Securing Network Information

Agendas of Today's Presentation

- What is Security
- Objective of Network Security
- Types of Network Security
- Network Vulnerabilities
- Security Threats
- Type of Attacks
- Security Measures

Securing Network Information

What is Network Security?

Network security is an activity designed to protect unwanted access to our network and data. It includes both hardware and software technologies.

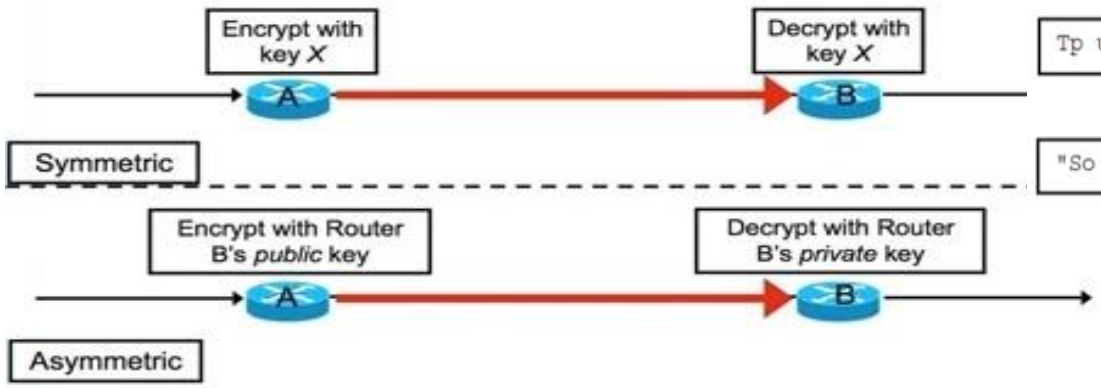
Objective of Network Security?

Network Security objectives usually involve three basic concepts, like, Confidentiality, Integrity and Availability

Confidentiality: Confidentiality means that only the authorized individuals or authorized systems can view or access sensitive or classified information or data.
This also implies that unauthorized individuals should not have any type of access to the data.

Securing Network Information

Objective of Network Security?



A Secret Message, Encrypted

```
Tp uijt jt uif tfdsfu nfttbhf.   Ju jt fbtz up ef-fodszqu jg zpv lopx uif lfz.
```

Results of Secret Message When Using the Correct "Key"

```
"So this is the secret message.   It is easy to de-encrypt if you know the key."
```

Encryption is a two-way function that takes clear text data as input and produces cipher text data as output.

Encryption uses KEYs to encrypt and decrypt traffic

Securing Network Information

Objective of Network Security?

Integrity: Integrity of data means the accuracy and consistency of data stored in a database.
Only the authorized individuals or systems can made changes in data.
Corruption of data is a failure to maintain data integrity.

Availability: Availability of data means that, data are available for authorized users for all the time.
Reasons of data unavailability: Network outage, Hardware failure or different types of attack, like denial-of-service (DoS/DDoS).

Securing Network Information

Types of Network Security?

Physical: Physical security for the network servers, equipment and infrastructure.

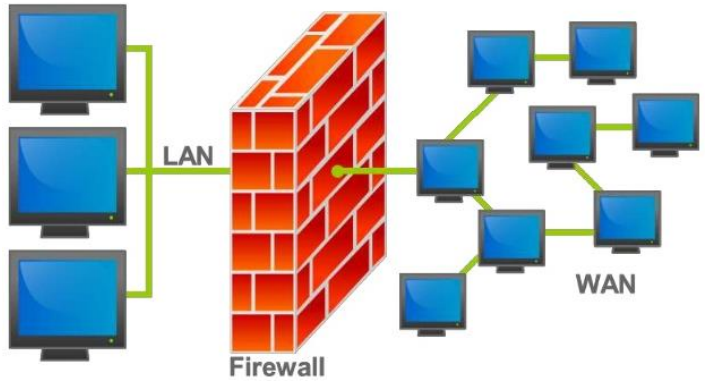
Logical: Includes passwords, NAC, firewalls, intrusion prevention systems, VPN tunnels etc.

Network Access Control (NAC):

Only the authorized users and devices would be allowed to get access to the network.

Firewall:

Is a mechanism for putting up a barrier between **trusted internal network and untrusted outside networks**, such as the Internet using hardware, software or both. They use a set of defined rules to allow or block traffic.



Securing Network Information

Network Vulnerabilities

A vulnerability is an exploitable weakness of some type that might result of data corruption or data missing.

Classification of Vulnerabilities:

- Policy flaws
- Design errors
- Protocol weaknesses
- Misconfiguration
- Software vulnerabilities
- Hardware vulnerabilities
- Human factors
- Malicious software
- Physical access to the network resources

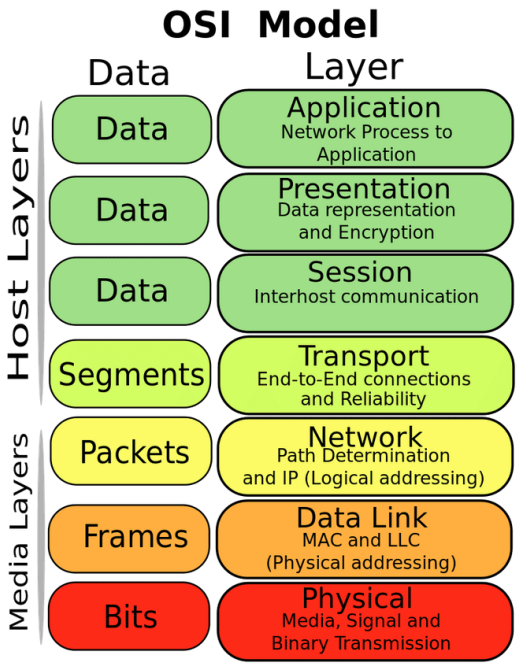
Securing Network Information

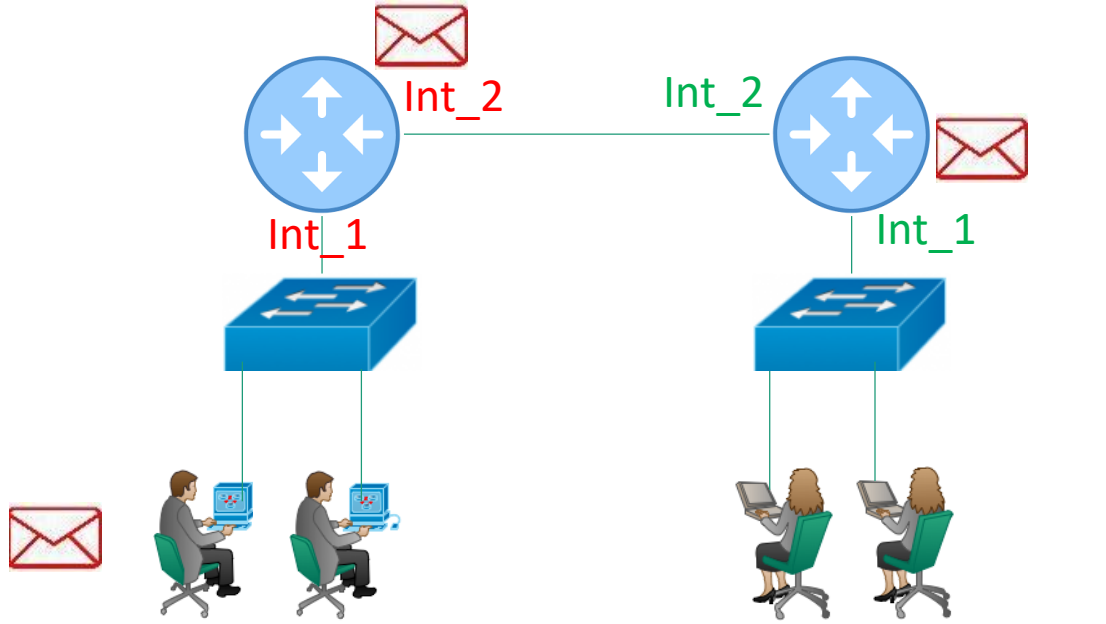
Security Threats

- IP Address Spoofing
- DoS/DDoS
- Unauthorized Access
- Route Injection
- Account Hijacking
- DNS Hijacking

Securing Network Information

Packet flow in the network





Src IP	Dst IP	Src MAC	Dst MAC
192.168.80.10	192.168.100.10	aa:aa:aa:aa:aa:aa	bb:bb:bb:bb:bb:bb

Securing Network Information

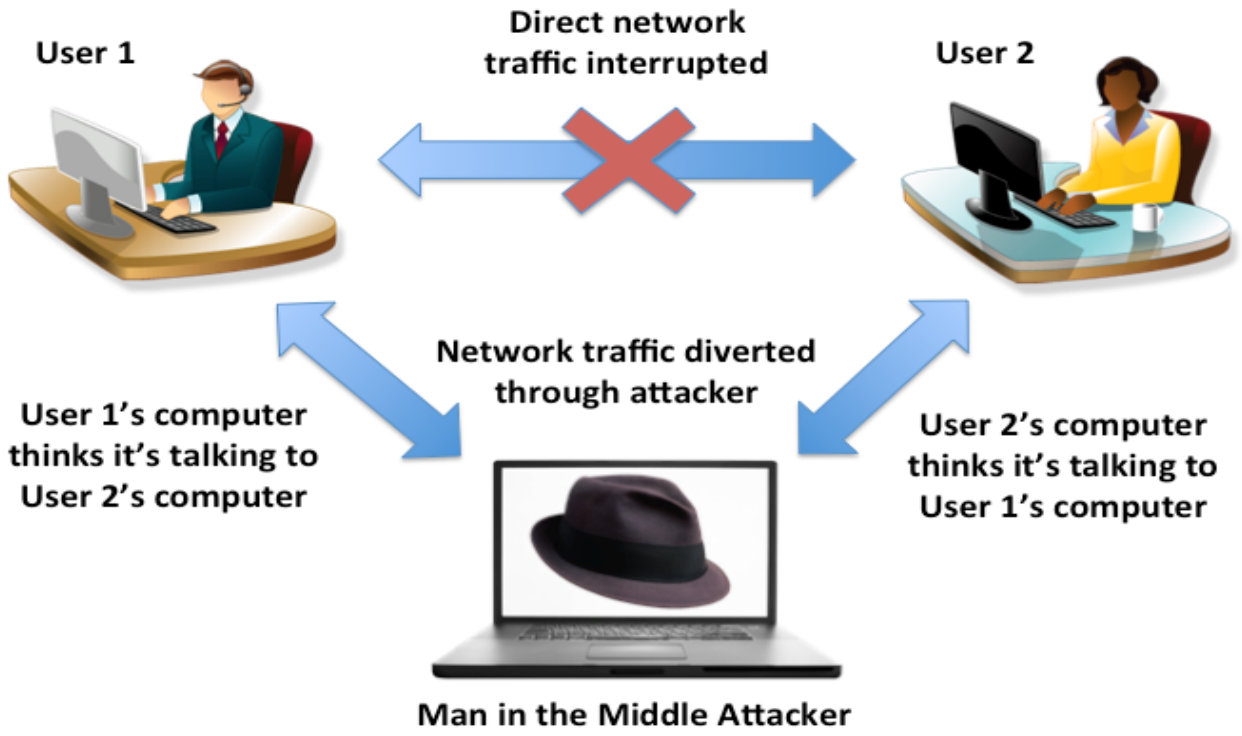
Types of Attacks

- Man-in-the-middle attack
- Distributed Denial-of-Service attack (DoS attack)
- Spoofing attack
- Zero-Days attack

Securing Network Information

Types of Attacks

- Man-in-the-middle attack



Securing Network Information

Types of Attacks

- Distributed Denial-of-Service attack (DDoS attack)
  - A Cyber attack on a specific Server or a Network from a number of sources.
  - An intended purpose of disrupting normal operation
  - Flooding the targeted host with a constant floor of traffic
  - System resources become exhausted
  - Network bandwidth become fully overwhelmed

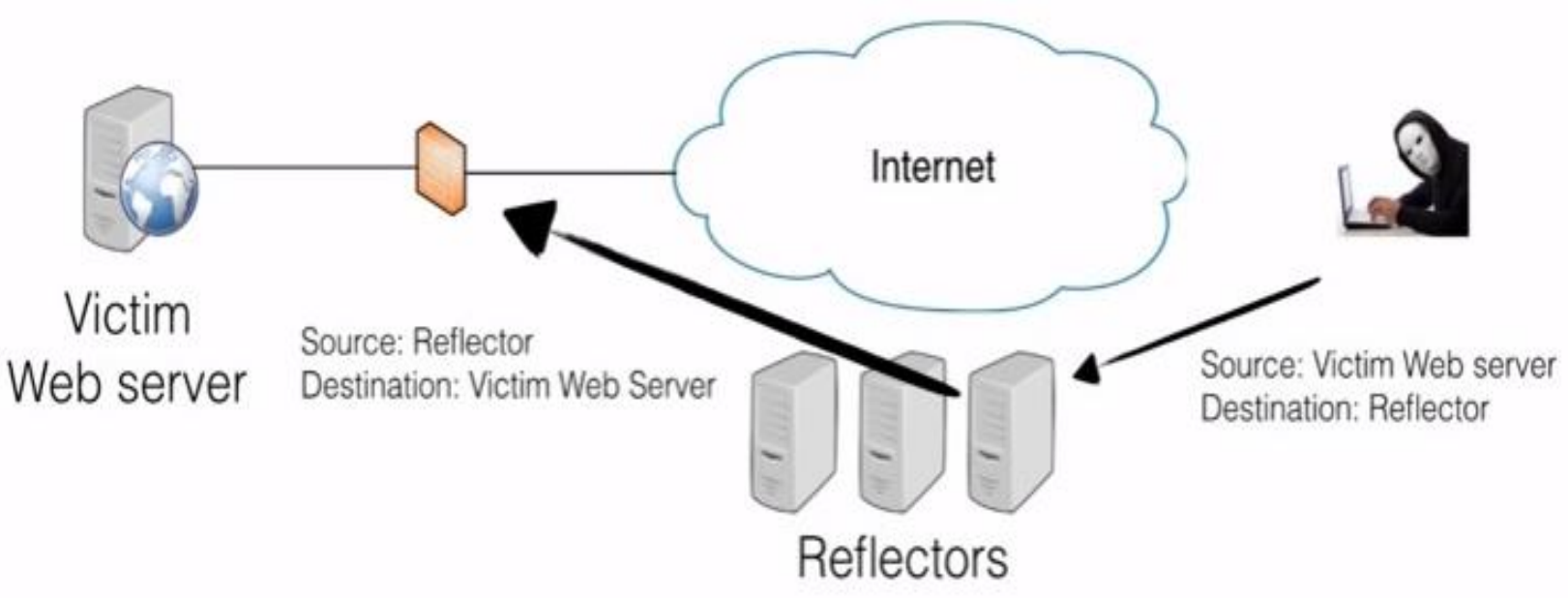
Securing Network Information

Types of Attacks

- Distributed Denial-of-Service attack (DDoS attack)

DDoS Categories

- Direct
- Reflected
- Amplification

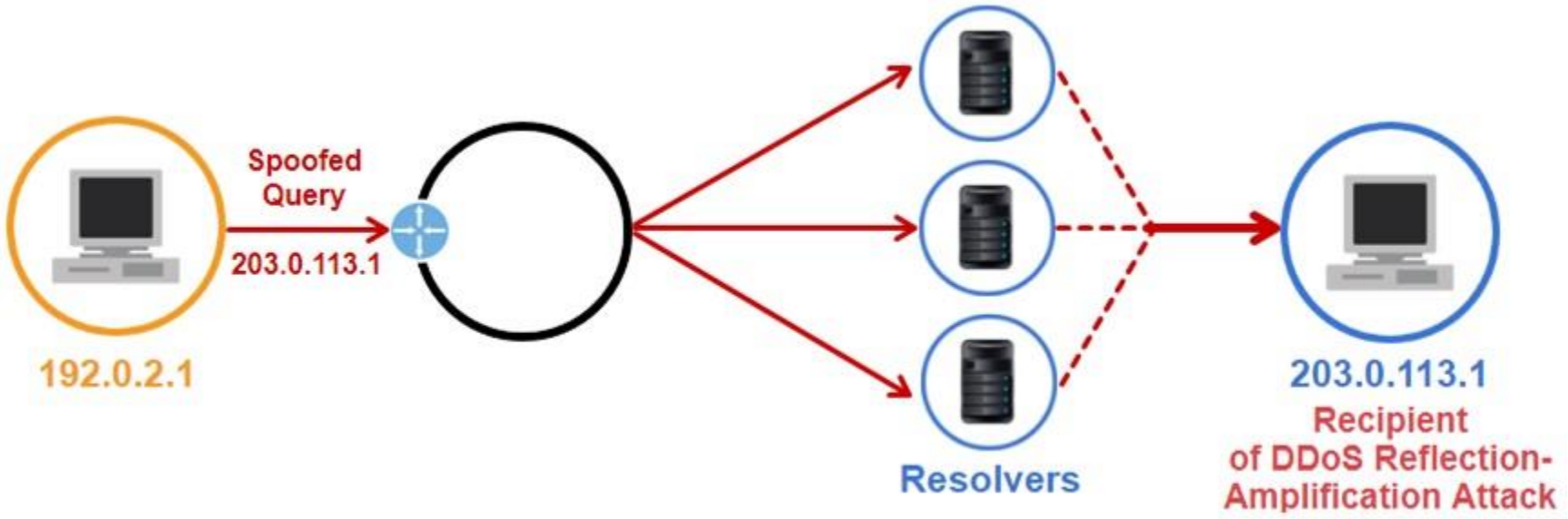


Securing Network Information

Types of Attacks

- Distributed Denial-of-Service attack (DDoS attack)

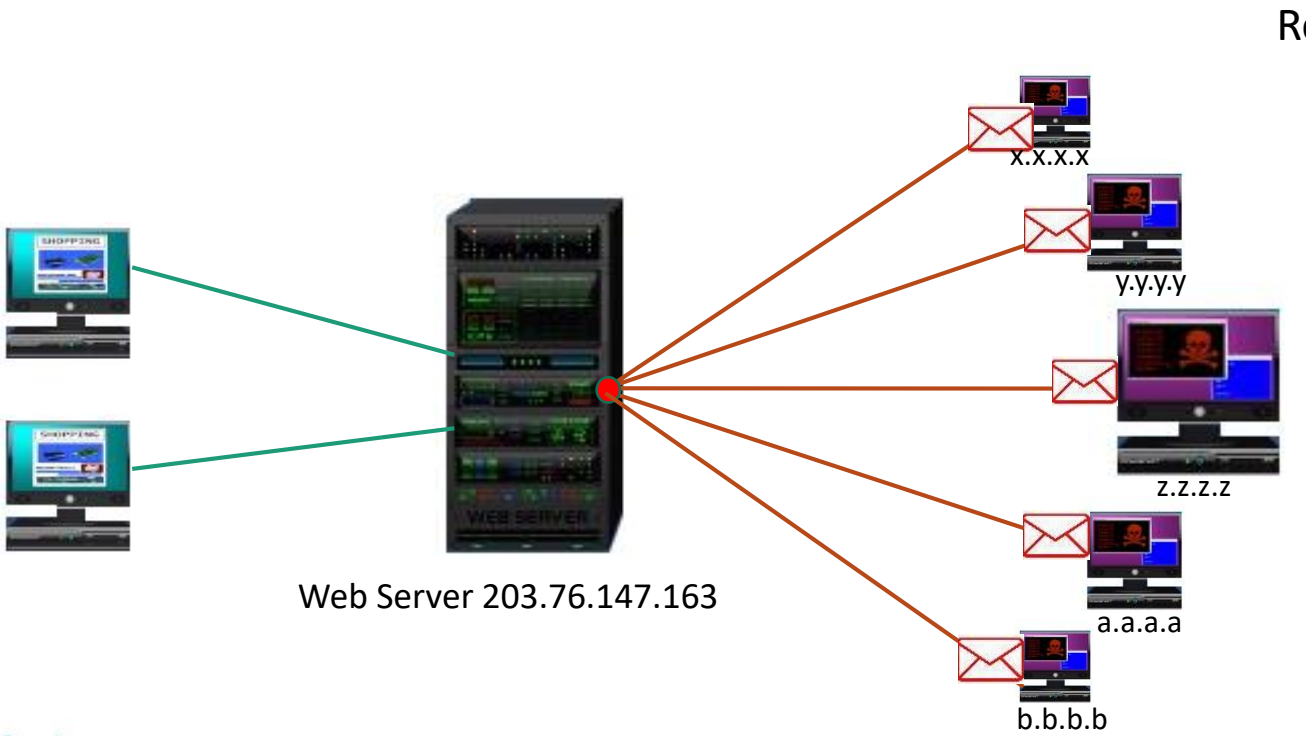
DDoS Categories



Securing Network Information

Types of Attacks

- Distributed Denial-of-Service attack (DDoS attack)



Received Spoofed packets

Source IP: 203.76.147.163
Destination IP: x.x.x.x

Source IP: 203.76.147.163
Destination IP: y.y.y.y

Source IP: 203.76.147.163
Destination IP: z.z.z.z

Source IP: 203.76.147.163
Destination IP: a.a.a.a

Source IP: 203.76.147.163
Destination IP: b.b.b.b

Securing Network Information

Security Measures

- Authorizing network access *(RADIUS Based Authentication)*
- Anti-Spoofing
- Using Firewall-Filter
- Using ACL *(Packet Filtering: Permit valid source and drop others/any)*
- Using VPN *(Remote Access and Site to Site VPN)*

Securing Network Information

Security Measures

- Authorizing network access *(RADIUS Based Authentication)*

RADIUS

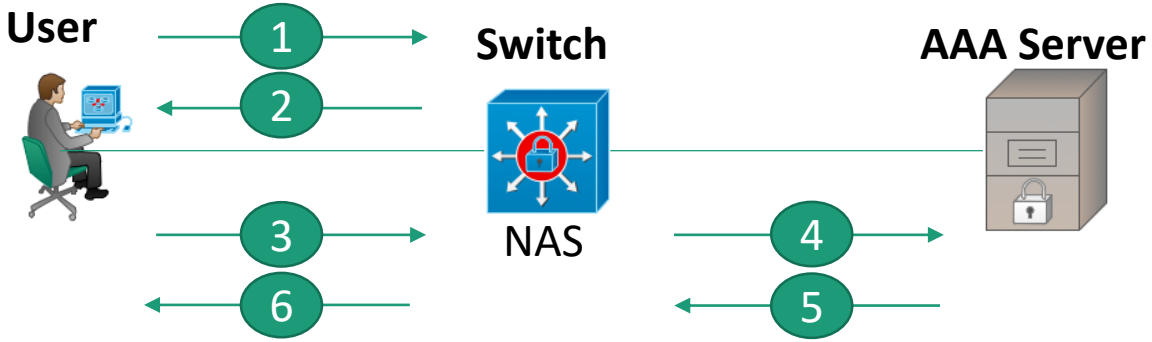
- Remote Authentication Dial-in User Service.
- Is a Client/Server Protocol, use UDP for communication and Provides three A (AAA).
- The client passes user information to designated RADIUS servers and acts on the response that is returned.
- RADIUS servers receive user connection requests, authenticate the user, and then return the configuration information necessary for the client to deliver service to the user.
- A RADIUS server can act as a proxy client to other RADIUS servers or other kinds of authentication servers.

Securing Network Information

Security Measures

- Authorizing network access *(RADIUS Based Authentication)*

RADIUS



1. User initiates a connection to the Switch/Router (NAS or Radius Client)
2. NAS prompts for username and password
3. User replies
4. NAS sends username and encrypted password to the RADIUS server.
5. RADIUS server responds with Accept, Reject, or Challenge.
6. The NAS acts upon services and services parameters bundled with Accept or Reject.

Securing Network Information

Security Measures

- Authorizing network access *(RADIUS Based Authentication)*

RADIUS

AAA

- **Authentication** validates user identity.
- **Authorization** deals with the access control to the network resources
- **Accounting** deals with user login session, amount of resources used during the session, billing information etc.

Securing Network Information

Security Measures

- Anti-Spoofing
  - DDoS Reflection-Amplification attacks would be **impossible without spoofing** – however, they are preventable
  - Implementing anti-spoofing filtering to **prevent packets with incorrect source IP address** from entering the network

Securing Network Information

Security Measures

- Anti-Spoofing Techniques

  - **Ingress Packet Filtering** (Source address validation)

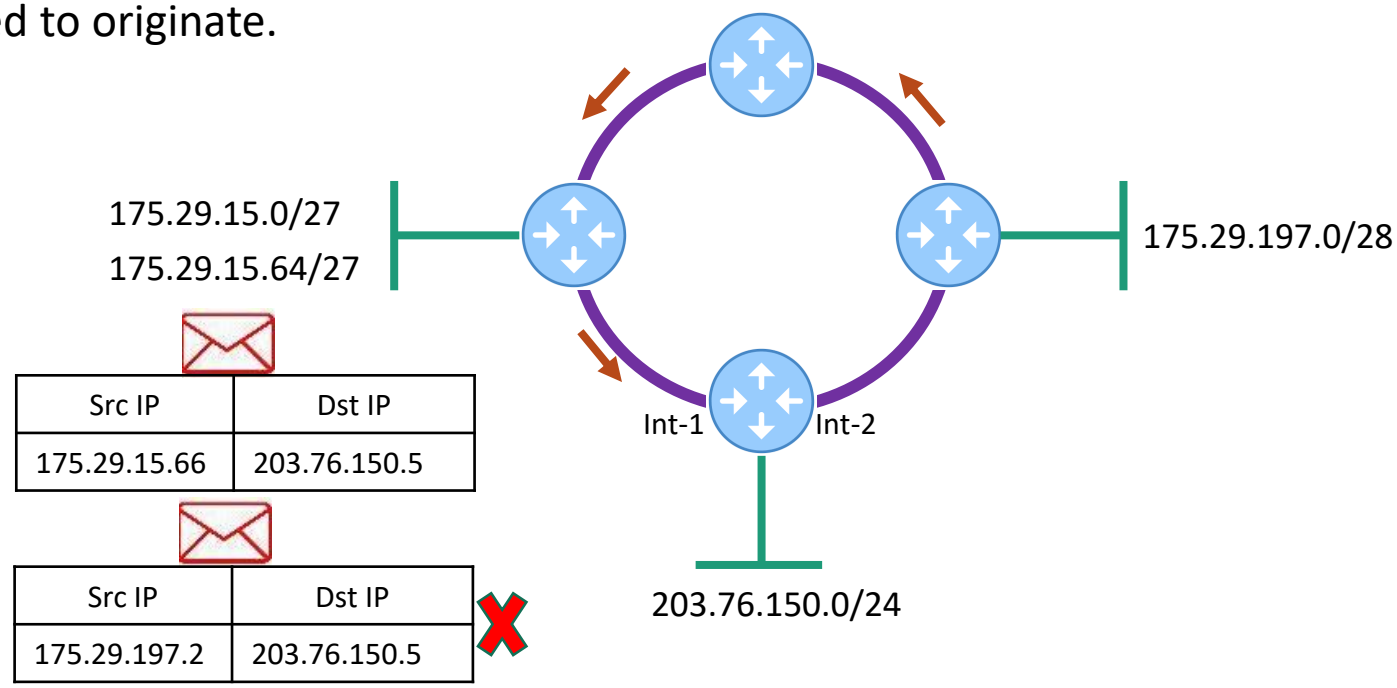
  - **Unicast Reverse Path Forwarding (uRPF)**

Securing Network Information

Security Measures

- Anti-Spoofing Techniques
  - **Ingress Packet Filtering**

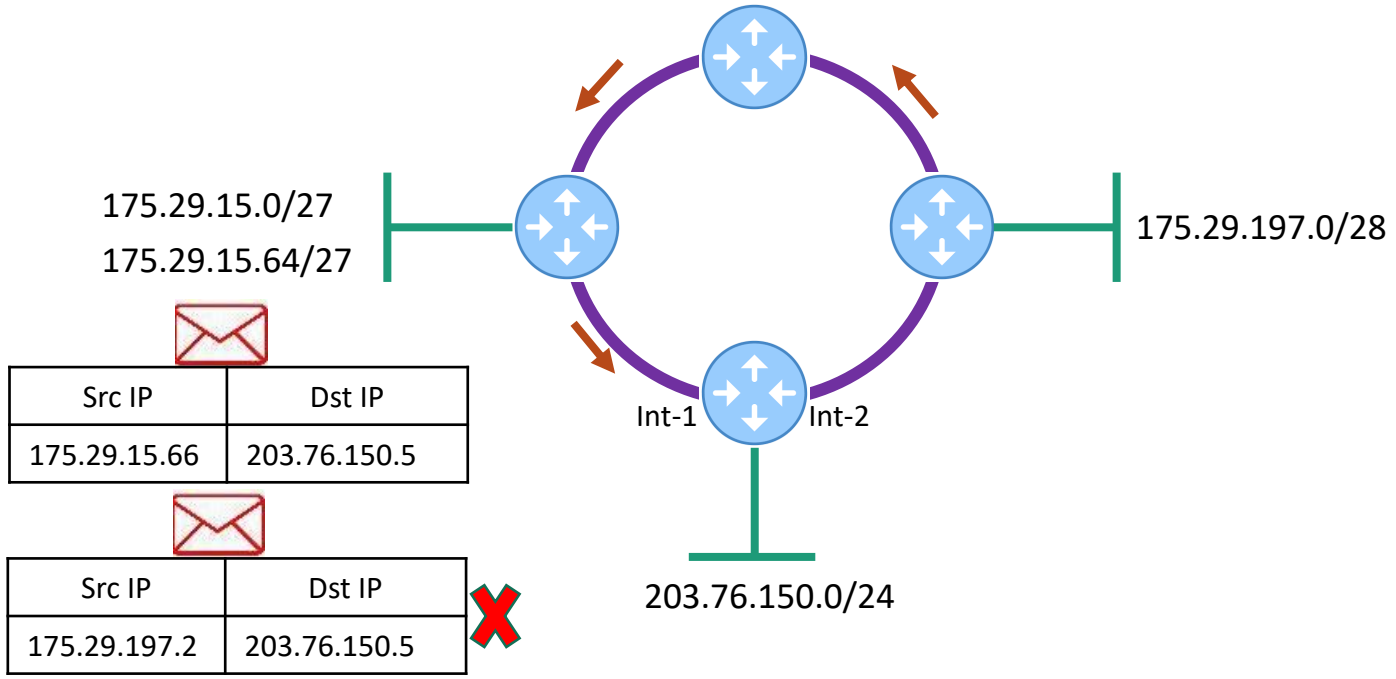
    Is a technique used to ensure that incoming packets are actually from the networks from which they claimed to originate.



Securing Network Information

Security Measures

- Anti-Spoofing Techniques



ip firewall filter add action=reject chain=forward dst-address=203.76.150.0/24 in-interface="!Int-1" src-address-list=!ALLOW

Address list

ALLOW = 175.29.15.0/27

ALLOW = 175.29.15.64/27

Securing Network Information

Security Measures

- Anti-Spoofing Techniques
  - **Unicast Reverse Path Forwarding (uRPF)**

How does uRPF works

- Routers typically makes decision based on destination IP
- With uRPF, routers now also looks at source IP
- Router looks at source IP and then the routing table
- If source IP is reachable via the input interface then its GOOD, else drop **(Strict)**
- If source reachable via any route in the routing table then its GOOD, else drop **(Loose)**
- Two modes of uRPF supported by MikrotiK router **(Strict and Loose)**

Securing Network Information

Security Measures

- Anti-Spoofing Techniques

uRPF Strict Mode

In **Strict mode** router will perform **two checks**

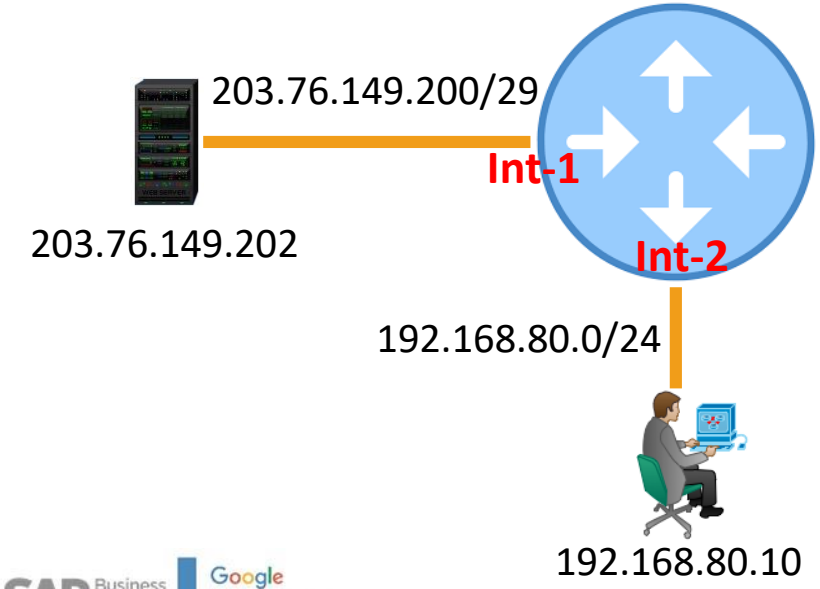
1. Is there any matching entry in the **routing table** for Source?
2. Is **same interface used to reach this source** as where it received previously?

Securing Network Information

Security Measures

- Anti-Spoofing Techniques

uRPF Strict Mode



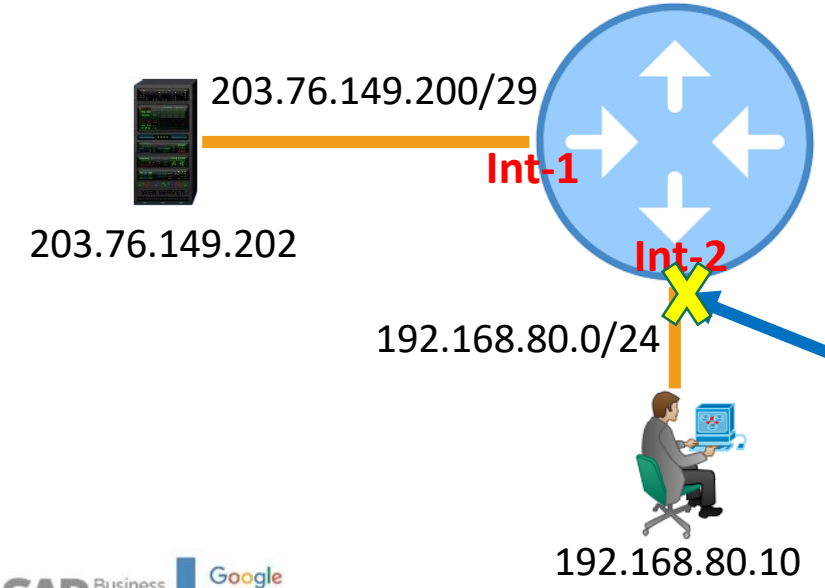
Routing Table		
Network	Distance	Instance
203.76.149.200/29	0	Interface_1
192.168.80.0/24	0	Interface_2

Securing Network Information

Security Measures

- Anti-Spoofing Techniques

uRPF Strict Mode



Routing Table

Network	Distance	Instance
203.76.149.200/29	0	Interface_1
192.168.80.0/24	0	Interface_2

Hey look, my routing table says the 203.76.149.204 reachable through my another interface.
Something is fishy.
This packet is not permitted.

Spoofed Packet

Src IP	Dst IP
203.76.149.204	203.76.149.202

Securing Network Information

Security Measures

- Anti-Spoofing Techniques

uRPF Loose Mode

In **Loose mode** router will perform **one checks Only**

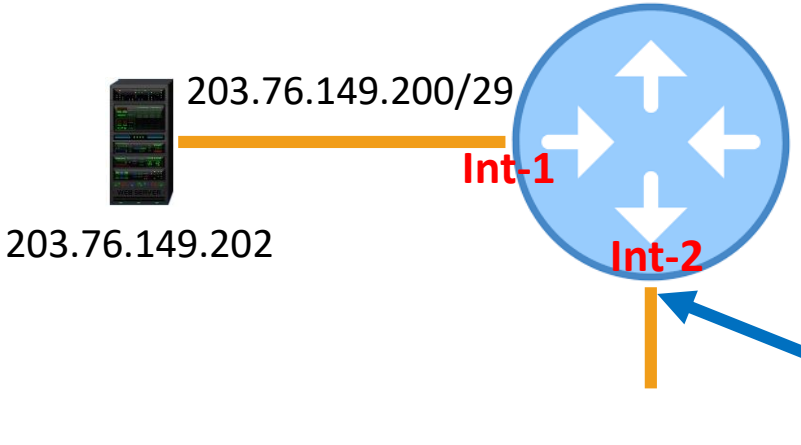
1. Is there any matching entry in the **routing table** for Source?

Securing Network Information

Security Measures

- Anti-Spoofing Techniques

uRPF Loose Mode



Routing Table		
Network	Distance	Instance
203.76.149.200/29	0	Interface_1
192.168.80.0/24	0	Interface_2
172.16.8.0/24	110	Interface_1

Src IP	Dst IP
172.16.8.10	203.76.149.202

Securing Network Information

Security Measures

- VPN (Virtual Private Network)
  - **Network** allows connectivity between two or more devices/Hosts
  - **Virtual** refers the logical connectivity between two devices/Hosts
  - The Virtual network created between two users would be **private** between those two parties.
  - Ensures data confidentiality (encryption) and integrity.

Securing Network Information

Security Measures

- VPN (Virtual Private Network)
  - **Types of VPN**

Remote Access VPN

Individual user establishes VPN connection to its corporate Headquarter
SSL and PPTP technologies are used in Remote Access VPN

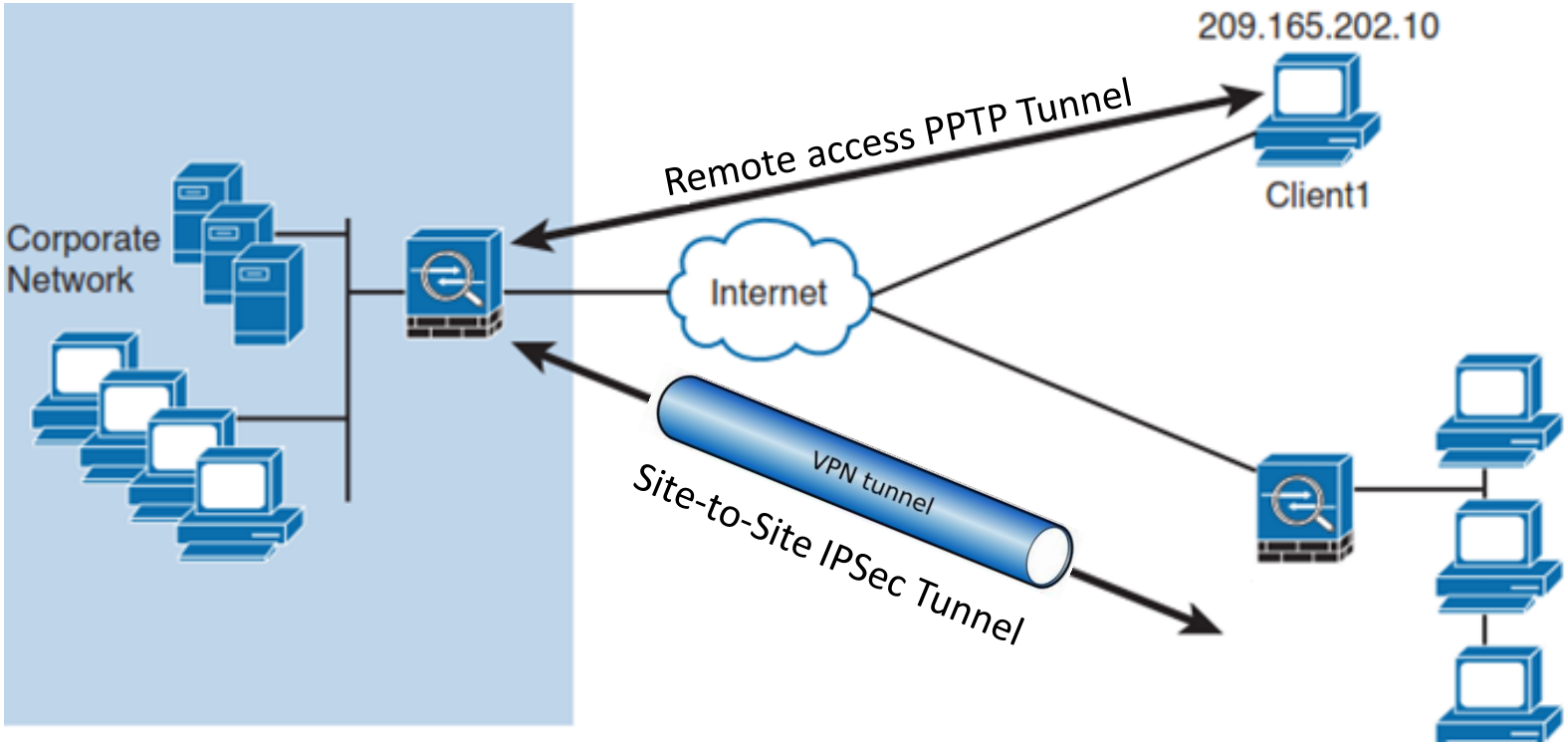
Site-to-Site VPN

Two individual site establishes VPN connection
IPSec technology used in Site-to-Site VPN

Securing Network Information

Security Measures

- VPN (Virtual Private Network)
  - **Types of VPN**



Securing Network Information

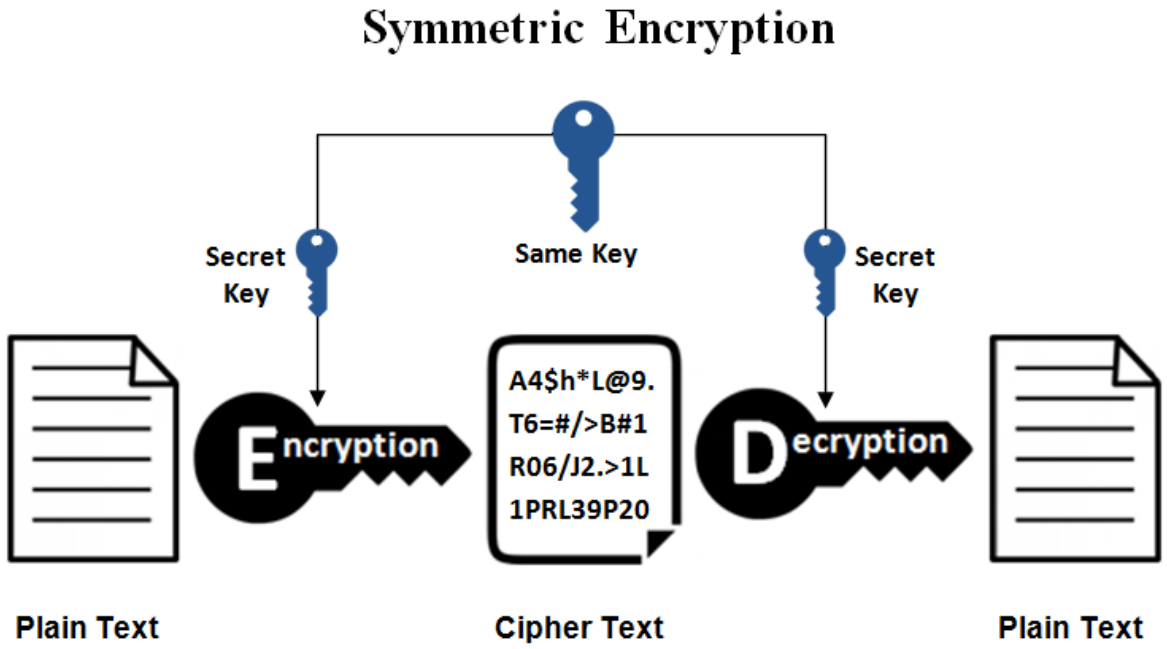
Security Measures

- **Main Benefits of VPN**
  - **Confidentiality**
    Is a function of encryption.
    Only the intended parties can understand the data that is sent.
  - **Data Integrity**
    Is a function of hashing.
    Ensures the accuracy and consistency of data being sent end to end.
  - **Authentication**
    Process of providing identity of the other side of the VPN tunnel
    - Pre-shared KEYs authentication
    - Public and Private KEY pairs authentication
    - User authentication

Securing Network Information

Security Measures

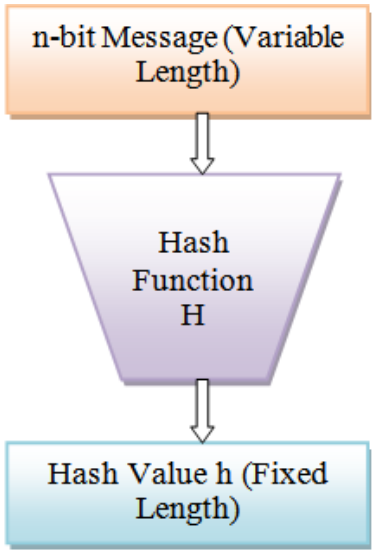
- **Main Benefits of VPN**
  - **Confidentiality**

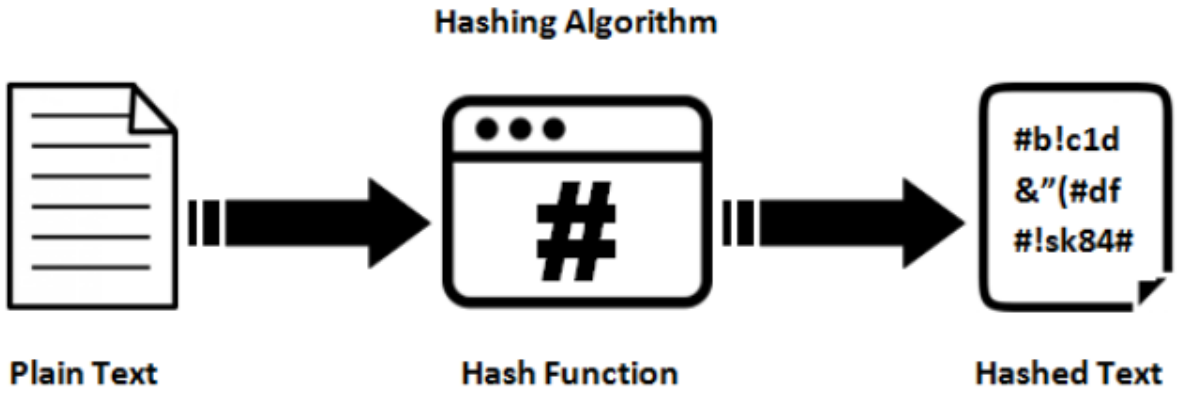


Securing Network Information

Security Measures

- **Main Benefits of VPN**
  - **Integrity**



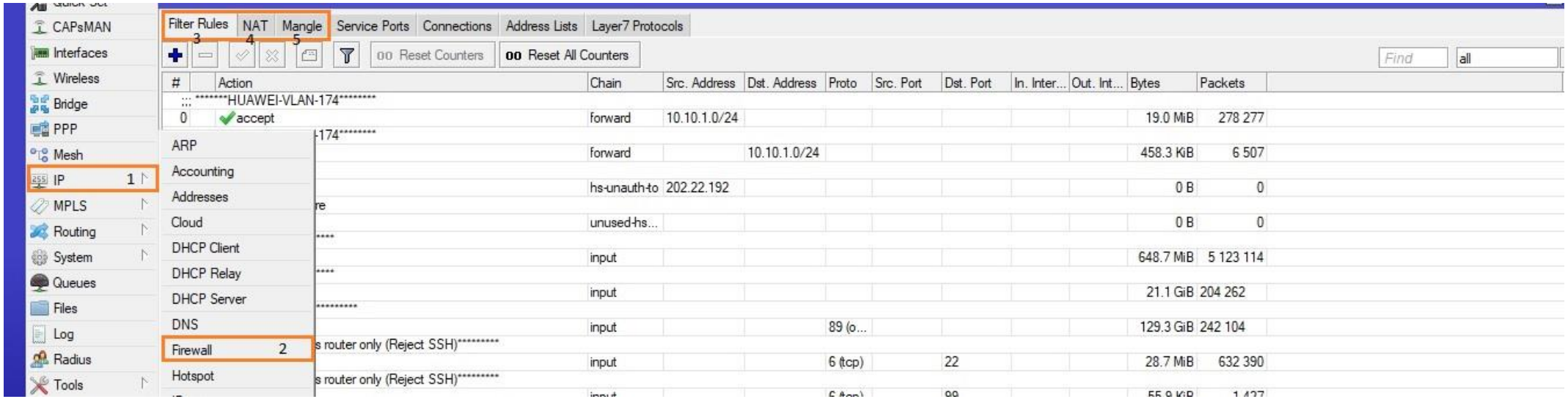


Securing Network Information

What is MikroTik Firewall?

It is a feature of

- Controlling network access **(Filter)**
- Modifying network header **(NAT)**
- Marking packet for further processing **(Mangle)**



Securing Network Information

MikroTik Firewall Filter

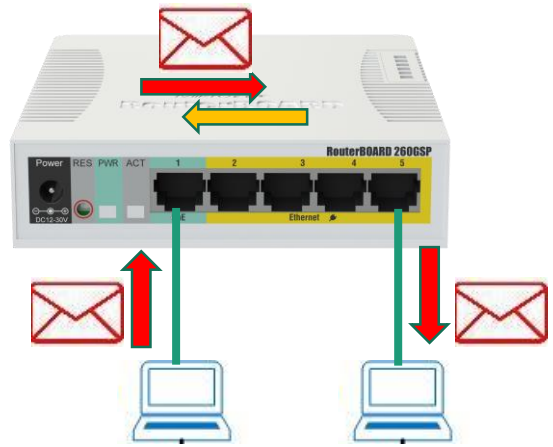
Configuring firewall filter in router network access can be controlled based on **network, protocol and ports**.

MikroTik Firewall Filter Chains

Input Chain: Used to process packets entering the router through one of the interfaces with the destination IP address which is one of the router's addresses

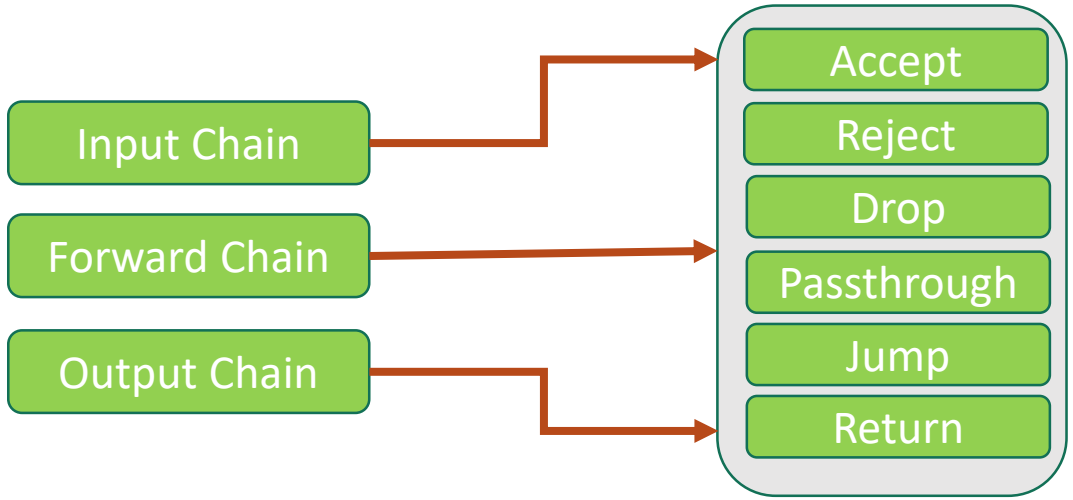
Forward Chain: Used to process packets passing through the router

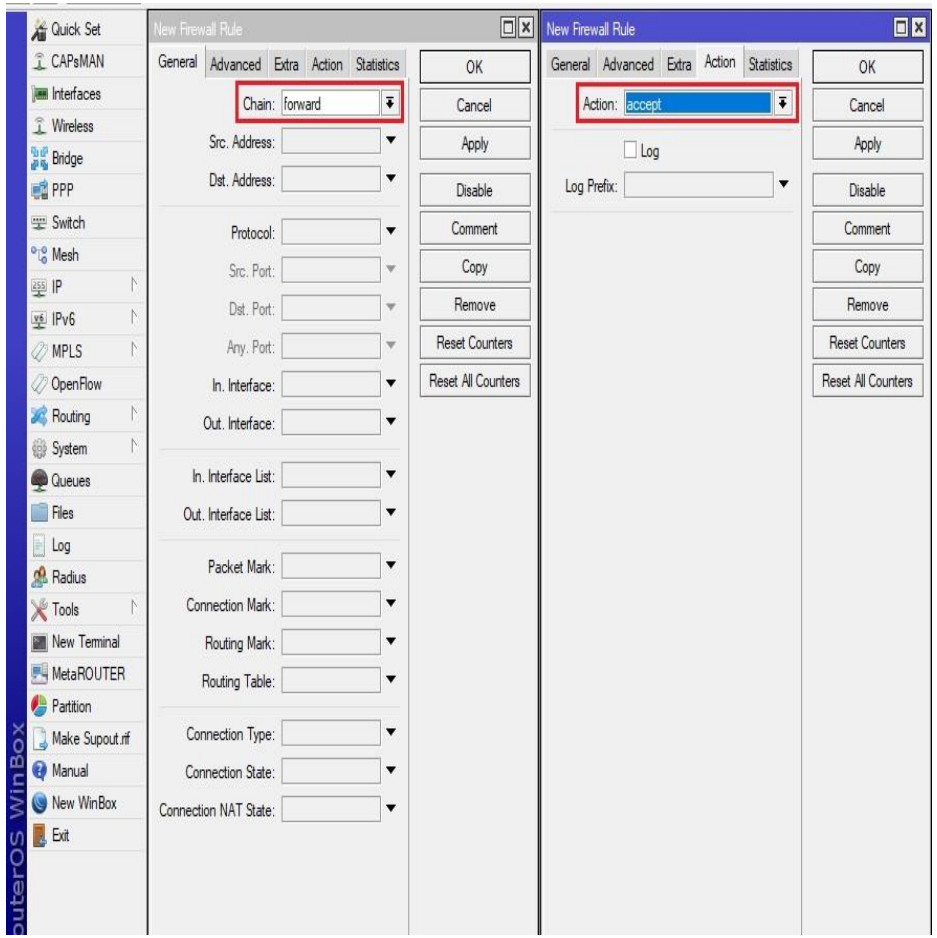
Output Chain: Used to process packets originated from the router and leaving it through one of the interfaces.



Securing Network Information

MikroTik Firewall Filter Chains





Securing Network Information

MikroTik Firewall NAT

NAT is used to translate hots of local area network to the **inside global address** for external communication.

The NAT gateway **(NAT router)** performs IP address rewriting on the way a packet travel from/to LAN.

Types of NAT

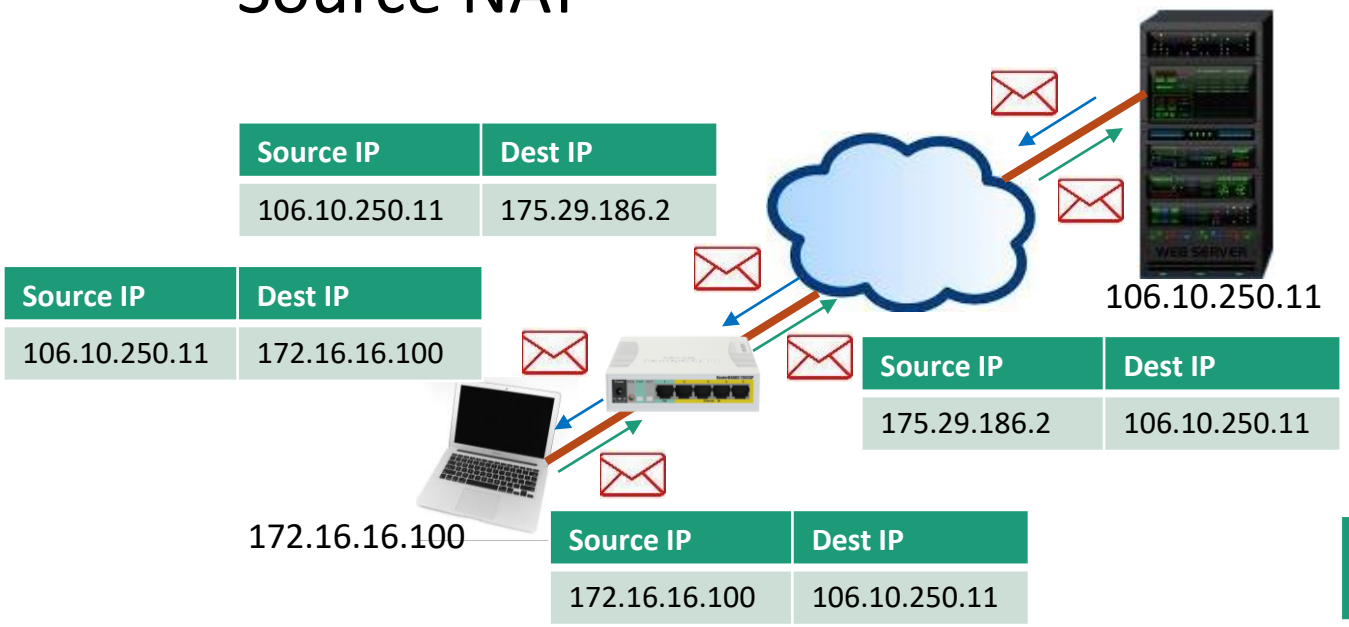
Source NAT: This type of NAT is performed on packets that are **originated from a NATTED network**. A NAT router replaces the private source address of an IP packet with a new public IP address as it travels through the router. A reverse operation is applied to the reply packets travelling in the other direction.

Destination NAT: This type of NAT is performed on packets that are **destined to the NATTED network**. It is most commonly used to make hosts on a private network to be accessible from the Internet. A NAT router performing dstnat replaces the destination IP address of an IP packet as it travel through the router towards a private network.

Securing Network Information

MikroTik Firewall NAT

Source NAT

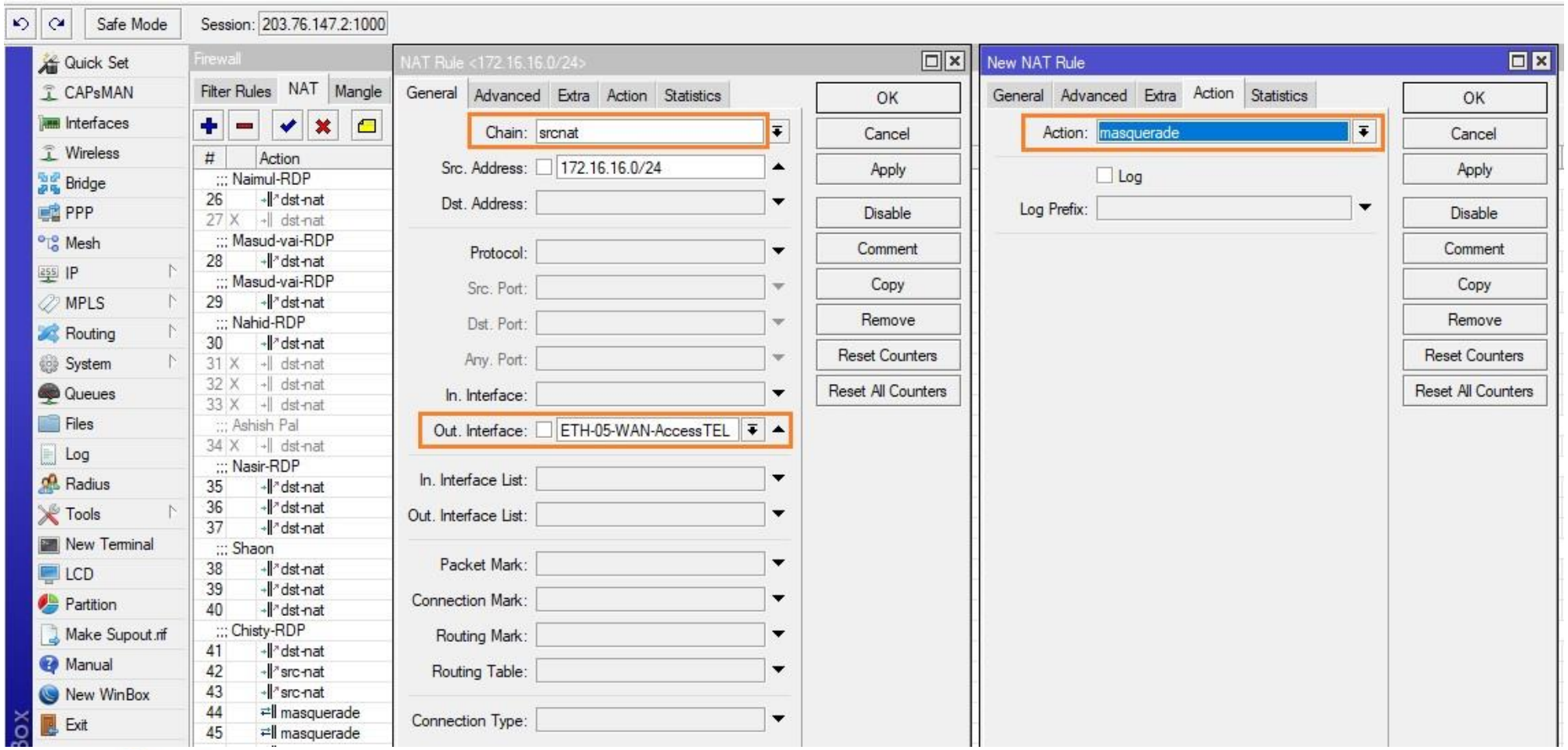


NAT Table

Inside Local IP address	Inside Global IP address
172.16.16.100	175.29.186.2

Securing Network Information

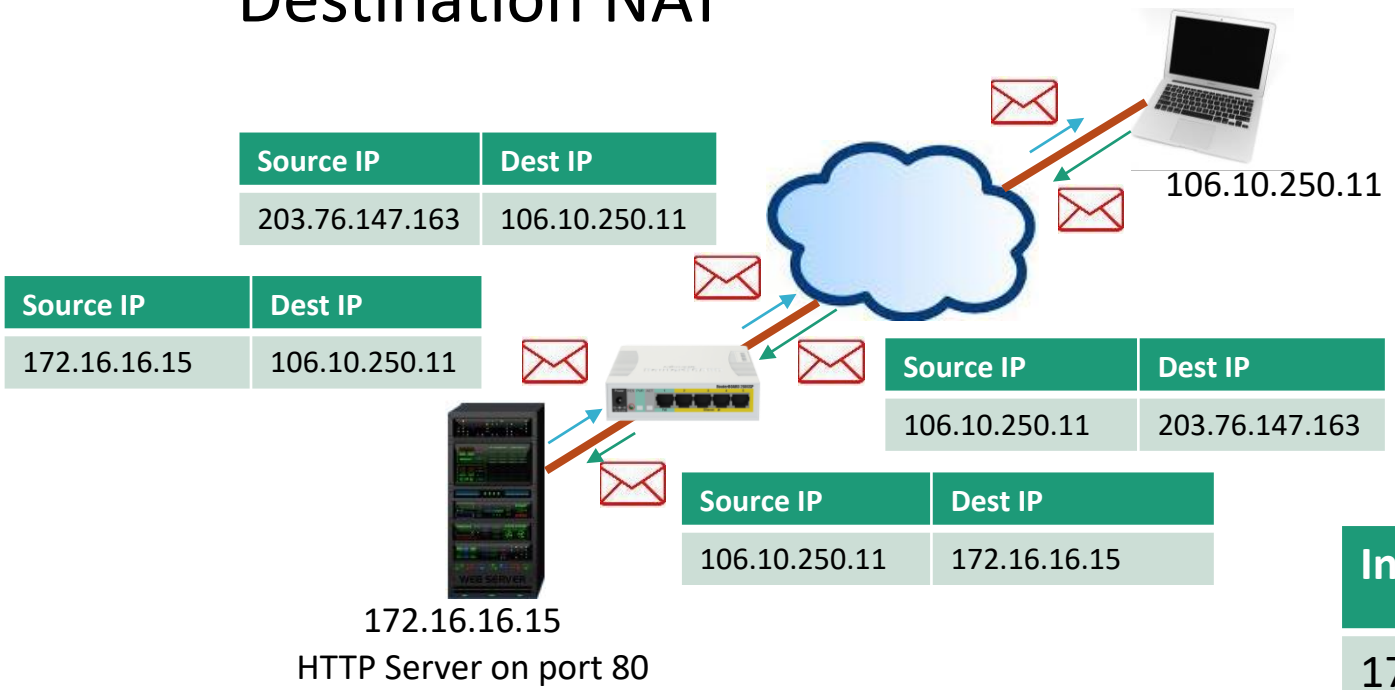
Source NAT



Securing Network Information

MikroTik Firewall NAT

Destination NAT

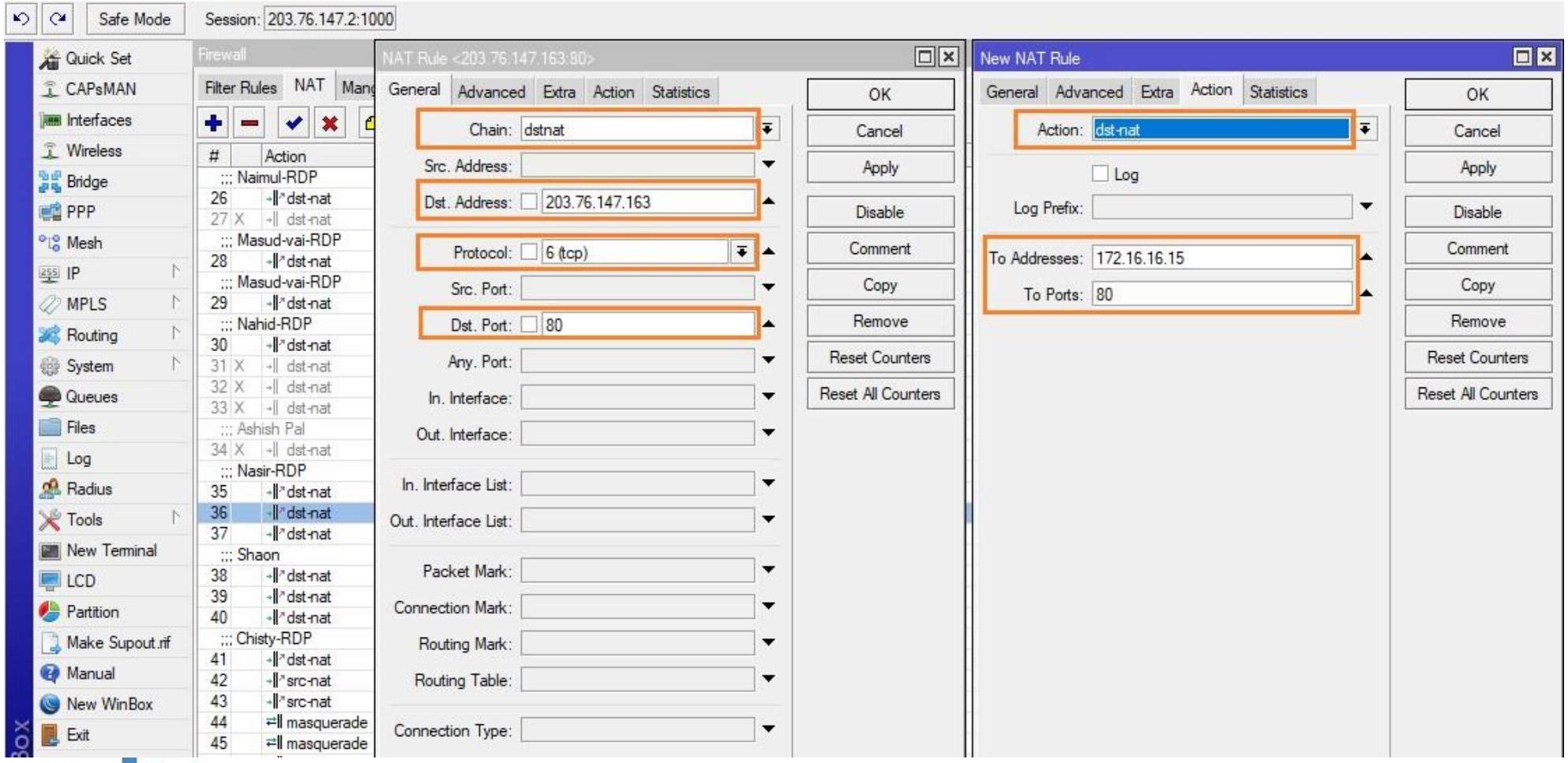


NAT Table

Inside Local IP address	Inside Global IP address
172.16.16.15:80	203.76.147.163:80

Securing Network Information

Destination NAT



Securing Network Information

MikroTik Firewall NAT

Mangle

- Mangle is a kind of 'marker' that marks packets/connection/route for future processing with special marks.
- Mangle marks exist only within the router, they are not transmitted across the network.
- Mainly used in policy based routing, Load balancing, Nating etc.

Securing Network Information

MikroTik Firewall NAT

Mangle

Properties

mark-connection - place a mark specified by the new-connection-mark parameter on the entire connection that matches the rule

mark-packet - place a mark specified by the new-packet-mark parameter on a packet that matches the rule

mark-routing - place a mark specified by the new-routing-mark parameter on a packet. This kind of marks is used for policy routing purposes only

passthrough - if packet is matched by the rule, increase counter and go to next rule (useful for statistics).

return - pass control back to the chain from where the jump took place

route - forces packets to a specific gateway IP by ignoring normal routing decision (prerouting chain only)

Securing Network Information

Thank you