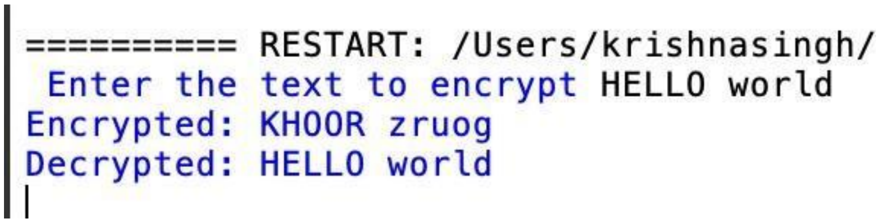
Practical No.1

Aim: Implementing Substitution and Transposition Ciphers: Design and implement algorithms to encrypt and decrypt messages using classical substitution and transposition techniques.

Code for implementing Substitution Cipher with Caesar Cipher:

```
   def caesar_cipher(text,
   shift):result = ""
    for char in text:
        if char.isalpha():
            offset = ord('a') if char.islower() else ord('A')
            result += chr((ord(char) - offset + shift) % 26 + offset)
        else:
            result += char
    return result

# Example usage:
message = input (" Enter the text to encrypt ")
shift = 3

encrypted_message = caesar_cipher(message, shift)
print("Encrypted:", encrypted_message)

decrypted_message = caesar_cipher(encrypted_message, -shift)
print("Decrypted:", decrypted_message)
```

Output :

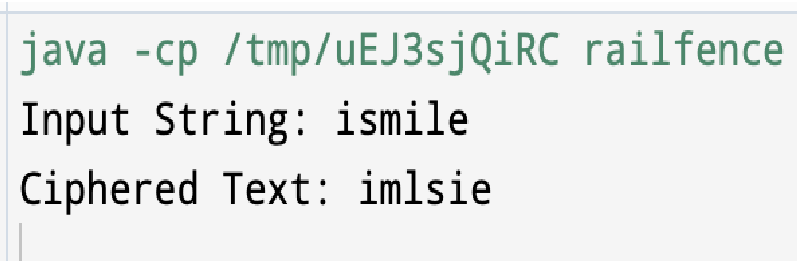


```
========== RESTART: /Users/krishnasingh/
 Enter the text to encrypt HELLO world
Encrypted: KHOOR zruog
Decrypted: HELLO world
```

Code for implementing transposition Cipher using Railfence Cipher

```
public class RailFence {
public static void main(String[] args) {
    String input = "ismile";
    String output = "";
    int len = input.length(); // Initialize 'len'
    System.out.println("Input String: " + input);

    for (int i = 0; i < len; i += 2) {
        output += input.charAt(i);
    }

    for (int i = 1; i < len; i += 2) {
        output += input.charAt(i);
    }

    System.out.println("Ciphered Text: " + output);
  }
  }
```

Output:



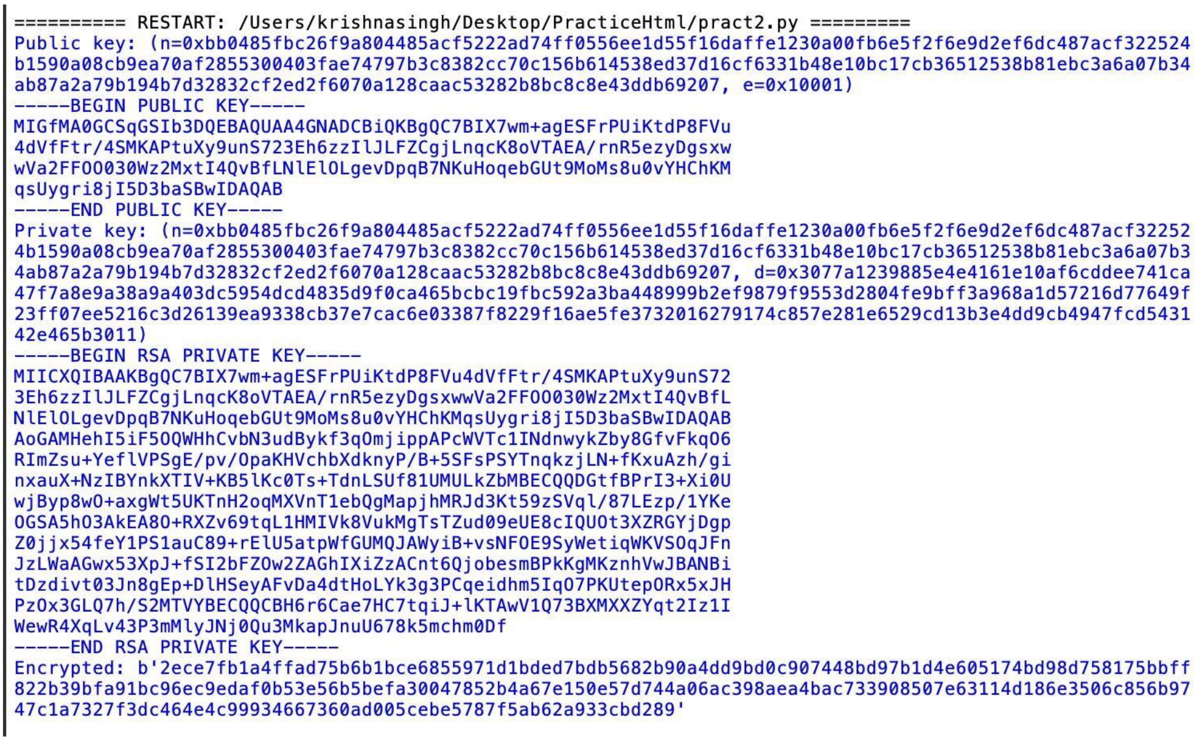
```
java -cp /tmp/uEJ3sjQiRC railfence
Input String: ismile
Ciphered Text: imlsie
```

Practical No.2

Aim: RSA Encryption and Decryption: Implement the RSA algorithm for public-key encryption and decryption, and explore its properties and security considerations.

```python
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP
import binascii
# Generate a new RSA key pair
keyPair = RSA.generate(1024)

# Extract the public key
pubKey = keyPair.publickey()
print(f"Public key: (n={hex(pubKey.n)}, e={hex(pubKey.e)})")

# Export the public key to a PEM format
pubKeyPEM = pubKey.exportKey()
print(pubKeyPEM.decode('ascii'))

# Extract the private key
privKey = keyPair
print(f"Private key: (n={hex(privKey.n)}, d={hex(privKey.d)})")

# Export the private key to a PEM format
privKeyPEM = privKey.exportKey()
print(privKeyPEM.decode('ascii'))

# Encryption
msg = b'SDSM College' # Convert the message to bytes
encryptor = PKCS1_OAEP.new(pubKey)
encrypted = encryptor.encrypt(msg)
print("Encrypted:", binascii.hexlify(encrypted))
```

Output:



```
========== RESTART: /Users/krishnasingh/Desktop/PracticeHtml/pract2.py =========
Public key: (n=0xbb0485fbc26f9a804485acf5222ad74ff0556ee1d55f16daffe1230a00fb6e5f2f6e9d2ef6dc487acf322524
b1590a08cb9ea70af2855300403fae74797b3c8382cc70c156b614538ed37d16cf6331b48e10bc17cb36512538b81ebc3a6a07b34
ab87a2a79b194b7d32832cf2ed2f6070a128caac53282b8bc8c8e43ddb69207, e=0x10001)
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC7BIX7wm+agESFrPUiKtdP8FVu
4dVfFtr/4SMKAPtuXy9unS723Eh6zzIlJLFZCgjLnqcK8oVTAEA/rnR5ezyDgsxw
wVa2FFO0030Wz2MxtI4QvBfLNlElOLgevDpqB7NKuHoqebGUt9MoMs8u0vYHChKM
qsUygri8jI5D3baSBwIDAQAB
-----END PUBLIC KEY-----
Private key: (n=0xbb0485fbc26f9a804485acf5222ad74ff0556ee1d55f16daffe1230a00fb6e5f2f6e9d2ef6dc487acf32252
4b1590a08cb9ea70af2855300403fae74797b3c8382cc70c156b614538ed37d16cf6331b48e10bc17cb36512538b81ebc3a6a07b3
4ab87a2a79b194b7d32832cf2ed2f6070a128caac53282b8bc8c8e43ddb69207, d=0x3077a1239885e4e4161e10af6cddee741ca
47f7a8e9a38a9a403dc5954dcd4835d9f0ca465bcbc19fbc592a3ba448999b2ef9879f9553d2804fe9bff3a968a1d57216d77649f
23ff07ee5216c3d26139ea9338cb37e7cac6e03387f8229f16ae5fe3732016279174c857e281e6529cd13b3e4dd9cb4947fcd5431
42e465b3011)
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQC7BIX7wm+agESFrPUiKtdP8FVu4dVfFtr/4SMKAPtuXy9unS72
3Eh6zzIlJLFZCgjLnqcK8oVTAEA/rnR5ezyDgsxwwVa2FFO0030Wz2MxtI4QvBfL
NlElOLgevDpqB7NKuHoqebGUt9MoMs8u0vYHChKMqsUygri8jI5D3baSBwIDAQAB
AoGAMHehI5iF5OQWHhCvbN3udBykf3qOmjippAPcWVTc1INdnwykZby8GfvFkqO6
RImZsu+YeflVPSgE/pv/OpaKHVchbXdknyP/B+5SFsPSYTnqkzjLN+fKxuAzh/gi
nxauX+NzIBYnkXTIV+KB5lKc0Ts+TdnLSUf81UMULkZbMBECQQDGtfBPrI3+Xi0U
wjByp8wO+axgWt5UKTnH2oqMXVnT1ebQgMapjhMRJd3Kt59zSVql/87LEzp/1YKe
OGSA5hO3AkEA8O+RXZv69tqL1HMIVk8VukMgTsTZud09eUE8cIQUOt3XZRGYjDgp
Z0jjx54feY1PS1auC89+rElU5atpWfGUMQJAWyiB+vsNFOE9SyWetiqWKVSOqJFn
JzLWaAGwx53XpJ+fSI2bFZOw2ZAGhIXiZzACnt6QjobesmBPkKgMKznhVwJBANBi
tDzdivt03Jn8gEp+DlHSeyAFvDa4dtHoLYk3g3PCqeidhm5IqO7PKUtepORx5xJH
PzOx3GLQ7h/S2MTVYBECQQCBH6r6Cae7HC7tqiJ+lKTAwV1Q73BXMXXZYqt2Iz1I
WewR4XqLv43P3mMlyJNj0Qu3MkapJnuU678k5mchm0Df
-----END RSA PRIVATE KEY-----
Encrypted: b'2ece7fb1a4ffad75b6b1bce6855971d1bded7bdb5682b90a4dd9bd0c907448bd97b1d4e605174bd98d758175bbff
822b39bfa91bc96ec9edaf0b53e56b5befa30047852b4a67e150e57d744a06ac398aea4bac733908507e63114d186e3506c856b97
47c1a7327f3dc464e4c99934667360ad005cebe5787f5ab62a933cbd289'
```

Practical No.3

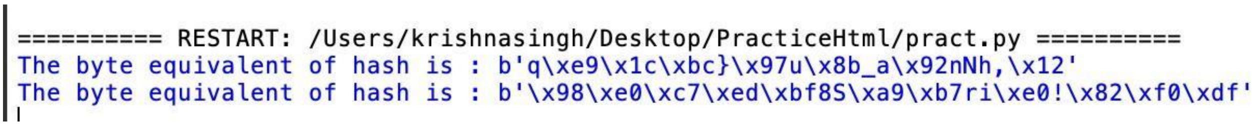
Aim: Message Authentication Codes:

Implement algorithms to generate and verify message authentication codes (MACs) for ensuring data integrity and authenticity.

Code for implementing MD5 Algorithm

```
import hashlib
result = hashlib.md5 (b'Priya')
result1 = hashlib.md5 (b'Diya')
# printing the equivalent byte value.
print ("The byte equivalent of hash is :", end ="")
print(result.digest ())
print ("The byte equivalent of hash is :", end ="")
print (result1.digest () )
```

Output:

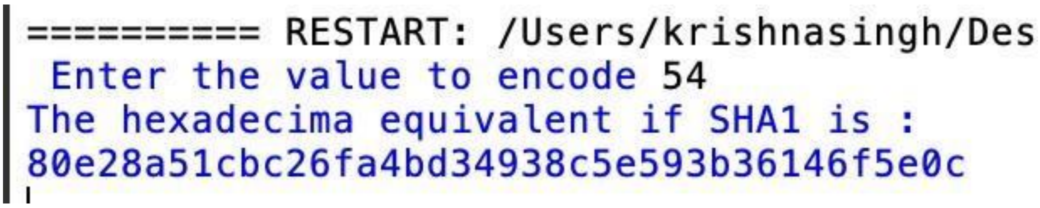


```
========== RESTART: /Users/krishnasingh/Desktop/PracticeHtml/pract.py ==========
The byte equivalent of hash is : b'q\xe9\x1c\xbc}\x97u\x8b_a\x92nNh,\x12'
The byte equivalent of hash is : b'\x98\xe0\xc7\xed\xbf8S\xa9\xb7ri\xe0!\x82\xf0\xdf'
```

Code for implementing SHA Algorithm

```
import hashlib
str = input("Enter the value to encode")
result = hashlib.sha1(str.encode())
print("The Hexadecimal Equivalent if SHA1 is: ")
print(result.hexdigest())
```

Output:



```
========== RESTART: /Users/krishnasingh/Des
 Enter the value to encode 54
The hexadecima equivalent if SHA1 is :
80e28a51cbc26fa4bd34938c5e593b36146f5e0c
```

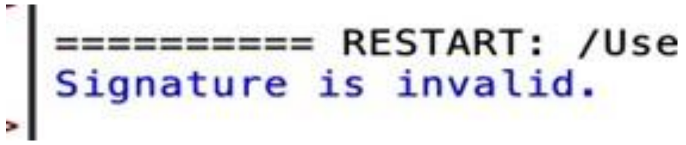
Practical No.4

Aim: Digital Signatures: Implement digital signature algorithms such as RSA-based signatures, and verify the integrity and authenticity of digitally signed messages.

Code: Python code for implementing SHA Algorithm

```python
from Crypto.PublicKey import RSA
from Crypto.Signature import pkcs1_15
from Crypto.Hash import SHA256

# Generate RSA key pair
key = RSA.generate(2048)
private_key = key.export_key()
public_key = key.publickey().export_key()

# Simulated document content
original_document = b"This is the original document content."
modified_document = b"This is the modified document content."

# Hash the document content
original_hash = SHA256.new(original_document)
modified_hash = SHA256.new(modified_document)

# Create a signature using the private key
signature = pkcs1_15.new(RSA.import_key(private_key)).sign(original_hash)

# Verify the signature using the public key with the modified content
try:
    pkcs1_15.new(RSA.import_key(public_key)).verify(modified_hash, signature)
    print("Signature is valid.")
except (ValueError, TypeError):
    print("Signature is invalid.")
```

Output:



```
========== RESTART: /Use
Signature is invalid.
```

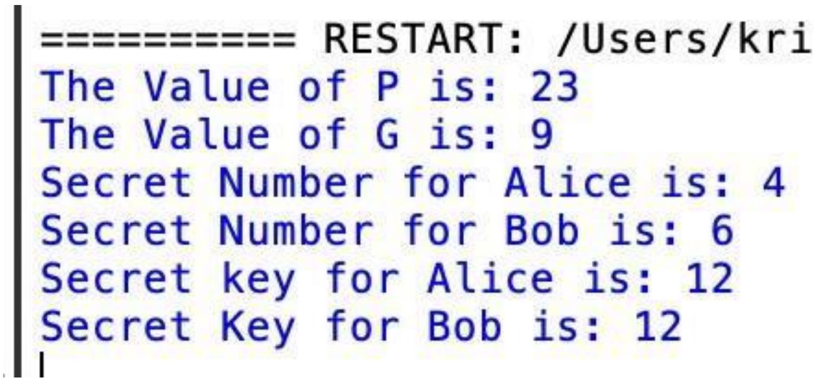
Practical No.5

Aim: Key Exchange using Diffie-Hellman:
Implement the Diffie-Hellman key exchange algorithm to securely exchange keys between two entities over an insecure network.

Code for implementing Diffie-Hellman Algorithm

```
from random import randint

if__name__== '__main__':
    P = 23
    G = 9

    print('The Value of P is: %d' % P)
    print('The Value of G is: %d' % G)
    a = 4
    print('Secret Number for Alice is: %d' % a)
    x = pow(G, a, P)  # Calculate Alice's public value
    b = 6
    print('Secret Number for Bob is: %d' % b)
    y = pow(G, b, P)  # Calculate Bob's public value
    ka = pow(y, a, P) # Calculate the shared secret key for Alice
    kb = pow(x, b, P) # Calculate the shared secret key for Bob

    print('Secret Key for Alice is: %d' % ka)
    print('Secret Key for Bob is: %d' % kb)
```

Output:



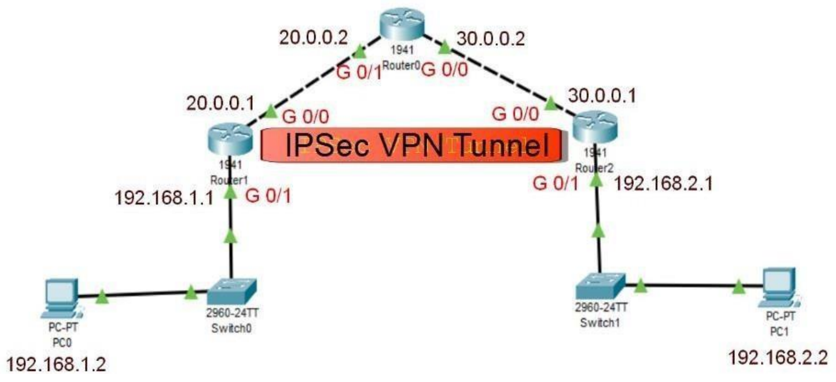
```
========== RESTART: /Users/kri
The Value of P is: 23
The Value of G is: 9
Secret Number for Alice is: 4
Secret Number for Bob is: 6
Secret key for Alice is: 12
Secret Key for Bob is: 12
```

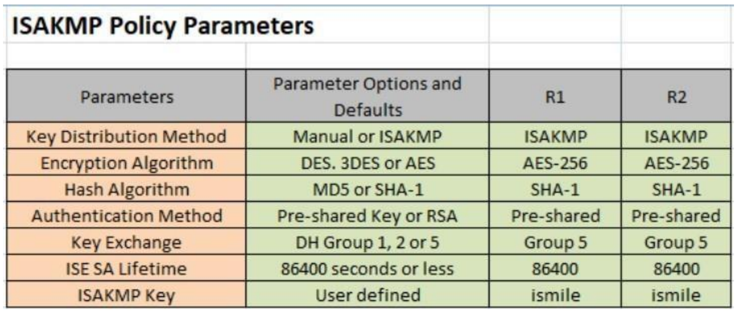
Practical No.6

Aim: IP Security (IPsec)

Configuration:

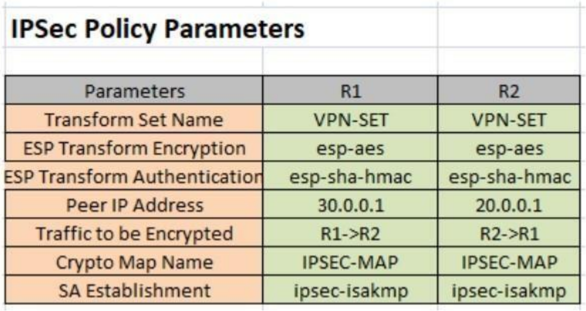
Configure IPsec on network devices to provide secure communication and protect against unauthorized access and attacks.





ISAKMP Policy Parameters

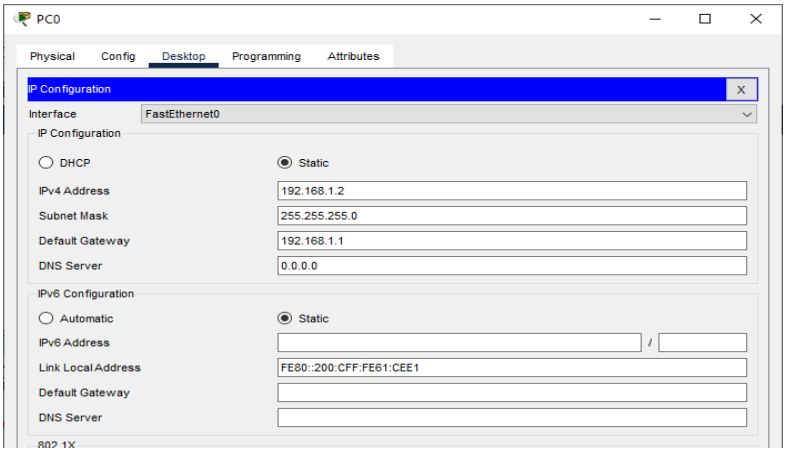
Parameters	Parameter Options and Defaults	R1	R2
Key Distribution Method	Manual or ISAKMP	ISAKMP	ISAKMP
Encryption Algorithm	DES. 3DES or AES	AES-256	AES-256
Hash Algorithm	MD5 or SHA-1	SHA-1	SHA-1
Authentication Method	Pre-shared Key or RSA	Pre-shared	Pre-shared
Key Exchange	DH Group 1, 2 or 5	Group 5	Group 5
ISE SA Lifetime	86400 seconds or less	86400	86400
ISAKMP Key	User defined	ismile	ismile



IPSec Policy Parameters

Parameters	R1	R2
Transform Set Name	VPN-SET	VPN-SET
ESP Transform Encryption	esp-aes	esp-aes
ESP Transform Authenticatior	esp-sha-hmac	esp-sha-hmac
Peer IP Address	30.0.0.1	20.0.0.1
Traffic to be Encrypted	R1->R2	R2->R1
Crypto Map Name	IPSEC-MAP	IPSEC-MAP
SA Establishment	ipsec-isakmp	ipsec-isakmp

Configuring PC0:



IP Configuration

Interface FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address 192.168.1.2

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address /

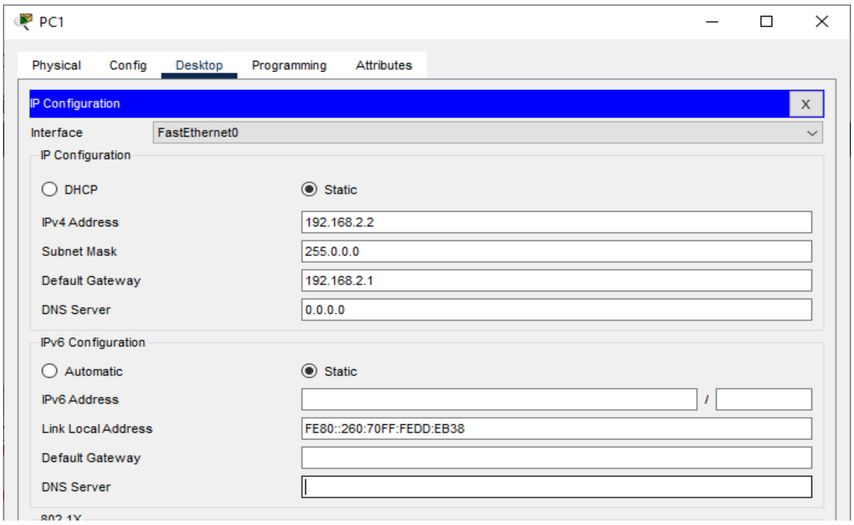
Link Local Address FE80::200:CFF:FE61:CEE1

Default Gateway

DNS Server

802.1X

Configuring PC1:



Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.2.2

Subnet Mask: 255.0.0.0

Default Gateway: 192.168.2.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::260:70FF:FEDD:EB38

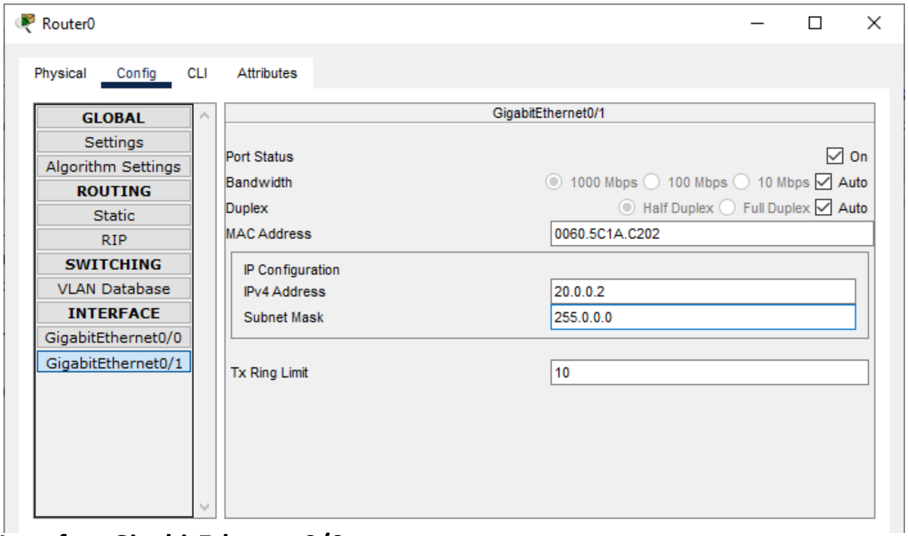
Default Gateway:

DNS Server:

802.1X

Configuring Router0:

Interface GigabitEthernet0/1:



GigabitEthernet0/1

Port Status ☑ On

Bandwidth ● 1000 Mbps ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ● Half Duplex ○ Full Duplex ☑ Auto

MAC Address: 0060.5C1A.C202

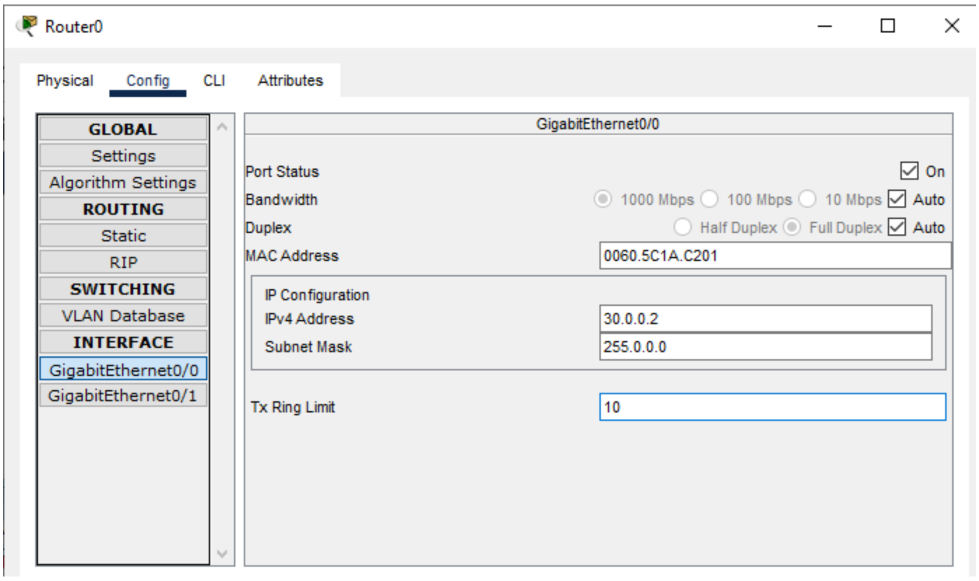
IP Configuration

IPv4 Address: 20.0.0.2

Subnet Mask: 255.0.0.0

Tx Ring Limit: 10

Interface GigabitEthernet0/0:



GigabitEthernet0/0

Port Status ☑ On

Bandwidth ● 1000 Mbps ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address: 0060.5C1A.C201

IP Configuration

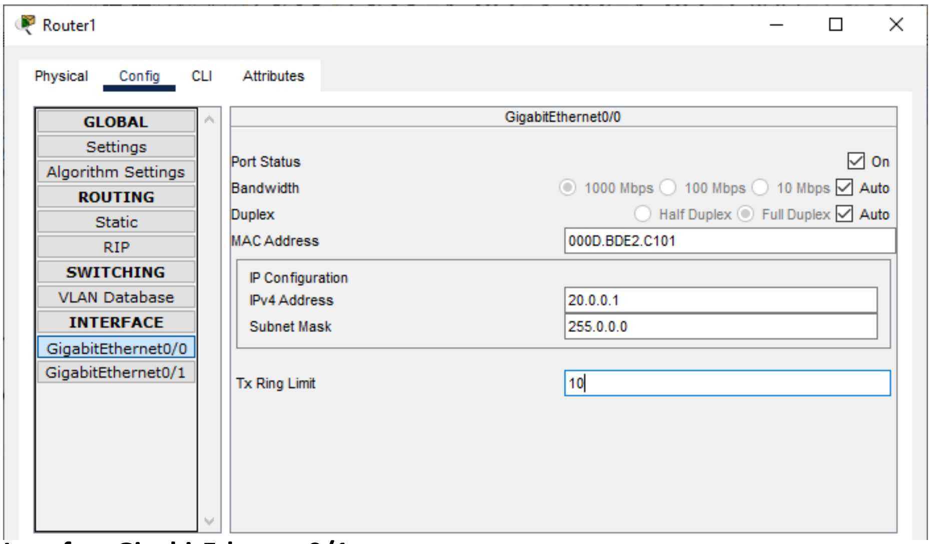
IPv4 Address: 30.0.0.2

Subnet Mask: 255.0.0.0

Tx Ring Limit: 10

Configuring Router1:

Interface GigabitEthernet0/1:



GigabitEthernet0/0

Port Status ☑ On

Bandwidth ● 1000 Mbps ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 000D.BDE2.C101

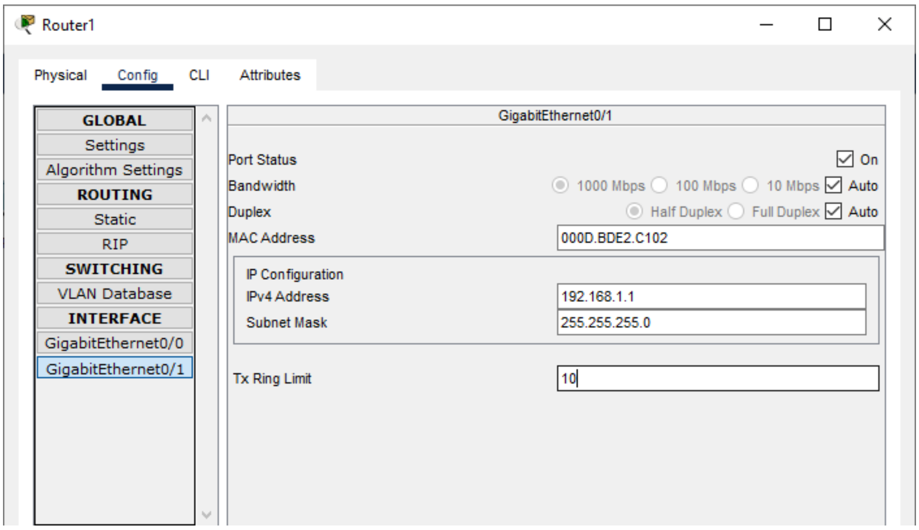
IP Configuration

IPv4 Address 20.0.0.1

Subnet Mask 255.0.0.0

Tx Ring Limit 10

Interface GigabitEthernet0/1:



GigabitEthernet0/1

Port Status ☑ On

Bandwidth ● 1000 Mbps ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ● Half Duplex ○ Full Duplex ☑ Auto

MAC Address 000D.BDE2.C102

IP Configuration

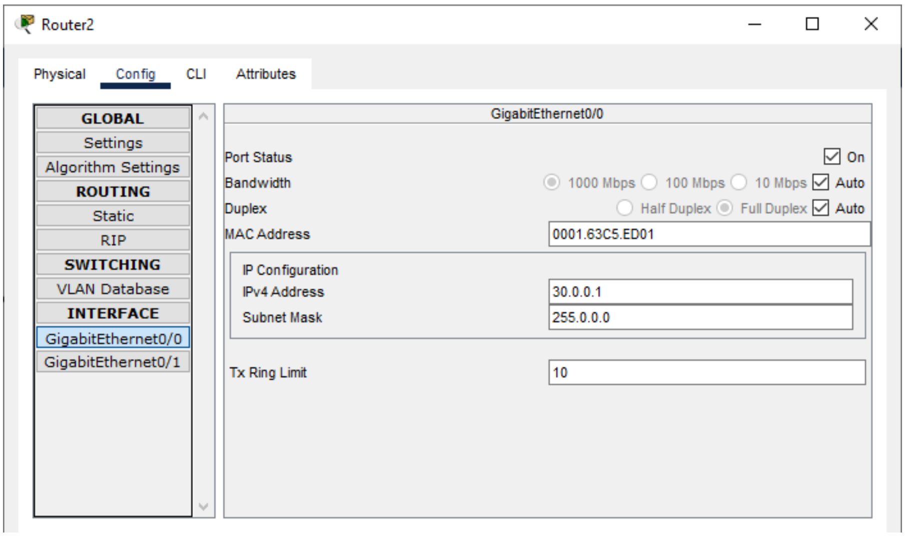
IPv4 Address 192.168.1.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Configuring Router2:

Interface GigabitEthernet0/0:



GigabitEthernet0/0

Port Status ☑ On

Bandwidth ● 1000 Mbps ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 0001.63C5.ED01

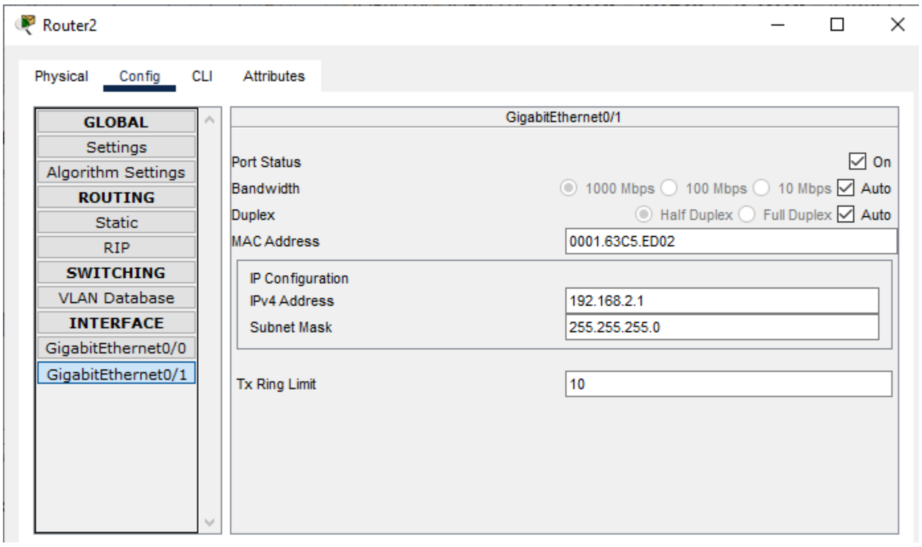
IP Configuration

IPv4 Address 30.0.0.1

Subnet Mask 255.0.0.0

Tx Ring Limit 10

Interface GigabitEthernet0/1:



GigabitEthernet0/1

Port Status ☑ On

Bandwidth ○ 1000 Mbps ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ○ Full Duplex ☑ Auto

MAC Address 0001.63C5.ED02

IP Configuration

IPv4 Address 192.168.2.1

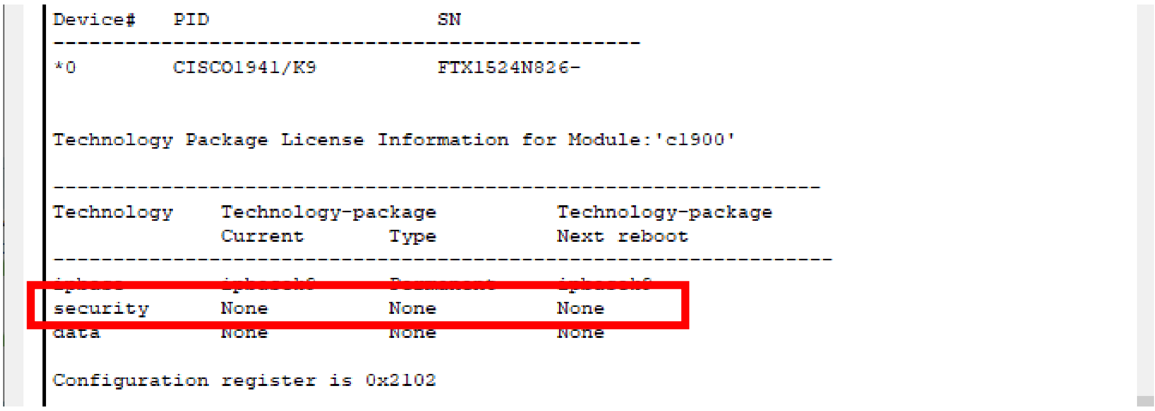
Subnet Mask 255.255.255.0

Tx Ring Limit 10

Checking and Enabling the Security features in Router R1 and R2:

Enter the following command in the CLI mode of Router1

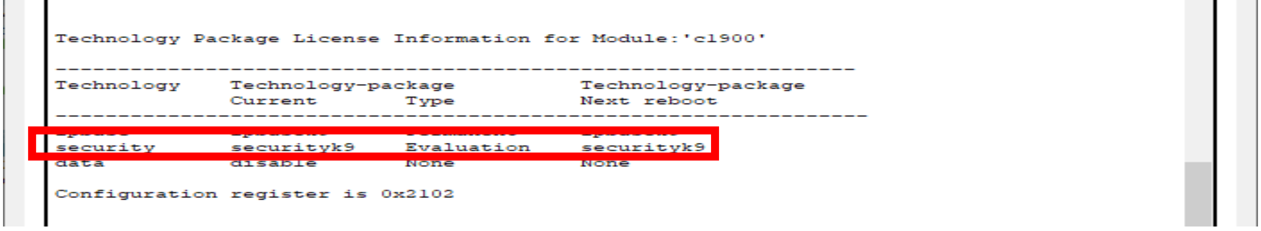
Router(config)#ip route 0.0.0.0 0.0.0.0 20.0.0.2
Router(config)#hostname R1
R1(config)#exit
R1#show version



```
Device#    PID                    SN
-------------------------------------------------
*0         CISCO1941/K9           FTX1524N826-


Technology Package License Information for Module:'c1900'

----------------------------------------------------------------
Technology    Technology-package           Technology-package
              Current       Type           Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent      ipbasek9
security      None          None           None
data          None          None           None

Configuration register is 0x2102
```

(We see that the security feature is not enabled, hence we need to enable the security packageR1#

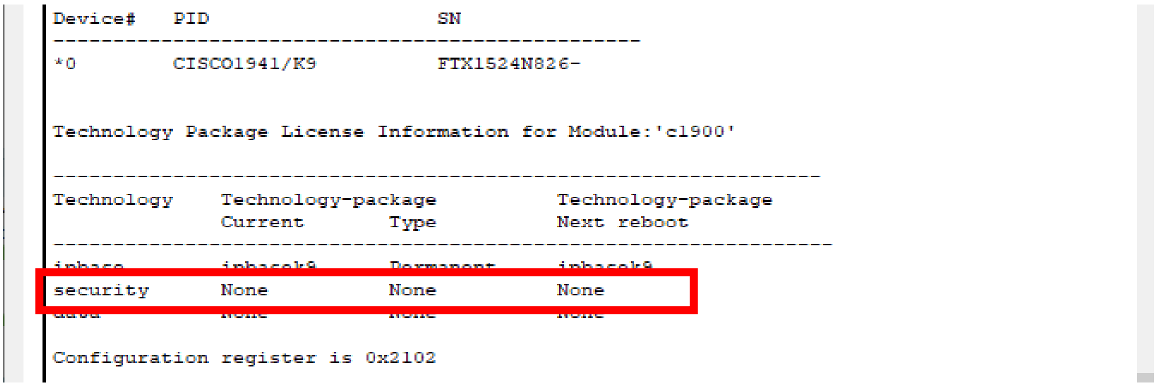
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
R1(config)#license boot module c1900 technology-package securityk9
R1(config)#exit
R1#
R1#copy runstartup-config
R1#reload
R1>enable
R1#show version
(The security package is enabled)



```
Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
------------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
data          disable       None          None

Configuration register is 0x2102
```

Enter the following command in the CLI mode of Router2

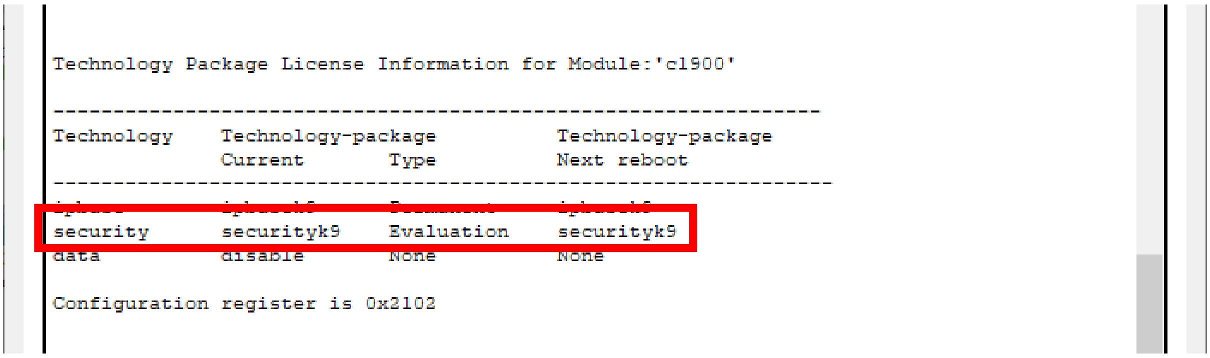
Router(config)#ip route 0.0.0.0 0.0.0.0 30.0.0.2
Router(config)#hostname R2
R2(config)#exit
R2#show version



```
Device#   PID                   SN
-------------------------------------------------
*0        CISCO1941/K9          FTX1524N826-


Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
------------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      None          None          None
data          None          None          None

Configuration register is 0x2102
```

(We see that the security feature is not enabled, hence we need to enable the security packageR2#

R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#
R2(config)#license boot module c1900 technology-package securityk9
R2(config)#exit
R2#
R2#copy run startup-
configR2#reload
R2>enable
R2#show version



```
Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
------------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
data          disable       None          None

Configuration register is 0x2102
```

(The security package is enabled)

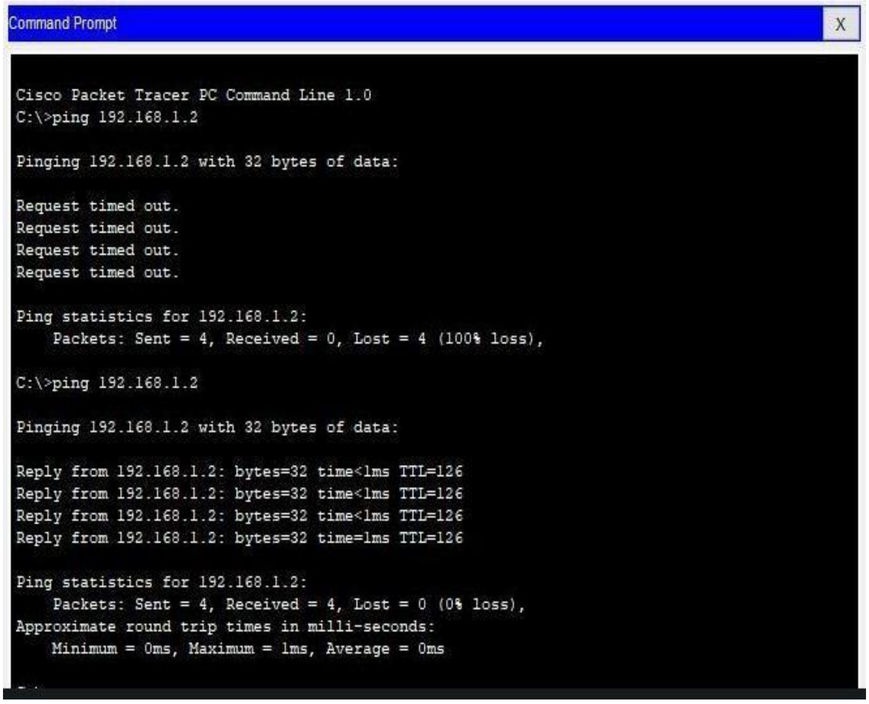
Enter the following command in the CLI mode of Router0

Router>enable Router#configure terminal
Router(config)#hostname R0
R0(config)#

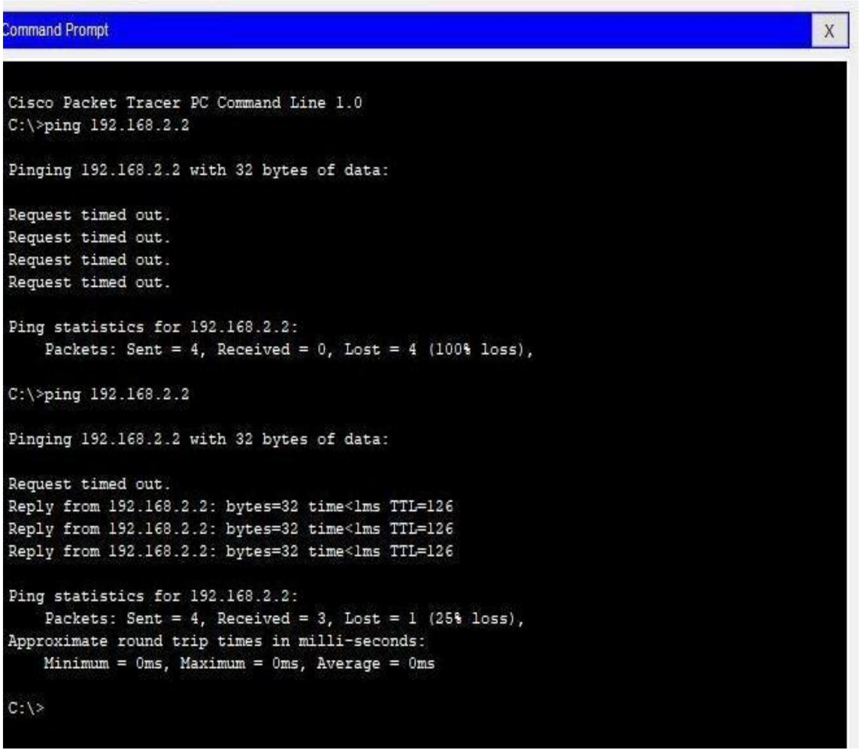
Defining the Hostname for all Routers and Configuring the Routers R1 and R2 for IPSec VPN tunnel

```
R1#configure terminal
R1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group
R1(config-isakmp)#exit
R1(config)#crypto isakmp key ismile address 30.0.0.1
R1(config)#crypto ipsec transform-set R1->R2 esp-aes 256 esp-sha-hmac
R1(config)#

R2#
R2#configure terminal
R2(config)#access-list 100 permit ip192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
R2(config)#crypto isakmp policy 10
R2(config-isakmp)#encryption aes 256
R2(config-isakmp)#authentication pre- share
R2(config-isakmp)#group 5
R2(config-isakmp)#exit
R2(config)#crypto isakmp key ismile address 20.0.0.1
R2(config)#crypto ipsec transform-set R2->R1 esp-aes 256 esp-sha-hmac
R2(config)#


R1>enable
R1#configure terminal
R1(config)#crypto map IPSEC-MAP 10 ipsec- isakmp
R1(config-crypto-map)#set peer 30.0.0.1
R1(config-crypto-map)#set pfs group5
R1(config-crypto-map)#set security-association lifetime seconds
86400R1(config-crypto-map)#set transform-set R1->R2
R1(config-crypto-map)#match address 100
R1(config-crypto-map)#exit
R1(config)#interface g0/0
R1(config-if)#crypto map IPSEC-MAP

R2>enable
R2#configure terminal
R2(config)#crypto map IPSEC-MAP 10 ipsec- isakmp
R2(config-crypto-map)#set peer 20.0.0.1
R2(config-crypto-map)#set pfs group5
R2(config-crypto-map)#set security-association lifetime seconds
86400R2(config-crypto-map)#set transform-set R2->R1
R2(config-crypto-map)#match address
100R2(config-crypto-map)#exit
R2(config)#interface g0/0
R2(config-if)#crypto map IPSEC-MAP
```

We verify the working of the IPSec VPN tunnel using the ping command as follows:
Output : 192.168.2.2) from PC1 and then PC1(192.168.1.2) from PC2



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```



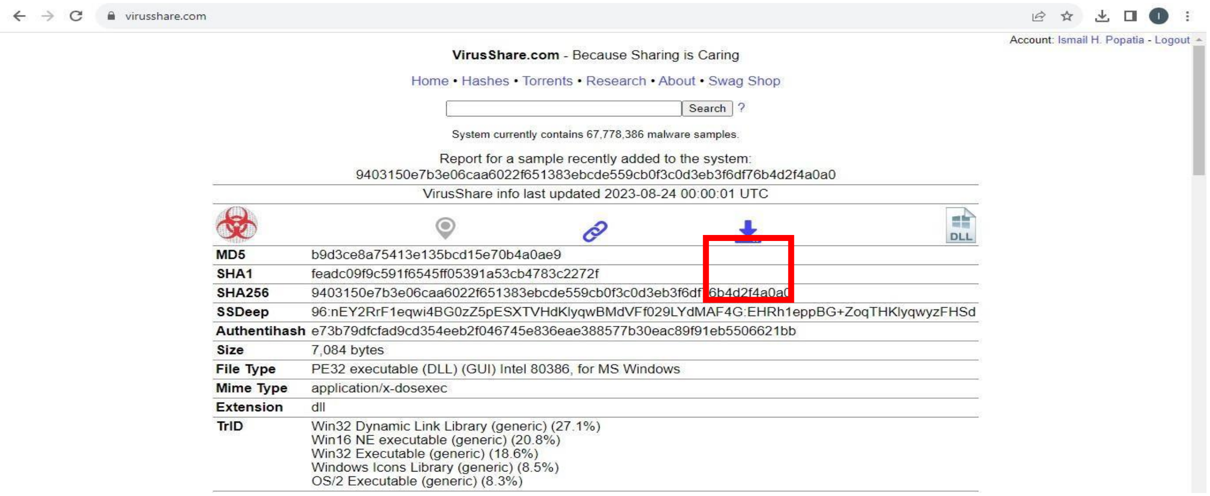
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Practical No.7

Aim: Malware Analysis and Detection

For analyzing the Malware, we need one. A clean sample of the Malware needs to be downloaded from a trusted website, the downloading and analysis is demonstrated by thefollowing steps:

1) We select the website www.virusshare.com for downloading the clean sample of Malware (an account needs to be created for the same). Any other source can be selected to download the Malware (clean sample and authorized site)



VirusShare.com - Because Sharing is Caring

Home • Hashes • Torrents • Research • About • Swag Shop

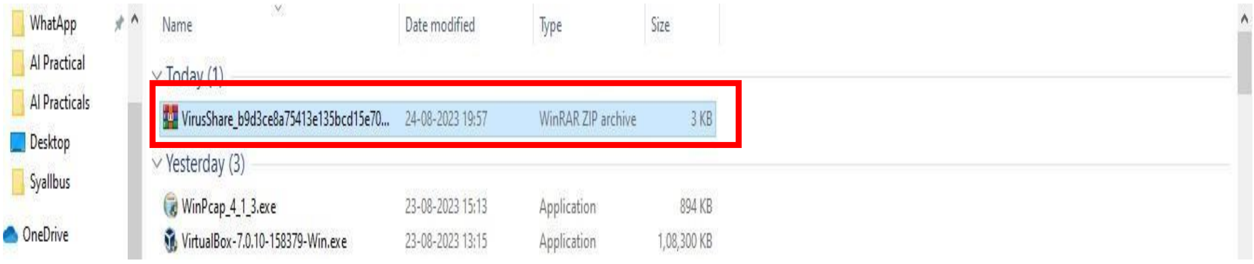
System currently contains 67,778,386 malware samples.

Report for a sample recently added to the system:
9403150e7b3e06caa6022f651383ebcde559cb0f3c0d3eb3f6df76b4d2f4a0a0

VirusShare info last updated 2023-08-24 00:00:01 UTC

MD5	b9d3ce8a75413e135bcd15e70b4a0ae9
SHA1	feadc09f9c591f6545ff05391a53cb4783c2272f
SHA256	9403150e7b3e06caa6022f651383ebcde559cb0f3c0d3eb3f6df 6b4d2f4a0a0
SSDeep	96:nEY2RrF1eqwi4BG0zZ5pESXTVHdKlyqwBMdVFf029LYdMAF4G:EHRh1eppBG+ZoqTHKlyqwyzFHSd
Authentihash	e73b79dfcfad9cd354eeb2f046745e836eae388577b30eac89f91eb5506621bb
Size	7,084 bytes
File Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Mime Type	application/x-dosexec
Extension	dll
TrID	Win32 Dynamic Link Library (generic) (27.1%) Win16 NE executable (generic) (20.8%) Win32 Executable (generic) (18.6%) Windows Icons Library (generic) (8.5%) OS/2 Executable (generic) (8.3%)

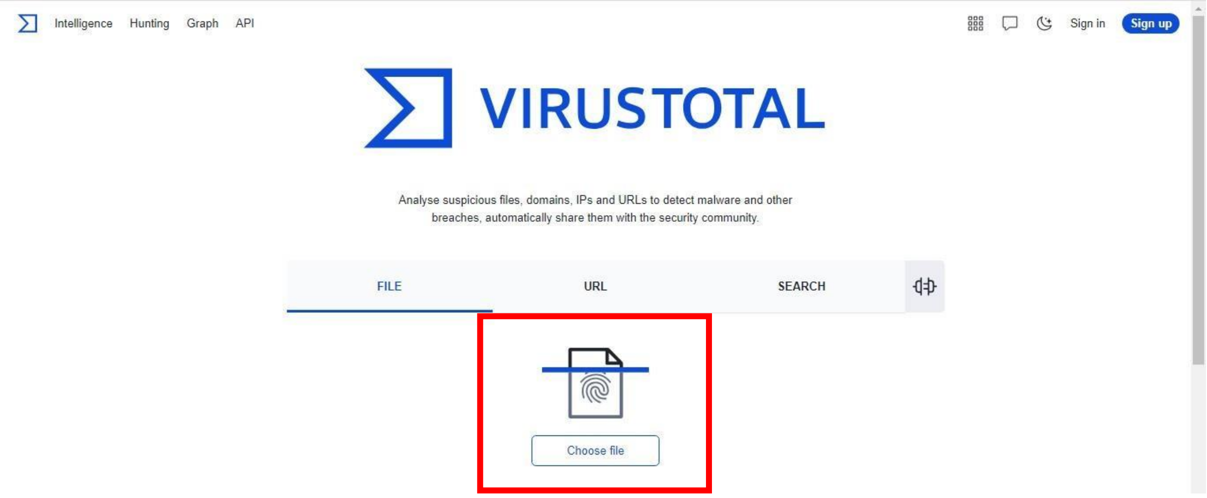
2) By clicking the above download icon the Malware gets downloaded in ZIP format.



Name	Date modified	Type	Size
Today (1)			
VirusShare_b9d3ce8a75413e135bcd15e70...	24-08-2023 19:57	WinRAR ZIP archive	3 KB
Yesterday (3)			
WinPcap_4_1_3.exe	23-08-2023 15:13	Application	894 KB
VirtualBox-7.0.10-158379-Win.exe	23-08-2023 13:15	Application	1,08,300 KB

3) For unzip the password is “infected”, there is no need to unzip the file, we create a folder “Malware” on desktop and save the file in the folder

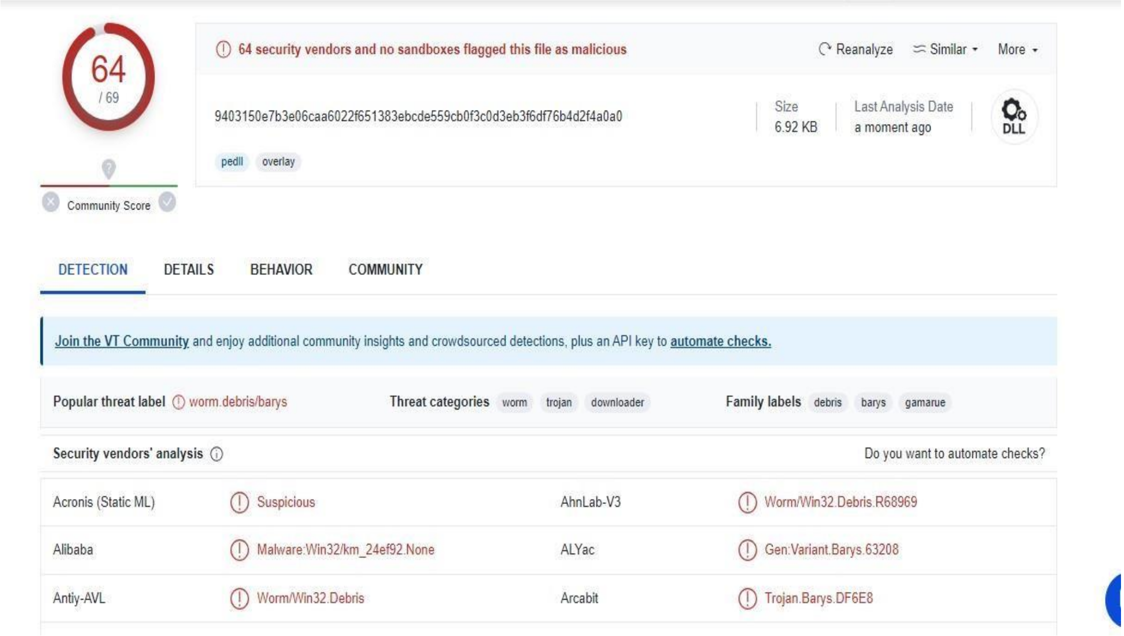
4) In order to analyze the Malware, we select the website www.virustotal.com



Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

5) Click on "Choose File" and select the file from the location (ZIP file will do, if asks for password enter infected)

6) We get the following after the upload is complete



64 security vendors and no sandboxes flagged this file as malicious

9403150e7b3e06caa6022f651383ebcde559cb0f3c0d3eb3f6df76b4d2f4a0a0

Size 6.92 KB

Last Analysis Date a moment ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

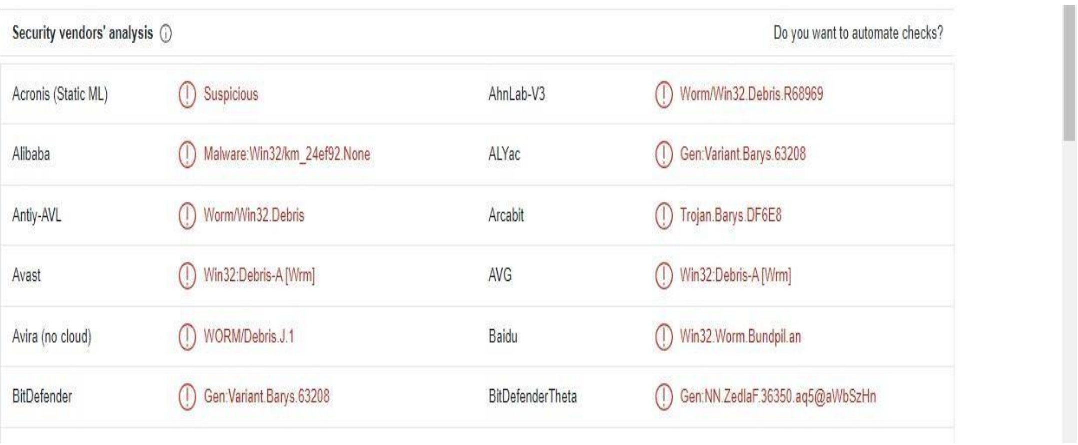
Popular threat label ⓘ worm.debris/barys   Threat categories worm trojan downloader   Family labels debris barys gamarue

Security vendors' analysis ⓘ   Do you want to automate checks?

Acronis (Static ML)	ⓘ Suspicious	AhnLab-V3	ⓘ Worm/Win32.Debris.R68969
Alibaba	ⓘ Malware:Win32/km_24ef92.None	ALYac	ⓘ Gen:Variant.Barys.63208
Antiy-AVL	ⓘ Worm/Win32.Debris	Arcabit	ⓘ Trojan.Barys.DF6E8

We interpret the following findings

a) 64 security vendors out of 69 flagged this file as malicious
The detection tab shows the threats-type which



Security vendors' analysis

Acronis (Static ML)	Suspicious	AhnLab-V3	Worm/Win32.Debris.R68969
Alibaba	Malware:Win32/km_24ef92.None	ALYac	Gen:Variant.Barys.63208
Antiy-AVL	Worm/Win32.Debris	Arcabit	Trojan.Barys.DF6E8
Avast	Win32:Debris-A [Wrm]	AVG	Win32:Debris-A [Wrm]
Avira (no cloud)	WORM/Debris.J.1	Baidu	Win32.Worm.Bundpil.an
BitDefender	Gen:Variant.Barys.63208	BitDefenderTheta	Gen:NN.ZedlaF.36350.aq5@aWbSzHn

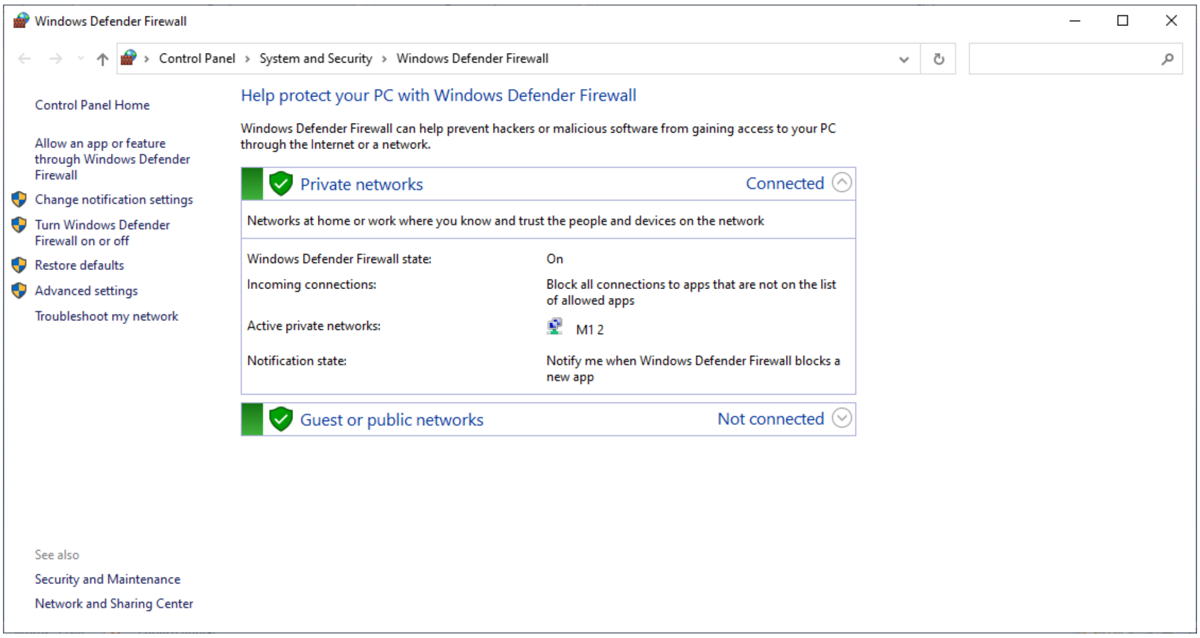
Practical No.8

Aim: Firewall Configuration and Rule-based Filtering:

Configure and test firewall rules to control network traffic, filter packets based on specified criteria, and protect network resources from unauthorized access.

Step 1: We access any website through the browser and confirm that the HTTP/HTTPS protocols are working.

Step 2: We open 'Windows Defender Firewall'



Windows Defender Firewall

Control Panel > System and Security > Windows Defender Firewall

Control Panel Home

Allow an app or feature through Windows Defender Firewall

Change notification settings

Turn Windows Defender 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 Defender Firewall

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

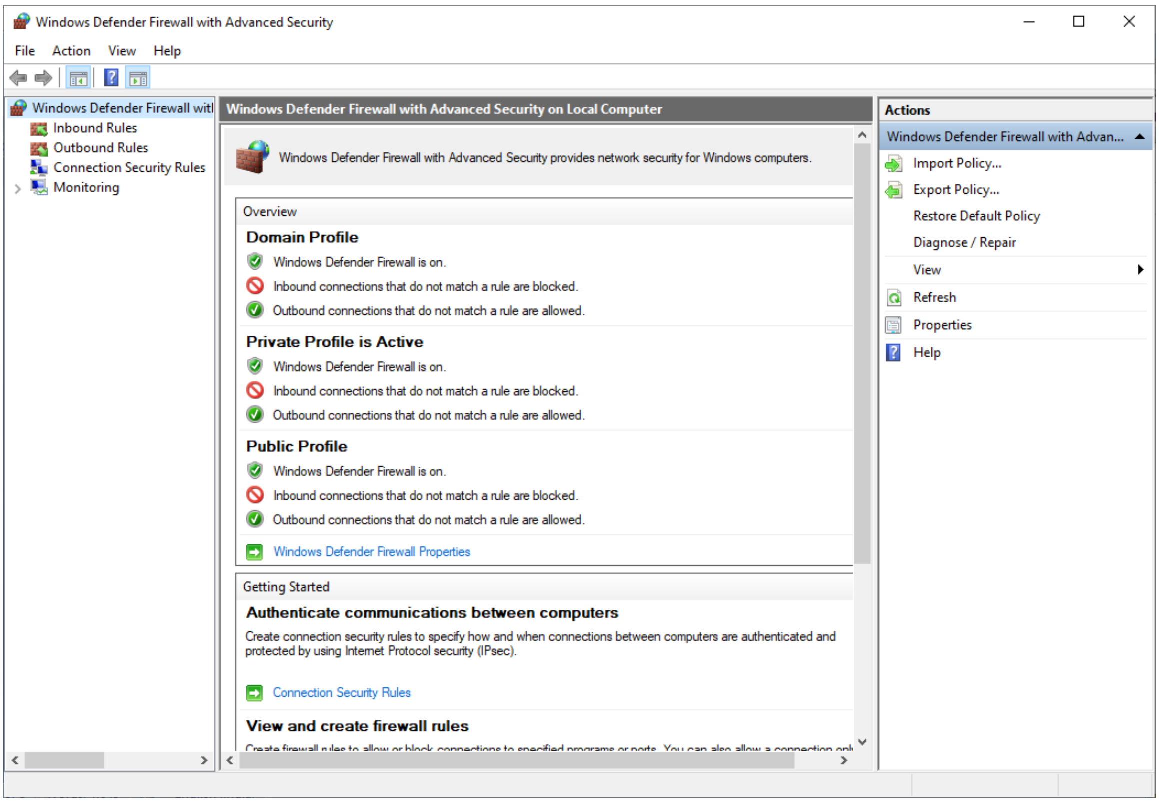
Private networks — Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active private networks:	M1 2
Notification state:	Notify me when Windows Defender Firewall blocks a new app

Guest or public networks — Not connected

Next we click on 'Advanced settings'



Windows Defender Firewall with Advanced Security

Windows Defender Firewall with Advanced Security on Local Computer

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

Overview

Domain Profile

- Windows Defender 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 is Active

- Windows Defender 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

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

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

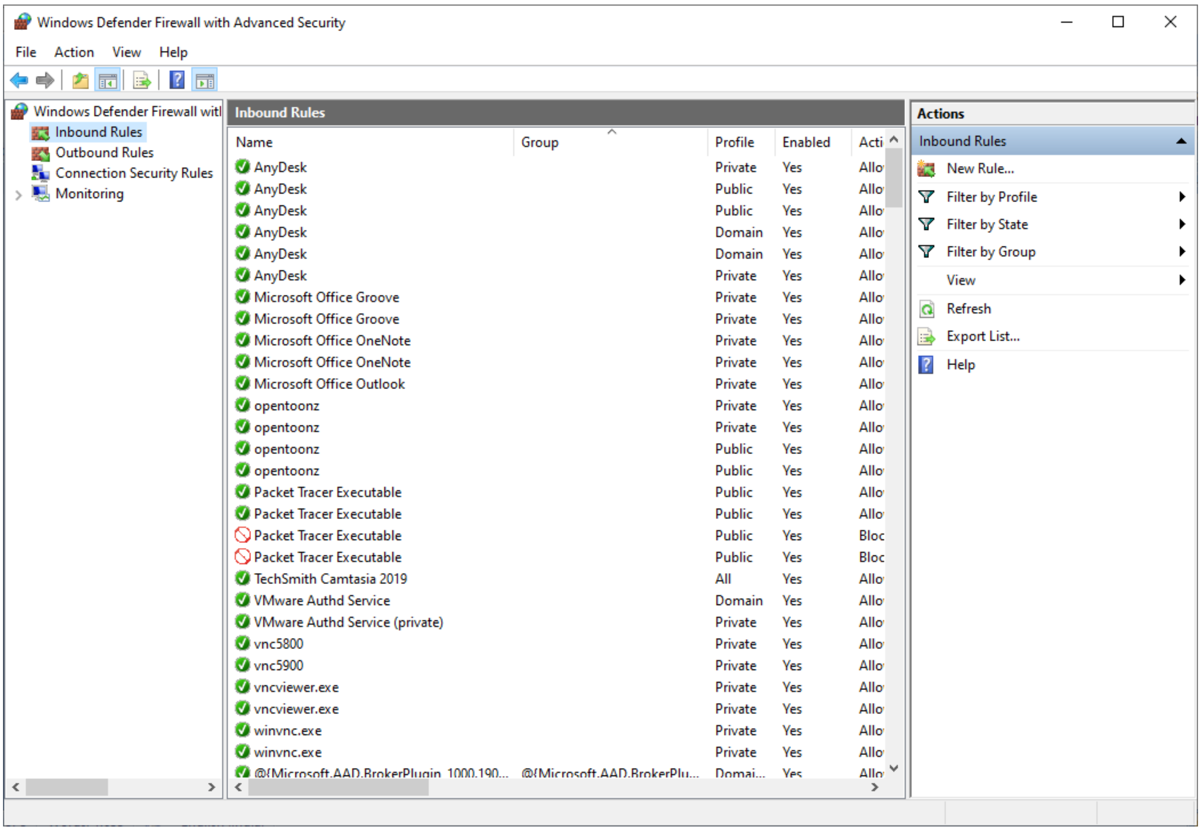
Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

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 onl

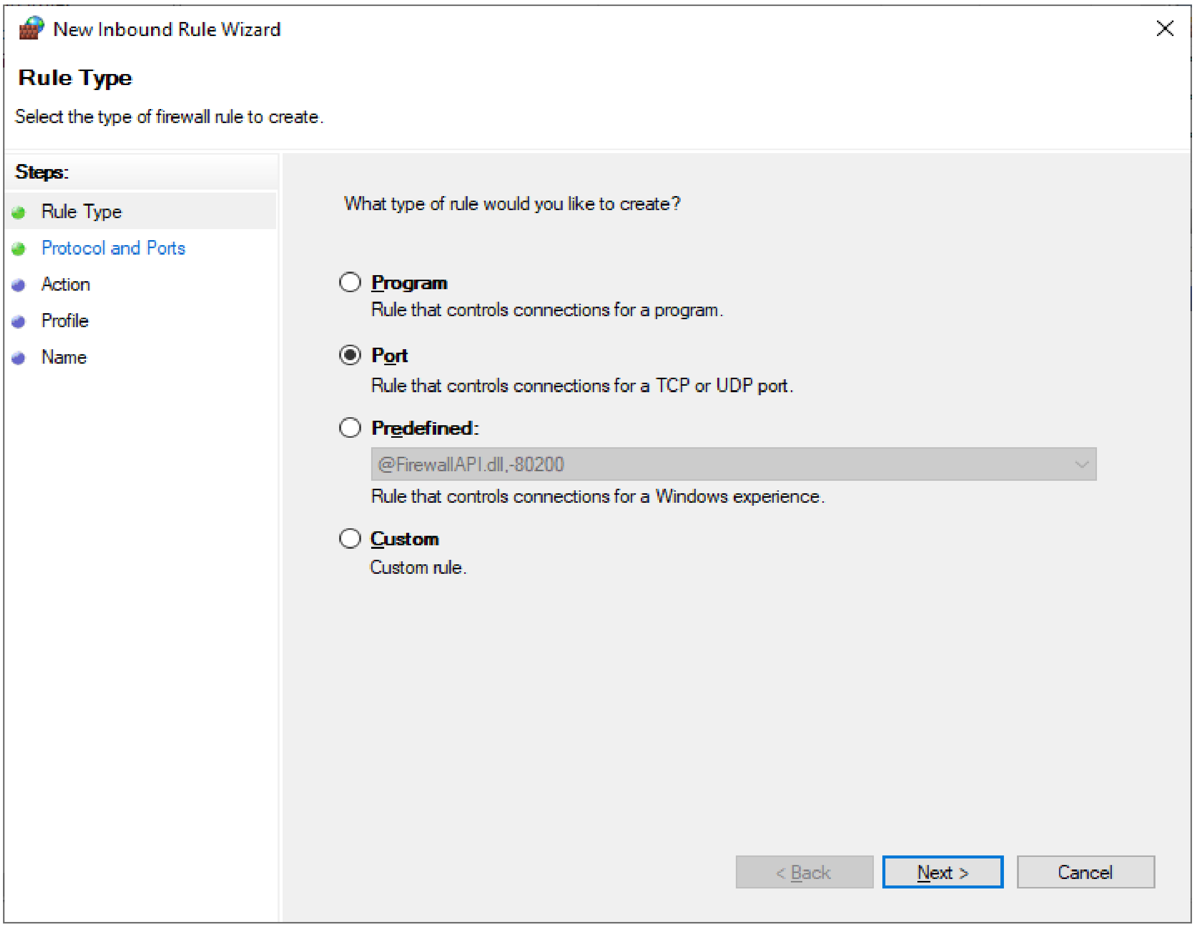
Next we click on ‘Inbound Rules’



Inbound Rules

Name	Group	Profile	Enabled	Acti
AnyDesk		Private	Yes	Allo
AnyDesk		Public	Yes	Allo
AnyDesk		Public	Yes	Allo
AnyDesk		Domain	Yes	Allo
AnyDesk		Domain	Yes	Allo
AnyDesk		Private	Yes	Allo
Microsoft Office Groove		Private	Yes	Allo
Microsoft Office Groove		Private	Yes	Allo
Microsoft Office OneNote		Private	Yes	Allo
Microsoft Office OneNote		Private	Yes	Allo
Microsoft Office Outlook		Private	Yes	Allo
opentoonz		Private	Yes	Allo
opentoonz		Private	Yes	Allo
opentoonz		Public	Yes	Allo
opentoonz		Public	Yes	Allo
Packet Tracer Executable		Public	Yes	Allo
Packet Tracer Executable		Public	Yes	Allo
Packet Tracer Executable		Public	Yes	Bloc
Packet Tracer Executable		Public	Yes	Bloc
TechSmith Camtasia 2019		All	Yes	Allo
VMware Authd Service		Domain	Yes	Allo
VMware Authd Service (private)		Private	Yes	Allo
vnc5800		Private	Yes	Allo
vnc5900		Private	Yes	Allo
vncviewer.exe		Private	Yes	Allo
vncviewer.exe		Private	Yes	Allo
winvnc.exe		Private	Yes	Allo
winvnc.exe		Private	Yes	Allo
@{Microsoft.AAD.BrokerPlugin_1000.190...	@{Microsoft.AAD.BrokerPlu...	Domai...	Yes	Allo

Then click on ‘New Rule’



Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

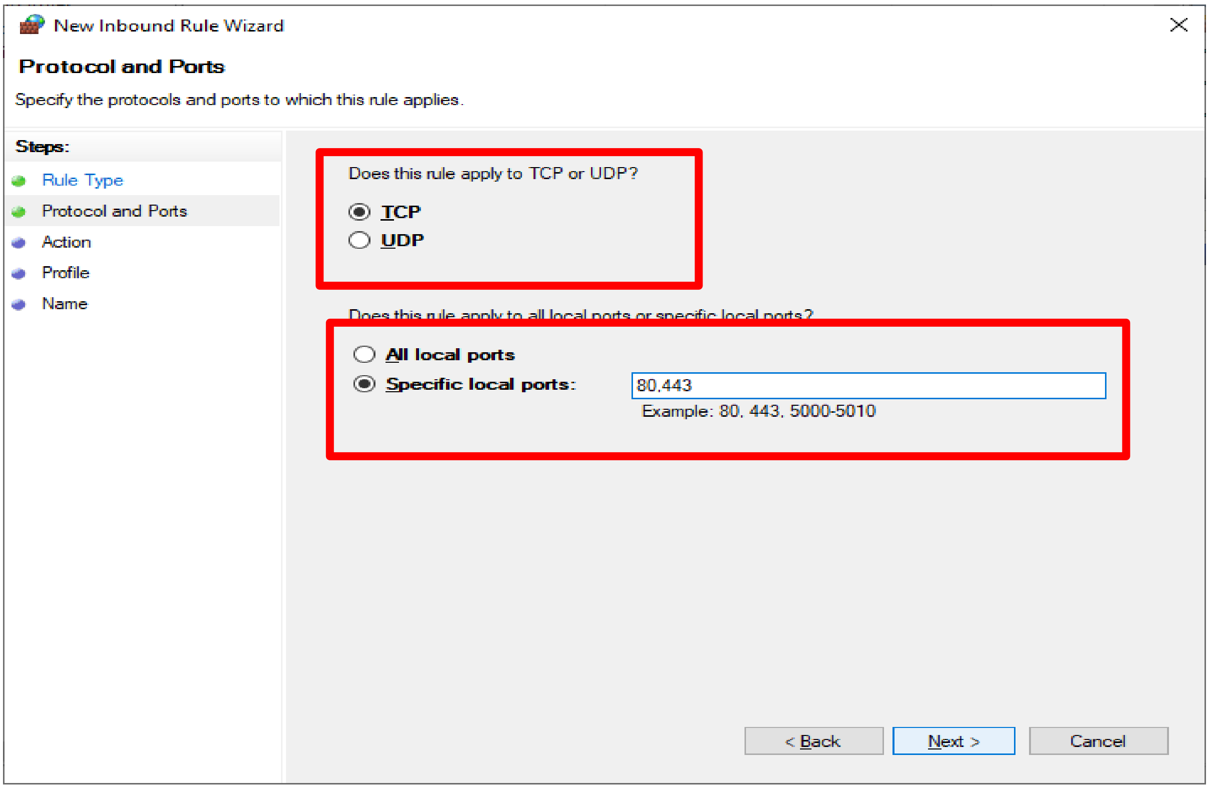
○ **Program**
Rule that controls connections for a program.

● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
@FirewallAPI.dll,-80200
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

Select the radio button 'Port' and click 'Next' and enter the following



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

● TCP

○ UDP

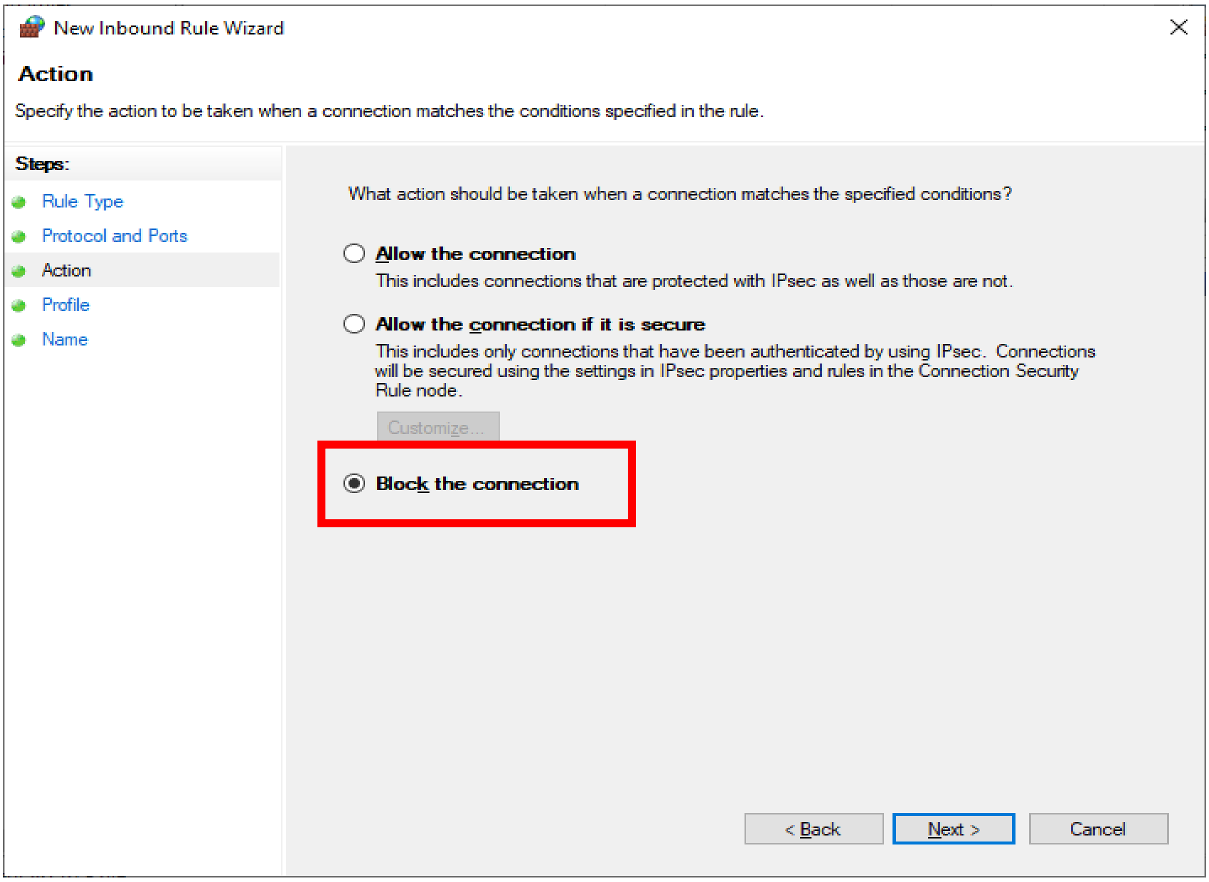
Does this rule apply to all local ports or specific local ports?

○ All local ports

● Specific local ports: 80,443

Example: 80, 443, 5000-5010

AZer next, we need to finalise the rule



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

○ Allow the connection

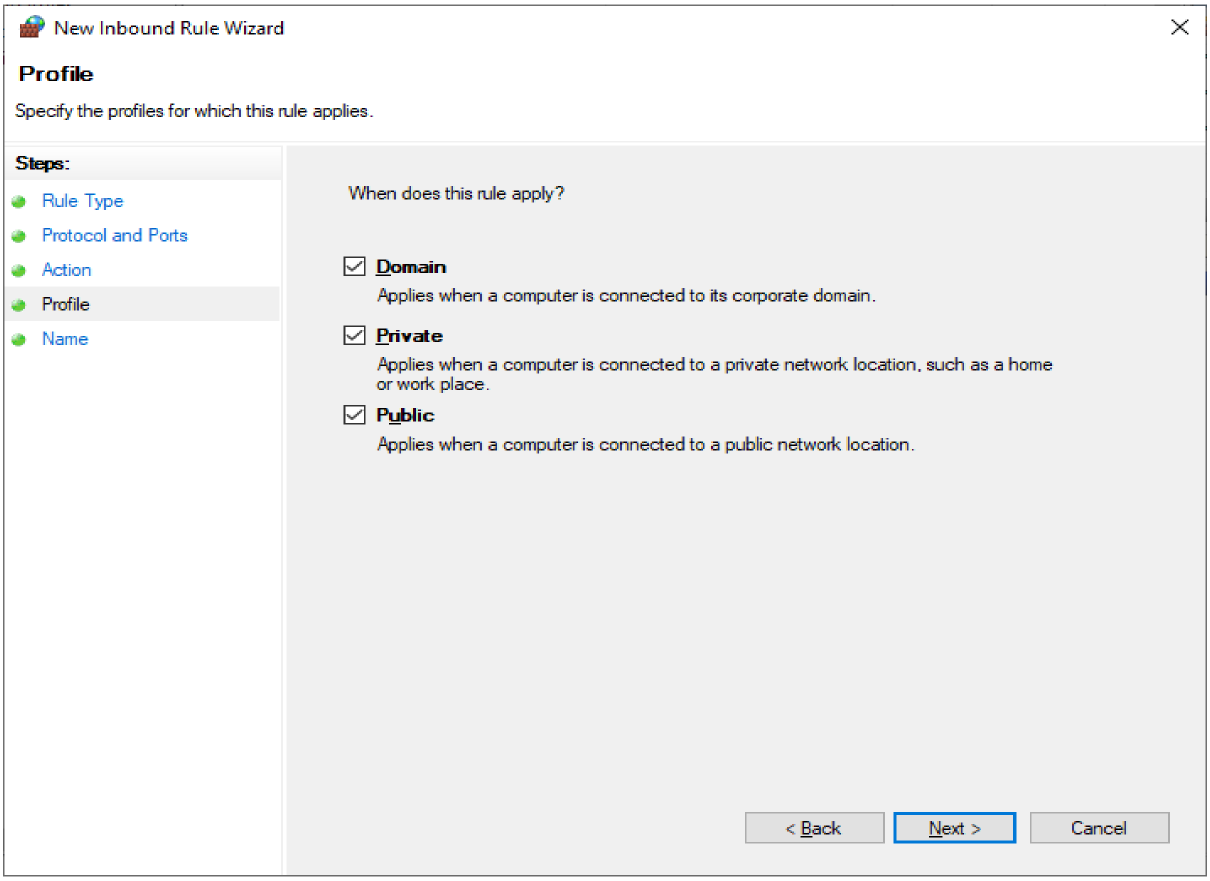
This includes connections that are protected with IPsec as well as those are not.

○ Allow the connection if it is secure

This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

● Block the connection

Click ‘Next’ and we get the following



New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

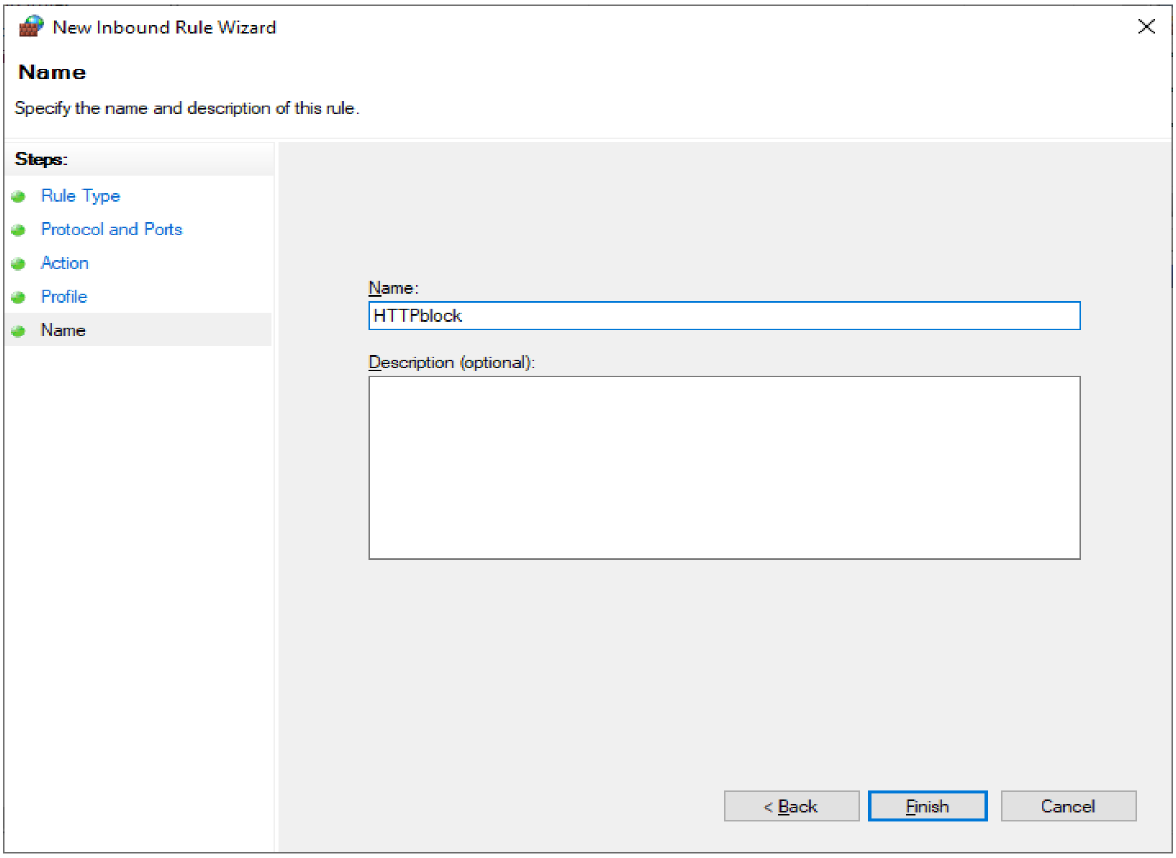
When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☑ **Public**
Applies when a computer is connected to a public network location.

AZer clicking the ‘Next’ button we need to name the rule and click finish



New Inbound Rule Wizard

Name

Specify the name and description of this rule.

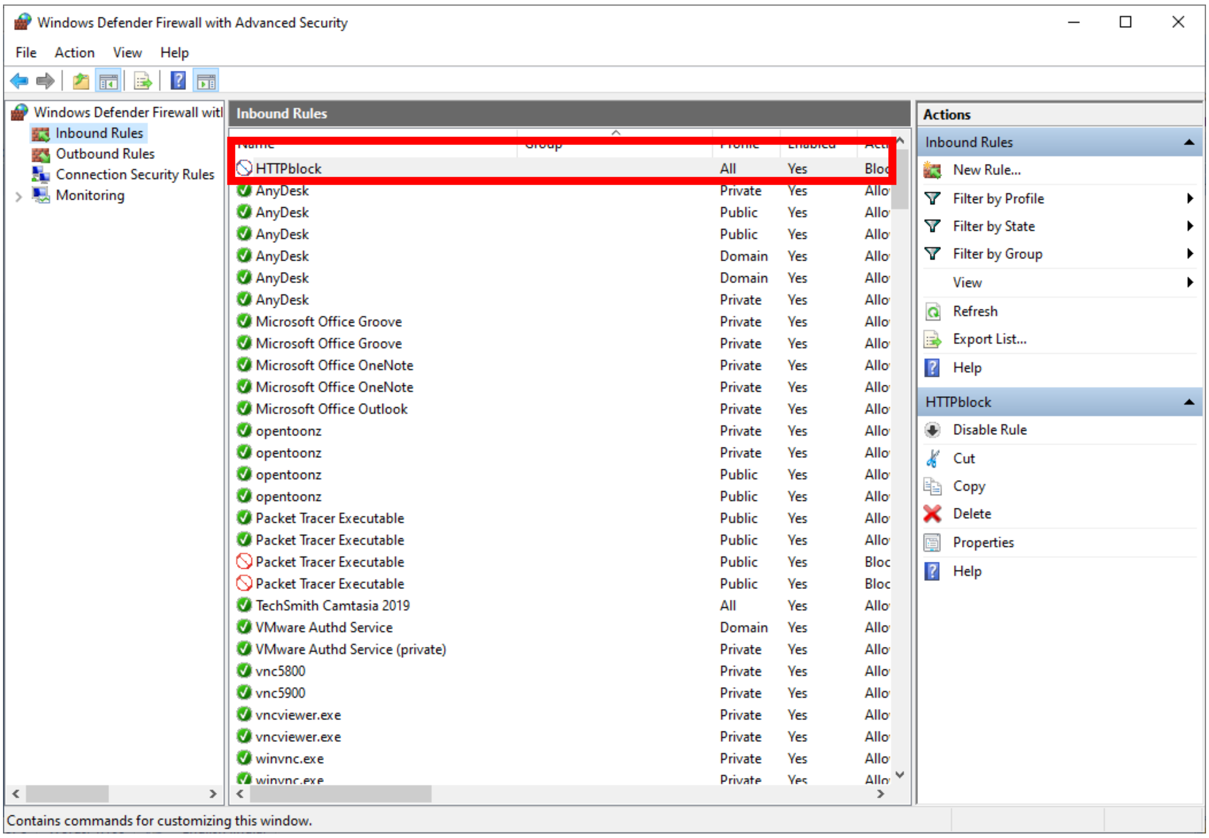
Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Name: HTTPblock

Description (optional):

The Inbound rule is added

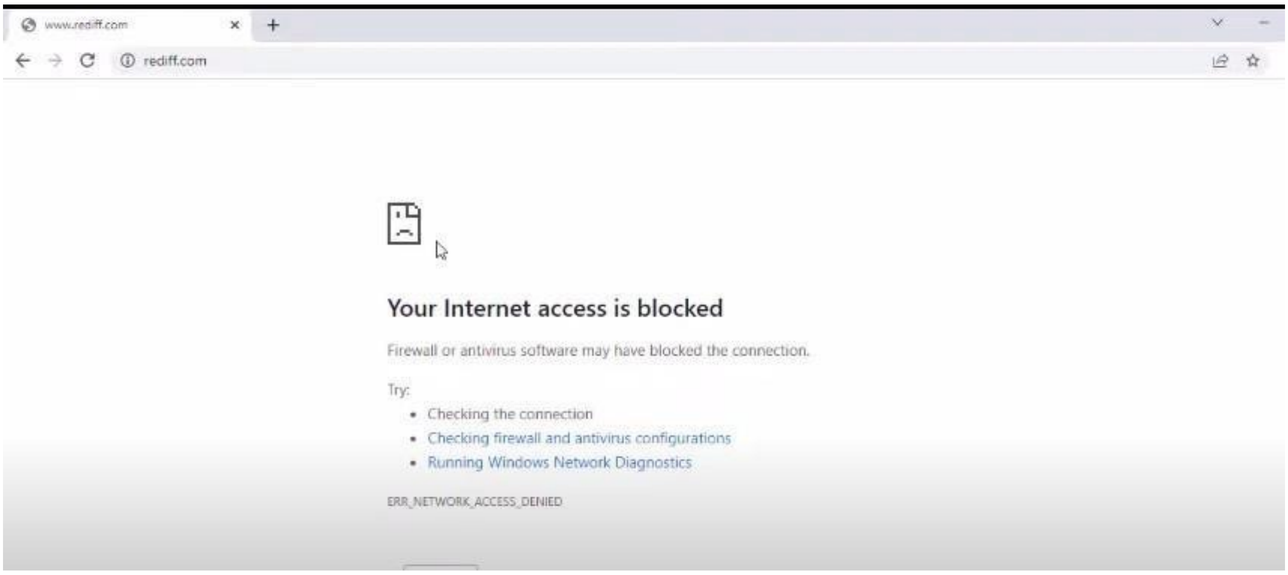


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall wit
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules

Name	Group	Profile	Enabled	Acti
HTTPblock		All	Yes	Bloc
AnyDesk		Private	Yes	Allo
AnyDesk		Public	Yes	Allo
AnyDesk		Public	Yes	Allo
AnyDesk		Domain	Yes	Allo
AnyDesk		Domain	Yes	Allo
AnyDesk		Private	Yes	Allo
Microsoft Office Groove		Private	Yes	Allo
Microsoft Office Groove		Private	Yes	Allo
Microsoft Office OneNote		Private	Yes	Allo
Microsoft Office OneNote		Private	Yes	Allo
Microsoft Office Outlook		Private	Yes	Allo
opentoonz		Private	Yes	Allo
opentoonz		Private	Yes	Allo
opentoonz		Public	Yes	Allo
opentoonz		Public	Yes	Allo
Packet Tracer Executable		Public	Yes	Allo
Packet Tracer Executable		Public	Yes	Allo
Packet Tracer Executable		Public	Yes	Bloc
Packet Tracer Executable		Public	Yes	Bloc
TechSmith Camtasia 2019		All	Yes	Allo
VMware Authd Service		Domain	Yes	Allo
VMware Authd Service (private)		Private	Yes	Allo
vnc5800		Private	Yes	Allo
vnc5900		Private	Yes	Allo
vncviewer.exe		Private	Yes	Allo
vncviewer.exe		Private	Yes	Allo
winvnc.exe		Private	Yes	Allo
winvnc.exe		Private	Yes	Allo

Contains commands for customizing this window.

We repeat all the above steps for creating ‘Outbound Rules’, and then try to access the internet. We see that the accessed is blocked



Your Internet access is blocked

Firewall or antivirus software may have blocked the connection.

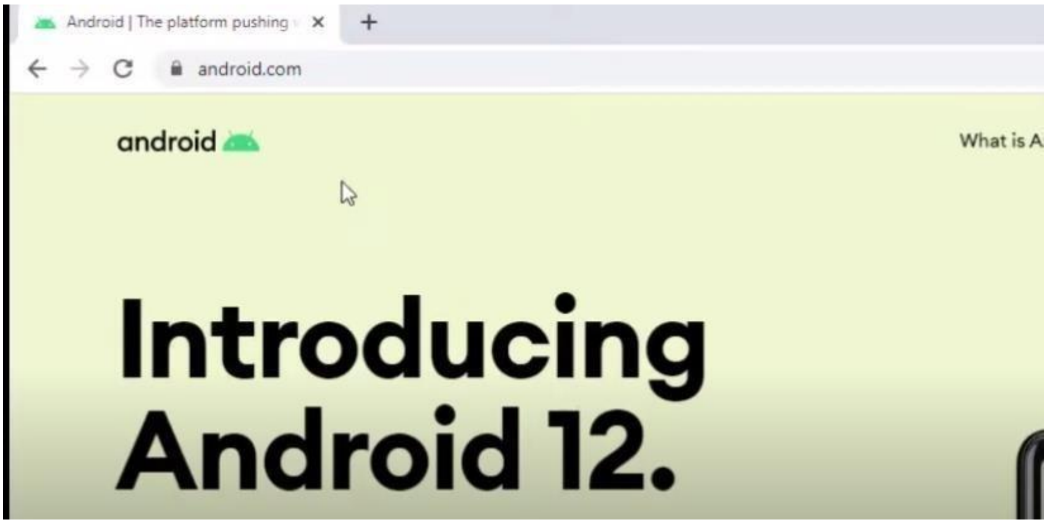
Try:

- Checking the connection
- Checking firewall and antivirus configurations
- Running Windows Network Diagnostics

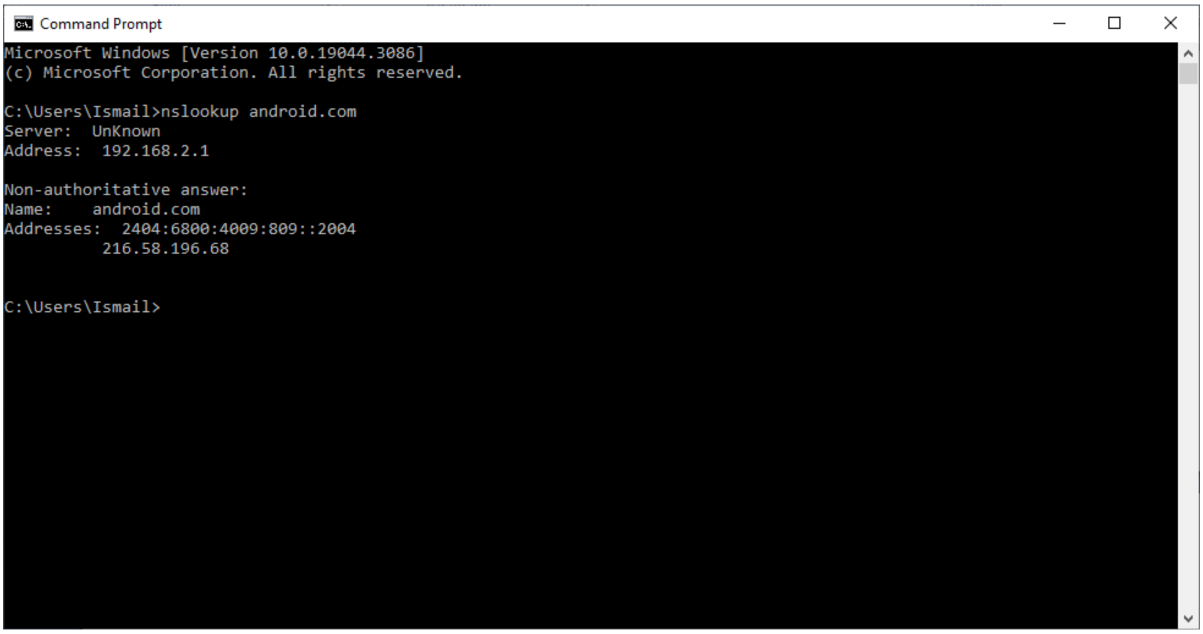
ERR_NETWORK_ACCESS_DENIED

Part 2: Blocking the website www.android.com

We open the browser and access the website, which is now accessible



We find the IP addresses of the website using the following command

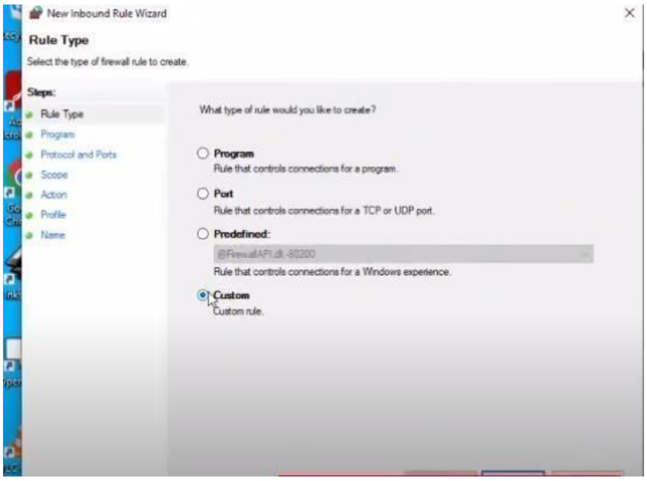


```
Microsoft Windows [Version 10.0.19044.3086]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Ismail>nslookup android.com
Server:  UnKnown
Address:  192.168.2.1

Non-authoritative answer:
Name:    android.com
Addresses:  2404:6800:4009:809::2004
          216.58.196.68


C:\Users\Ismail>
```

We save the IP addresses

IPv4	216.58.196.68
IPv6	2404:6800:4009:809::2004

We open the windows Firewall settings and apply the Inbound Rule



Rule Type

Select the type of firewall rule to create.

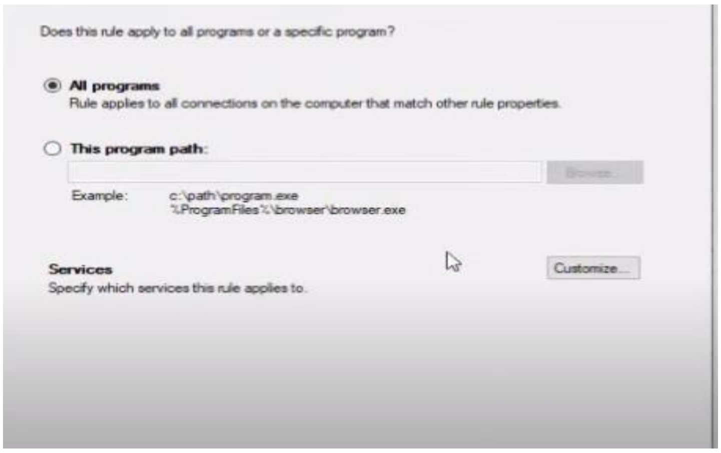
What type of rule would you like to create?

○ Program
Rule that controls connections for a program.

○ Port
Rule that controls connections for a TCP or UDP port.

○ Predefined:
@FirewallAPI.dll,-80200
Rule that controls connections for a Windows experience.

● Custom
Custom rule.



Does this rule apply to all programs or a specific program?

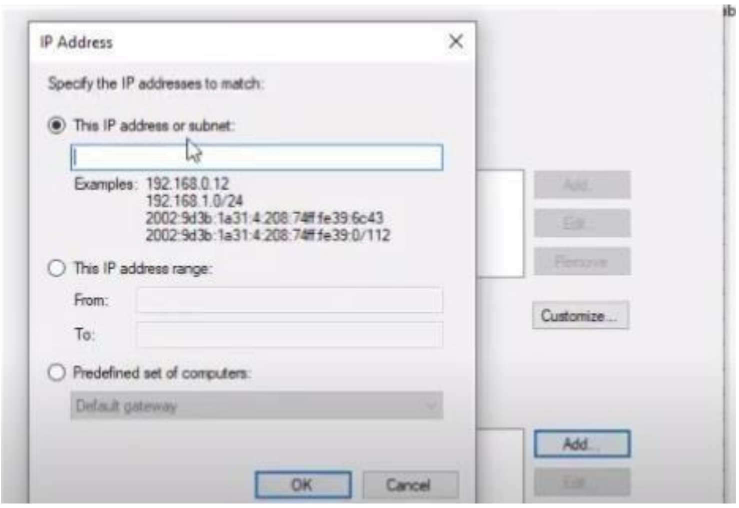
● All programs
Rule applies to all connections on the computer that match other rule properties.

○ This program path:

Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

Services
Specify which services this rule applies to.

Insert the IP addresses both IPv4 and IPv6



Specify the IP addresses to match:

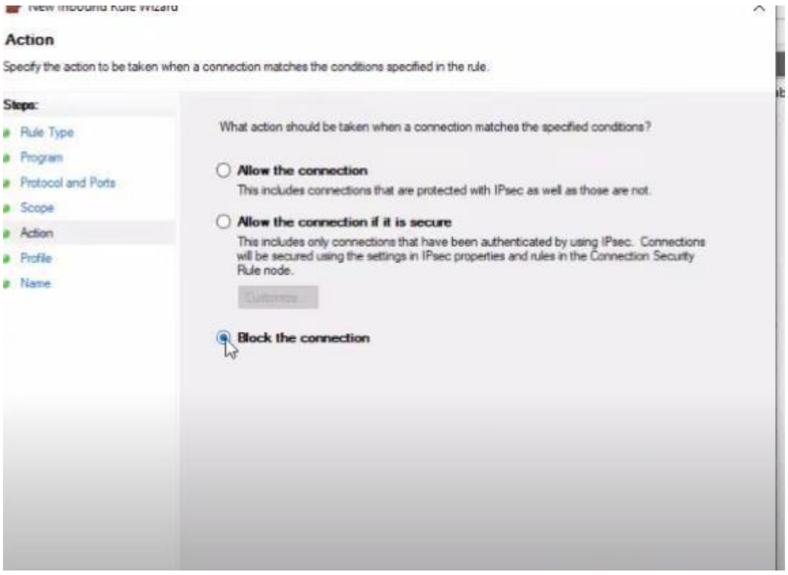
● This IP address or subnet:

Examples: 192.168.0.12
192.168.1.0/24
2002:9d3b:1a31:4:208:74ff:fe39:6c43
2002:9d3b:1a31:4:208:74ff:fe39:0/112

○ This IP address range:
From:
To:

○ Predefined set of computers:
Default gateway

Select Block connection



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

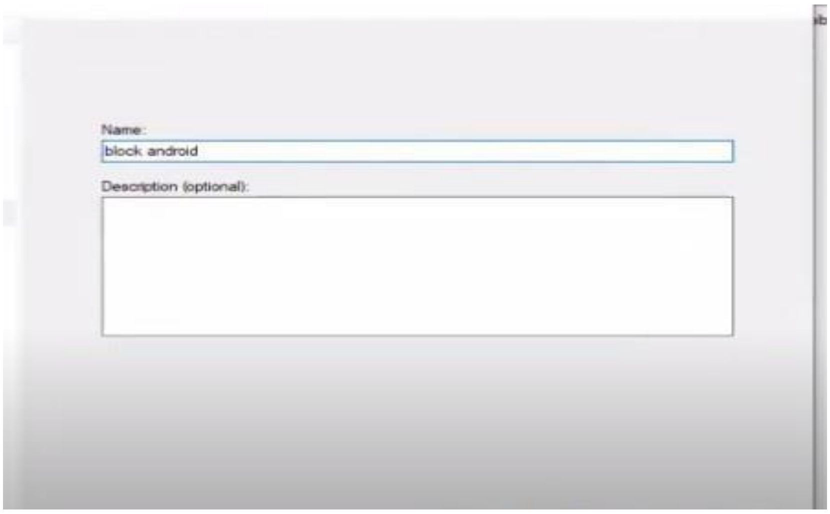
What action should be taken when a connection matches the specified conditions?

○ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

● **Block the connection**

Provide a suitable name and finish

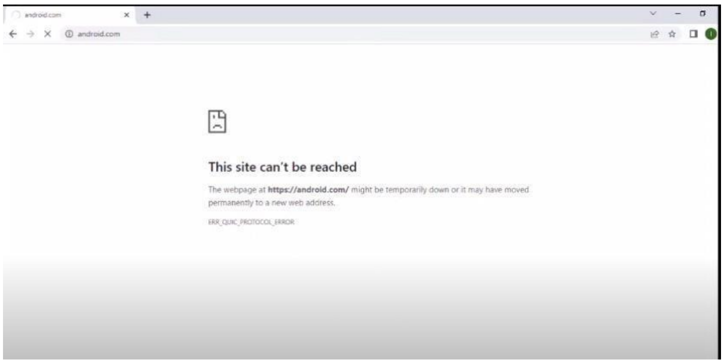


Name:
block android

Description (optional):

Repeat the above for Outbound Rules

Now if we try to access the website www.android.com , it would be blocked.



This site can't be reached

The webpage at **https://android.com/** might be temporarily down or it may have moved permanently to a new web address.

ERR_QUIC_PROTOCOL_ERROR