SD-WAN Solution

Taking NU-6000 as the main model

What is SD-WAN?

SD-WAN is a mechanism that can bind any combination of outbound connection or VPN tunnels into a unified control. As long as the tunnel can independently connect to others remotely, it can be combined freely and weighted differently according to users' needs.
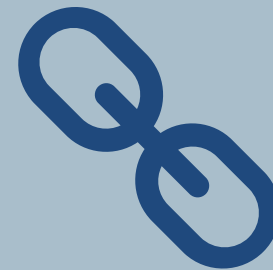
Advantages of SD-WAN

Save money

- MPLS normally costs a lot, especially when the environments require a lot of lines.

High integration

- Can combine multiple connections through the mechanism of SD-WAN
- Be able to customize the weights for each connections
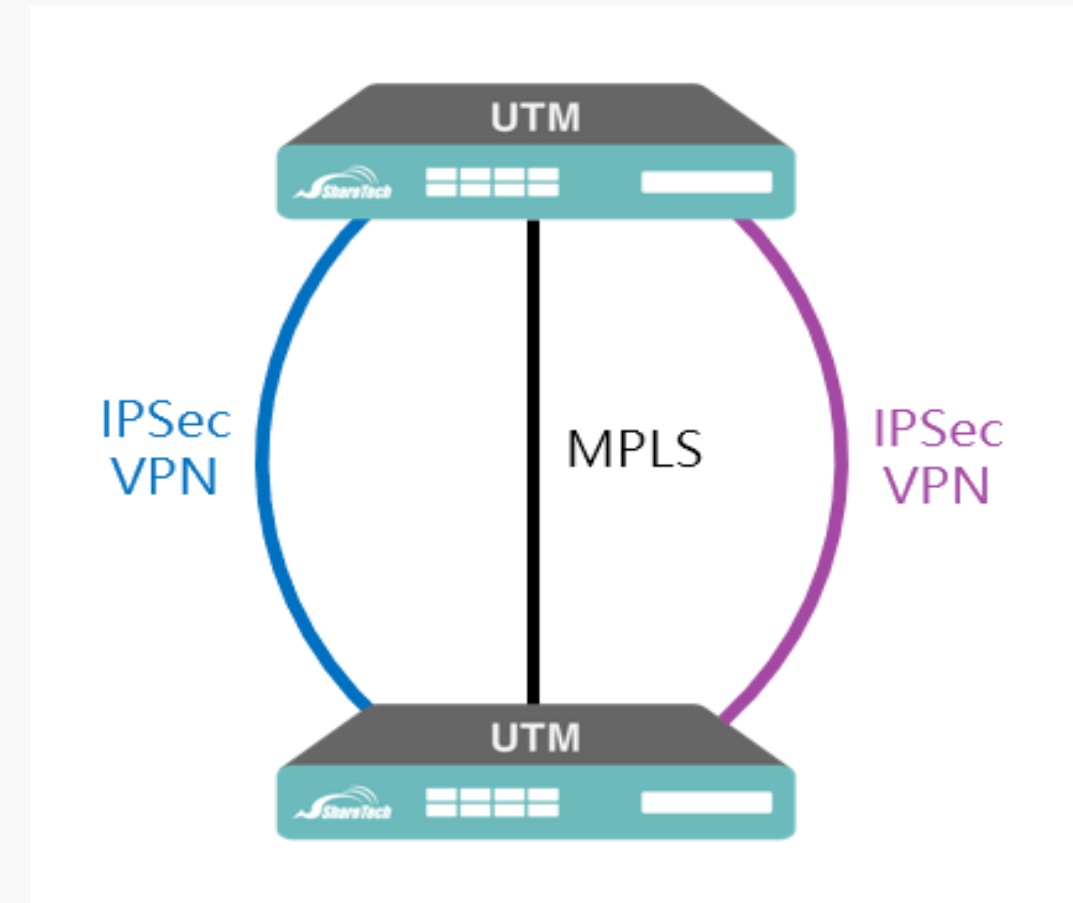- Easy deployment and central management.

No limit on quantity of IPSec

- Increase bandwidth
- Reduce network congestion and packet loss

Scenario 1

What if the MPLS is needed but the redundancy is also required?
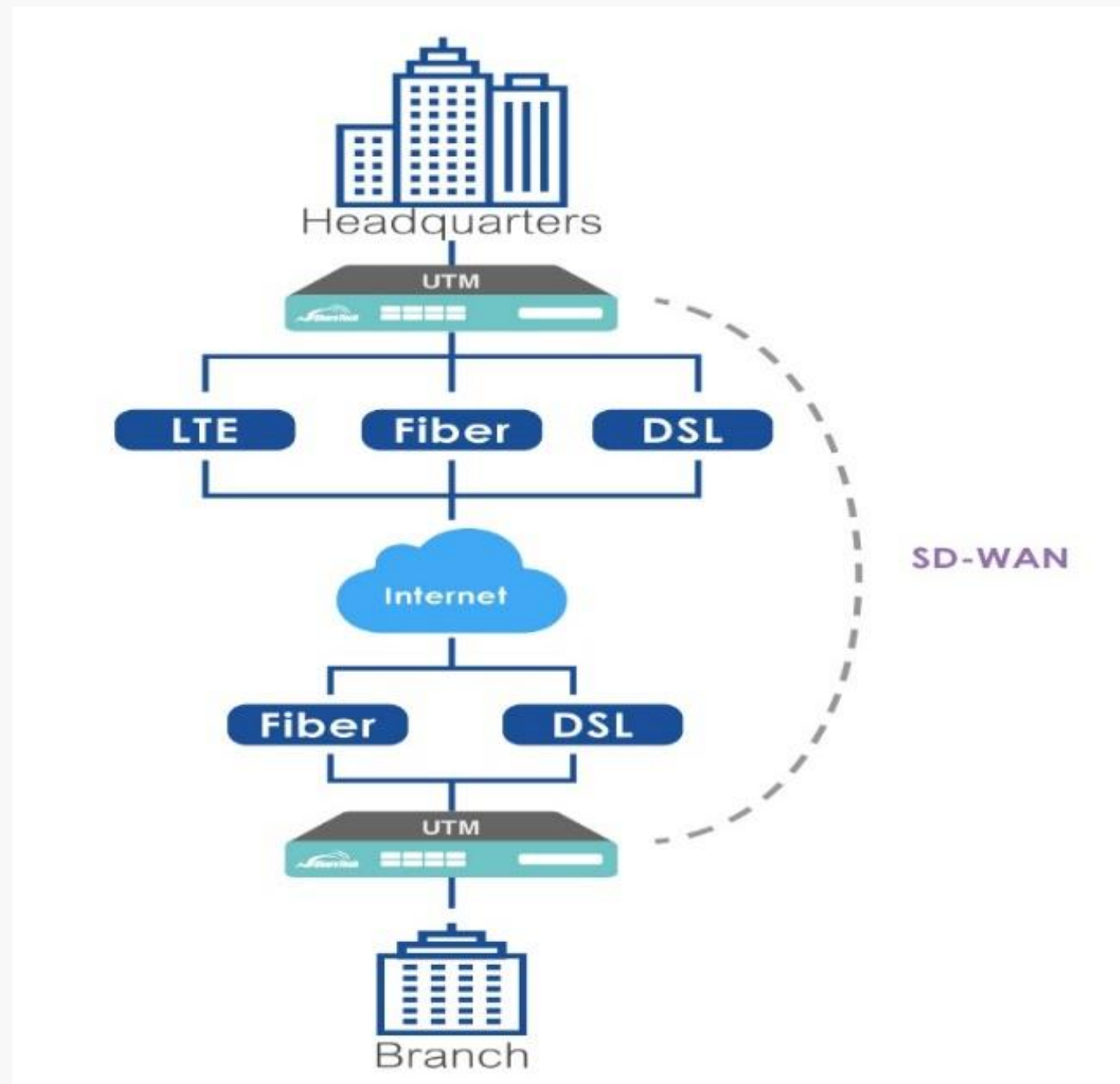

- Using two IPSec as MPLS backups. If any line is disconnected, it will automatically switch to another line to maintain a smooth connection.
- Dual IPSec can also do the load balance.

IPSec VPN

Scenario 2

**Two UTM are in different places,
how can the client get them connected?**

Integrate multiple lines

- No need to set up complex lines so that the administrators can easily manage.
- Integrate multiple lines from A to B.
- Much cheaper than using MPLS to connect them all

Connect multiple UTM using the SD-WAN technique

- Not only two, SD-WAN can be applied to connect multiple UTM and effortlessly connect them together.
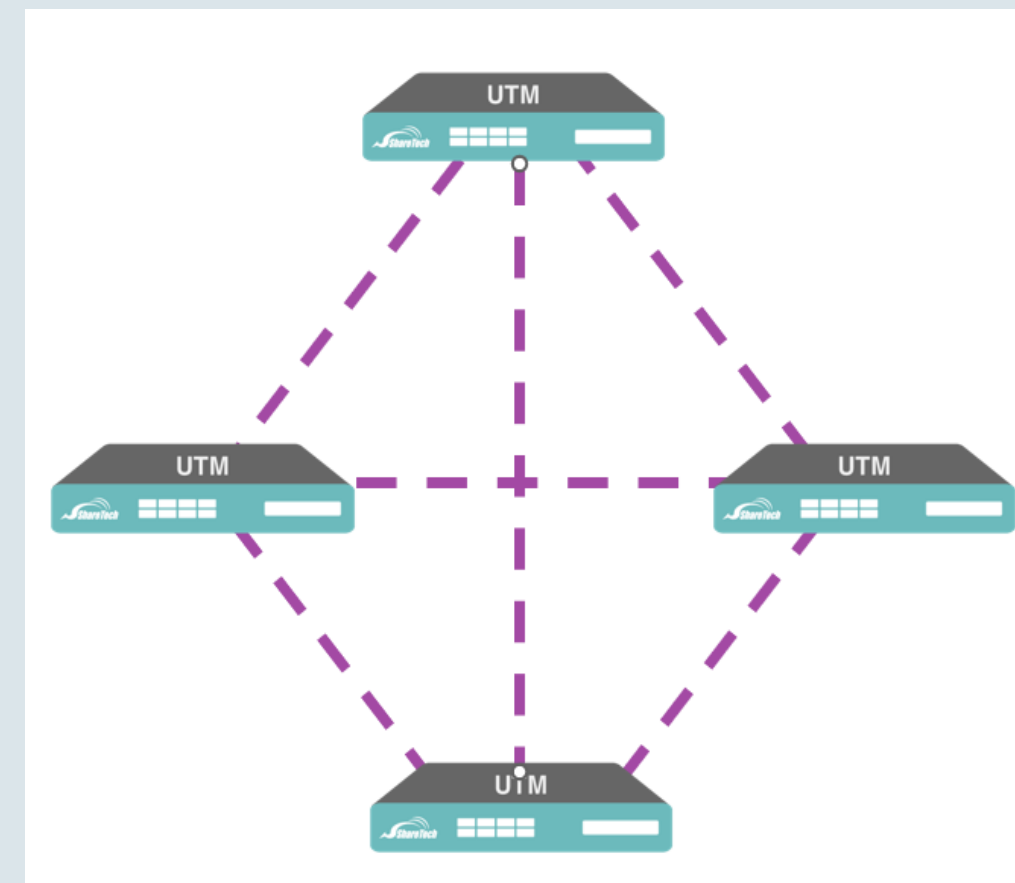
Scenario 3

How to solve the problem of bandwidth and connection congestion caused by single line?

Add SD-WAN :

Group Name: SD-WAN

Weight	IPSec Tunnel	Weight	Gateway
☐ 1	test vpn (60.249.5.0/24 -- 192.168.1.0/24)	☑ 1	**wan189** (192.168.189.1) (zone2 (wireless))
☐ 1	yyyy (192.168.100.0/24 -- 192.168.1.0/24)	☐ 1	**WAN221** (192.168.189.1) (zone2 (wireless))
☐ 1	yyyy (--)	☐ 1	**sharetech** (60.249.5.254) (zone2 (wireless))
☑ 1	tunnel (--)	☐ 1	**test(ppp4001)** ( ) (ppp4001 (test))

- Each link can be assigned different weights, enabling the selection of the optimal path for packet transmission.
- Reduce connection congestion and facilitates effective load balancing.

NU-6000

Used as SD-WAN Model

Software Spec

- Antivirus engine
- Basic firewall protection
- Safety gateway
- Traffic analysis

Hardware Spec

- 6 Gigabit Ports (5 Customed)
- LAN BYPASS
- Storage 32G eMMC
- Memory 4G
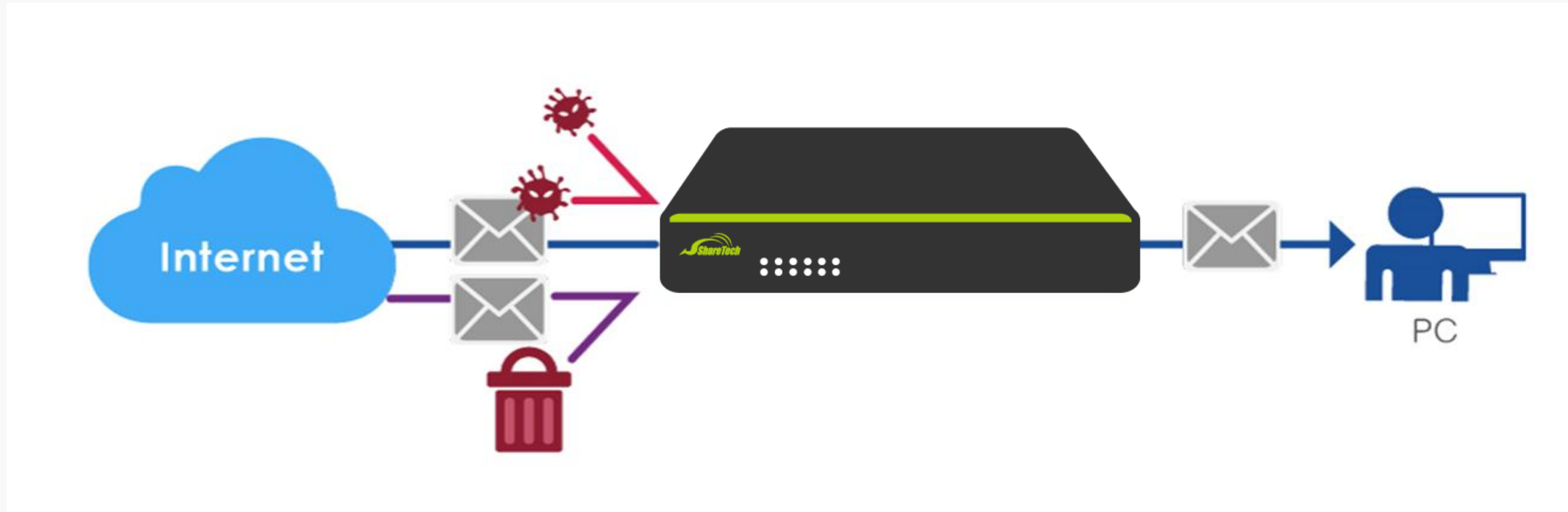- NAT Transmission up to 4 Gbps

Specialties

NU-6000 is a small firewall that supports VPN and SD-WAN mechanisms, providing protection for various branch locations while enabling simple, centralized management. It offers businesses a cost-effective way to manage and secure their networks.

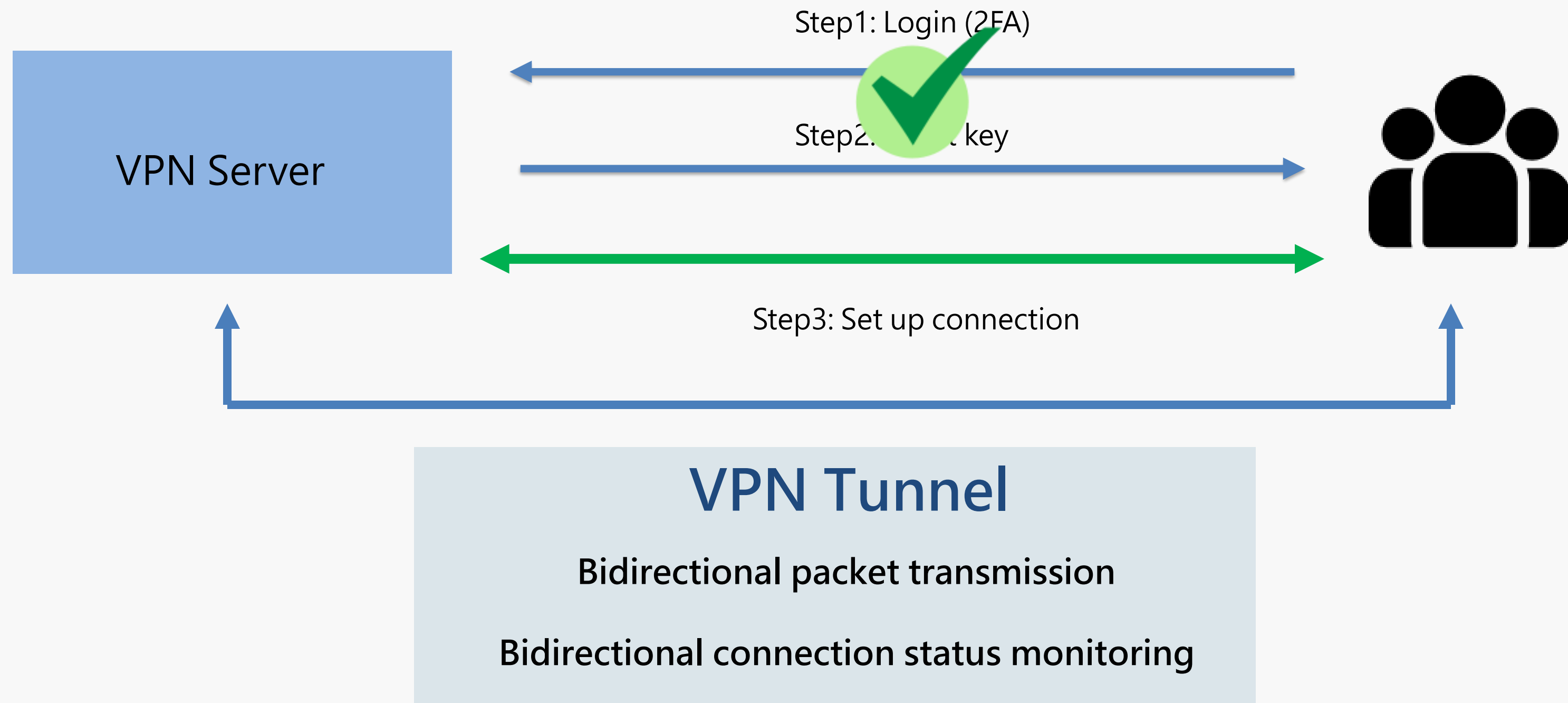## Comprehensive VPN

- IPSec
- PPTP
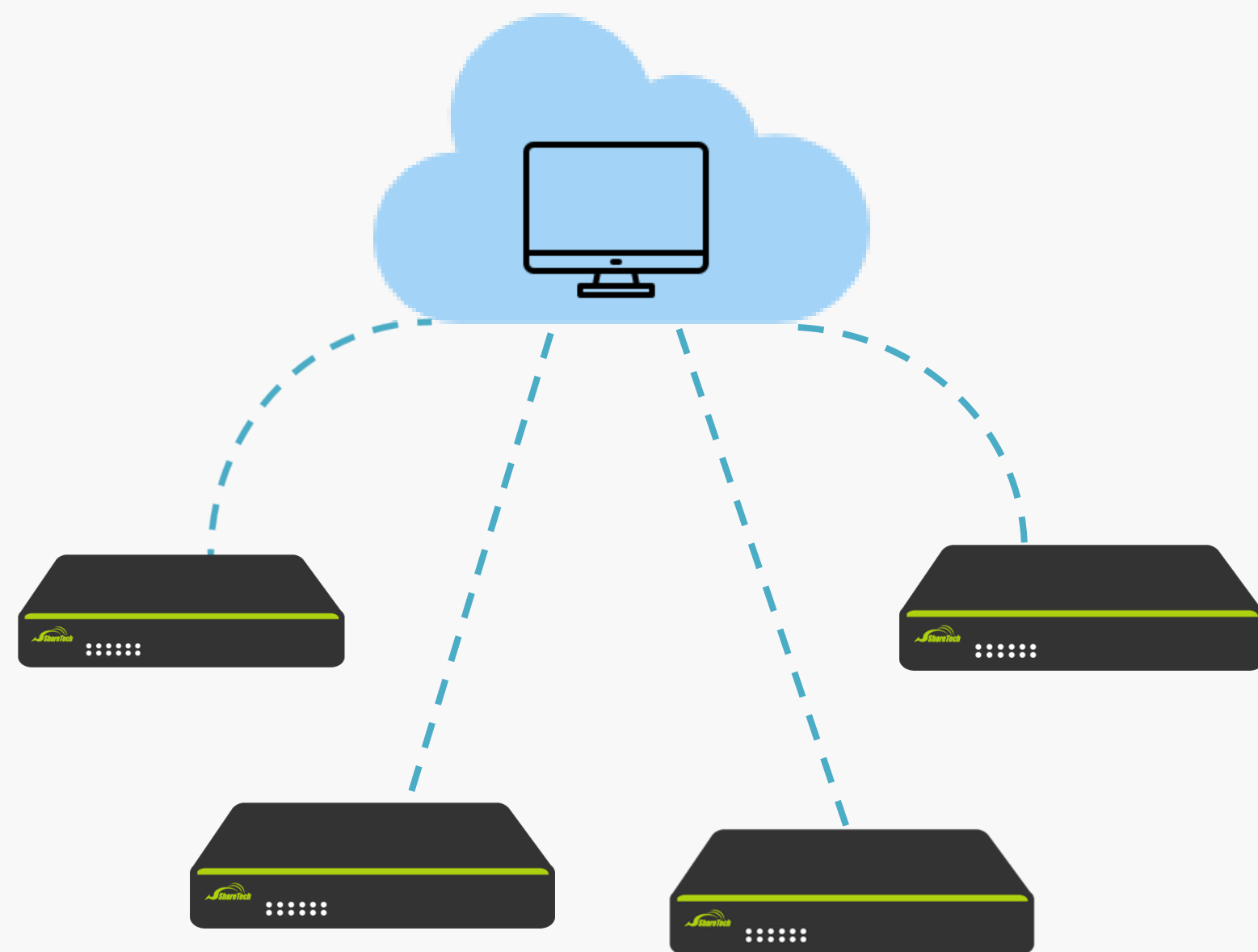- L2TP
- SSL VPN

Feature1 Anti-Virus Engine

- The anti-virus engine in NU-6000 is capable of detecting over millions of viruses, worms, and Trojans.
- Automatically scans emails for viruses and updates virus base via the internet, giving strong protection to the devices.

Feature2 VPN

- Adopting Zero Trust Architecture and establish secure connections using authentication mechanisms.
- When the connection is lost, the server will remove the channel key, and the client must re-authenticate to obtain a new key to re-establish the connection.
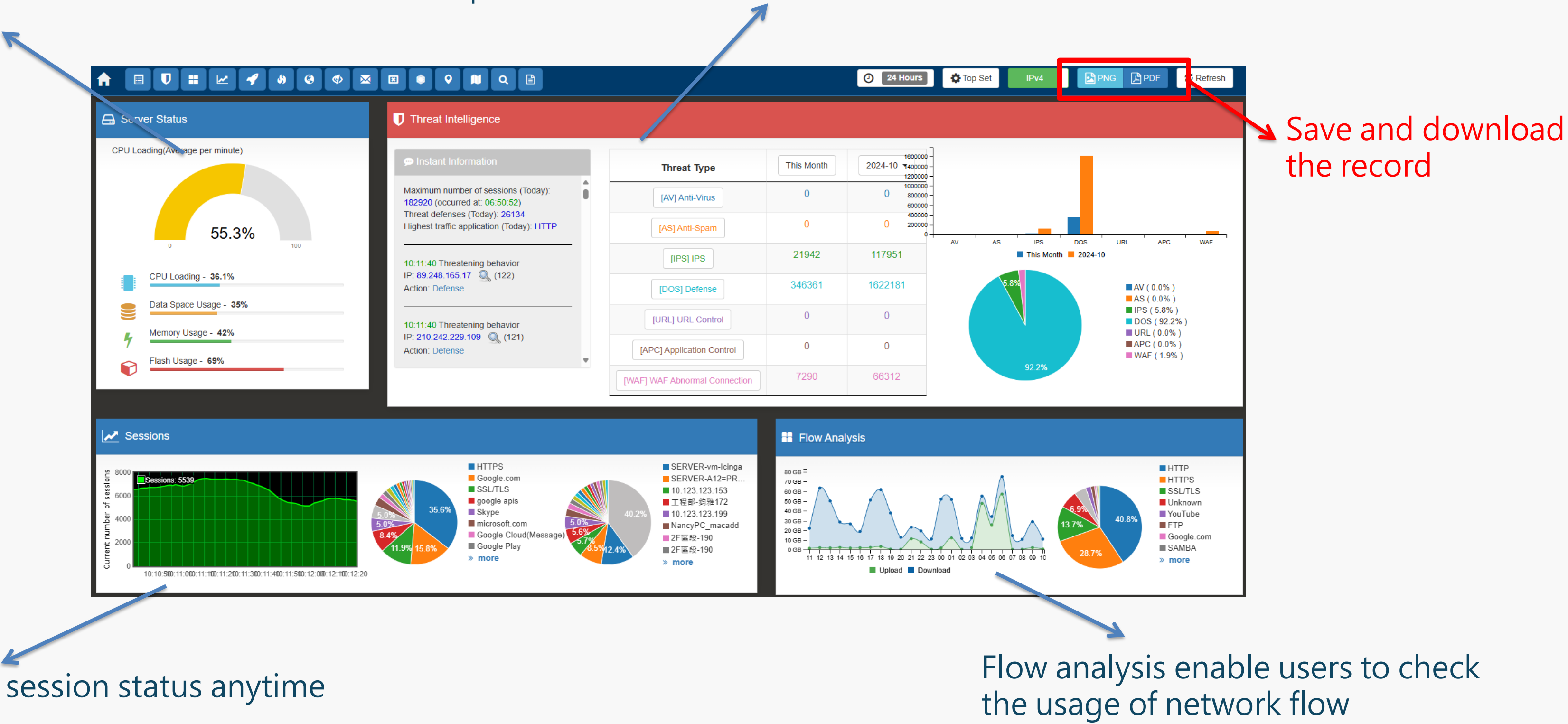
Step1: Login (2FA)

VPN Server

Step2: ~~~ key

Step3: Set up connection

VPN Tunnel

Bidirectional packet transmission

Bidirectional connection status monitoring

Feature3 Central Management

- EyeCloud platform provides the functions of remote monitoring, activating, rebooting, and managing multiple devices in different branches.

Feature 4 Dashboard

Visualize the data for users to see the real time operation

Categorize threats into seven different types for users to view the security strategies

Save and download the record

Monitor the session status anytime

Flow analysis enable users to check the usage of network flow

Thank you