



H3C SecPath T1000-AI

IPS Series



Overview

H3C SecPath T1000-AI series, a family of industry-leading IPS products deployed on key paths on customer networks, provides deep analysis on Layer 4 through Layer 7 information of data flows passing through the key paths, and supports the following security and network features:

- Prevention against common attacks such as hackers, worms, viruses, Trojans, DoS/DDoS attacks, scanning attacks, spyware, protocol anomalies, and Web phishing.
- P2P and IM traffic identification and control.
- Powerful bandwidth management and URL filtering.
- Security protection and access control based on users, applications, time, and security status. Security protection features include IPS, antivirus, app control, URL category, WAF, and user-defined filtering.
- Comware 7-based virtualization and HA features, including IRF and 1:N virtualization, which satisfies the flexible extension requirements of cloud computing.

H3C SecPath T1000-AI series is a set of high-performance GE and 10-GE IPS products designed for vertical and small-and medium-sized enterprise markets. Built based on multi-core processor architecture, it provides powerful processing capability. Within a 1U footprint, it provides multiple types of interfaces and great hardware scalability. The interface module slots allow flexible interface expansion and the two drive slots can accommodate growing storage needs.

H3C SecPath T1000-AI IPS Series



H3C SecPath SecPath T1000-AI-25/T1000-AI-35



H3C SecPath T1000-AI-55/T1000-AI-65



H3C SecPath T1000-AI-50/T1000-AI-60



H3C SecPath T1000-AI-70/T1000-AI-80/ T1000-AI-90

Features and Benefits

High-performance software and hardware platform

The SecPath T1000-AI delivers high system performance with advanced architecture and components:

- **64-bit multi-core high-performance processor and high-speed cache**—Provides high-performance security processing capability.
- **CPU+switch structure**—Uses the CPU to process security services and the switch to implement service port extension.
- **Hardware scalability**—The interface module slots allow flexible interface expansion and the two drive slots can accommodate growing storage needs.

Powerful security protection features

Industry-leading virtualization solution

N:1, 1:N, and N:1:M virtualization solutions allow resource pooling for cloud computing.

Powerful security protection features

- **Intrusion prevention and detection**—Integrates IPS, antivirus, bandwidth management, and URL filtering features. By inspecting and analyzing Layer 7 application information of the traffic, the system can identify and block attacks and malicious behaviors in the network in real-time to secure the network applications, infrastructure, and performance.
- **Attack prevention technologies**—Supported in both IPv4 and IPv6 network. In addition to the stateful firewall technology. The system detects and prevents various attacks, including:

- Single packet attacks, such as Land, Smurf, Fraggle, WinNuke, ping of death, Teardrop, and invalid TCP flag.
- IP spoofing attacks.
- IP scanning attacks and port scanning attacks.
- Flood attacks, such as Ack flood, DNS flood, Fin flood, HTTP flood, ICMP flood, ICMPv6 flood, Reset flood, SYNACK flood, SYN flood, and UDP flood.

Complete and updated security signature database

- H3C has a professional team to track the security bulletins of global security organizations and enterprises. The team provides an up-to-date security signature database based on the threat analysis results.
- The signature database not only provides all vulnerability signatures for the mainstream operation systems, network devices, database systems, and application software systems, but also includes signatures for attacks such as hackers, worms, viruses, Trojans, DoS/DDoS attacks, scanning attacks, spyware, Web fishing, and traffic of P2P, IM, and network games.
- As a partner of Microsoft Active Protections Program, H3C has early access to the vulnerability information so that H3C can provide updated protections to customers faster.
- With certificate of Common Vulnerabilities & Exposures (CVE) compatibility, H3C provides industry-leading vulnerability research and attack prevention technologies. At the same time, H3C pays close attention to the domestic network security events and provides real-time prevention methods.

- With a global honeypot system deployed, H3C understands the latest attack technologies and trends, and use the following releasing methods:
 - Weekly and emergency (for critical security vulnerability) security update publishing.
 - Automatic or manual deployment to the IPS devices for real-time attack prevention.

Flexible and extensible, integrated and advanced DPI security

- **Integrated security service processing platform**—Highly integrates the basic and advanced security protection measures to a security platform.
- **Highly precise and effective intrusion inspection engine**—Uses the H3C-proprietary Full Inspection with Rigorous State Test (FIRST) engine and various intrusion inspection technologies to implement highly precise inspection of intrusions based on application states. The FIRST engine also supports software and hardware concurrent inspections to improve the inspection efficiency.
- **Real-time virus protection**—Uses the Kaspersky stream-based antivirus engine to prevent, detect, and remove malicious code from network traffic.
- **Fast URL category filtering**—Provides basic URL filtering blacklist and whitelist and allows you to query the URL category filtering server on line.
- **Complete and updated security signature database**—H3C has a senior signature database team and professional attack protection labs that can provide a precise and up-to-date signature database.

Various protection methods

- Abundant protection actions for packet inspection results, including blocking, dropping, permit, TCP

Reset, raw packet capture, redirection, logging, and sending alarms.

- Flexible combination of actions for detected threats. Common combinations of actions are defined in the factory default settings.

Industry-leading IPv6 features

- All features are supported in IPv6 networks.
- Support for deployment in the IPv6 networks, IPv6 feature management, and IPv6 logs and auditing.

Carrier-level high availability

- 1:1 active/active and active/standby stateful failover for load balancing and service backup.
- IRF for flexible management and extension.
- Fault isolation. Modular design-based Comware 7 ensures one process fault does not affect the running of other processes, the kernel, and the hardware.

Intelligent management and monitoring

- Configuration and management through Web, CLI, and SSH.
- RBAC for controlling user access to functions, command lines, and menus based on user roles.
- SSM unified management platform for configuration management, performance monitoring, and log auditing.
- MIB nodes to manage and monitor performance.

Publicly available system interfaces

- **Programming interfaces**—The Linux-based Comware 7 provides open standard programming interfaces for users to define dedicated features. Currently, the system provides NETCONF interfaces.
- **Tcl scripts**—Comware 7 provides a built-in tool command language (Tcl) interpreter. You can use the Tcl language to execute the Tcl command and the Comware commands, the SNMP GET and SET operations, and the programming interfaces to implement specific features.
- **Embedded Automation Architecture**—EAA allows you to self-define monitored events and actions to take in response to an event. EAA not only ensures HA, but also meets specific user requirements.

Technical Specifications

Hardware specifications

Item	T1000-AI-25/T1000-AI-35
Ports	1 × console port (CON)
	2 × USB host ports
	1 × management port
	16 × GE copper ports
	6 × GE fiber ports
	2 × 10-GE ports
	4 × combo interfaces
Expansion slots	2
Power supply slots	2
	Support for AC and DC power supplies 1+1 power supply redundancy
Dimensions (H × W × D)	44.2 × 440 × 435 mm (1.74 × 17.32 × 17.13 in)
Ambient temperature	Operating: 0°C to 45°C (32°F to 113°F)
	Storage: -40°C to +70°C (-40°F to +158°F)



H3C SecPath T1000-AI IPS Series

Ambient humidity	Operating humidity: 10% RH to 95% RH, noncondensing Storage humidity: 5% RH to 95% RH, noncondensing
Item	T1000-AI-55/T1000-AI-65
Ports	1 × console port (CON)
	2 × USB host ports
	1 × management port
	16 × GE copper ports
	4 × GE fiber ports
	6 × 10-GE ports
	4 × combo interfaces
Expansion slots	2
	2
Power supply slots	Support for AC and DC power supplies 1+1 power supply redundancy
Dimensions (H × W × D)	44.2 × 440 × 435 mm (1.74 × 17.32 × 17.13 in)
Ambient temperature	Operating: 0°C to 45°C (32°F to 113°F) Storage: -40°C to +70°C (-40°F to +158°F)
Ambient humidity	Operating humidity: 10% RH to 95% RH, noncondensing Storage humidity: 5% RH to 95% RH, noncondensing
Item	T1000-AI-50/T1000-AI-60
Ports	1 × console port (CON)
	2 × USB host ports
	2 × management ports
	14 × GE copper ports
	12 × GE fiber ports
Expansion slots	4 × 10-GE ports
	4
	2
Power supply slots	Support for AC and DC power supplies 1+1 power supply redundancy
Dimensions (H × W × D)	44.2 × 440 × 435 mm (1.74 × 17.32 × 17.13 in)
Ambient temperature	Operating: 0°C to 45°C (32°F to 113°F) Storage: -40°C to +70°C (-40°F to +158°F)
Ambient humidity	Operating humidity: 10% RH to 95% RH, noncondensing Storage humidity: 5% RH to 95% RH, noncondensing
Item	T1000-AI-70/T1000-AI-80/ T1000-AI-90
Ports	1 × console port (CON)



H3C SecPath T1000-AI IPS Series

	2 × USB host ports
	2 × management ports
	14 × GE copper ports
	8 × GE fiber ports
	8 × 10-GE ports
Expansion slots	4
	2
Power supply slots	Support for AC and DC power supplies
	1+1 power supply redundancy
Dimensions (H × W × D)	44.2 × 440 × 435 mm (1.74 × 17.32 × 17.13 in)
Ambient temperature	Operating: 0°C to 45°C (32°F to 113°F)
	Storage: -40°C to +70°C (-40°F to +158°F)
Ambient humidity	Operating humidity: 10% RH to 95% RH, noncondensing
	Storage humidity: 5% RH to 95% RH, noncondensing

Software features

Item	Specifications
	IPS
	Application control, application bandwidth management
	Anti-virus protection
	URL filtering
	Application identification
	Bypass
	Worms, viruses
	Trojans
	Back door
	DoS/DDoS attacks
	Probing/scanning attacks
Network security	Spyware
	Phishing
	Network attacks and abuses defended against
	Attack exploiting vulnerabilities
	SQL injection attacks
	Buffer overflow attacks
	Protocol exceptions
	IDS/IPS bypassing attacks
	P2P abuses
	IM abuses
	Online game abuses
	Firewall
	Basic and advanced ACLs
	Security zone-based access control



H3C SecPath T1000-AI IPS Series

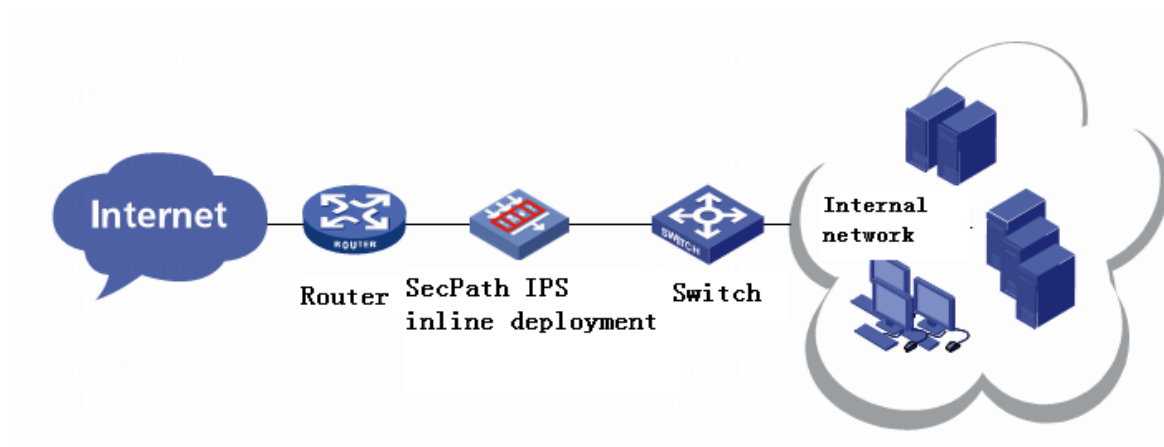
		Time range-based access control		
		ASPF		
		Prevention of DoS/DDoS attacks, such as SYN flood attack, UDP flood attack, ICMP flood attack, ACK flood attack, RST flood attack, DNS flood attack, and HTTP flood attack		
		Malformed packet attacks, such as land, Smurf, Fraggle, WinNuke, Ping of Death, Teardrop, IP spoofing, IP fragment, tiny fragment, invalid TCP flag, large ICMP packet, ICMP redirect, and ICMP destination unreachable attacks		
		Prevention of scanning attacks, such as port scanning and address scanning attacks		
		Tracert		
		Static denylist, dynamic denylist		
		Connection limit		
		Attack logs in real time		
		Security zone policy-matching logs		
	Security audit	Denylist logs		
		Connection limit logs		
		Session logs		
		Traffic statistics and analytics		
		Security event statistics		
		IP services	Static ARP entries, dynamic ARP entries, proxy ARP, gracious ARP	
			Local static domain name, DNS client	
			NTP client, NTP server	
		Network protocol	IP routing	Static routing management
				Policy-based routing
Dynamic routing: RIPv1, RIPv2, OSPF, routing policy				
Cluster management				
1:1 backup in a cluster				
	High availability	Stateful failover		
		Static link aggregation, dynamic link aggregation, multi-chassis link aggregation		
		NQA		
		BFD		
		Hot patch		
	Configuration management	ISSU		
		Local management from the console port		
		Local or remote management through Telnet or SSH		
		RBAC for controlling access to commands based on user roles		
		Multiple authentication and authorization methods for users		

Web management interface	Configuration from the Web interface
	Automatic logoff of the Web administrator after the idle timer expires
	Access control and authentication for Web users
	RBAC for controlling access to Web menu based on roles
SNMP	SNMPv1, SNMPv2c, SNMPv3

Application Scenarios

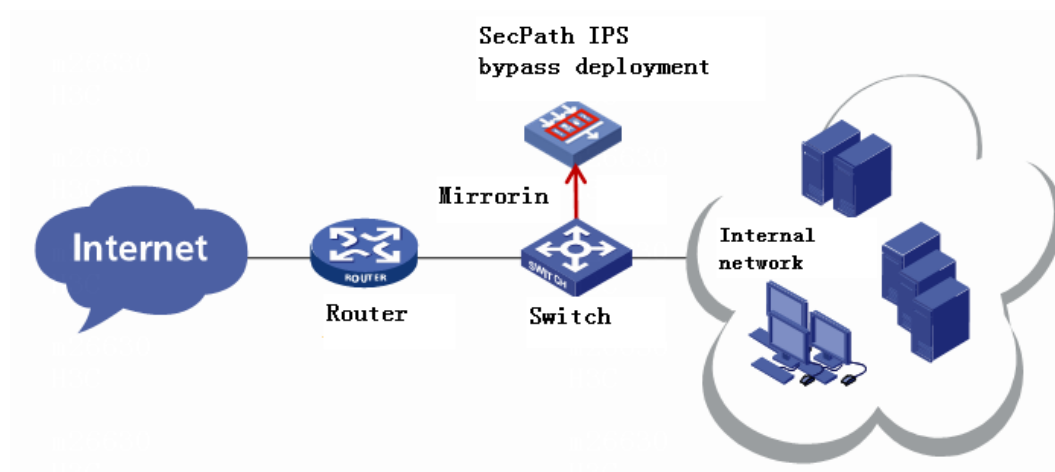
IPS inline deployment

The IPS device is deployed on the key path on the network. It prevents internal and external network attacks by analyzing the Layer 4 through Layer 7 information of the traffic flows that pass through the device.



IPS bypass deployment

The device monitors and analyzes network traffic, records attack events, and sends alarms.



The Leader in Digital Solutions

New H3C Technologies Co., Limited

Beijing Headquarters

Tower 1, LSH Center, 8 Guangshun South Street, Chaoyang

District, Beijing, China

Zip: 100102

Hangzhou Headquarters

Copyright ©2021 New H3C Technologies Co., Limited Reserves all rights

Disclaimer: Though H3C strives to provide accurate information in this document, we cannot guarantee that details do not contain any technical error or printing error. Therefore, H3C cannot accept responsibility for any inaccuracy in this document.