Specifications

Model	INF-8400H	INF-8600T	INF-8700C	INF-8700F
Interfaces				
Form Factor	1U	1U	1U	1U
Memory	4G RAM	8G RAM	8G RAM	8G RAM
HD	240G SSD	480G SSD	480G SSD	480G SSD
I/O Ports	6 x Giga Ports	6 x Giga Ports 2 x 10G Fiber Ports	14 x Giga Ports	6 x Giga Ports 8 x 1G Fiber Ports
Watchdog Bypass	O	O	O	O
LAN Bypass	1 pair	1 pair	2 pairs	2 pairs
Supported Mode	Bridge	Bridge	Bridge	Bridge
Applicable Environment	Under 50	Under 100	Under 200-300	Under 200-300
System Performance				
Firewall Throughput	4.2 Gbps	9 Gbps	13 Gbps	13 Gbps
Concurrent Sessions	2,000,000	2,000,000	3,000,000	3,000,000
New Sessions/Second	65,000	120,000	350,000	350,000
Threat Protection Throughput (IPS, Anti-Virus, and Web Filtering)	900 Mbps	900 Mbps	1,200 Mbps	1,200 Mbps
Anti-Virus Throughput (bidirectional)	750 Mbps	1,300 Mbps	1,600 Mbps	1,600 Mbps
IPS Throughput	600 Mbps	1,000 Mbps	1,200 Mbps	1,200 Mbps
Software Security				
Virus Engine(s)	ClamAV & Optional Kaspersky	ClamAV & 1-year Kaspersky	ClamAV & 1-year Kaspersky	ClamAV & 1-year Kaspersky
FTP Virus Scan	O	O	O	O
Spam Filtering	O	O	O	O
Mail Audit	O	O	O	O
IPS	O	O	O	O
WAF	O	O	O	O
Sandstorm	O	O	O	O
Application Control	1-year	1-year	1-year	1-year
URL Database	1-year	1-year	1-year	1-year
Anomaly Flow Analysis	O	O	O	O
Co-Defense (Switch)	O	O	O	O
AP Management	O	O	O	O
Intranet Protection	O	O	O	O
Geo IP	O	O	O	O
Network Testing Tools	O	O	O	O
Logging	O	O	O	O
QoS	O	O	O	O
Offline Update	O	O	O	O
Dashboard	Optional	O	O	O
UPS	O	O	O	O
Eye Cloud/CMS (Client)	O	O	O	O

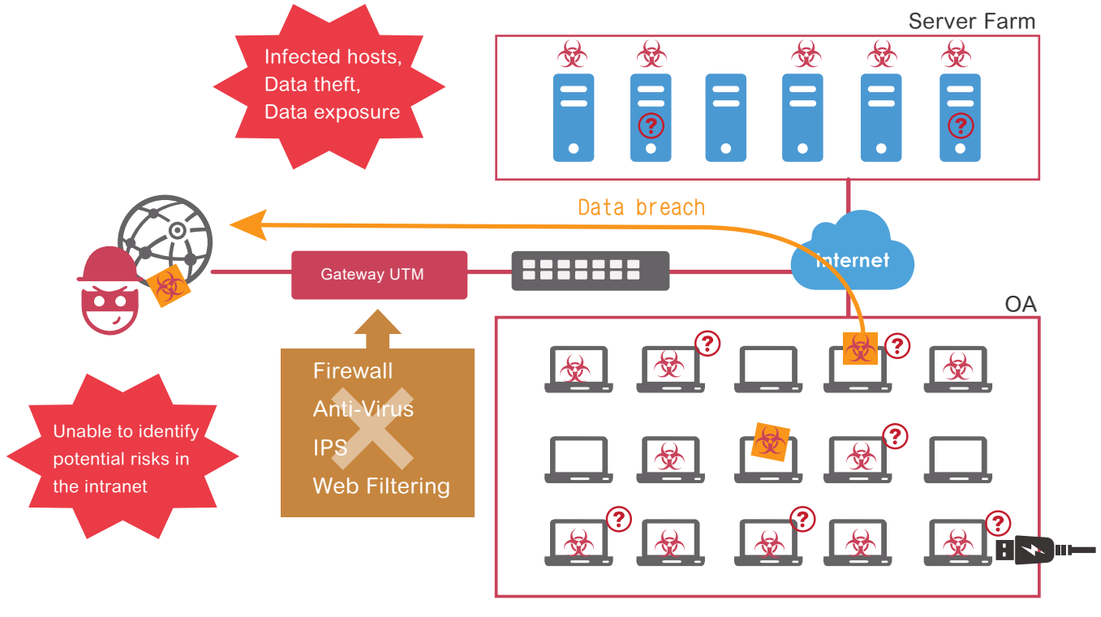
ShareTech

Internal Firewall

INF Series

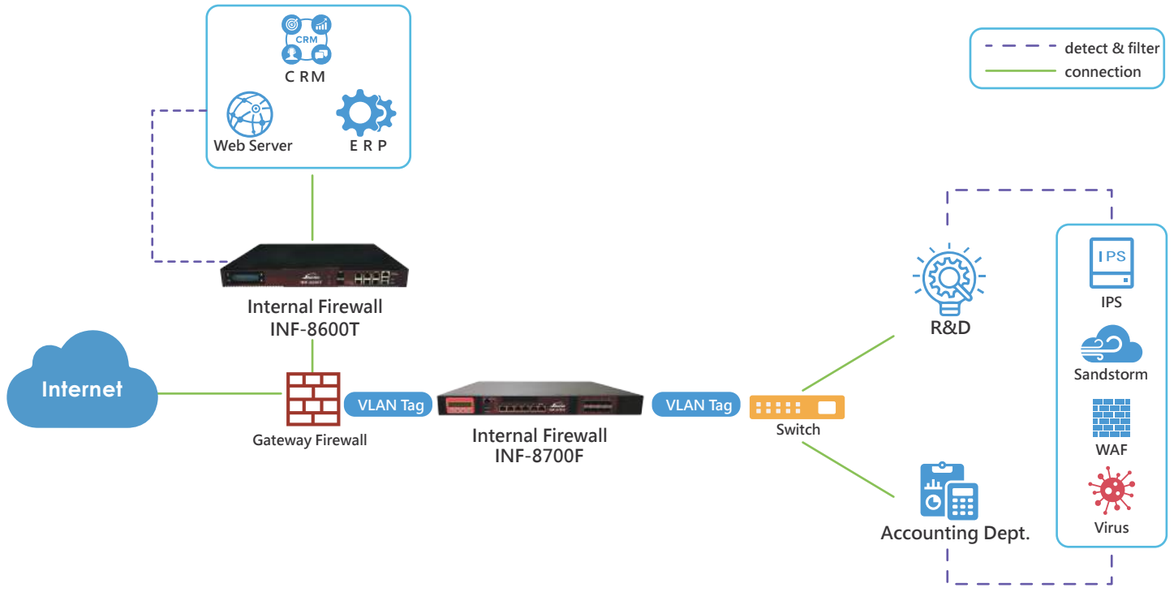
Various intranet security threats in business

- The intranet would never be 100% safe, and your network might have been hacked
- Ineffective response to any cyber incidents
- Malware-infected servers
- Lack of network segmentation
- Relatively less secure wireless network
- Weaker integration within collaborating and sharing
- Failure to patch the vulnerability
- Lack of visibility into processes and applications



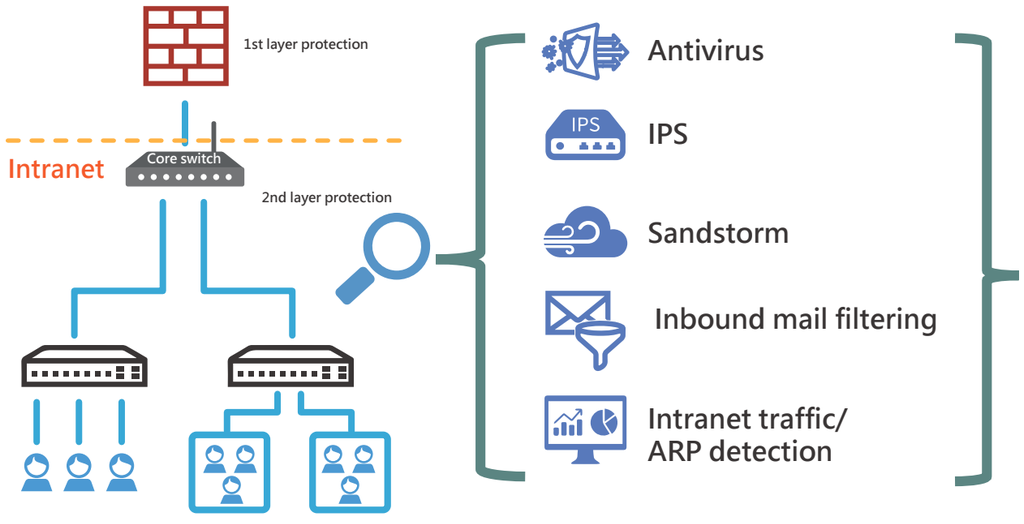
ShareTech internal firewall decreased intranet security risks.

ShareTech intranet firewall (INF Series) has a unique combination that allows businesses to stay ahead of intranet attacks, detect-and-response to threats, and collaborate effectively in other networking peripherals. Aside from regular next-generation firewalls designed to detect and combat attacks across the entire network, ShareTech INF Series ensures a network is protected from the inside out, providing higher visibility, spotting relevant attacks, and collecting all suspicious security events.



I. Minimize the possibility of a zero-day attack

Most network appliances are used as a border defense that analyzes packets, isolates an organization's internal network, and assumes nothing got past the firewall. However, infections in the intranet may not be detectable, so that malware might have been spreading throughout an organization. ShareTech INF Series can detect anomaly-based behaviors in the internal network environment. By using anti-virus engines, IPS, WAF, and Sandstorm, malicious activities can either get responded to appropriately or banned proactively.

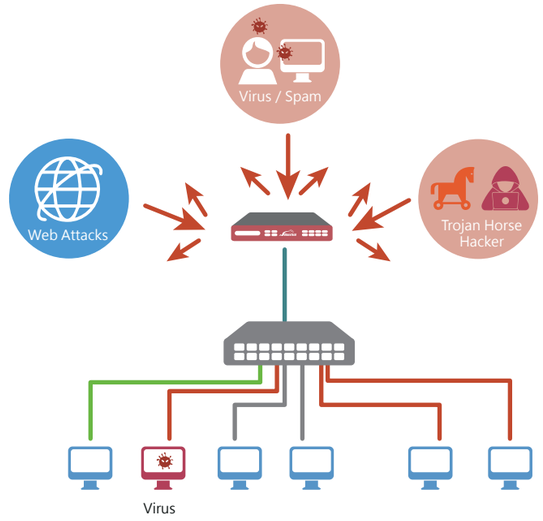


II. Secure vitally important and dedicated servers

ShareTech INF Series can perform scans and detect many security vulnerabilities in web applications, such as cross-site forgery, cross-site scripting (XSS), file inclusion, and SQL injection, among others. To perform in-depth detection, ShareTech INF Series has a built-in web application firewall (WAF), a protocol layer 7 defense, is a type of reverse proxy that protects critical servers from exposure. It operates through policies that aim to protect against vulnerabilities in the application by filtering out malicious traffic. Meanwhile, users can maintain speed and ease.

III. Guard intranet security with switches

Once any abnormal behavior gets detected in protected segments, ShareTech INF Series will actively block all packets to/from the source of infection and isolate associated traffics going through the network segment. At the same time, collected data will be displayed and expressed visually, allowing IT administrators to analyze the data further and see if it is a malicious hacking attack. Moreover, by integrating with switches, IT administrators can clearly understand the switch architecture deployment and the usage status of each node via the network topology.



IV. Gain a comprehensive overview of dashboard reporting

Built-in ShareTech Dashboard is specially designed for intranet security. Loggings and event data of the device can be simplified and centralized for analysis, collection, storage, query, and reporting. IT administrators can inspect and search all traffics for enhanced security and define possible risk sources or suspicious activities through event correlation.

Important Dashboard Features

- Monitor network traffics and analyzes threats
- Support flow-generated Syslog
- Track events
- Collect and correlate logs for queries
- Gain complete visibility of the whole system