound rules " chose " new rule " A window appears " new inbound rule wizard " chose the type to create " custom " after that which remote IP addresses does this rule apply to ? select " these IP addresses " enter the IP address the website after that add



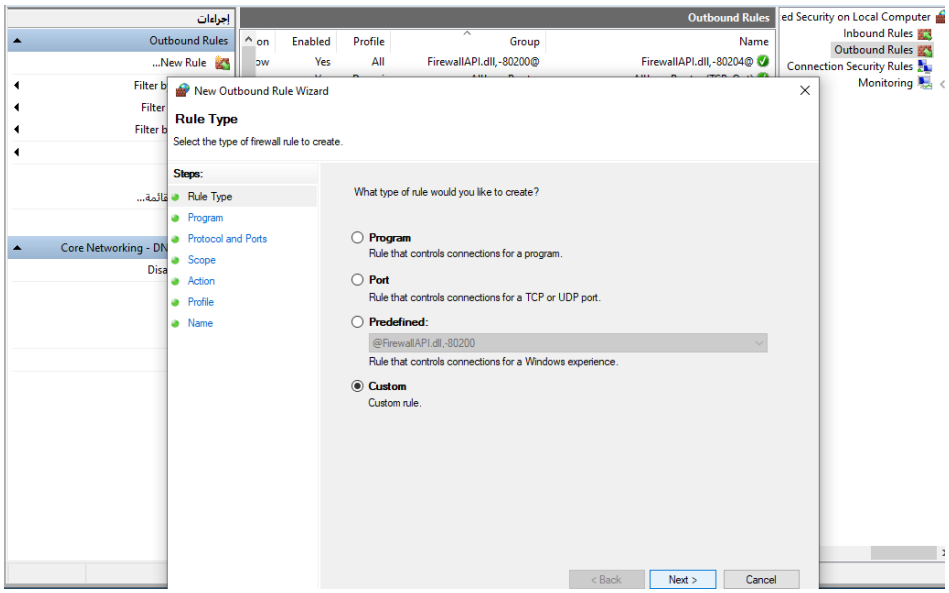
After that select "block the connection "



Write the name " block Al Rajhi "

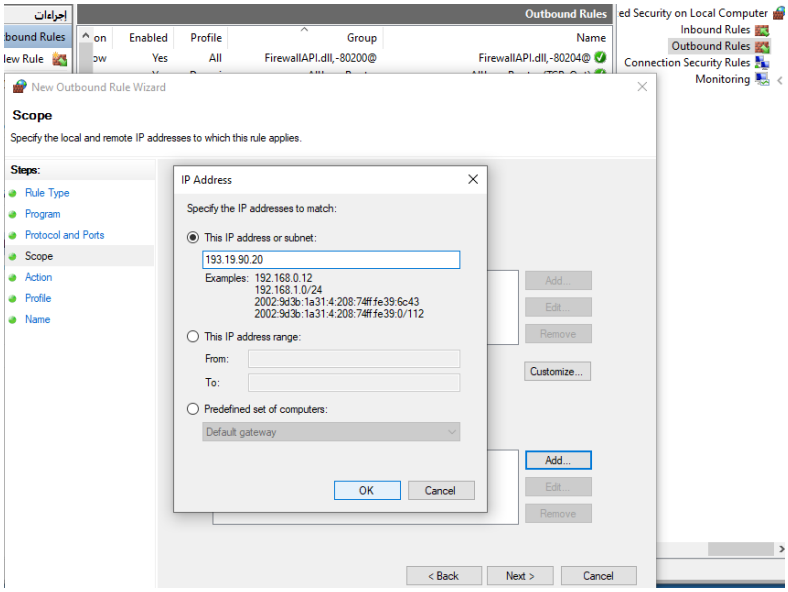


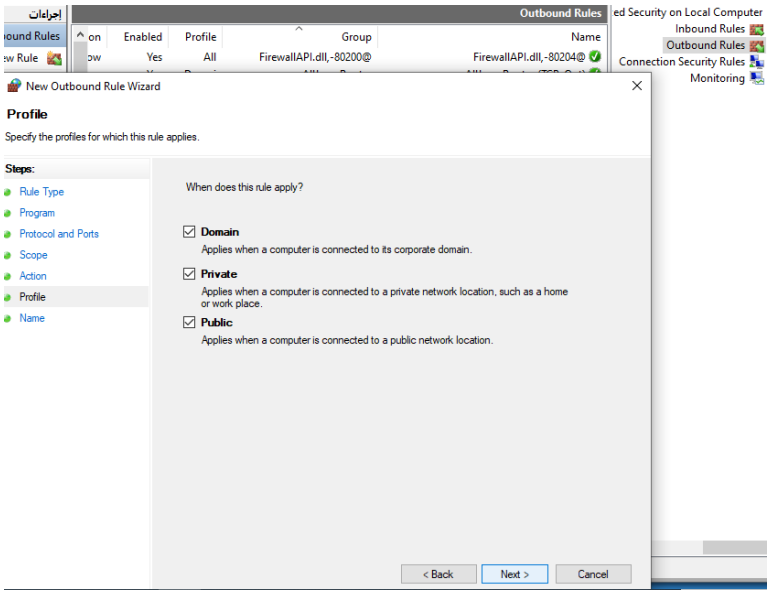
Now it appears in the list " inbound rules "

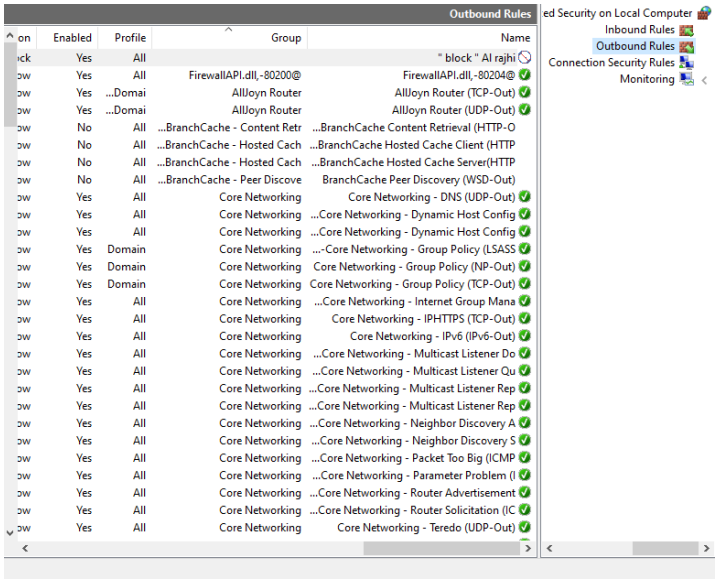


We now move to the other list type " outbound rules "

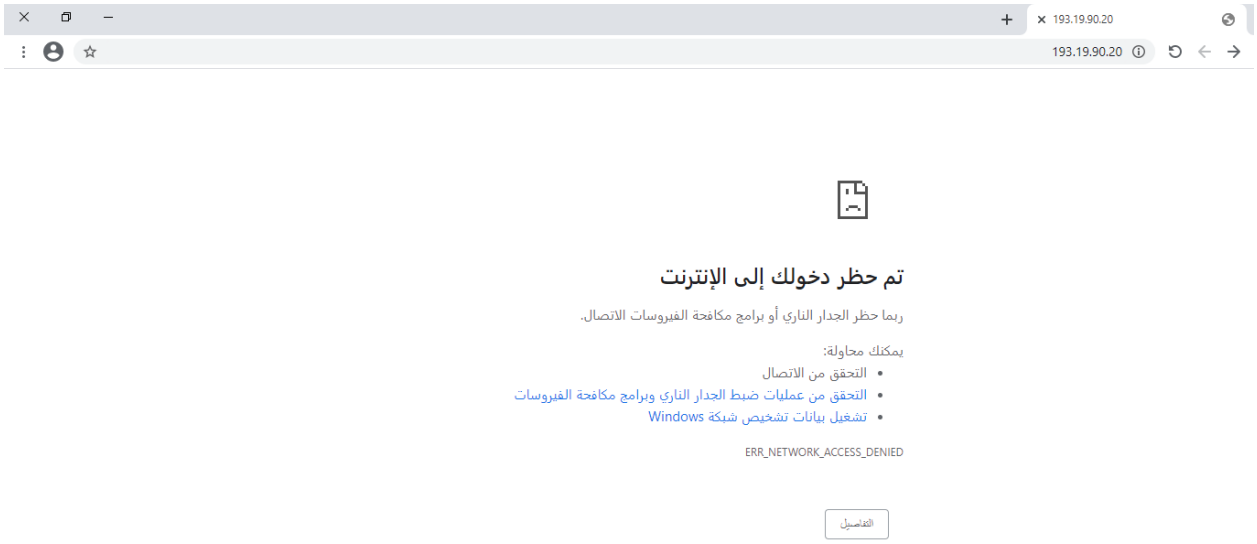
The same steps as the previous process.



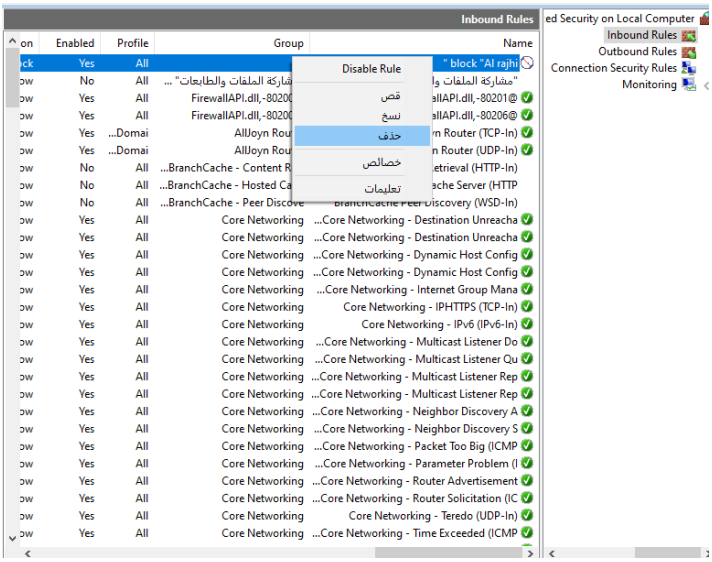


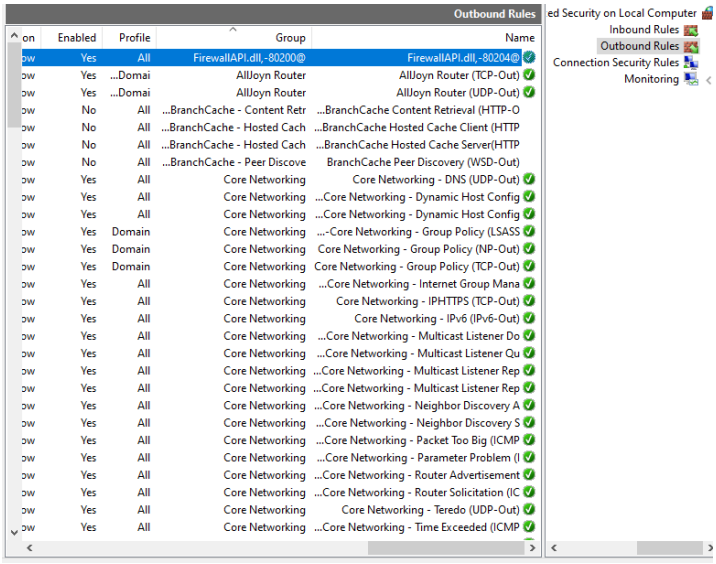


It also appears in the list here " outbound rules "



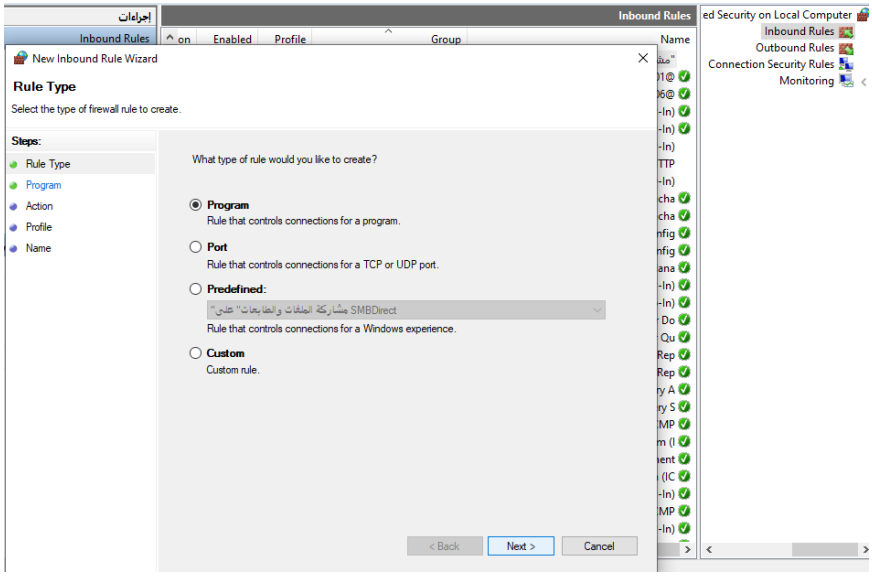
We go to the site and it will show us that the Al Rajhi site has been banned .



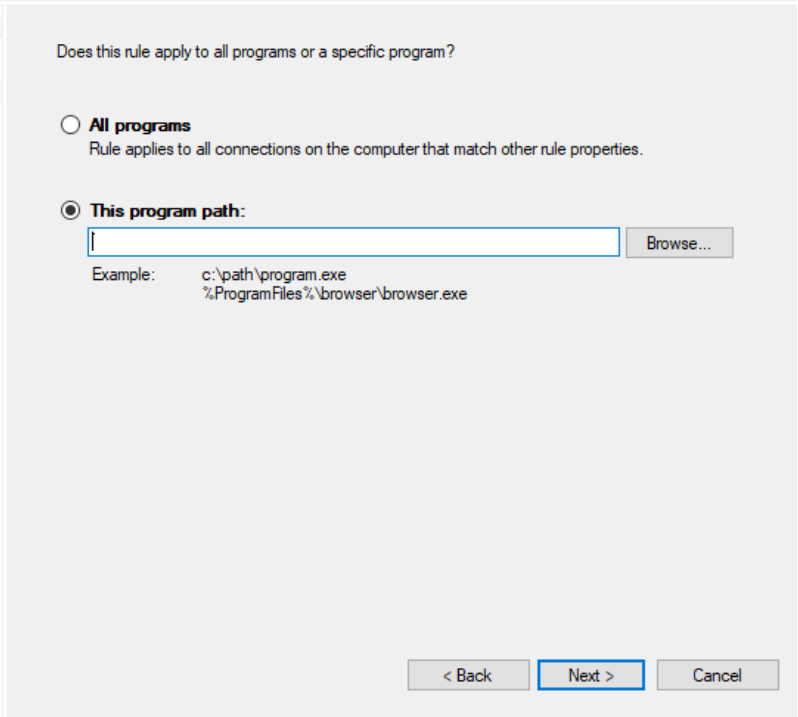


Now, I can lift the ban from the website from each of the two lists " inbound rules & outbound rules " and delete it.

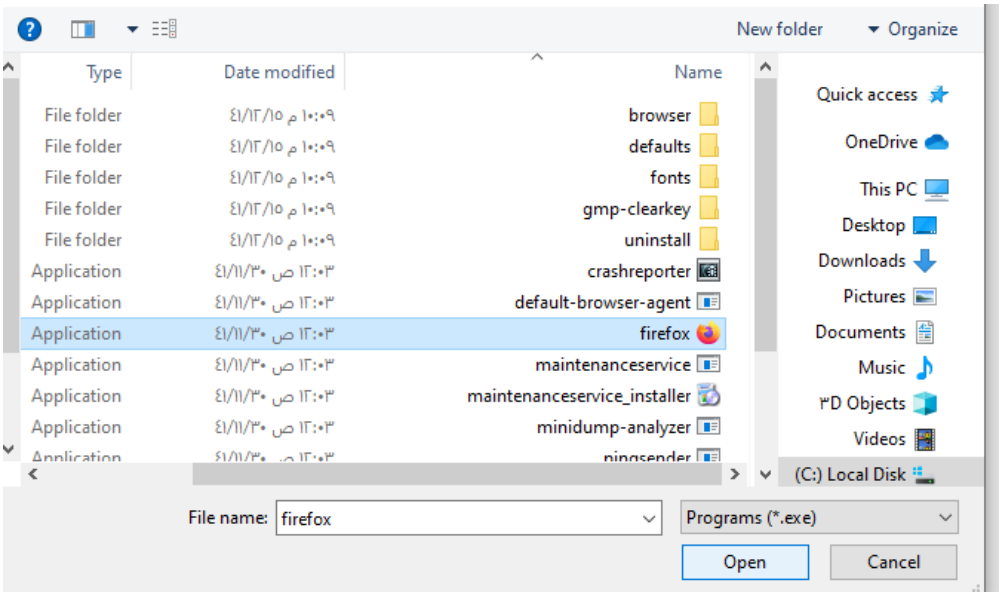
The screenshot below depicts Block your browser from sending or receiving network traffic from your device:



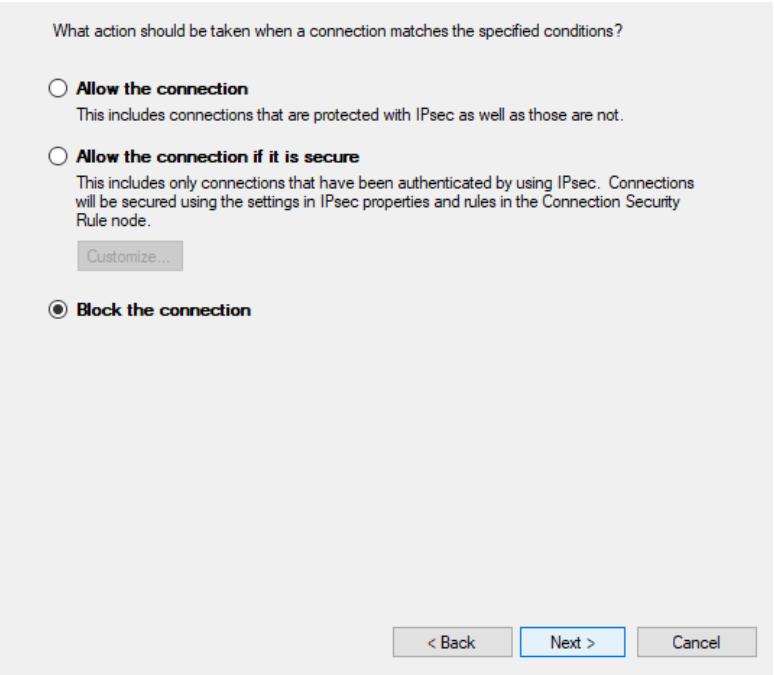
Once again, we go in and do the same previous steps, but with a slight difference. For the "inbound rules " chose " new rules "
Here select the type " program "



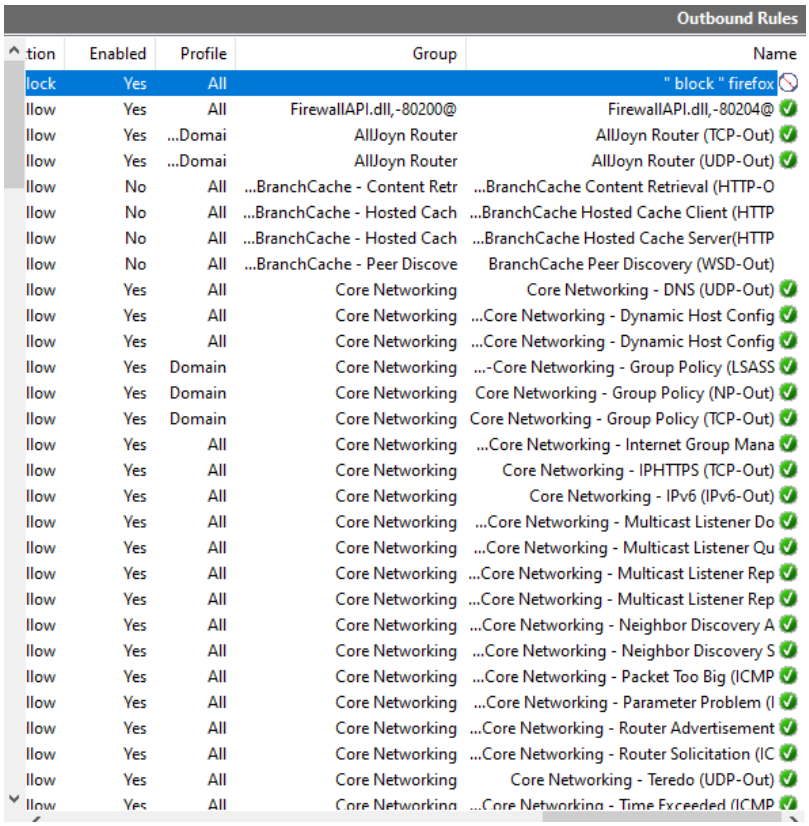
The program path enter the browser



Chose the browser " firefox "



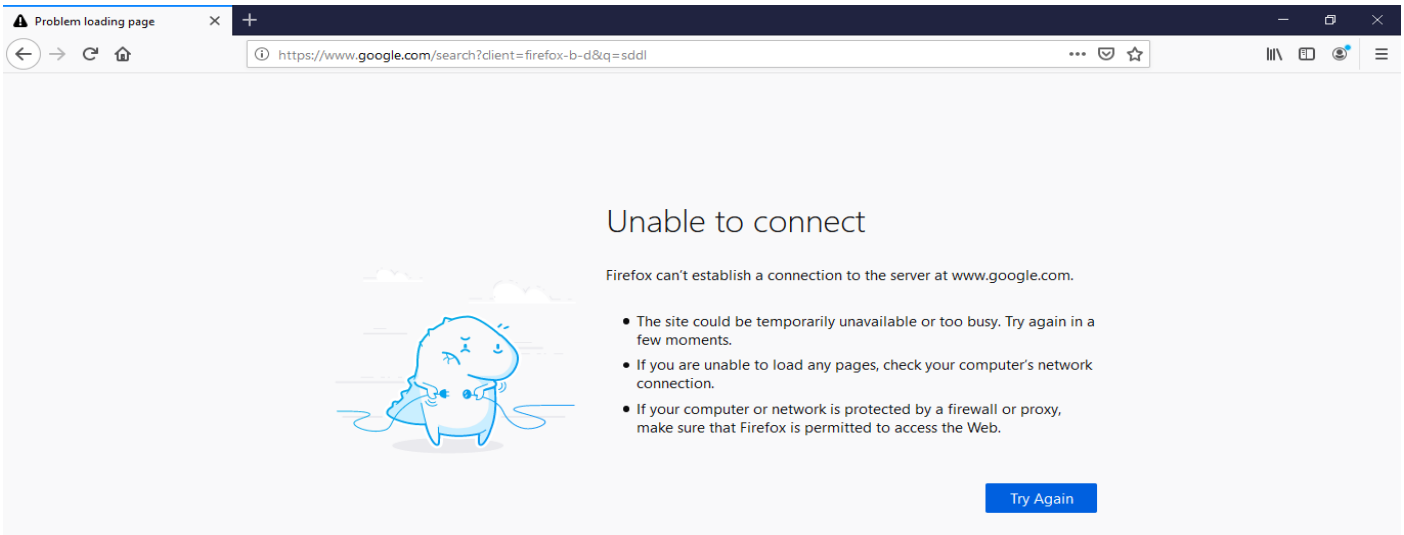
Select block the connection .



Inbound Rules

tion	Enabled	Profile	Group	Name
lock	Yes	All		" block " firefox
llow	No	All	"مشاركة الملفات والطابعات" ...	"مشاركة الملفات والطابعات" على SMBDire...
llow	Yes	All	FirewallAPI.dll,-80200@	FirewallAPI.dll,-80201@
llow	Yes	All	FirewallAPI.dll,-80200@	FirewallAPI.dll,-80206@
llow	Yes	...Domai	AllJoyn Router	AllJoyn Router (TCP-In)
llow	Yes	...Domai	AllJoyn Router	AllJoyn Router (UDP-In)
llow	No	All	...BranchCache - Content Retr	BranchCache Content Retrieval (HTTP-In)
llow	No	All	...BranchCache - Hosted Cach	...BranchCache Hosted Cache Server (HTTP
llow	No	All	...BranchCache - Peer Discove	BranchCache Peer Discovery (WSD-In)
llow	Yes	All	Core Networking	...Core Networking - Destination Unreacha
llow	Yes	All	Core Networking	...Core Networking - Destination Unreacha
llow	Yes	All	Core Networking	...Core Networking - Dynamic Host Config
llow	Yes	All	Core Networking	...Core Networking - Dynamic Host Config
llow	Yes	All	Core Networking	...Core Networking - Internet Group Mana
llow	Yes	All	Core Networking	Core Networking - IPHTTPS (TCP-In)
llow	Yes	All	Core Networking	Core Networking - IPv6 (IPv6-In)
llow	Yes	All	Core Networking	...Core Networking - Multicast Listener Do
llow	Yes	All	Core Networking	...Core Networking - Multicast Listener Qu
llow	Yes	All	Core Networking	...Core Networking - Multicast Listener Rep
llow	Yes	All	Core Networking	...Core Networking - Multicast Listener Rep
llow	Yes	All	Core Networking	...Core Networking - Neighbor Discovery A
llow	Yes	All	Core Networking	...Core Networking - Neighbor Discovery S
llow	Yes	All	Core Networking	...Core Networking - Packet Too Big (ICMP
llow	Yes	All	Core Networking	...Core Networking - Parameter Problem (I
llow	Yes	All	Core Networking	...Core Networking - Router Advertisement
llow	Yes	All	Core Networking	...Core Networking - Router Solicitation (IC
llow	Yes	All	Core Networking	Core Networking - Teredo (UDP-In)
llow	Yes	All	Core Networking	...Core Networking - Time Exceeded (ICMP
llow	Yes	All	Delivery Optimization	Delivery Optimization (TCP-In)

Now in both lists " inbound rules and outbound rules " the block is done.



We go the browser it's the block is done .

References

1- .R. Zimmermann. *The Official PGP User's Guide*. MIT Press, 1995.

2- A. Jøsang. A Subjective Metric of Authentication. In J. Quisquater et al., editors, *Proceedings of ESORICS'98*, Louvain-la-Neuve, Belgium, 1998. Springer.

3- A. Jøsang. The right type of trust for distributed systems. In C. Meadows, editor, *Proc. of the 1996 New Security Paradigms Workshop*. ACM, 1996.

4- Abdullah M. Jaafar and Azman Samsudin**,** A New Public-Key Encryption Scheme Based on Non-Expansion [10]P. C. O. A.J Menezes, and S.A. Vanstone, Handbook of Applied Cryptography: CRC Press, 1996.

5- Povey D., Developing Electronic Trust Policies Using a Risk Management Model, 1999 http://security.dstc.edu.au/staff/povey/papers/CQRE/123.pdf

6- Building a Foundation of Trust in the PC, 2000, The Trusted Computing Platform Alliance, http://www.trustedpc.org

7- N. Naik and P. Jenkins, "Enhancing Windows Firewall Security Using Fuzzy Reasoning," 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), Auckland, 2016, pp. 263-269, doi: 10.1109/DASC-PICom-DataCom-CyberSciTec.2016.64.

8- D. Kuobin, "PGP E-Mail Protocol Security Analysis and Improvement Program," *2011 International Conference on Intelligence Science and Information Engineering*, Wuhan, 2011, pp. 45-48, doi: 10.1109/ISIE.2011.144.

9- A. von Bidder and N. Weiler, "Key Exchange (KX) - a next generation protocol to synchronise PGP Keyservers," WET ICE 2003. Proceedings. Twelfth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2003., Linz, Austria, 2003, pp. 249-254, doi: 10.1109/ENABL.2003.1231416.