KJK Firewall Implementation Notes

A. Network Configuration IP Address

1. Router Interfaces & Gateways

Device Name	Role	Interface	IP Address	Subnet Mask	Description
Edge Router	Internet Gateway	`ether1`	*DHCP (Dynamic)*	-	Connection to Internet (GNS3 NAT)
		`ether2`	**10.0.0.1**	/30	Uplink to Core Firewall
Firewall	Core Security	`ether1`	**10.0.0.2**	/30	Uplink to Edge Router
		`ether2`	**10.1.40.1**	/30	Downlink to **Admin** Router
		`ether3`	**10.1.20.1**	/30	Downlink to **Akademik** Router
		`ether4`	**10.1.30.1**	/30	Downlink to **Riset/IoT** Router
		`ether5`	**10.1.10.1**	/30	Downlink to **Mahasiswa** Router
		`ether6`	**10.1.50.1**	/30	Downlink to **Guest** Router
		`ether7`	**10.1.60.1**	/30	Downlink to **DMZ** Router
Admin Router	Trusted Zone	`ether1`	**10.1.40.2**	/30	Uplink to Firewall
		`ether2`	**10.20.40.1**	/24	**Gateway for Admin PCs**
Akademik Router	Staff Zone	`ether1`	**10.1.20.2**	/30	Uplink to Firewall
		`ether2`	**10.20.20.1**	/24	**Gateway for Staff PCs**
Riset Router	IoT Zone	`ether1`	**10.1.30.2**	/30	Uplink to Firewall
		`ether2`	**10.20.30.1**	/24	**Gateway for IoT Devices**
Mahasiswa Router	Student Zone	`ether1`	**10.1.10.2**	/30	Uplink to Firewall
		`ether2`	**10.20.10.1**	/22	**Gateway for Students**
Guest Router	Public Zone	`ether1`	**10.1.50.2**	/30	Uplink to Firewall
		`ether2`	**10.20.50.1**	/22	**Gateway for Guests**
DMZ Router	Server Zone	`ether1`	**10.1.60.2**	/30	Uplink to Firewall

Device Name	Role	Interface	IP Address	Subnet Mask	Description
		`ether2`	**10.20.60.1**	/24	**Gateway for Public Servers**

2. Client Network Summary

This table will explain the **CIDR** allocations.

Department	Network Address	Prefix	Usable Host Range	Gateway IP
Admin	`10.20.40.0`	`/24`	`.2` to `.254`	`10.20.40.1`
Akademik	`10.20.20.0`	`/24`	`.2` to `.254`	`10.20.20.1`
Riset & IoT	`10.20.30.0`	`/24`	`.2` to `.254`	`10.20.30.1`
DMZ Servers	`10.20.60.0`	`/24`	`.2` to `.254`	`10.20.60.1`
Mahasiswa	`10.20.8.0`*	`/22`	`8.1` to `11.254`	`10.20.10.1`
Guest	`10.20.48.0`*	`/22`	`48.1` to `51.254`	`10.20.50.1`

*Note: For the /22 networks, the IP address `.10.1` and `.50.1` fall comfortably inside the valid range of their respective blocks.

B. Network Defense Layers

1. Perimeter Defense (Edge Router)

Security Function: *Attack Surface Reduction & Obfuscation.*

- **NAT (Masquerade):**
  - **Function:** It hides your entire internal structure (`10.20.x.x`) behind a single public IP.
  - **Security Value:** An attacker on the internet cannot route directly to your Admin PC or IoT devices. They can only see the Edge Router.
- **Management Plane Hardening (Input Chain):**
  - **Function:** You configured the Edge Router to **DROP** all Telnet/SSH attempts from the Internet and from Unauthorized Internal Zones (Guests/Students).
  - **Security Value:** This protects the **Integrity** of the network. Even if a student guesses your password, they cannot even get the login prompt to type it in.

2. Core Segmentation (Firewall)

Security Function: *Traffic Control & Isolation.*
This is the "Brain" of your security. It implements a **Positive Security Model** (Default Drop). Instead of trying to list all "Bad" things (which is impossible), you blocked *everything* and only listed the "Good" things.

- **Stateful Inspection:**
  - **Function:** The rule `connection-state=established,related action=accept`.
  - **Security Value:** The firewall remembers who started a conversation. If a Student asks for a website (Outbound), the firewall remembers this and automatically lets the website's reply (Inbound) come back. But if a hacker tries to *start* a connection to the Student, it is dropped.

- **Lateral Movement Prevention:**
  - **Function:** The rule `DROP All Other Forward`.
  - **Security Value:** This prevents a compromised device in one department (e.g., a virus on a Student Laptop) from spreading to other departments (like the Admin Server). This preserves **Confidentiality**.

3. Zone-Based Security Policies

Security Function: *Least Privilege Access.*
You divided the network into "Zones" based on trust levels.

Zone	Trust Level	Security Policy	Functionality
Admin	**High**	"God Mode"	**Availability:** Admins need to reach everywhere to fix problems.
Akademik	**Medium**	Selective Access	**Operational Security:** Staff can pull data from IoT sensors (Riset) to do their jobs, but cannot touch Admin data (Confidentiality).
IoT/Riset	**Medium**	Selective Access	**Functionality:** Devices can report data to servers, but are blocked from sensitive networks.
Mahasiswa/Guest	**Zero**	Internet Only	**Isolation:** These are treated as "Hostile." They are granted internet access (Availability) but are strictly firewalled from the Intranet (Confidentiality).
DMZ	**Isolated**	Public Facing	**Containment:** If a Web Server in the DMZ gets hacked, the hacker is trapped. They cannot use the server as a stepping stone to jump into the Admin network.

4. Resilience & Availability (DoS Defense)

Security Function: *Resource Protection.*

- **The "Drop" Logic:**
  - **Function:** As proven in your Flood Test, the Firewall creates a hard wall.
  - **Security Value:** When the Mahasiswa network launched a Traffic Surge (DoS), the firewall absorbed the packets at the gateway level. This ensured that the **Admin Network remained Available**. The attack consumed bandwidth on the *link*, but it did not crash the *target servers*.

Summary of the Network Defense Layer

> *"The configured network ecosystem functions as a **Zero-Trust inspired architecture**. It utilizes **Network Segmentation** to isolate broadcast domains and a **Stateful Core Firewall** to enforce granular Access Control Lists (ACLs).
>
> The system ensures **Confidentiality** by blocking unauthorized lateral movement (e.g., Student to Admin), preserves **Integrity** by hardening the management plane of network devices against internal and external tampering, and maintains **Availability** by filtering malicious traffic surges (DoS) before they reach critical servers."*

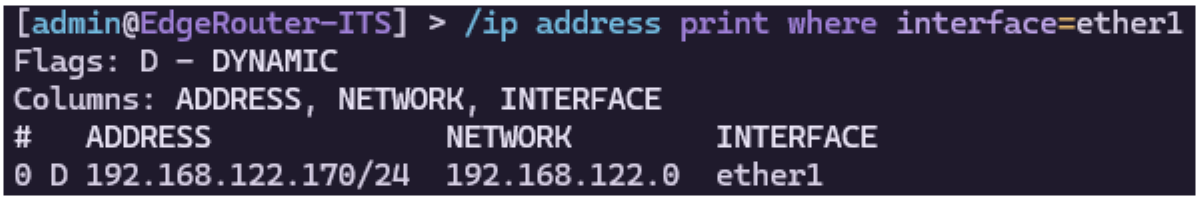
C. Network Defense Layers Testing

1. Perimeter Defense Testing

a. NAT (Network Address Translation)

1. Get the Edge Router's WAN IP by running the command below on **Edge Router**

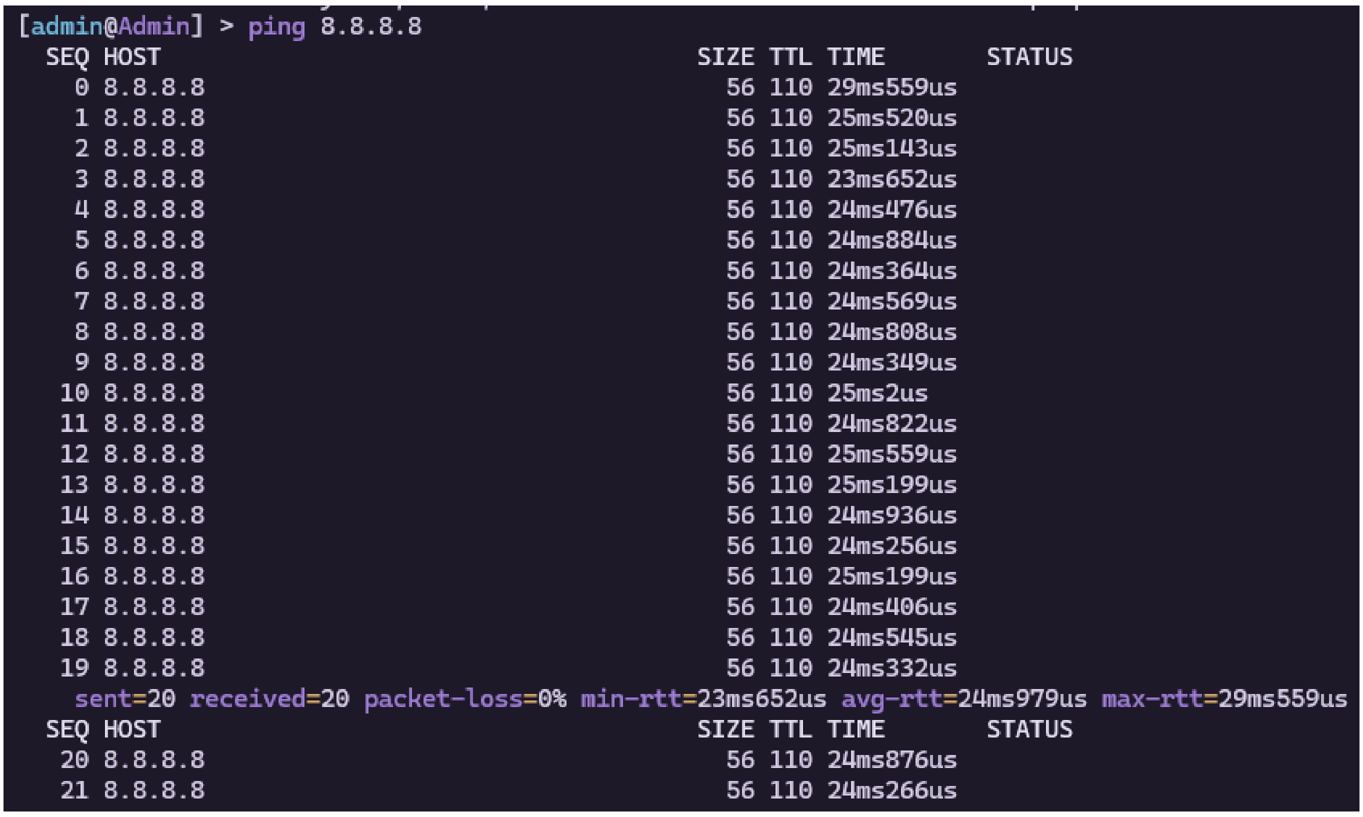
```
/ip address print where interface=ether1
```



```
[admin@EdgeRouter-ITS] > /ip address print where interface=ether1
Flags: D - DYNAMIC
Columns: ADDRESS, NETWORK, INTERFACE
#   ADDRESS              NETWORK        INTERFACE
0 D 192.168.122.170/24  192.168.122.0  ether1
```

2. Generate traffic from the **Admin Router**

```
ping 8.8.8.8
```



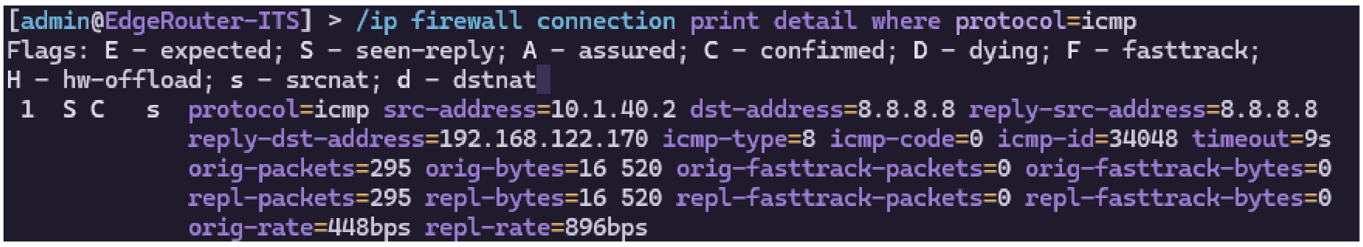
```
[admin@Admin] > ping 8.8.8.8
  SEQ HOST                                     SIZE TTL TIME       STATUS
    0 8.8.8.8                                    56 110 29ms559us
    1 8.8.8.8                                    56 110 25ms520us
    2 8.8.8.8                                    56 110 25ms143us
    3 8.8.8.8                                    56 110 23ms652us
    4 8.8.8.8                                    56 110 24ms476us
    5 8.8.8.8                                    56 110 24ms884us
    6 8.8.8.8                                    56 110 24ms364us
    7 8.8.8.8                                    56 110 24ms569us
    8 8.8.8.8                                    56 110 24ms808us
    9 8.8.8.8                                    56 110 24ms349us
   10 8.8.8.8                                    56 110 25ms2us
   11 8.8.8.8                                    56 110 24ms822us
   12 8.8.8.8                                    56 110 25ms559us
   13 8.8.8.8                                    56 110 25ms199us
   14 8.8.8.8                                    56 110 24ms936us
   15 8.8.8.8                                    56 110 24ms256us
   16 8.8.8.8                                    56 110 25ms199us
   17 8.8.8.8                                    56 110 24ms406us
   18 8.8.8.8                                    56 110 24ms545us
   19 8.8.8.8                                    56 110 24ms332us
    sent=20 received=20 packet-loss=0% min-rtt=23ms652us avg-rtt=24ms979us max-rtt=29ms559us
  SEQ HOST                                     SIZE TTL TIME       STATUS
   20 8.8.8.8                                    56 110 24ms876us
   21 8.8.8.8                                    56 110 24ms266us
```

or use this instead:

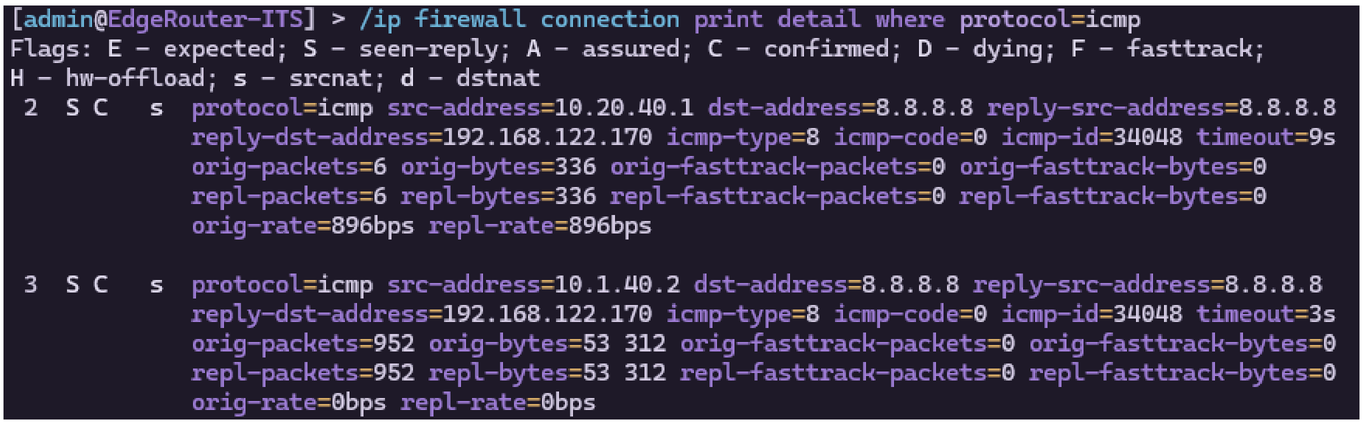
```
ping 8.8.8.8 src-address=10.20.40.1
```

3. Look at the Connection Table on **Edge Router**

```
/ip firewall connection print detail where protocol=icmp
```



```
[admin@EdgeRouter-ITS] > /ip firewall connection print detail where protocol=icmp
Flags: E - expected; S - seen-reply; A - assured; C - confirmed; D - dying; F - fasttrack;
H - hw-offload; s - srcnat; d - dstnat
 1  S C   s  protocol=icmp src-address=10.1.40.2 dst-address=8.8.8.8 reply-src-address=8.8.8.8
             reply-dst-address=192.168.122.170 icmp-type=8 icmp-code=0 icmp-id=34048 timeout=9s
             orig-packets=295 orig-bytes=16 520 orig-fasttrack-packets=0 orig-fasttrack-bytes=0
             repl-packets=295 repl-bytes=16 520 repl-fasttrack-packets=0 repl-fasttrack-bytes=0
             orig-rate=448bps repl-rate=896bps
```



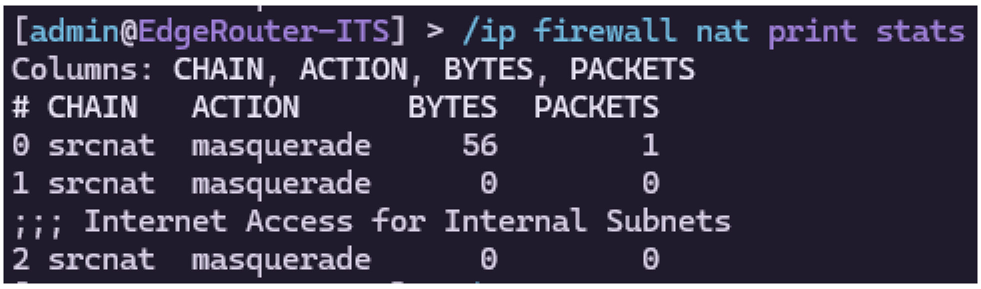
```
[admin@EdgeRouter-ITS] > /ip firewall connection print detail where protocol=icmp
Flags: E - expected; S - seen-reply; A - assured; C - confirmed; D - dying; F - fasttrack;
H - hw-offload; s - srcnat; d - dstnat
 2   S C   s  protocol=icmp src-address=10.20.40.1 dst-address=8.8.8.8 reply-src-address=8.8.8.8
              reply-dst-address=192.168.122.170 icmp-type=8 icmp-code=0 icmp-id=34048 timeout=9s
              orig-packets=6 orig-bytes=336 orig-fasttrack-packets=0 orig-fasttrack-bytes=0
              repl-packets=6 repl-bytes=336 repl-fasttrack-packets=0 repl-fasttrack-bytes=0
              orig-rate=896bps repl-rate=896bps

 3   S C   s  protocol=icmp src-address=10.1.40.2 dst-address=8.8.8.8 reply-src-address=8.8.8.8
              reply-dst-address=192.168.122.170 icmp-type=8 icmp-code=0 icmp-id=34048 timeout=3s
              orig-packets=952 orig-bytes=53 312 orig-fasttrack-packets=0 orig-fasttrack-bytes=0
              repl-packets=952 repl-bytes=53 312 repl-fasttrack-packets=0 repl-fasttrack-bytes=0
              orig-rate=0bps repl-rate=0bps
```

- We can know if it had worked if

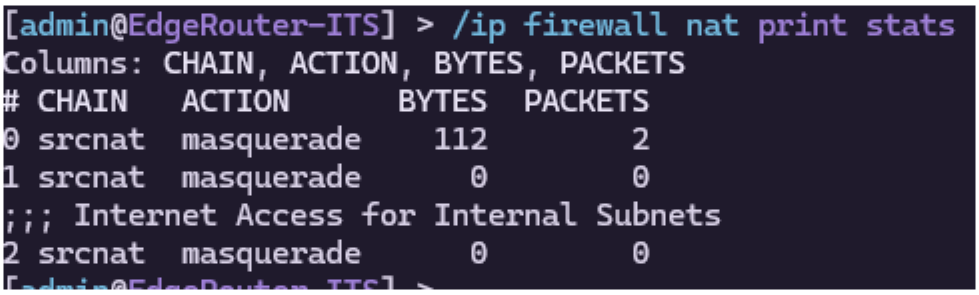
Other than the 3rd step from above, we can also use this method:

```
/ip firewall nat print stats
```

- Look at the **masquerade** rule
- If the **Packets** column is **increasing** while you run the ping from the Admin Router, **NAT is working**.



```
[admin@EdgeRouter-ITS] > /ip firewall nat print stats
Columns: CHAIN, ACTION, BYTES, PACKETS
# CHAIN   ACTION      BYTES  PACKETS
0 srcnat  masquerade     56        1
1 srcnat  masquerade      0        0
;;; Internet Access for Internal Subnets
2 srcnat  masquerade      0        0
```



```
[admin@EdgeRouter-ITS] > /ip firewall nat print stats
Columns: CHAIN, ACTION, BYTES, PACKETS
# CHAIN   ACTION      BYTES  PACKETS
0 srcnat  masquerade    112        2
1 srcnat  masquerade      0        0
;;; Internet Access for Internal Subnets
2 srcnat  masquerade      0        0
[admin@EdgeRouter-ITS] >
```