ShareTech

# ShareTech UTM Solution

Website
www.sharetech.com.tw/en-us

Sales Info
sales@sharetech.com.tw

Tech Support
help@sharetech.com.tw

# How to Set Up a VPN Firewall Between the Head Office and Branch Offices?

A VPN (Virtual Private Network) creates an encrypted “private channel” over the Internet, connecting the internal networks of two or more locations. This allows remote computers to operate as if they were part of the same internal network, providing convenience and security. The main purpose of a VPN is to enable businesses or organizations to connect private networks at different locations, ensuring seamless communication (e.g., between a company's head office and branch offices).

ShareTech’s UTM solution offers a comprehensive VPN application package (IPSec, Wireguard VPN, SSL VPN, IP Tunnel). In this configuration, endpoints in a virtual private network can communicate through connections between firewalls, reducing the cost of establishing VPN connections at each endpoint, minimizing maintenance efforts, and enhancing data transmission security between locations.

## How to Establish a VPN Connection Between Two Locations (Head Office and Branch Offices)?

Assume **Company A (Head Office)** is in Taichung, while its **branch offices B** (in Taipei) and **C** (in Kaohsiung) need to connect to the head office via VPN. In this setup:

1. The subnets of branch offices **B** and **C** can communicate with the subnet of the head office (**A**).
2. The subnets of **B** and **C** can communicate with each other.

### Assumptions:

- **Head Office (Company A):** Subnet is configured as a B-Class network with an IP range of **192.168.1.0/16**.
- **Branch Office B:** Subnet is configured as a C-Class network with an IP range of **192.168.2.0/24**, and a subnet mask of **255.255.255.0**.
- **Branch Office C:** Subnet is configured as a C-Class network with an IP range of **192.168.3.0/24**, and a subnet mask of **255.255.255.0**.

**Steps for Configuration:**

### 1. Configure VPN on the Head Office Firewall:

- Set up a VPN server on the head office firewall.
- Define the head office's internal network range (**192.168.1.0/16**) and allow VPN connections from branch offices **B** and **C**.
- Enable routing and forwarding to ensure connected VPN clients can communicate with each other.

### 2. Configure VPN Clients at the Branch Offices:

- **Branch Office B:** Configure the branch office firewall as a VPN client to connect to the head office, using the internal network range **192.168.2.0/24**.
- **Branch Office C:** Similarly, configure the branch office firewall as a VPN client, using the internal network range **192.168.3.0/24**.

### 3. Set Up Routing Rules:

- On the head office firewall, create routing rules to forward traffic from the **192.168.1.0/16** network to branch office networks (**192.168.2.0/24** and **192.168.3.0/24**).
- On the branch office firewalls, set up routing rules to forward traffic to the head office network.

### 4. Enable Communication Between Branch Offices:

- On the head office firewall, configure routing rules to allow traffic between **192.168.2.0/24** (Branch Office B) and **192.168.3.0/24** (Branch Office C).
- On the branch office firewalls, set up corresponding routing rules to allow direct communication through the VPN.

In this architecture, while establishing VPN tunnels between the head office and branch offices, it is recommended to consider scalability and security at the head office. Using the **NU-840 and NU-860 series** UTM at the head office ensures connection quality and internal security. For branch offices with fewer functional requirements and a focus on connecting to the head office via VPN, **HiGuard XI** UTM is suitable.

For large chain stores (e.g., convenience stores), the headquarters can be set as a relay point. Each branch can connect to the head office by VPN, allowing the head office to monitor the network usage and status of all branches in real-time. Data transmitted may include the branch office's WAN IP address, custom ID string, internal IP, and MAC address. This setup provides administrators with a centralized view of all network statuses and sales data while enabling efficient data transmission for all branches.