



# ShareTech UTM Solution

Website  
[www.sharetech.com.tw/en-us](http://www.sharetech.com.tw/en-us)

Sales Info  
[sales@sharetech.com.tw](mailto:sales@sharetech.com.tw)

Tech Support  
[help@sharetech.com.tw](mailto:help@sharetech.com.tw)



## Intelligent Co-Defense Cybersecurity Solution — ShareTech x Proscend Cross-Device Defense Architecture

As cyberattacks become increasingly frequent—particularly ransomware, APT attacks, and internal lateral movement—enterprises today face not only external boundary threats but also critical defense gaps between internal devices. Traditional security systems focus heavily on firewalls and endpoint antivirus solutions, but they lack real-time responsiveness to internal traffic and device access.

### Key Pain Points:

- Inability to immediately block lateral spread from already compromised devices
- Lack of coordinated defense mechanisms between endpoints and access-layer switches
- High costs and manpower burden for SMEs implementing security systems

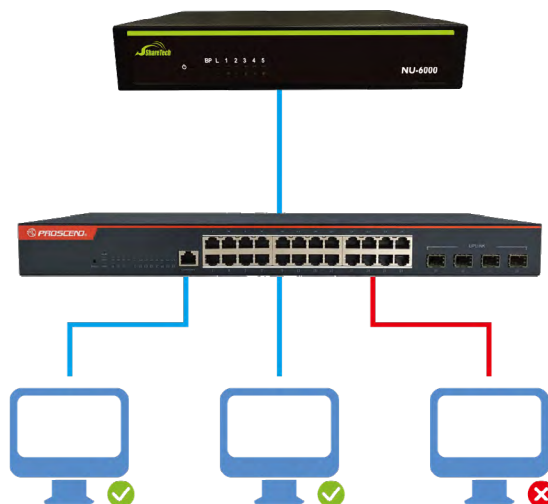
### Co-Defense Architecture

ShareTech has partnered with Taiwan industrial IoT expert Proscend to launch a cross-device cybersecurity collaboration system. Through a coordinated firewall + switch defense mechanism, when the firewall detects suspicious traffic, abnormal host behavior, or malicious connections, it instantly notifies the switch to execute blocking actions. This effectively prevents threats from spreading within the internal network, creating a proactive defense against ransomware and APT intrusions.

The architecture is built upon two core devices:

- ShareTech NU Series Firewalls: Equipped with Layer 3–7 protection, built-in IPS (Intrusion Prevention System), virus and malicious behavior detection, packet analysis, and traffic management. Acting as the frontline threat detector, it immediately triggers response mechanisms once abnormal traffic or suspicious internal device activity is identified.
- Proscend 850 Series L2+ Managed Switches: Supporting VLAN segmentation, ACL access control, QoS traffic optimization, and Port Security. Once integrated with the firewall under Co-defense mode, the switch can instantly receive alerts and rapidly execute specific port shutdowns or device isolation to effectively stop lateral movement.

This design transforms a single-device system into a multi-point collaborative, real-time responsive security defense network. It successfully bridges traditional internal protection weaknesses, significantly enhancing both defense speed and accuracy.



## Co-defense Mode

The collaborative defense mechanism is built upon SNMP extensions and leverages Telnet or SSH to control switches, enabling device binding, real-time blocking, and proactive co-defense. It provides three binding mechanisms to strengthen endpoint access security. The following explains the first mechanism in detail.

### 1. MAC + PORT Binding

This method restricts a device to connect only through a specific switch port. If the device is moved to another port, it cannot obtain an IP address or establish a connection.

#### Defense Effectiveness:

- Ensures devices can only connect to designated switch ports, preventing unauthorized relocation or connection to other network points, thereby reducing risks of internal network sniffing or bypassing.
- Blocks unauthorized devices from accessing the network. Even if someone gains physical access (e.g., plugging in a cable), they cannot pass the switch's access control, preventing rogue terminals or data theft.
- Strengthens physical security and segment boundary control by treating each switch port as a security checkpoint. Only pre-registered MAC addresses are allowed, improving overall network trustworthiness and manageability.



## Application Scenarios

- Enterprise Office Network Control

Each desk is restricted to allow only the designated employee's laptop or desktop to access the network.

**Benefit** → Prevents employees from unplugging authorized devices and connecting personal equipment (e.g., laptops, NAS, mobile phones), thereby avoiding data leakage or Trojan infiltration.

- Industrial Control Networks

Each PLC controller or HMI (Human-Machine Interface) has a fixed position and only authorized devices are allowed to connect.

**Benefit** → Prevents engineers from mistakenly plugging in laptops or attackers from accessing test ports to conduct lateral penetration.

- Campus Data Centers & Computer Classrooms

Every computer in classrooms is a fixed device; students are prohibited from swapping cables or connecting private equipment.

**Benefit** → Maintains a secure teaching environment and blocks unauthorized Wi-Fi routers, personal access points, or other devices that may disrupt the network.

- Government / Military / Financial Institutions (High-Security Environments)

Physical access is strictly controlled under the principle of "one port, one device; one user, one privilege."

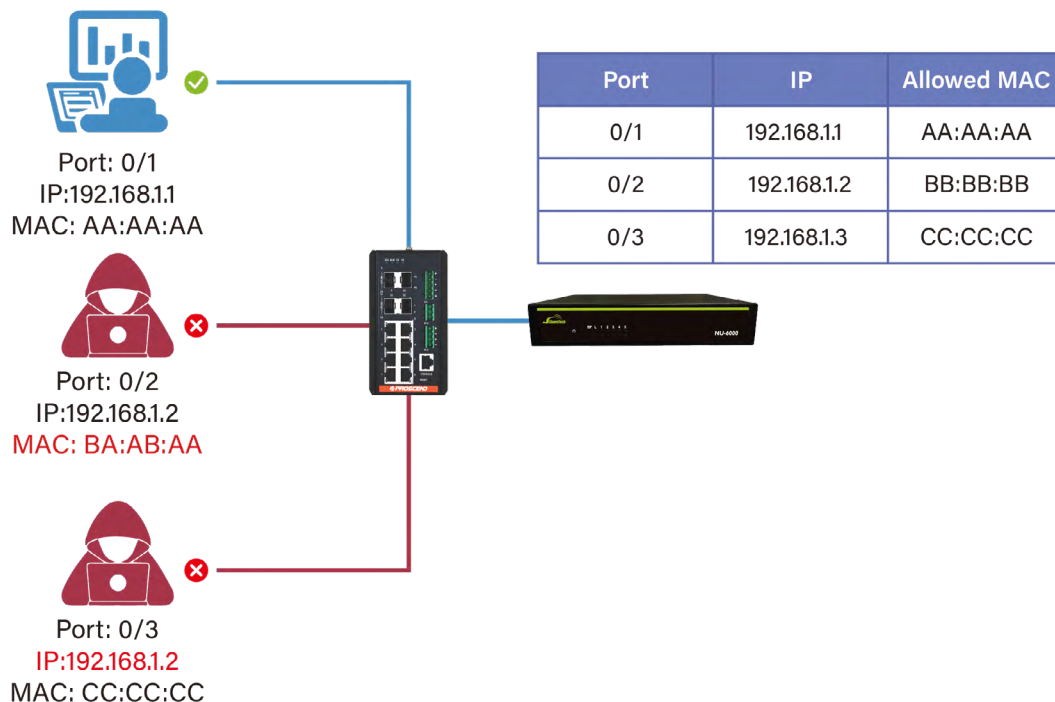
**Benefit** → Eliminates risks from USB NICs or unauthorized devices, ensuring that the entire network segment complies with cybersecurity standards.

## 2. IP + MAC + PORT Binding

A device's IP address, MAC address, and switch port must all match; otherwise, network access is denied. This prevents spoofing, relocation, or configuration changes.

### Defense Effectiveness:

- Blocks unauthorized IP spoofing attempts
- Prevents devices from connecting through the wrong port
- Rejects all devices not in the binding list
- Enables precise tracking of device identity and location



### Application Scenarios:

- Healthcare & Smart Medical

Devices require stable, uninterrupted connectivity; patient data is highly sensitive.

Benefit → Prevents unauthorized workstations or guest devices from entering medical networks.

- Large Enterprises & Data Centers

Complex environments with numerous users and devices.

Benefit → Restricts high-privilege segments to specific bound devices/ports, avoiding misuse of access rights.

- Banking & Financial Institutions

Must comply with strict regulatory and cybersecurity laws.

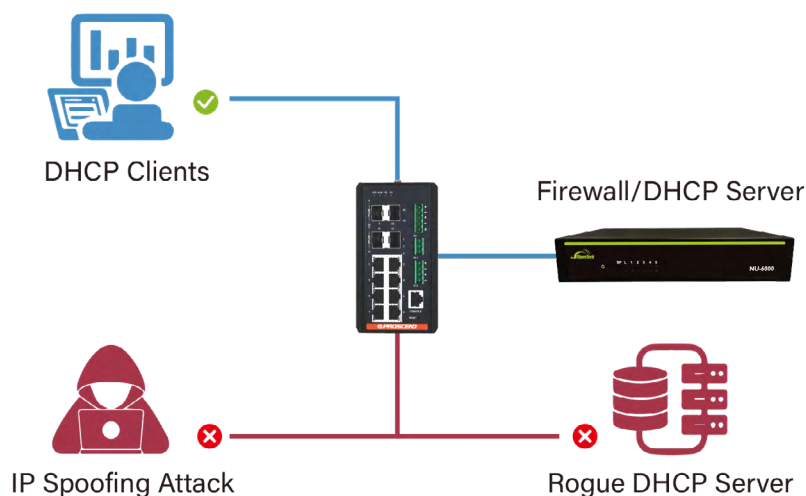
Benefit → Core systems (e.g., e-banking servers, reporting terminals, ATMs) are strictly bound; any device relocation, misconnection, or rogue insertion is instantly blocked and reported to SIEM.

### 3. IP Source Guard (with DHCP Snooping)

Designed for networks using dynamic IP allocation (DHCP). When DHCP Snooping is enabled, the switch automatically records the valid IP/MAC/Port bindings of devices and creates a temporary binding table. This table is then used to validate or block traffic.

#### Defense Effectiveness:

- Combines advantages of the first two mechanisms
- Blocks rogue DHCP servers (DHCP Spoofing)
- Prevents lateral scanning or IP spoofing attacks



### Application Scenarios:

- Office Wi-Fi Networks

Enable DHCP Snooping to whitelist trusted DHCP servers, then apply IP Source Guard to validate packet sources. Devices with static IPs not assigned by DHCP or unauthorized MACs are blocked, preventing rogue connections and data leakage.

- Smart Factories / Industrial Control Networks

Use IP Source Guard + DHCP Snooping to ensure only authorized MACs on specific ports can obtain DHCP IPs. This prevents unauthorized engineering devices from entering control networks and effectively isolates OT from IT traffic, enhancing security and stability.

- Campus Networks

Configure trusted ports for authorized DHCP servers and block DHCP replies from all others. With IP Source Guard, only DHCP-assigned devices gain access. This eliminates rogue DHCP attacks at the root, improves stability, and allows administrators to trace unauthorized devices.

## Comparison of Binding Mechanisms

Binding Method	MAC + PORT	IP + MAC + PORT	IP Source Guard
Defense Effect	<ul style="list-style-type: none"> <li>Prevents unauthorized device relocation</li> </ul>	<ul style="list-style-type: none"> <li>No parameter can be changed (IP, MAC, or Port)</li> </ul>	<ul style="list-style-type: none"> <li>Blocks rogue DHCP servers, prevents IP spoofing attacks, supports VLAN</li> </ul>
Application Scenarios	<ul style="list-style-type: none"> <li>Office PCs / company laptops</li> <li>PLC controllers / HMI panels</li> <li>Printers</li> <li>Smart home devices</li> <li>Financial terminals</li> </ul>	<ul style="list-style-type: none"> <li>Data center servers</li> <li>Critical enterprise servers</li> <li>Core switches / router management hosts</li> </ul>	<ul style="list-style-type: none"> <li>Industrial control equipment (PLC, HMI, sensors, engineering devices)</li> <li>Campus networks (dorms, student devices, staff systems)</li> </ul>

## Building Taiwan's Autonomous and Resilient Smart Cybersecurity Defense

In an era where digital transformation goes hand in hand with growing threats, enterprises need more than just additional tools—they need an intelligent security framework that enables proactive defense, cross-layer collaboration, and real-time response.

The Co-defense mechanism, co-developed by ShareTech and industrial networking expert Proscend, embodies this vision. It delivers a new-generation solution that is autonomous, horizontally integrated, and deployment-flexible.

More than just a technology, it represents Taiwan's pursuit of technical sovereignty, while providing enterprises with a practical path to simplified deployment, enhanced internal network protection, and reduced cybersecurity risks.

Co-defense is not only defense—it is the starting point of digital resilience.