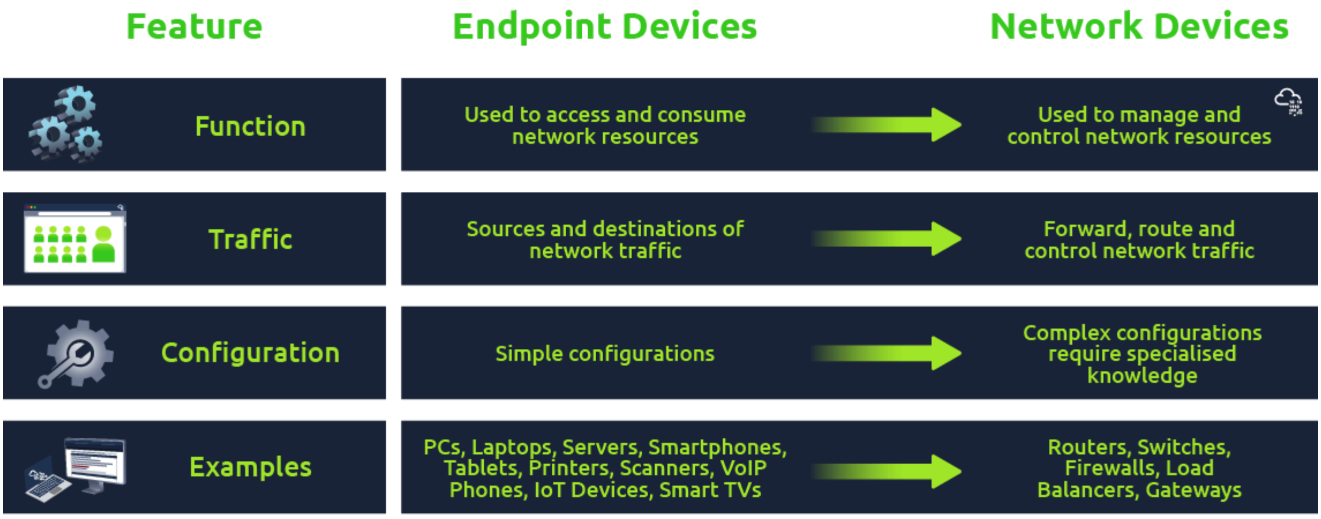
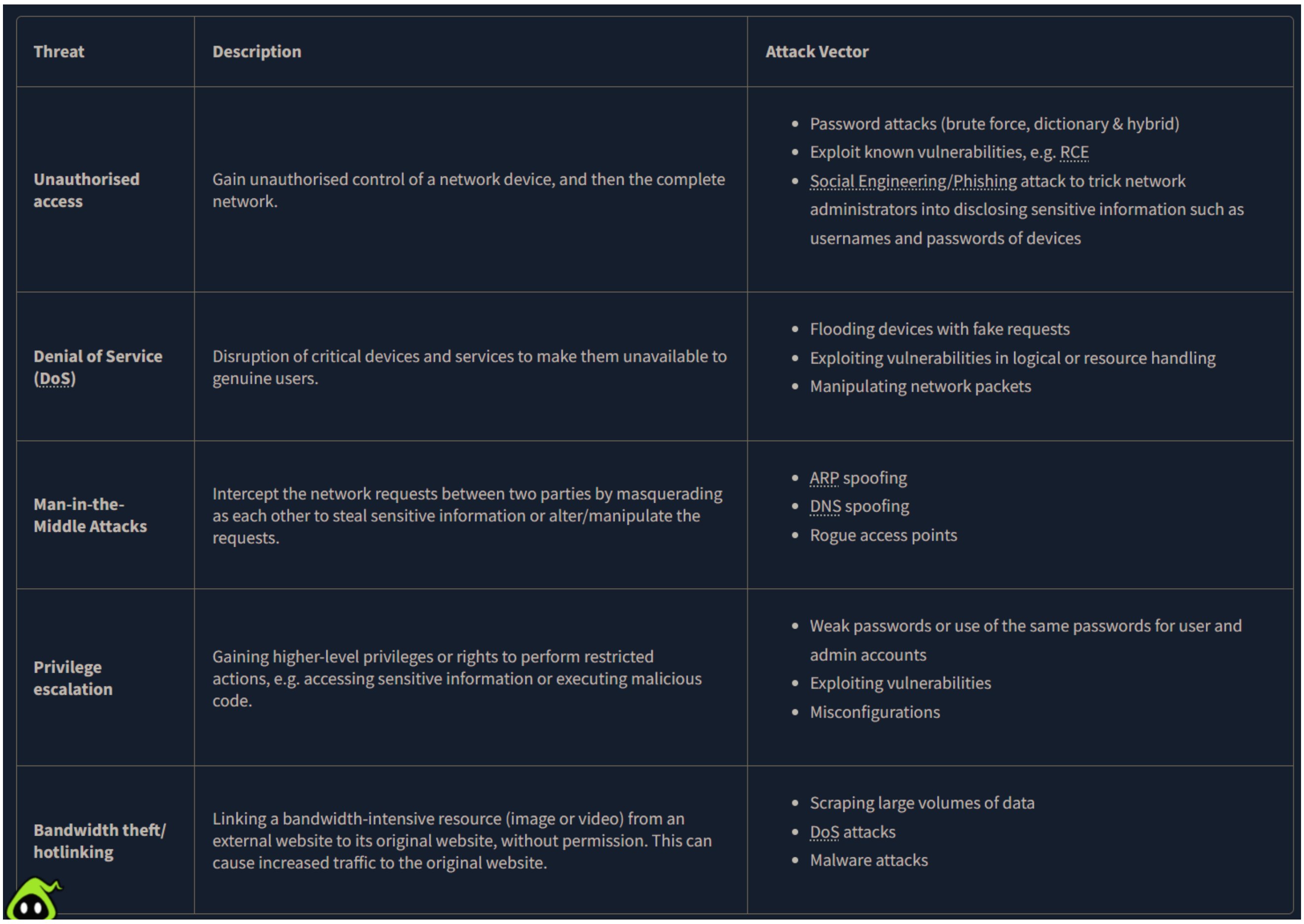
Network Device Hardening

Common Treat and Attack Vectors



Feature	Endpoint Devices	Network Devices
Function	Used to access and consume network resources	Used to manage and control network resources
Traffic	Sources and destinations of network traffic	Forward, route and control network traffic
Configuration	Simple configurations	Complex configurations require specialised knowledge
Examples	PCs, Laptops, Servers, Smartphones, Tablets, Printers, Scanners, VoIP Phones, IoT Devices, Smart TVs	Routers, Switches, Firewalls, Load Balancers, Gateways



Threat	Description	Attack Vector
Unauthorised access	Gain unauthorised control of a network device, and then the complete network.	• Password attacks (brute force, dictionary & hybrid) • Exploit known vulnerabilities, e.g. RCE • Social Engineering/Phishing attack to trick network administrators into disclosing sensitive information such as usernames and passwords of devices
Denial of Service (DoS)	Disruption of critical devices and services to make them unavailable to genuine users.	• Flooding devices with fake requests • Exploiting vulnerabilities in logical or resource handling • Manipulating network packets
Man-in-the-Middle Attacks	Intercept the network requests between two parties by masquerading as each other to steal sensitive information or alter/manipulate the requests.	• ARP spoofing • DNS spoofing • Rogue access points
Privilege escalation	Gaining higher-level privileges or rights to perform restricted actions, e.g. accessing sensitive information or executing malicious code.	• Weak passwords or use of the same passwords for user and admin accounts • Exploiting vulnerabilities • Misconfigurations
Bandwidth theft/ hotlinking	Linking a bandwidth-intensive resource (image or video) from an external website to its original website, without permission. This can cause increased traffic to the original website.	• Scraping large volumes of data • DoS attacks • Malware attacks

Common Hardening Techniques

- **Updating & Patching**: Ensuring the latest version of the Operating System and underlying applications of all devices and systems and installing regular security patches is the core hardening measure. Outdated OS and applications contain vulnerabilities that attackers can exploit.

- **Disabling unnecessary services & ports**: Turn off all unnecessary services and block all ports (physical and virtual) that are not needed for system functionality. This will reduce the attack surface by minimizing the number of entry points an attacker can exploit.
- **Principle of Least Privilege (POLP)**: Restrict users and processes to only the minimum necessary permissions required to perform their functions.
- **Logs Monitoring**: Implement a log monitoring system to monitor for unusual activity or security events.
- **Backup regularly**: Take routine backups of systems and configurations as they can help recover from a security incident or system failure.
- **Enforcing Strong Passwords**: Change default login passwords and use strong passwords that are at least ten characters long with a combination of small letters, capital letters, special characters, and numbers. These types of passwords protect against dictionary and brute-force attacks.
- **Multi-Factor Authentication (MFA)**: MFA is an additional security layer requiring two or more types of identification before accessing the account or system. The two factors are generally something we know (like passwords) and something we have (like biometrics).

Importance of Secure Protocols

- Secure protocols play a critical role in network device hardening by protecting against unauthorized access and data breaches.
- They ensure that sensitive data transmitted between devices is encrypted and cannot be intercepted by malicious actors. Moreover, secure protocols also help prevent man-in-the-middle attacks and other network-based exploits.
- Using secure protocols, network administrators can ensure that only authorized personnel can access sensitive information and perform system administration tasks. Necessary security protocols include **HTTPS, SSH, SSL/TLS, and IPsec.**

Removal/Blocking of Insecure Protocols

In addition to using secure protocols, removing and blocking access to those insecure protocols is equally essential, which will decrease an attacker's attack surface.

- Most important are the protocols that transmit data in clear text without encrypting them, like **FTP, HTTP, Telnet, SMTP**, and more. Moreover, there are inherently secure protocols (e.g. LDAP, RDP, SIPS); however, they can allow attackers to exploit the network if configured incorrectly.

Implementation of Monitoring and Logging Controls

Logging in network devices is essential for detecting and investigating security incidents, identifying performance issues, and complying with regulatory requirements. It provides a record of events and activities on the device, which can be used for troubleshooting, forensic analysis, and auditing purposes. The following techniques are generally used for logging:

- **Syslog**: A protocol to standardize the transfer of log messages, with the purpose of storing and analyzing log messages to a central server.
- **SNMP**: Traps a notification sent by a network device to a management system when a predefined event occurs.
- **NetFlow**: A protocol used to collect and analyze network traffic data for monitoring and security analysis.
- **Packet Captures**: Capturing network traffic and storing it for analysis using a tool like Wireshark.

Some of the significant hardening practices for a VPN server:

- Use strong encryption algorithm: Configure the VPN gateway to use strong encryption to protect data in transit.
- The **cipher** directive in the config file can be used to select the encryption scheme. The possible options for cipher include **AES, Blowfish, Camellia,** and more. For example, **AES-128-CBC** mode means to use the AES encryption algorithm with a key size of 128-bit in Cipher Block Chaining (CBC) mode, as seen below. **AES-256-CBC** is typically considered one of the strongest cipher encryption nowadays.

Some of the significant hardening practices for a VPN server:

- Use strong encryption algorithm: Configure the VPN gateway to use strong encryption to protect data in transit. The **cipher** directive in the config file can be used to select the encryption scheme. The possible options for cipher include AES, Blowfish, Camellia, and more. For example, **AES-128-CBC** mode means to use the AES encryption algorithm with a key size of 128-bit in Cipher Block Chaining (CBC) mode, as seen below. **AES-256-CBC** is typically considered one of the strongest cipher encryption nowadays.

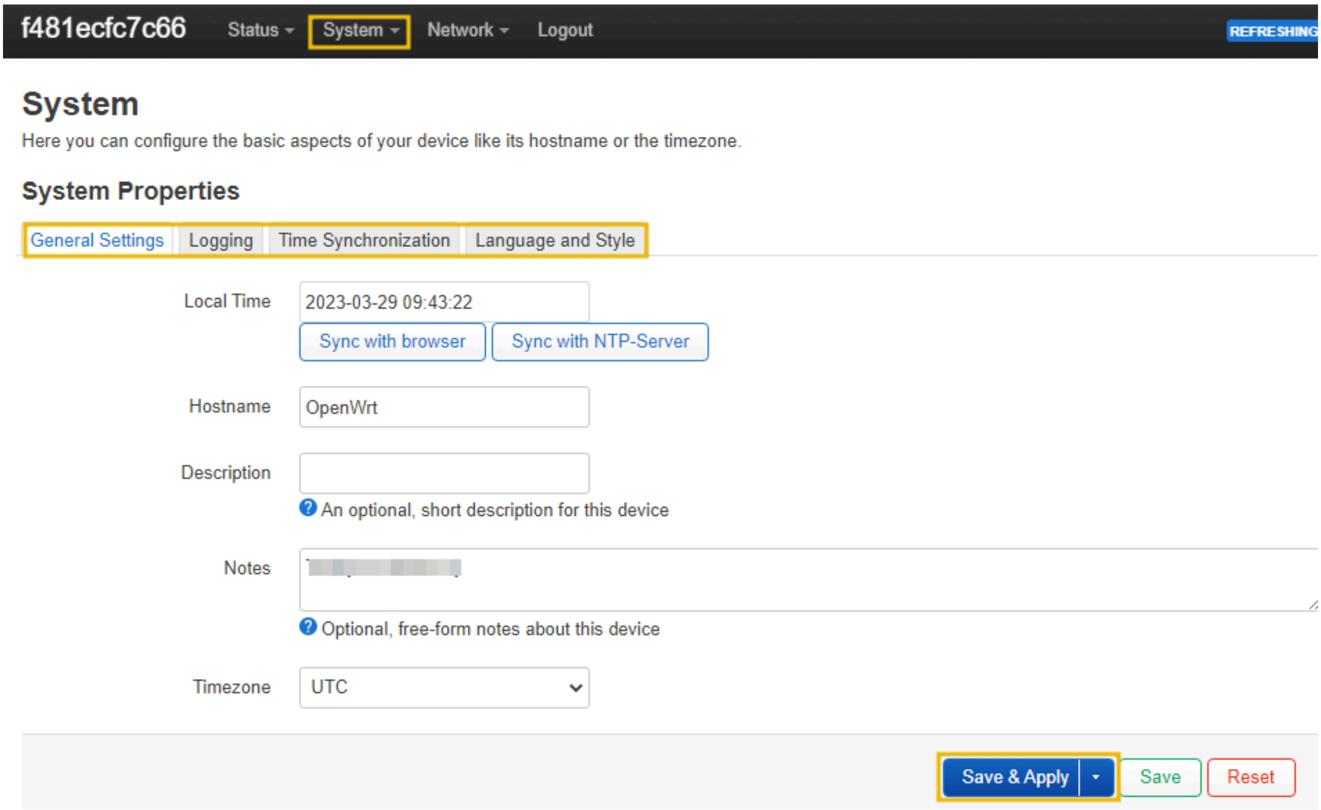
Implement strong authentication:

- Use strong authentication mechanisms such as a combination of Transport Layer Security (TLS) and a secure hashing algorithm. We can use the `auth` directive to specify the exact algorithm in the OpenVPN configuration file to ensure that a secure hashing algorithm will be used for packet authentication.
- Some of the options for auth directive are **SHA1, SHA128, SHA256, SHA512 and MD5**. You can set the auth directive through the following command:
- **Change default settings**: Change the default usernames and passwords to something unique to reduce the risk of unauthorised access to the VPN gateway.

Hardening Routers, Switches & Firewalls

Recommended Hardening Techniques

- **Setting up the device**: While setting up any network device, it is necessary to fill in all relevant details like hostname, time zone, logging, and more. These features assist in conducting incident handling in case of a compromise.
- **For example**, logging must be enabled to log all the events with the default alert level `Debug`. Similarly, time zone and time synchronization must be set accurately to properly correlate events with their occurrence time. You can enable and modify these settings through `System > System` and select the desired option.



System

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

Local Time: 2023-03-29 09:43:22

Hostname: OpenWrt

Description:

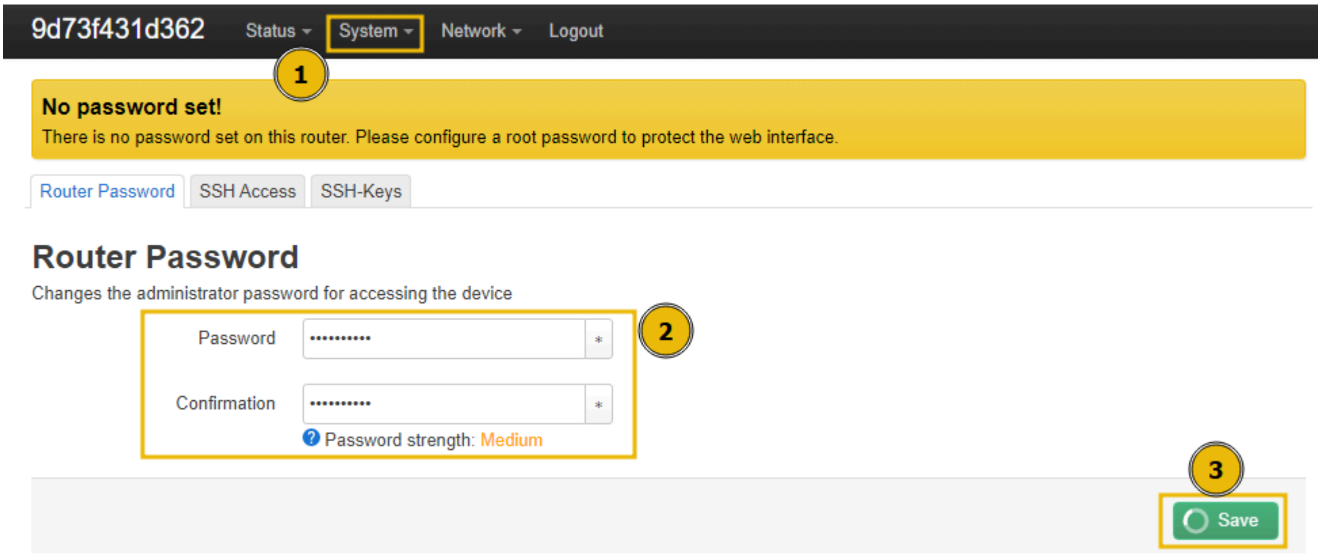
An optional, short description for this device

Notes: [redacted]

Optional, free-form notes about this device

Timezone: UTC

- **Change default credentials**: Usually, the admin web interface is protected through a username and password, and people tend to ignore changing the default.
- A threat actor can access the router's admin interface and compromise the whole network using default credentials. We can change the default password in OpenWrt through `System > Administration`, enter a new password, and click the `Save` button.



No password set!

There is no password set on this router. Please configure a root password to protect the web interface.

Router Password

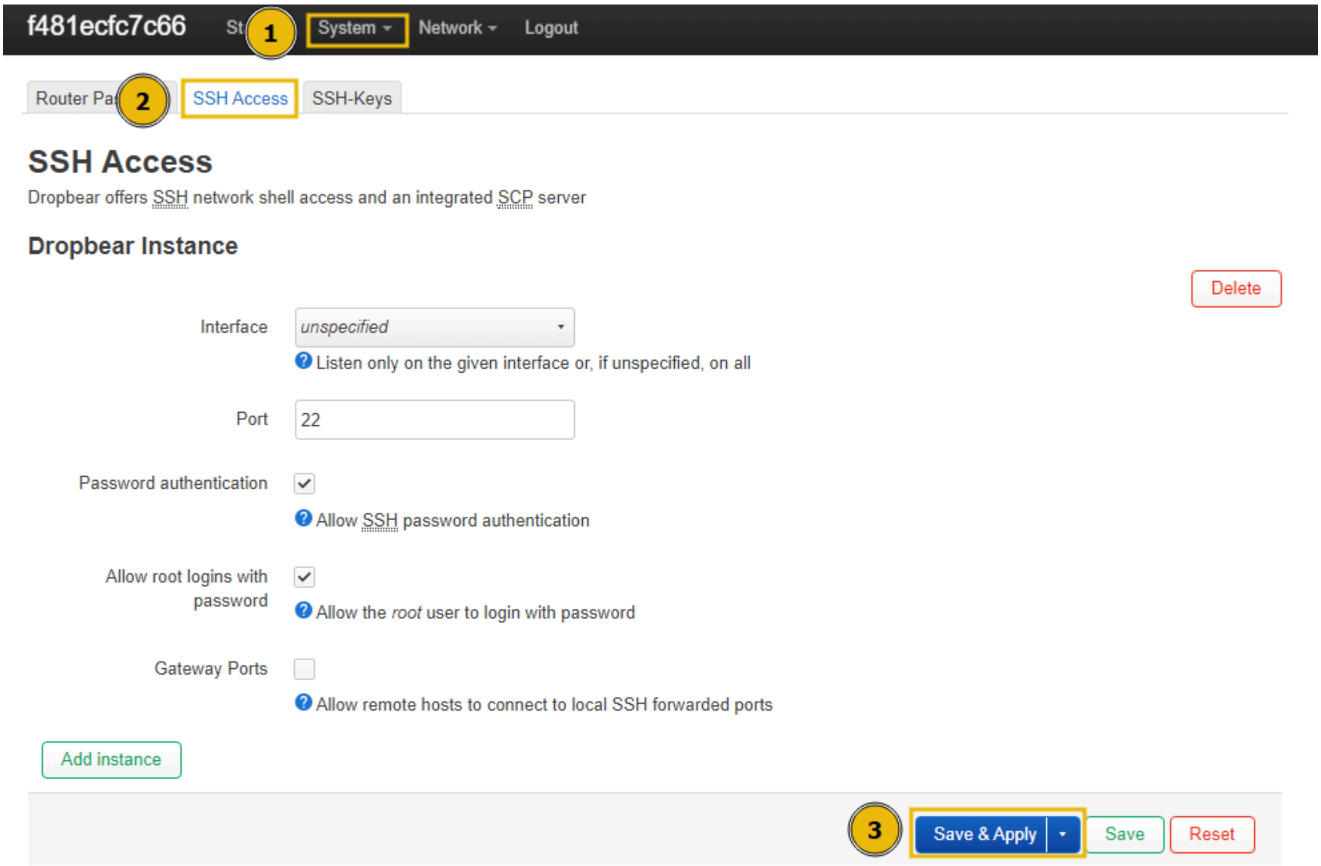
Changes the administrator password for accessing the device

Password: ••••••••••

Confirmation: ••••••••••

Password strength: Medium

- **Enable secure network protocols**: For a network device to maintain the confidentiality, integrity, and availability of network traffic, secure protocols must be enabled. Secure protocols like **HTTPS, SSH, and SSL/TLS** offer encrypted authentication mechanisms and communications to stop unauthorized access and eavesdropping.
- By enabling secure protocols on a router, you can reduce the risk of data breaches, man-in-the-middle attacks, and other security threats. You can enable SSH in OpenWrt through `System > Administration > SSH Access`, then select the interface and port number and click `Save & Apply`. Moreover, you can also add specific public SSH-Keys for passwordless login.



SSH Access

Dropbear offers SSH network shell access and an integrated SCP server

Dropbear Instance

Interface: *unspecified*

Listen only on the given interface or, if unspecified, on all

Port: 22

Password authentication ☑

Allow SSH password authentication

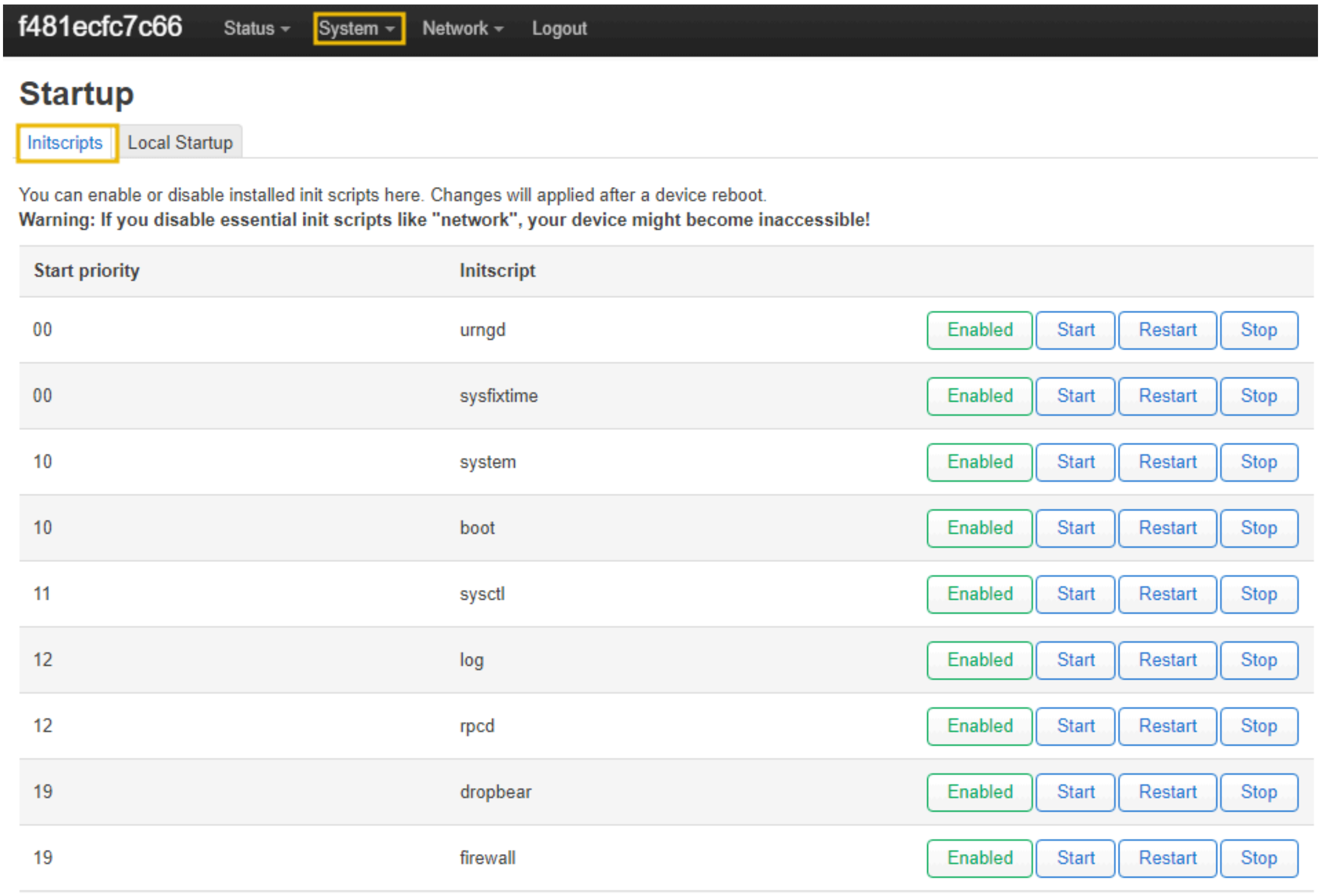
Allow root logins with password ☑

Allow the *root* user to login with password

Gateway Ports ☐

Allow remote hosts to connect to local SSH forwarded ports

- **Disabling unnecessary scripts**: Almost every network device executes some startup scripts to provide a better user experience to a user.
- For example, crontab is executed on startup to verify and execute any cron job. Threat actors try to gain persistent access on a network device by adding their malicious scripts on the startup. We can add/remove startup scripts and set the priority through `System > Startup`.

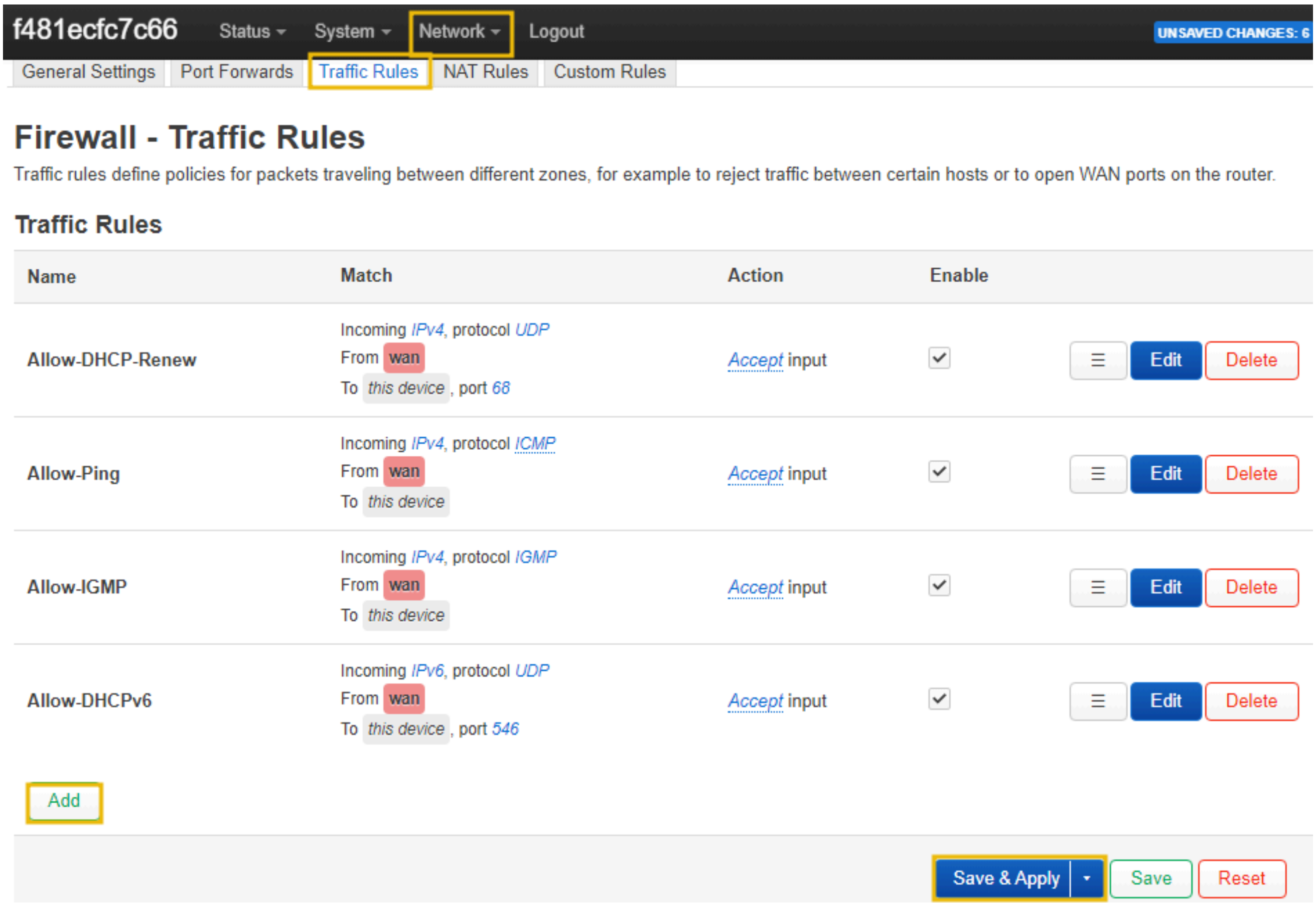


Startup

You can enable or disable installed init scripts here. Changes will applied after a device reboot.
Warning: If you disable essential init scripts like "network", your device might become inaccessible!

Start priority	Initscript	
00	urngd	Enabled Start Restart Stop
00	sysfixtime	Enabled Start Restart Stop
10	system	Enabled Start Restart Stop
10	boot	Enabled Start Restart Stop
11	sysctl	Enabled Start Restart Stop
12	log	Enabled Start Restart Stop
12	rpcd	Enabled Start Restart Stop
19	dropbear	Enabled Start Restart Stop
19	firewall	Enabled Start Restart Stop

- **Securing Wi-Fi**: If the router has Wi-Fi capabilities, securing the Wi-Fi by enabling strong encryption like **WPA2/WPA3, disabling SSID** broadcast, changing default passwords, and more.
- **Manage traffic rules**: Network devices allow you to create and implement traffic rules that accept/deny network traffic.
- For example, we notice that the data of users connected with our network device is being exfiltrated to a command and control server IP address. We can create a rule to block all traffic where the destination IP matches the attacker's command and control server. We can add/edit traffic rules through `Network > Firewall > Traffic Rules`, and click `Add` to create a new rule.



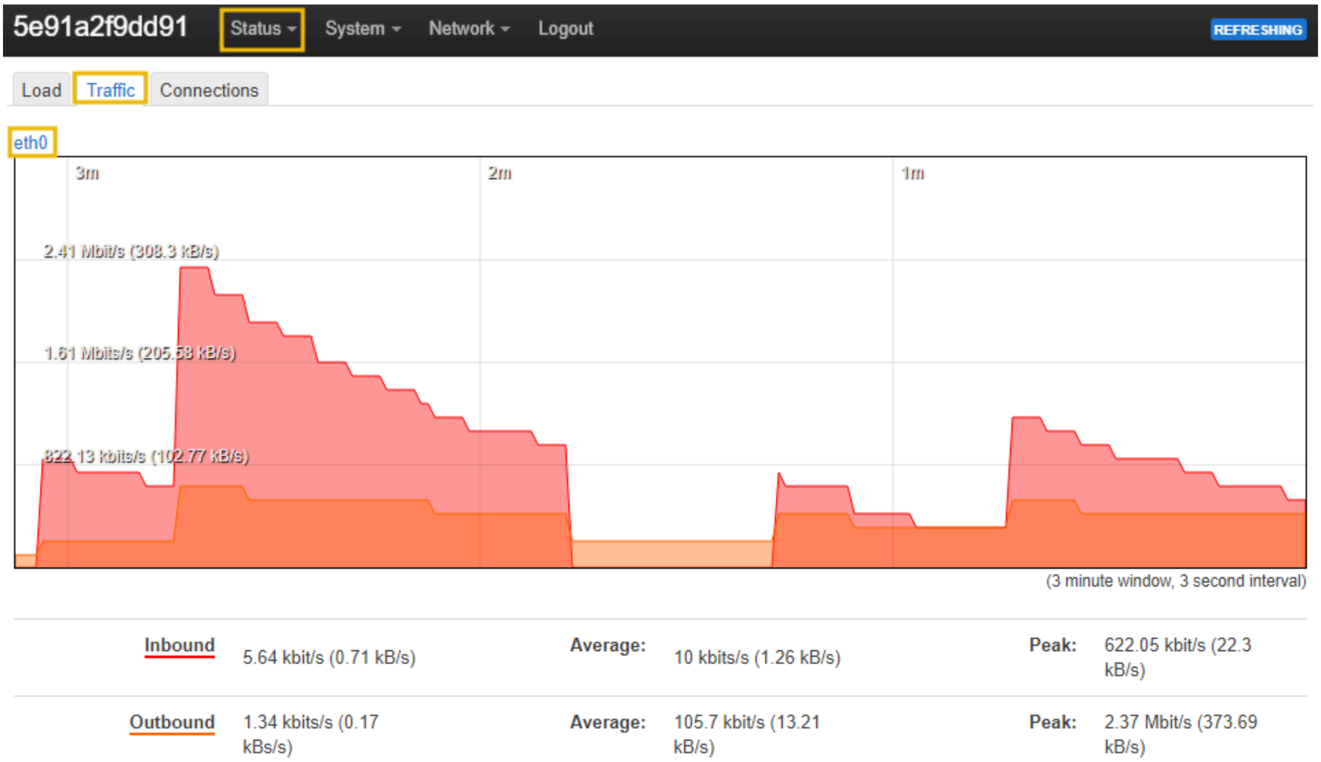
Firewall - Traffic Rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

Traffic Rules

Name	Match	Action	Enable	
Allow-DHCP-Renew	Incoming *IPv4*, protocol *UDP* From wan To *this device* , port *68*	*Accept* input	☑	☰ Edit Delete
Allow-Ping	Incoming *IPv4*, protocol *ICMP* From wan To *this device*	*Accept* input	☑	☰ Edit Delete
Allow-IGMP	Incoming *IPv4*, protocol *IGMP* From wan To *this device*	*Accept* input	☑	☰ Edit Delete
Allow-DHCPv6	Incoming *IPv6*, protocol *UDP* From wan To *this device* , port *546*	*Accept* input	☑	☰ Edit Delete

- **Monitor traffic**: As a network administrator, keeping track of network traffic, like uploads and downloads of data at different intervals, is essential.
- For example, you have excessive data uploaded from one of the email servers to an unknown IP address. Such alerts enable you to take remedial measures and stop data pilferage timely. Usually, network devices provide real-time graphs to monitor the traffic. We can view real-time traffic statistics through `Status > Realtime Graph > Traffic`.

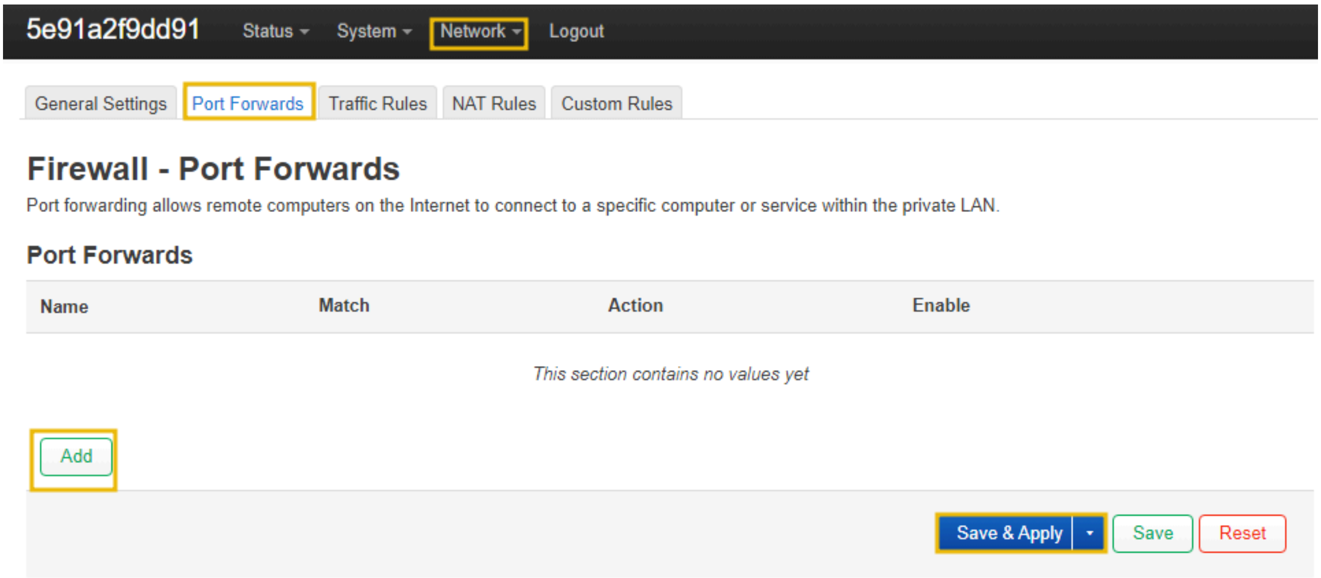


(3 minute window, 3 second interval)

Inbound	5.64 kbit/s (0.71 kB/s)	Average:	10 kbit/s (1.26 kB/s)	Peak:	622.05 kbit/s (22.3 kB/s)
Outbound	1.34 kbit/s (0.17 kB/s)	Average:	105.7 kbit/s (13.21 kB/s)	Peak:	2.37 Mbit/s (373.69 kB/s)

Note: Since no client is connected with the network device, you won't see any traffic in the real-time traffic statistics on the target machine.

- **Configuring port forwarding**: A firewall's port forwarding capability enables inbound traffic from the internet or other sources to be routed to a particular device or service on the internal network. The firewall can send incoming traffic to the appropriate device or service on the internal network by establishing port forwarding rules while blocking any other incoming traffic that does not comply with the rules.
- This feature helps host applications that need outside access, granting remote control of internal devices. Port forwarding should be used carefully because it can expose internal devices and services to potential security issues if improperly secured and configured.
- Threat actors could add new rules here for creating connections to external command and control servers. We can configure port forwarding through `Network > Firewall > Port Forwards`, and click the `Add` button.



Firewall - Port Forwards

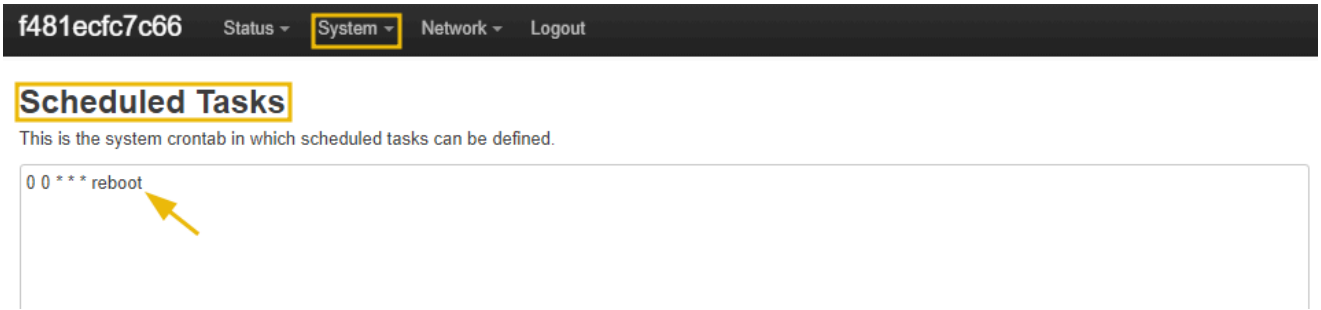
Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Port Forwards

Name	Match	Action	Enable

This section contains no values yet

- **Monitoring scheduled tasks**: It is important to monitor scheduled tasks to confirm that the original scheduled tasks lists are not modified by a threat actor. To add or remove scheduled tasks, which in our case are handled by cron, navigate to `System > Scheduled Tasks`, add the new cron job, and click `Save`. You can learn how to create cron jobs here.

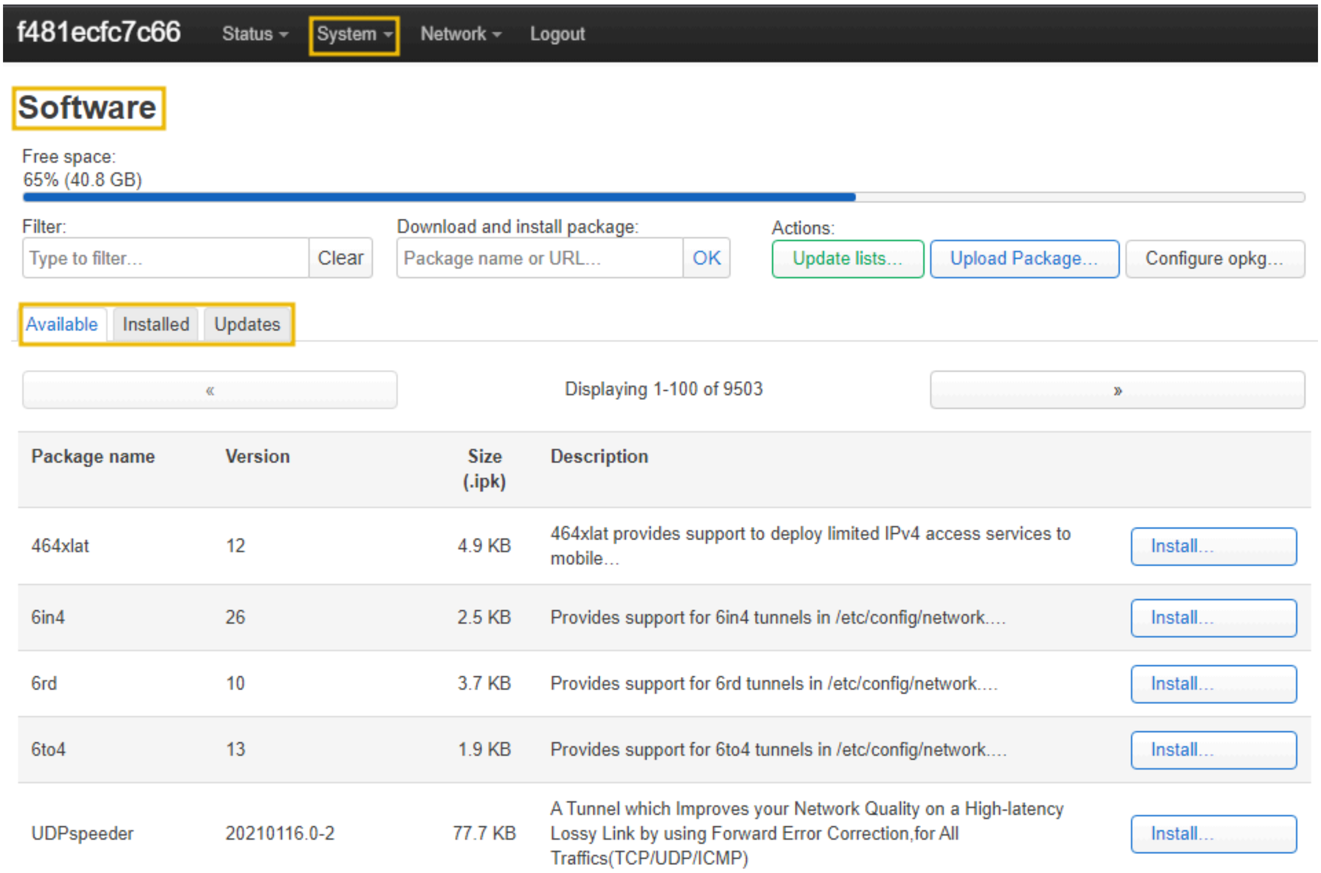


Scheduled Tasks

This is the system crontab in which scheduled tasks can be defined.

```
0 0 * * * reboot
```

- **Update firmware**: It is essential to update the firmware and installed packages on a regular basis to avoid any know/unknown attacks. We can update the firmware through `System > Software`.



Free space:
65% (40.8 GB)

Displaying 1-100 of 9503

Package name	Version	Size (.ipk)	Description	
464xlat	12	4.9 KB	464xlat provides support to deploy limited IPv4 access services to mobile...	Install...
6in4	26	2.5 KB	Provides support for 6in4 tunnels in /etc/config/network....	Install...
6rd	10	3.7 KB	Provides support for 6rd tunnels in /etc/config/network....	Install...
6to4	13	1.9 KB	Provides support for 6to4 tunnels in /etc/config/network....	Install...
UDPspeeder	20210116.0-2	77.7 KB	A Tunnel which Improves your Network Quality on a High-latency Lossy Link by using Forward Error Correction,for All Traffics(TCP/UDP/ICMP)	Install...

Additional Techniques in an Enterprise Environment

A network device deployed in an enterprise environment generally provides an increased attack surface for an attacker to launch attacks. As enterprise environments include a variety of devices with different models, makes, and types, there are no definite rules to harden network devices; however, a few important ones are mentioned below:

- **Configuring port security**: This includes limiting the number of MAC addresses registered on a switch port and taking particular action whenever unauthorised access is detected. Enabling port security enables an administrator that data is coming from a valid source and will be forwarded to a legitimate receiver.
- **Preventing ARP spoofing**: ARP spoofing is one of the most common vectors for launching man-in-the-middle attacks on the network. The threat can be mitigated by enabling static ARP tables and implementing MAC address filtering. You can learn more about mitigating ARP spoofing here.
- **Preventing rogue DHCP servers**: The attacker creates a spoofed DHCP server that can be later on used for assigning IPs to clients and launching MITM attacks. Mitigation measures to prevent such attacks include configuring static DHCP binding and ensuring no unknown devices are added to a network through network mapping tools. You can learn more about DHCP here.
- **Enabling IPv6**: Unlike IPv4, IPv6 has built-in support of IPsec that can be used to secure network communication and provide confidentiality, integrity, and authenticity. Moreover, this will help in protection against MITM, eavesdropping, and tampering of packets in transit.

A network device is configured with many options for protection against cyberattacks. We have discussed some of the most common and important ones in this task.