CSE 4215

Chapter 4

Authentication Authorization Accounting(AAA)

Authentication Authorization Accounting (AAA)

AAA Protocol

Authentication involves checking the identity being used is being used by the correct owner of the identity.
Authorization checks what the identity has permissions (access rights) to and
Accounting records what the identity does.

Types of authentication

1. **something a person knows**
2. **something a person has**
3. **something a person is**

Something a person knows
Something a person knows is commonly referred to as authentication by knowledge. examples

- a password
- a PIN
- combination numbers (e.g. for a lock)
- secret answers (e.g. mother's maiden name)

Authentication Authorization Accounting (AAA)

Something a person has

Something a person has is commonly referred to as authentication by ownership. Examples:

- Swipe cards
- Unique tokens
- Keys

Something a person is

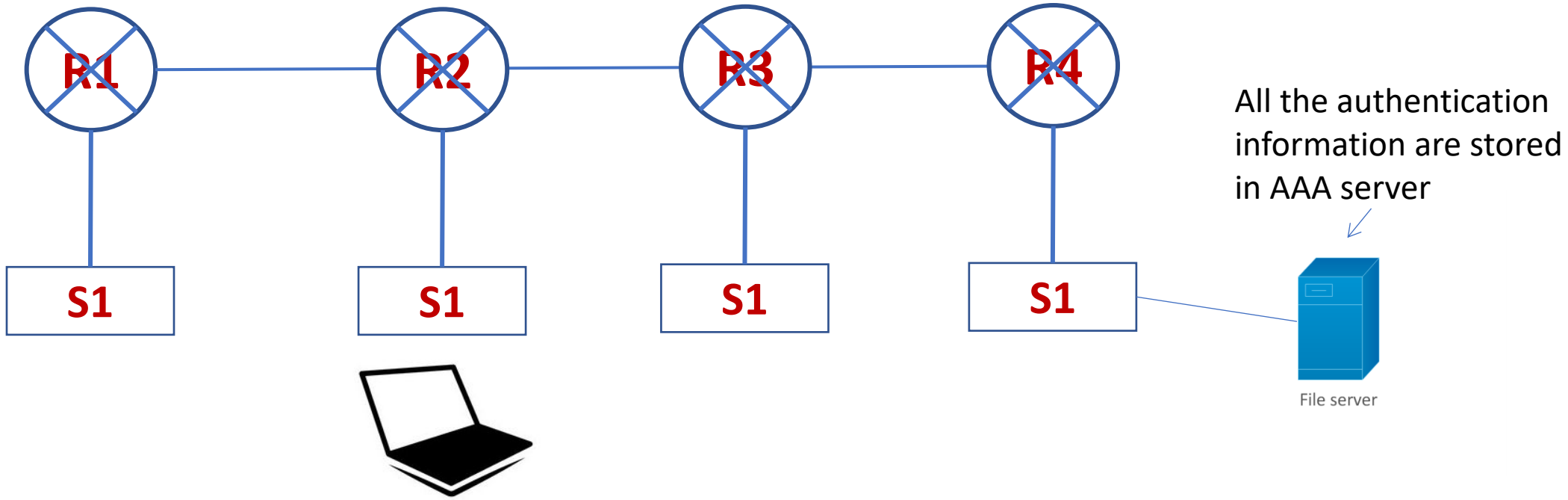
commonly referred to as authentication by characteristic. The characteristic is a physical characteristic which is unique to the person, that way. Different types of something a person is include:

- Fingerprints
- Retinal scans
- Face Identification (Face Id on smartphones)

Authentication Authorization Accounting (AAA)

Benefits of AAA

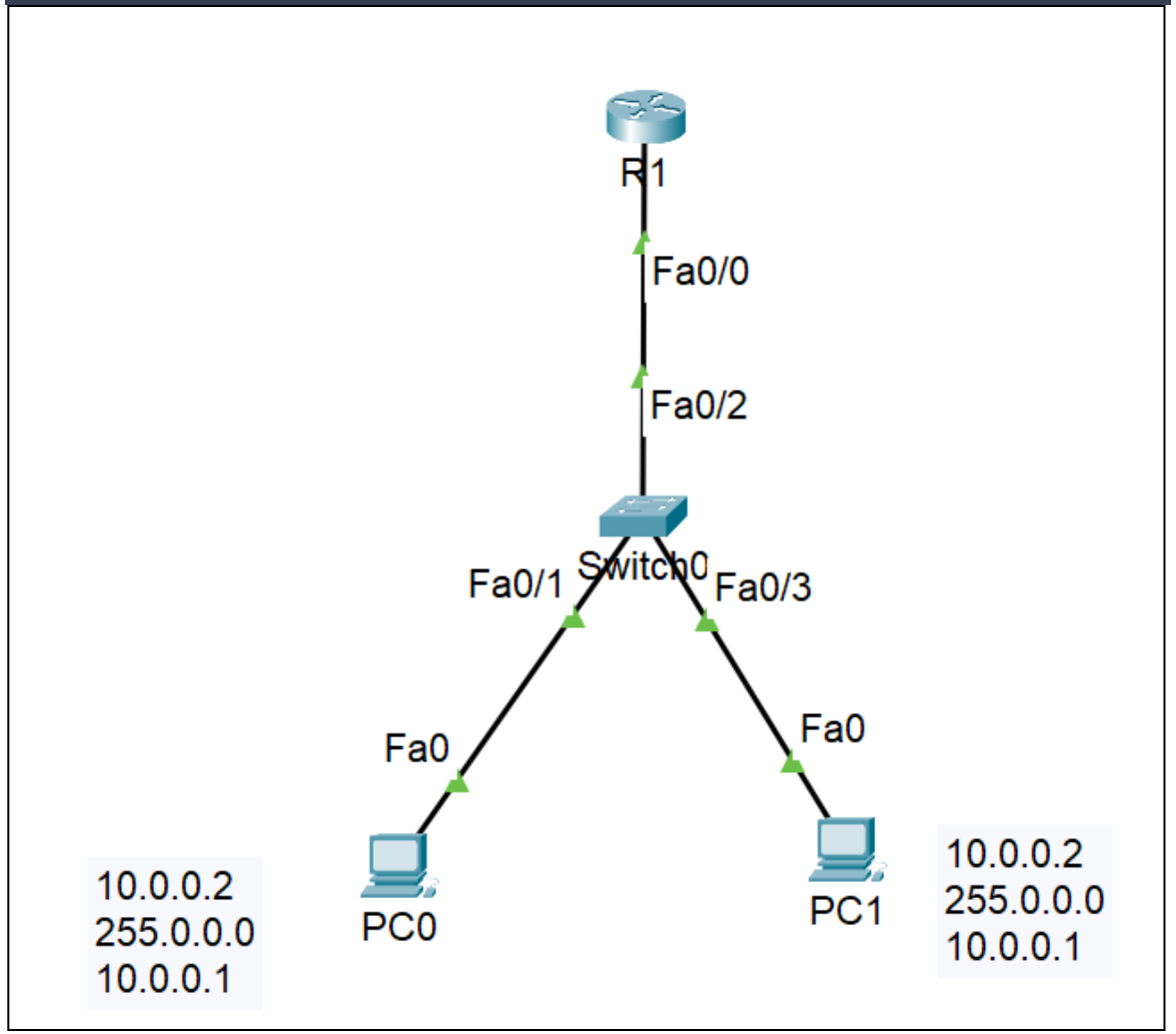
For big network, there are several router/switches, it is difficult to store authentication data to every device. For example for a new user John, admin should enter login/password to every device which is troublesome



Suppose an user wants access to router 2, At first user sends request to R2, then R2 sends the request to the server to check, if it is valid then user can get access to R2.
To add a new user, admin just insert authentication data in AAA server.

Authentication Authorization Accounting (AAA)

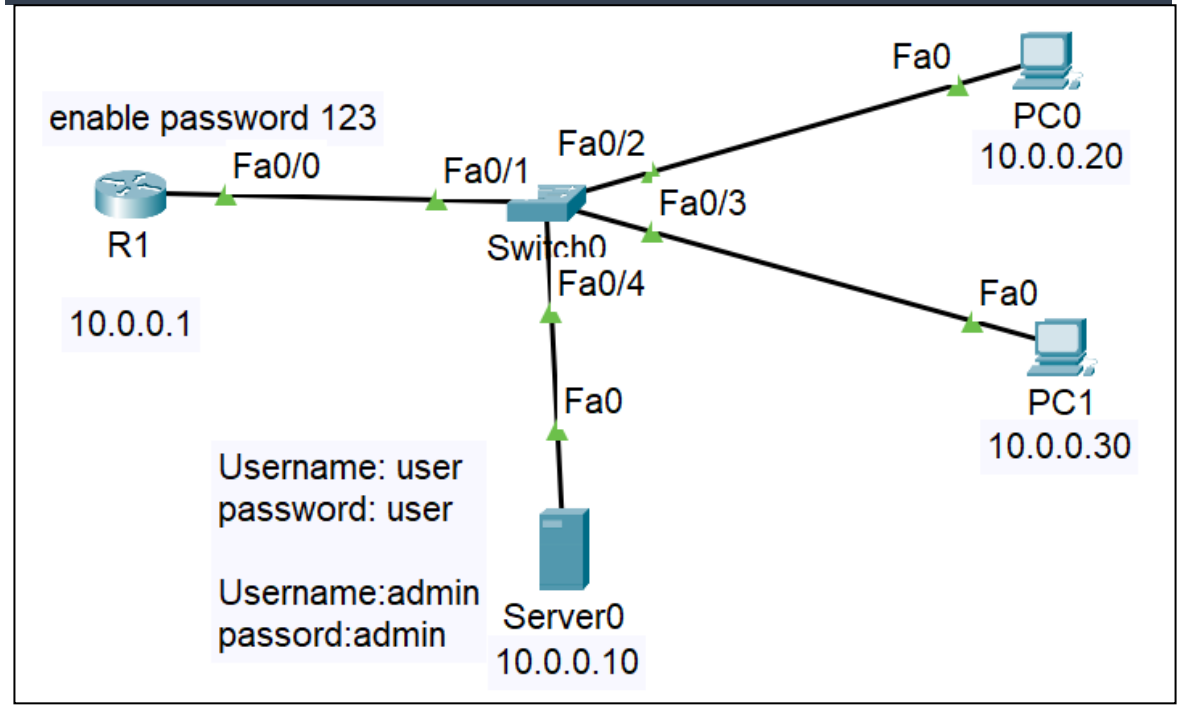
Packet Tracer Example using AAA




```
//**** Basic Level of Remote Security ****
//Set PC0 & PC1 with IP, Subnet and Gateway
//Interface router0
Router(config)#host R1
R1(config)#int f0/0
R1(config-if)#ip address 10.0.0.1 255.0.0.0
R1(config-if)#no shut
//Activate telnet from router
R1(config)#line vty 0
R1(config-line)#password 123
R1(config-line)#enable password 123

//password not encrypted
R1#show running-config

//password encrypted
R1(config)#service password-encryption

//** Advanced Level of Security**
R1(config)#aaa new-model
R1(config)#aaa authentication login default local
R1(config)#username root password root
```

Authentication Authorization Accounting (AAA)

Packet Tracer Example using AAA



Here authentications are verified in AAA server

```
//configure server, PC0 & PC1
R1(config)#int f0/0
R1(config-if)#ip address 10.0.0.1 255.0.0.0
R1(config-if)#no shut

R1(config)#enable password 123
R1(config)#ip domain-name ruet.com
R1(config)#crypto key generate rsa
R1(config)#ip ssh version 2
R1(config)#aaa new-model
R1(config)#radius-server host 10.0.0.10 key 123
R1(config)#aaa authentication login ssh group radius local
R1(config)#line vty 0 5
R1(config-line)#login authentication ssh
R1(config-line)#transport input ssh

//configure AAA service of server, Client is R1
//and users are admin & user with passwords

//login R1 from PC0
C:\>ssh -l admin 10.0.0.1
password:admin
```

Email Security

Email Security

Email

Email is one of the widely used & regarded network service.
Currently message contents are not secure.

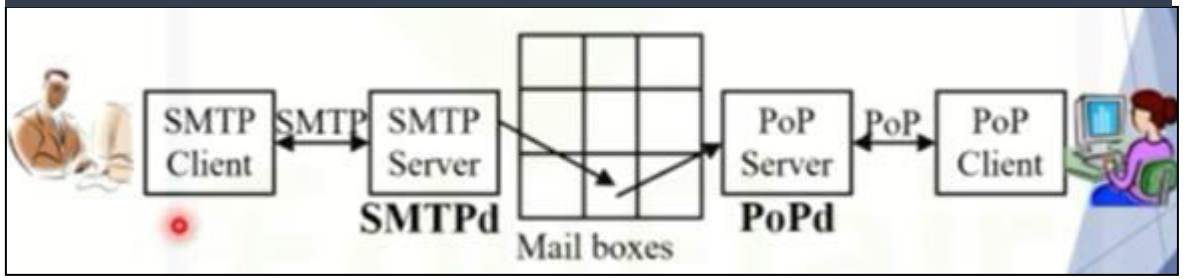
Email Security Requirement

1. Confidentiality- protection from disclosure
2. Authentication- of sender of message
3. Integrity- protection from modification
4. Non-repudiation- protection from deniel by sender

Protocols of Email

- ✓ Simple Mail Transfer Protocol (SMTP)
- ✓ Post Office Protocol (PoP)
- ✓ Internet Mail Access Protocol (IMAP)
- ✓ Multipurpose Internet Mail Extension (MIME)

Basic working of Email system



MIME is used for non-text content

Email Security

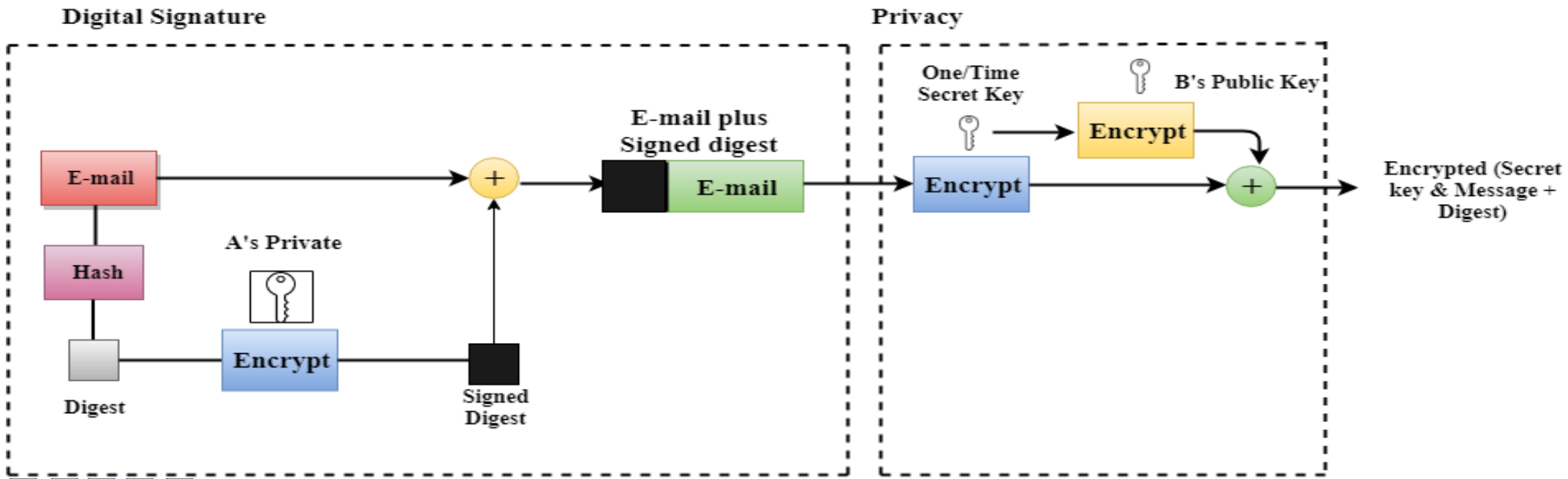
Pretty Good Service (PGP)

–PGP stands for Pretty Good Privacy (PGP) which is invented by Phil Zimmermann.
–PGP was designed to provide all four aspects of security, i.e., privacy, integrity, authentication, and non-repudiation in the sending of email.
–PGP uses a digital signature (a combination of hashing and public key encryption) to provide integrity, authentication, and non-repudiation. PGP uses a combination of secret key encryption and public key encryption to provide privacy. Therefore, we can say that the digital signature uses one hash function, one secret key, and two private-public key pairs.
–PGP is an open source and freely available software package for email security.
–PGP provides authentication through the use of Digital Signature.
–It provides confidentiality through the use of symmetric block encryption.
–It provides compression by using the ZIP algorithm, and EMAIL compatibility using the radix-64 encoding scheme.

Email Security

PGP Steps to secure e-mail at the sender site

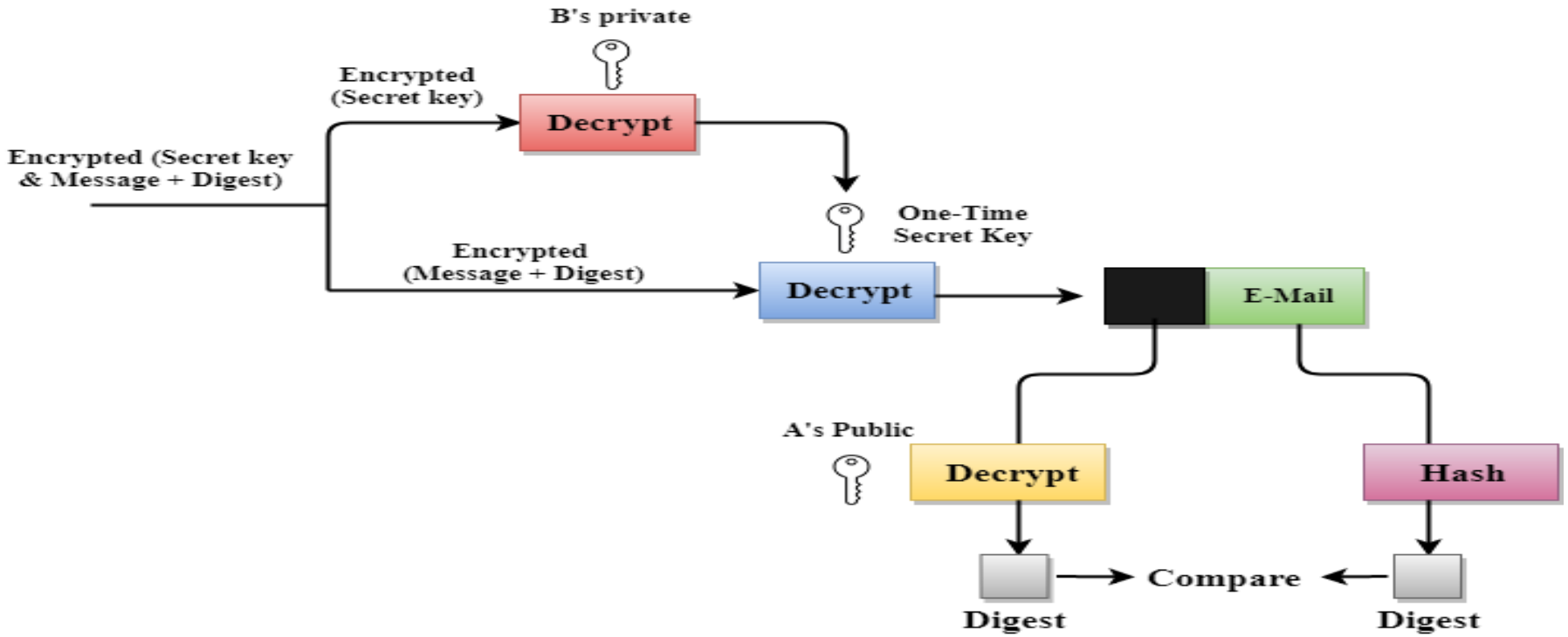
1. The e-mail message is hashed by using a hashing function to create a digest.
2. The digest is then encrypted to form a signed digest by using the sender's private key, and then signed digest is added to the original email message.
3. The original message and signed digest are encrypted by using a one-time secret key created by the sender.
4. The secret key is encrypted by using a receiver's public key.
5. Both the encrypted secret key and the encrypted combination of message and digest are sent together.



Email Security

PGP Steps to receive e-mail at the receiver site

1. The receiver receives the combination of encrypted secret key and message digest is received.
2. The encrypted secret key is decrypted by using the receiver's private key to get the one-time secret key.
3. The secret key is then used to decrypt the combination of message and digest.
4. The digest is decrypted by using the sender's public key, and the original message is hashed by using a hash function to create a digest.
5. Both the digests are compared if both of them are equal means that all the aspects of security are preserved.



Email Security

Mailvelop for PGP

Steps:

1. Add Mailvelop extension from Google Chrome. Download and install it.
2. From Setting button (upper right) enter to the configuration
3. Select **Generate** key. It will create both public and private keys.
4. **Import** Receiver's Public key.
5. Use **Encrypt** tag to encrypt message for a particular receiver. Download encrypted file.
6. Now from Gmail window select **Compose** tag. Write the receiver's address and attach the previous encrypted file and send.
7. For decryption, use **Decryption** tag and add encrypted file.

Sandbox

Sandbox

Sandboxing

- A security mechanism that allows you to run software in isolated space
- Helpful for executing untrusted Applications.
- Prevents programs from making permanent changes to system
- Secure web browsing: malware downloaded from websites can't infect your system
- Popular tool that implements sandboxing: **Sandboxie**

Requirement Sandbox for Window

- 64-bit Operating System
- Virtualization capabilities
- 4GB of RAM
- 1GB free disk space
- 2 CPU cores
- Version 19.0.3 or later (May 2019 Update)

To check version type **winver** at start button

Sandboxing creates a virtual machine inside the machine. For example Creates Windows 10 inside Windows 10 .

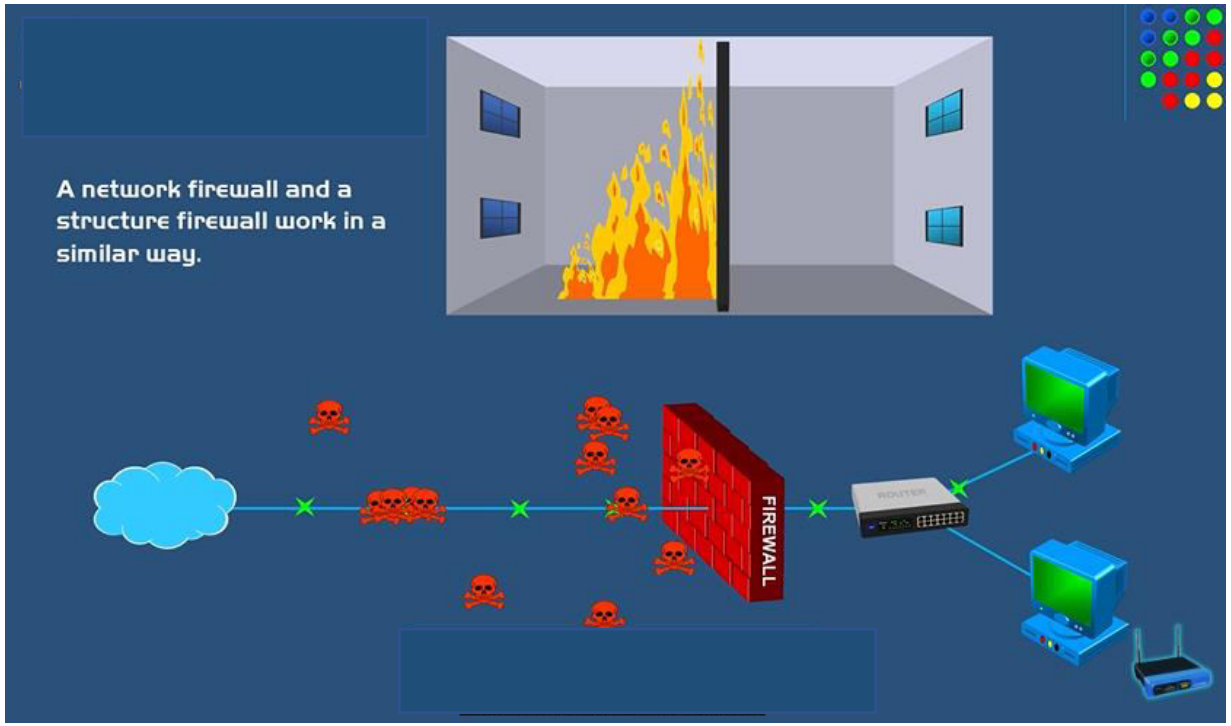
Setup Sandbox

1. First Check whether the machine is virtually enabled or not
2. To check it go to Task Manager→Performance→CPU and check virtualization. It should be enabled.
3. If NOT enabled then choose advance start up from start /run button, from Recovery→advance startup→Restart now→Troubleshoot→advance option→UEFI Firmware Settings
4. If Virtualization Enabled then from windows Start→ Turn on/off windows features→windows sandbox
5. If still no windows sandbox feature exist then install Tool Sandboxie from Internet (one link follows).
6. After installation open Sandboxie and sandbox→new box→right click and proceed

https://mega.nz/file/XY1HHY4T#ljrm4hEAVm6-R3Up0LUUOGoHzIABNRvTKgGjX-q0I8Y

Firewall

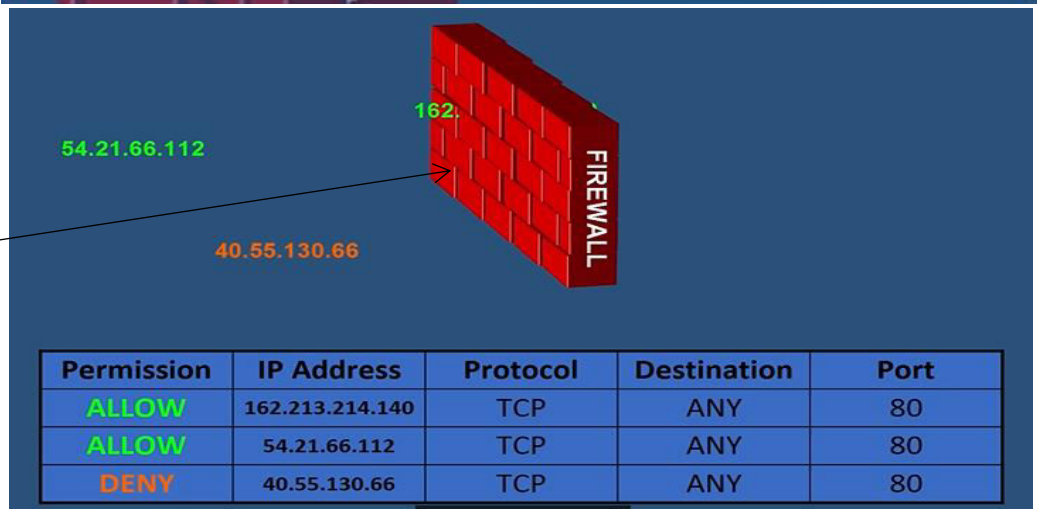
Firewall



Firewall Rules (Access Control List)

Permission	IP Address	Protocol	Destination	Port
ALLOW	162.213.214.14	TCP	10.10.10.2	80
ALLOW	54.21.66.112	TCP	ANY	80
DENY	192.168.1.1	TCP	ANY	80
ALLOW	65.252.1.2	TCP	ANY	80
DENY	ANY	TCP	ANY	80
ALLOW	ANY	TCP	ANY	80
DENY	ANY	UDP	10.10.10.1	23
DENY	255.255.255.0	TCP	ANY	25
ALLOW	10.10.0.1	TCP	ANY	110

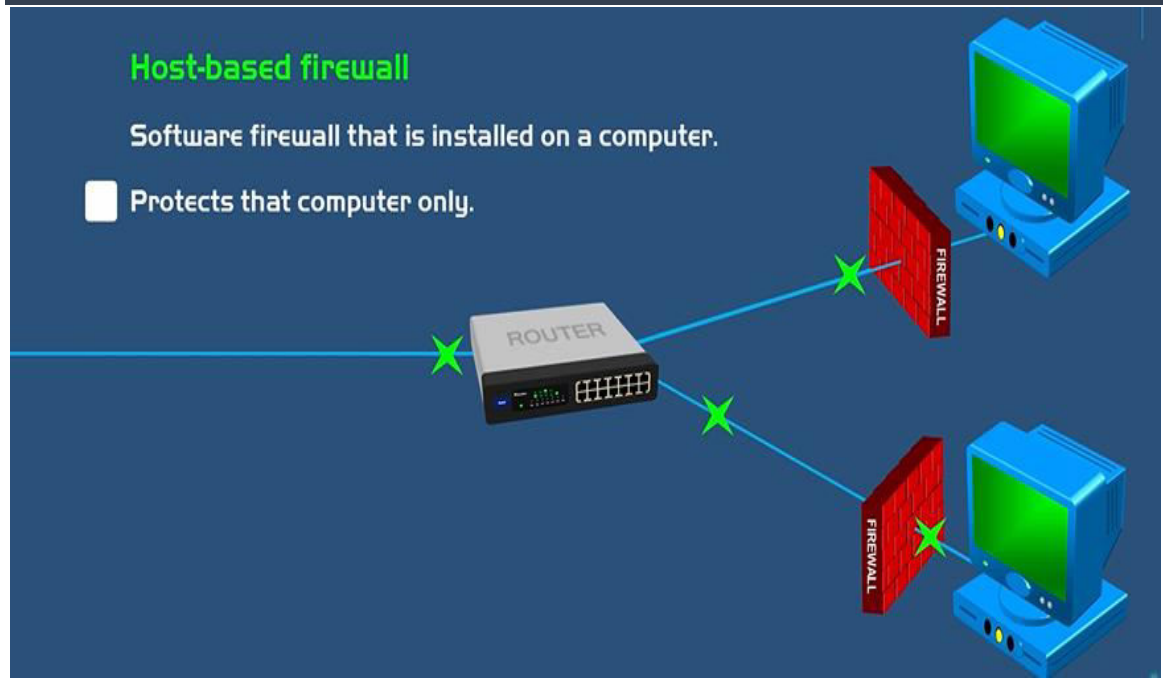
Only allowable IP address can access through Firewall



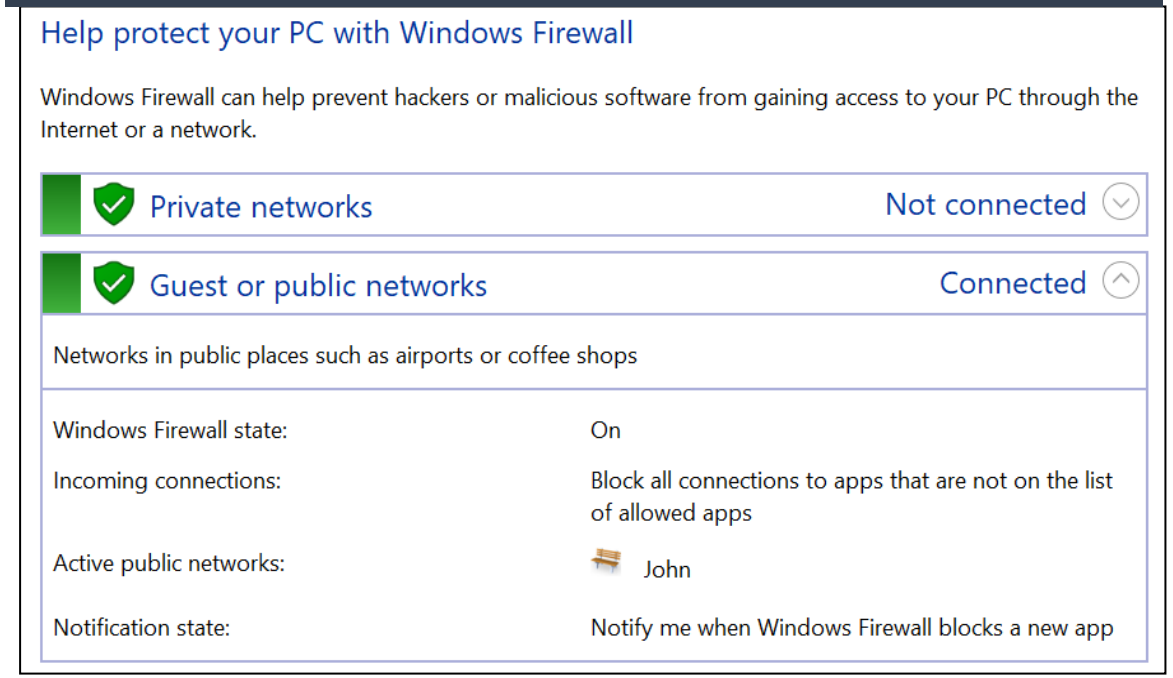
Permission	IP Address	Protocol	Destination	Port
ALLOW	162.213.214.140	TCP	ANY	80
ALLOW	54.21.66.112	TCP	ANY	80
DENY	40.55.130.66	TCP	ANY	80

Firewall

Firewall Types



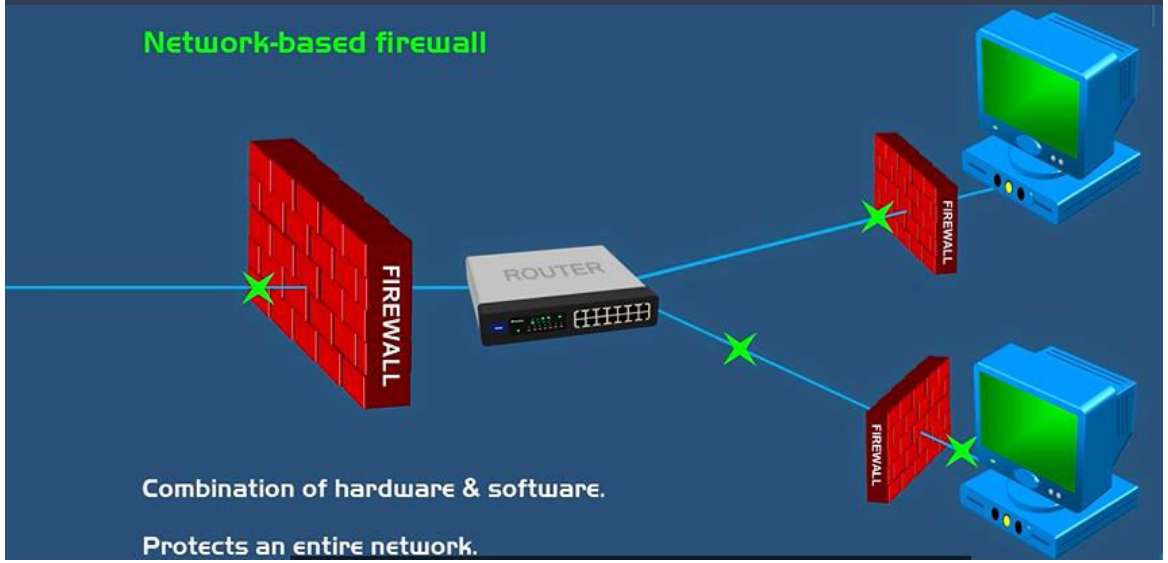
Windows Personal Firewall



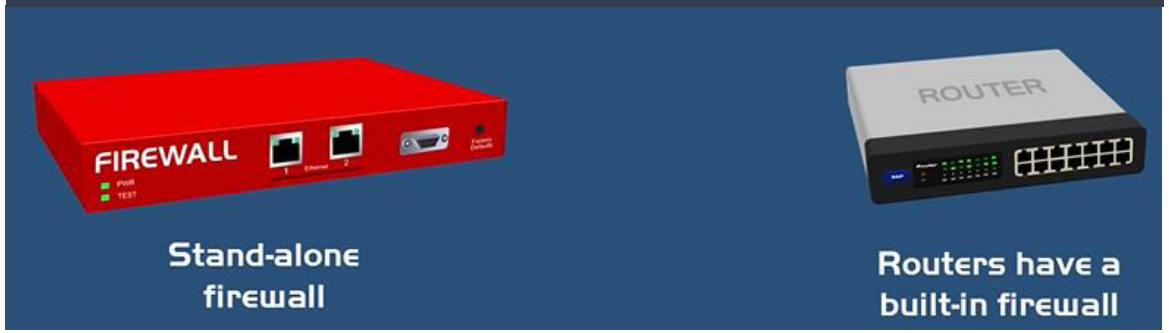
- Windows Firewall is installed automatically for each PC
- Also a 3rd Party host-based software can provide Firewall like Zone Alram.
- An anti-virus can also provide host-based Firewall

Firewall

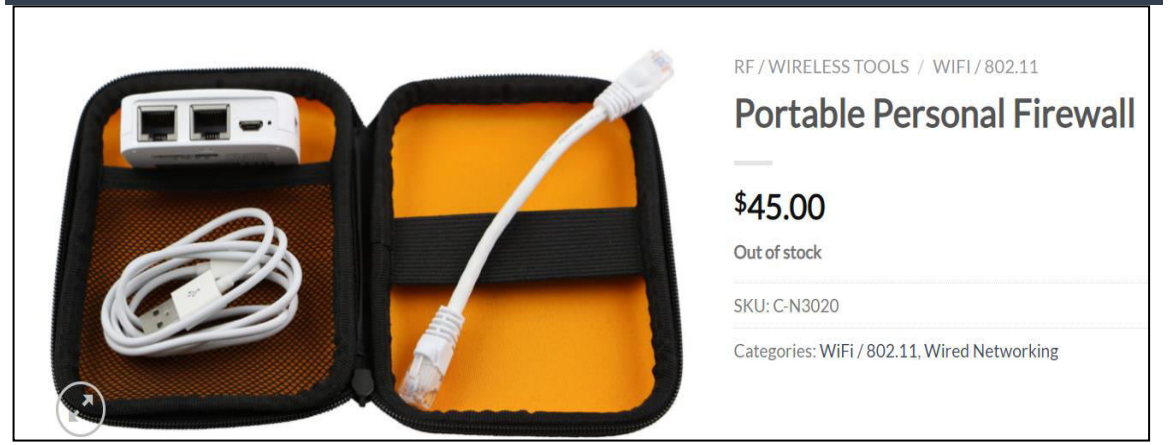
Network-based Firewall



Firewall Devices



Standalone Wireless Firewall Device



FG-60E 10 x GE RJ45 ports Max managed FortiAPs firewall FG-60E for network firewall security

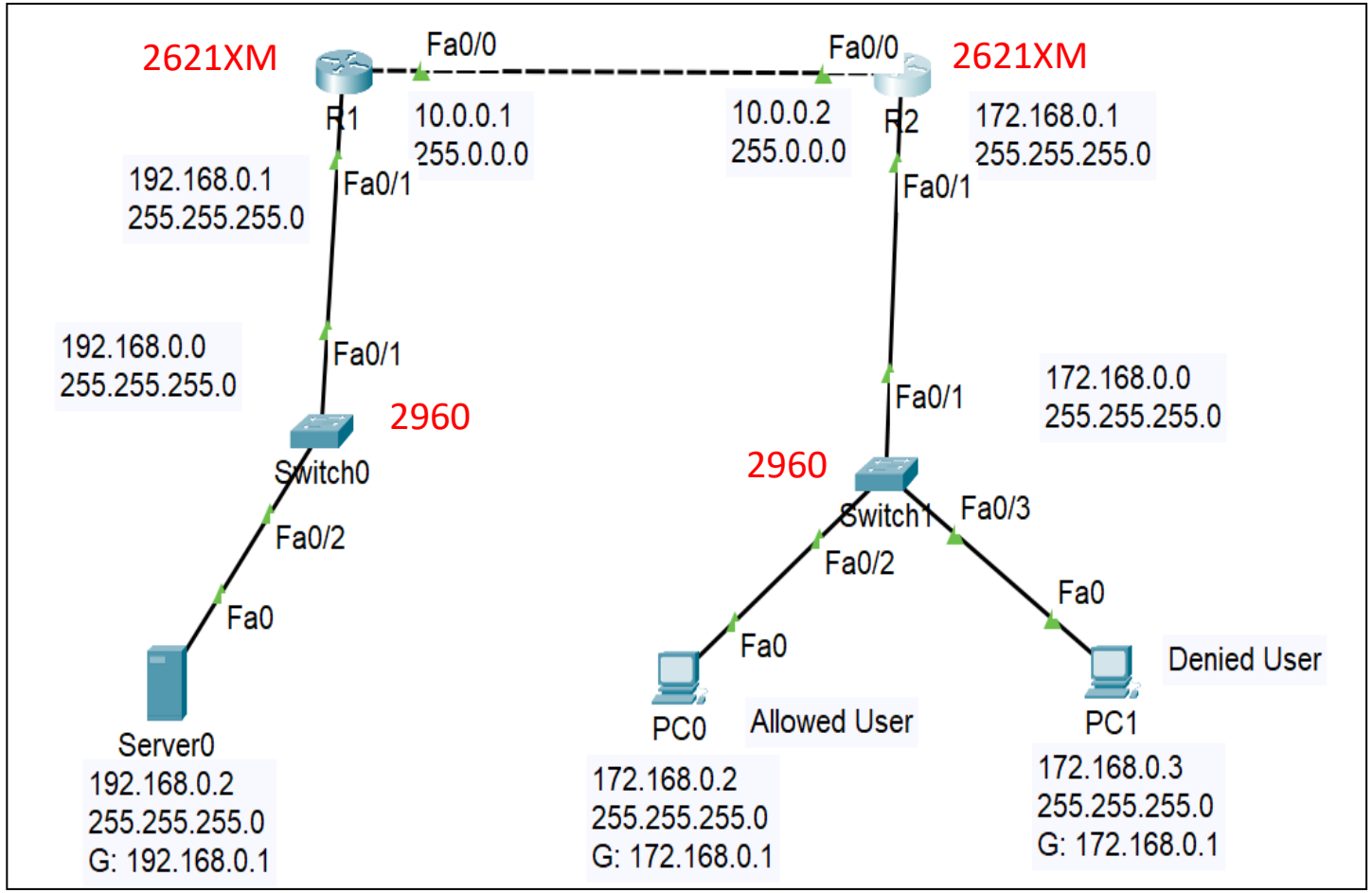
FOB **Reference** Price: Get Latest Price

>=1 pieces

$630.00

Firewall

Access Control List (ACL) by PT



Target: PC1 is to denied to access the server

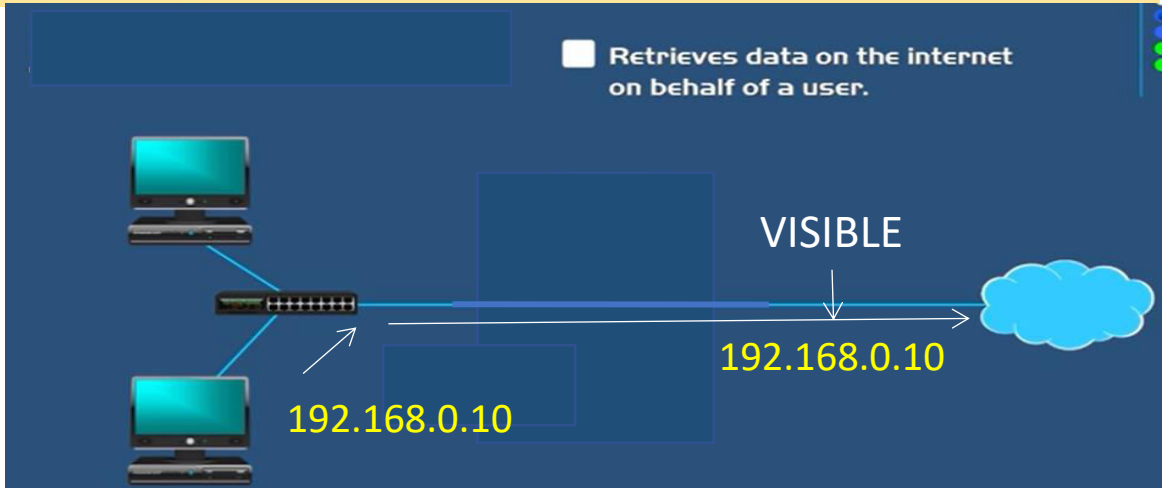
```
//Configure all the hosts and ports
//use rip protocol between routes

R1(config)#router rip
R1(config-router)#network 10.0.0.0
R1(config-router)#network 192.168.0.0
R2(config)#router rip
R2(config-router)#network 10.0.0.0
R2(config-router)#network 172.168.0.0

//Configure R2 to deny user 172.168.0.3
R2(config)#access-list 10 deny host 172.168.0.3
R2(config)#access-list 10 permit any
R2(config)#int f0/0
R2(config-if)#ip access-group 10 out
R2(config-if)#int f0/1
R2(config-if)#ip access-group 10 in
R2#show access-lists

//To block all host of network 172.168.0.0
R2(config)#no access-list 10 deny host 172.168.0.3
R2(config)#no access-list 10 permit any
R2(config)#access-list 10 deny 172.168.0.0
//no need to configure f0/0 & f0/1
```

Proxy Server

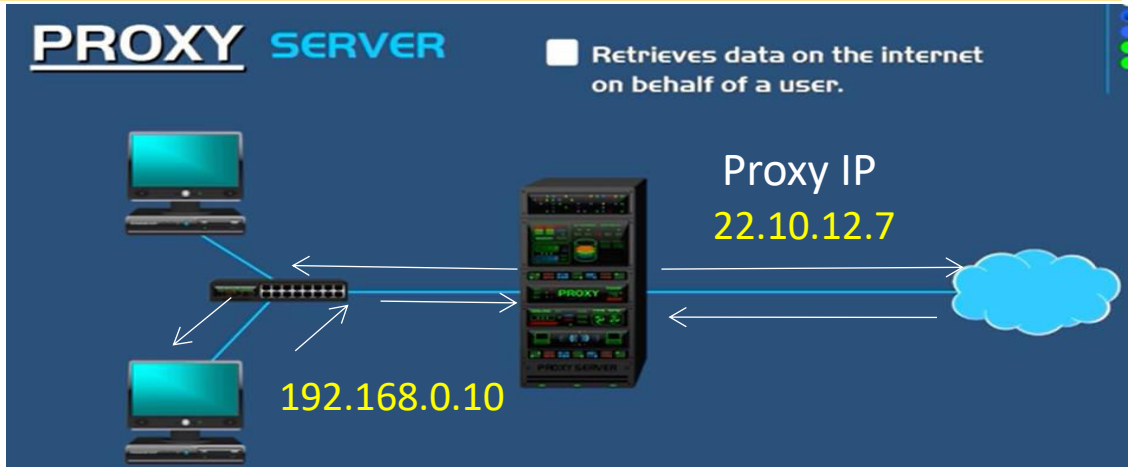
Proxy Server

What is Proxy Server

To visit a website host IP is visible in the network



But Host IP is NOT visible when Proxy is used. The proxy use its own IP to serve on behalf of host.

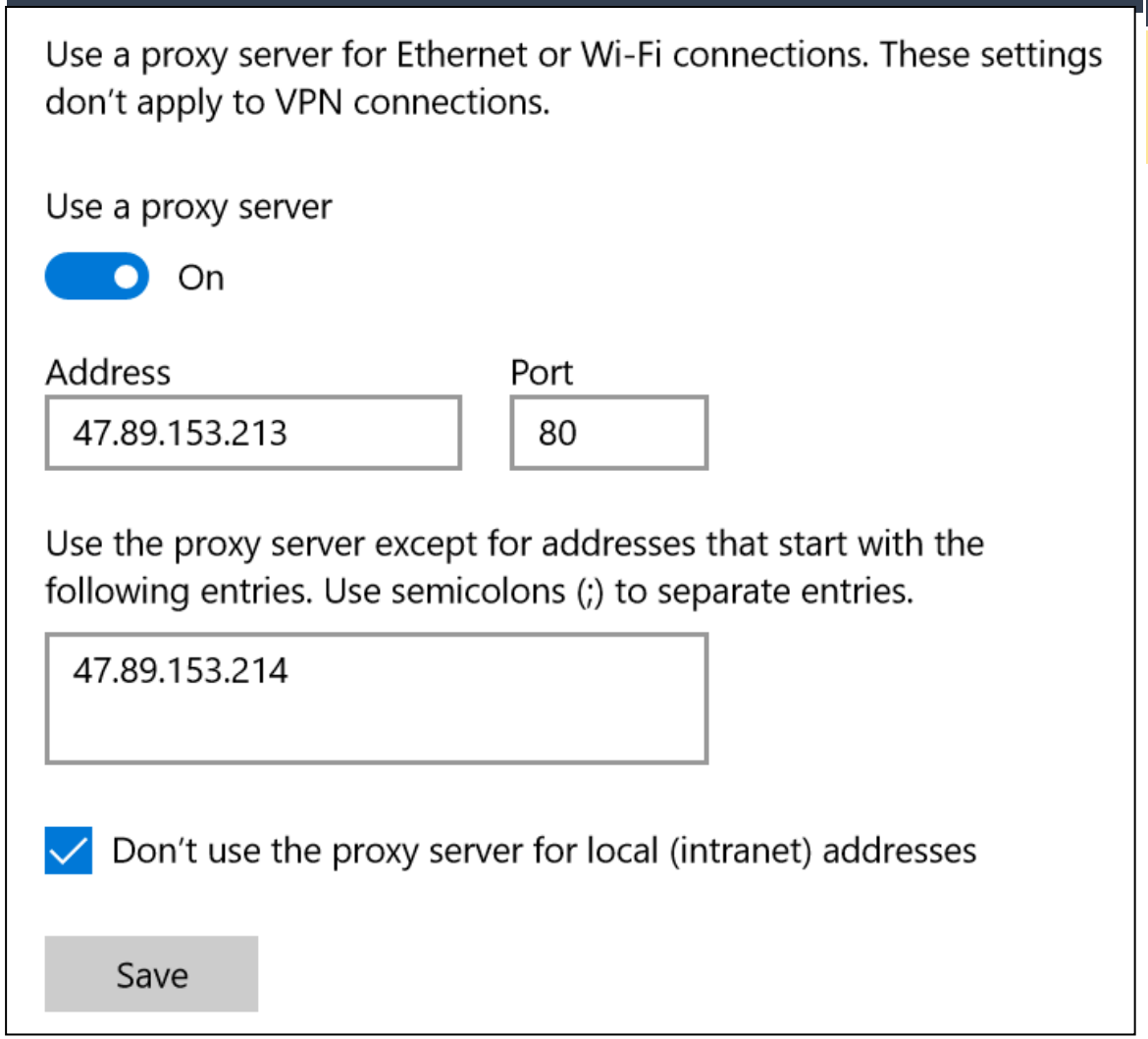


Proxy Benefits

- **Privacy**: Host IP is hidden
- **Speed**: Webpage stored in proxy database, so if another user want to access the same webpage, it can be accessed from proxy database, no need to go through internet.
- **Reduced Bandwidth**: because of centralized proxy database
- **Activity logging**: record users activity in internet

Proxy Server

Windows Proxy Settings



From Start→Settings→write Proxy→Manual Settings
Then set address and prot