AADONA
GOING BEYOND VISION

ICARUS : INU-7184H

Enterprise Grade 18 Port NG-UTM for up to 600 Concurrent Users

OVERVIEW

Gateway Security

INU-7184H integrates firewall, Deep Packet Inspection (DPI), virus scanning, IPS, SSL Inspection and blocking, moreover, extended APT prevention is provided to stay one step ahead for impr compliance and security.

1. Stateful packet inspection (SPI) firewall technology examines the packet header and destination port for authentication and checks the entire packet's content before determining whether to allow its passage into the network.
2. SPI firewalls can drop any packet that is identified as potentially dangerous and automatically blocks DoS, DDOS, and UDP Flood attacks.
3. Web filtering to block HTTP/HTTPS access
4. Intrusion Prevention System (IPS)
5. Application control
6. Virus scanning and spam filtering
7. Network traffic monitoring

Integrated Next-Gen UTM and Layer3-7 Switching into One Single Appliance

INU-7184H is an integrated appliance that combines the security features of Next-Gen UTM and layer 3 core switch, upgrading management from Layer 3 routing capability to the higher application layer. It is an advanced firewall with 18 gigabit Ethernet ports, firewall throughput up to 24 Gbps improved VPN throughput of 2 Gbps.

1. AADONA INU-7184H differs from other competitors in multiple physical Gigabit Ethernet interfaces, allowing IT administrators to bind ports into port groups.
2. Going beyond the traditional Layer 3 routing mechanism among port groups, DPI is embedded as an advanced method to filter packets functioning at the application layer and allows business to be much more precise in their control of what enters or exits the network.

Supports SDN Controller

Being the core of an SDN network, SDN controller is designed to manage fiow control to enable intelligent networking. Based on protocols, the controller configures network devices and chooses the optimal network path for application traffic. IEEE 802.1Q VLAN is supported to provide a degree of isolation by dividing the network into isolated islands as if provided by separate physical networks.

Data Loss Prevention (DLP) and Application Control

DLP detects potential data breaches / data ex-filtration transmissions and prevents them b monitoring, detecting and blocking sensitive data. Having application layer firewall technolog INU-7184H is able to inspect both HTTP and HTTPS packets and prevents losing sensitive information or subsequently acquired by unauthorized party. Unique DPI performs traffic signature analysis by inspecting all packets for new application signatures, score up the signatures, and append them to the relevant database. More importantly, having recorded these collected data will be available for future audits.

1. Support for protocols and applications, including video streaming, peer-to-peer communication, social networking, and instant messaging
2. Detailed control over file sharing, remote control, VoIP, online games, browsers, etc.
3. SSL/HTTPS Inspection
4. Cloud database updates

Single-Pane-of-Glass Dashboard

INU-7184H dynamic dashboard in the web user interface (web UI) displays a graphic view of the system status including concurrent connections, application classification, network resource usage, HTTP/HTTPS traffic and intrusion defense to help in tracking and diagnosis. IT administrators are given visibility about network users, their devices, and their applications.

Complete VPN Solutions

Using IPsec, PPTP, L2TP, and SSL VPN connections, INU-7184H provides data confidentiality, data integrity, and data authentication. At the same time, popular protocols such as web, SMTP, and POP3 that contain packets transmitting within tunnels can be controlled.

1. Supports IPsec, PPTP, L2TP, SSL and GRE Tunnel
2. Supports DES, 3DES, and AES encryption and SHA-1/MD5 authentication algorithms
3. SSL VPN mobility client for Android and Apple iOS
4. Controls connectivity of remote sites from the central site

Cloud-based Management

I-Cloud is a next-gen cloud service platform providing user friendly interface to support ins equipment maintenance and management. It is an all-inclusive solution to monitor various networking appliances deployed in either external or internal networks such as UTM. When anomaly occurs, administrators will be notified of the problem.

- Central management system designed for multi-site network security appliances deployments.

Exceptional Performance and Consolidated Security Features

INU-7184H adopts best-in-class multi-core x86 CPU platform to deliver exceptional performance and intelligent network security features. AADONA develops high-performance security modules an delivers enterprise-class security, high connection capacity, and supports USB instant recovery.

IPv4 / v6 Dual Mode

Native dual-stack supported. To cope with IPv4 depletion, AADONA provides a solution that covers both IPv4 and IPv6 network and can be configured for IPv4 only, IPv6 only, or to suppo protocols simultaneously. Furthermore, all AADONA appliances have been certified with IPv6 Ready logo.

SSL Inspection

To protect your network from network threats, SSL inspection is the key used to unlock encrypted sessions, look into encrypted packets, find threats, and block them. Several security features that can be applied using SSL certificate inspection are IPS, gateway anti-virus, web filtering, applica control, and QoS.

Inbound/Outbound Load Balance

Load balancing is provided for distributing incoming HTTP requests across multiple servers, improving server utilization and maximizing availability. When one of the links is down, the other link will take over the work and handle the traffic until former one returns to normal, in either manual or auto distribution mode. Built-in DNS server functionality enables inbound Load Balancing and distributes inbound data traffic over multiple WAN links to devices behind UTM for more reliable net connectivity.

Intrusion Prevention System (IPS)

Built-in IPS inspects the packets from OSI layer 4-7 (transport to application layer) and bl concealed malicious code and worms delivered in TCP/IP protocols. As soon as an attack is suspected, IT administrator will be notified immediately and an extensive range of reports will be available later for analysis. AADONA regularly updates the predefined attack-signature database and makes available as IPS security package.

Advanced Threat Defense

In addition to firewall, Intrusion Prevention System (IPS), and virus scanning, INU-7184H can monitor malware or threats within traffics based on analysing fiows, webpages, and email. By performing different security mechanisms, business network is given more effective and profound protection against active cyberattacks, targeted attacks, and sophisticated malware.

Gateway

For companies that have deployed mail servers in their network environments but lack advanced filtering, INU-7184H can be placed at gateway to secure email and get simple and powerful protection from spam, virus and malware.

Anti-Virus

INU-7184H for large enterprises offer Clam AV for virus scanning which can detect over millions of viruses, worms, and Trojans. Once suspicious emails are detected, the administrator can decide to delete or block them. Moreover, websites will be scanned once the function of anti-virus is enabled in policy. Customers may choose to purchase a Kaspersky module for their security needs. (INU-7184H contains 1-year Kaspersky license.)

Anti-Spam

INU-7184H employs multi-spam filters: ST-IP Network Rating, Bayesian Filtering, spam characteristics filtering, fingerprinting, auto learning, and personal B/W list. It also gives administrators the fiexibility to enforce custom filtering. These help industries create their own database by importing the latest spam update. Following actions like forward, delete, quarantine can be taken on the mail identified as the spam. Email accessed by users from LAN to DMZ can be especially filtered and logged.

IP Traffic Streams Analysis

Outgoing/incoming concurrent sessions, upload/download fiow, and time duration are fiow parameters collected for packet-based traffic analysis. Using a combination of pattern matcl administrators can determine whether an activity is performed normally or not. If employees violate the rules and exceed the download fiow, IT administrators are allowed to define the trusted IP list and take appropriate actions to block network access, limit maximum bandwidth or simply rece notifications.

QoS

QoS offers more agile bandwidth management for industries and organizations. All the servers and defined users can be assigned minimum and maximum bandwidth; the remaining bandwidth will be allotted to the other users according to their usage/configuration.

Content Filtering

IT administrators can configure Web filtering profiles that block URLs to inappropriate webpages like violence and pornography and hacking attacks like malware and virus. Moreover, UTM filters out ActiveX objects, Cookies or Java applets that may pose a security threat in certain situations. Both keywords and URLs of specified websites can be added to Blacklist and Whitelist.

URL Database

Built-in URL database collects almost 1,000,000 URLs and updates regularly without additior charge. All these URLs and their contents are analyzed and classified into 12 categories, including Aggressive, Audio-Video, Drugs, Gambling, Hacking, Porn, Proxy, Redirector, Spyware, Suspect Violence, and Warez. IT administrator is able to block any category in the database easily without entering keywords or desired URL addresses individually.

WEB and Email Records

1. Record each user online behavior (computer name, IP address, MAC address, and traffics) time stamps, items and locations

2. Record incoming and outgoing mail (Webmail) and their attachments passing through the mail gateway

3. Email is saved in an .eml format that can easily be viewed and searched

Flow Analysis

No matter whether internal users' devices are on or off, fiow analysis tools can display statistics, protocol distribution list, and rankings of traffic fiows.

Application Control

In order to prevent data leakage and ensure regulatory compliance, the access to applications which are unrelated to business should be controlled during working hours. INU-7184H can enforce policy for applications like P2P, VOIP, GoToMyPc, Webpages, Games, Media Player, Bit Torrent, Foxy (Gnutella), stock market, Instant Messaging, Xunlei, Gator, Yahoo Manager, Virus and Malware, file na extension, Kazaa, Facebook, etc.

Graphical Reports

AADONA reporting allows administrators to customize how the chart types (bar, pie, line, and table) or texts will be displayed at the top of the report. INU-7184H displays operation status for the time frame specified (day, week, or month), including CPU, RAM, modification times, security level and monitor reports.

Remote-Access VPN

Remote-access VPNs allow secure access to corporate resources by establishing an encrypted tunnel across the Internet. The ubiquity of the Internet, combined with VPN technologies, allows organizations to cost-effectively and securely extend the reach of their networks to anyone, anyplace, anytime. AADONA offers IPSec, PPTP, and L2TP VPN technologies on a single platform with unified management. IPsec VPN securing the site-to-site connections allows headquarters and their branch offices to be on the same network and sharing resources among offices. Moreover, PPTP and L2TP VPN offer point to point connection for employees working remotely. Employees can easily access industry's network in a secured way.

SSL VPN

SSL-based VPNs provide remote-access connectivity from almost any Internet-enabled location using a Web browser and its native SSL encryption. It does not require any special-purpose client software to be pre-installed on the system. For remote clients, there are two different types of access. One is access to the internal network and the other is access to the Internet over VPN server. Administrators can control bandwidth usage, VPN service and time from both types.

FEATURES

Features	Description
Threats Defense (Anti-Virus/IPS/SSL Inspection)	1. Uses open source Clam AV engine with huge database includes millions of signatures 2. Kaspersky module (Optional); built-in 1 year for INU-7184H 3. Clam AV team has fast response time, updates signature regularly and requires no yearly subscription fees 4. Provides IPS attack-signature database 5. IPS risk management is divided into 3 levels (high, medium, and low) 6. Provides scalable SSL inspection
Malicious URL Filtering (URL & Databases)	1. Provides URL filtering and database 2. URL filtering policies are allowed to be configured by administrators 3. IT administrator can add keywords or URLs to Black/White lists
Firewall Security	1. Coordinated DoS/DDOS attacks and UDP Flood performed by hackers can be blocked automatically. 2. QoS provides bandwidth guarantee and a priority command can be given for min/max bandwidth guarantee. 3. Limit the bandwidth using source IP in both directions 4. Supports IPv4, IPv6, and Dual Stack 5. Supports load balancing and failover for both outbound and inbound traffic 6. Provides DNS service and Dynamic DNS service
Potential Risks Detection (Flow Analysis)	1. Flow/behavior-based anomaly detection allows both up and down sessions to be analyzed and see if a performance challenge exists 2. An anomaly can be recorded, blocked, and notify subscribers. 3. Prevents ARP spoofing
Mail Security (Anti-Spam, Mail Filtering)	1. Employs multiple spam mechanisms: ST-IP network rating, fingerprinting, Bayesian filtering, auto learning, auto-whitelist, system and personal Blacklist/Whitelist and spam characteristics filtering. 2. Offers Email virus scanning 3. Offers Email auditing, advanced filtering and quarantine 4. Client-side spam mail search is available on web-based interface 5. Additional actions such as quarantine, delete, blocking IP, and carbon copies can be performed to all mail. 6. Searching recorded email available
Application Access Control	Multiple application categories e.g. P2P, IM, VOIP, Web, WebMail, game, video, spyware, stock and others. Administrators can use policies to prohibit users from accessing applications

User Identity (Radius)	1. The host computers are established to ensure user identity and also support the use of LDAP, Radius, AD or POP3 servers for authentication. 2. Desired user groups can be customized 3. Applies access control methods 4. Provides authentication record and connection status
Content Record	1. Logs all incoming/outgoing emails with delivery date and time 2. Archived email is exported in. eml format 3. Records browsing history
Load Balance	1. Ensuring the network is never disconnected 2. Provides inbound & outbound load balancing 3. Users can assign load balancing automatically, manually, or by source-destination IP 4. Built-in Smart DNS Server
VPNs Connection	1. IPSec and Site-to-Site PPTP and L2TP VPN 2. Reliable SSL VPN connection 3. Users can create, edit, and control over VPN connections 4. Supports IP Tunneling and definable policy control
QoS	1. Supports QoS 2. Supports bandwidth guarantee, max/min-limit, and priority commands 3. Bandwidth usage from the internal/external source IP can be limited 4. Efficient priority scheme is available
Operation Modes	NAT, Routing
Logging & Reports	Multiple event logs can be centrally logged and monitored. And it includes configuration, networking and route, objects, services, advanced protection, mail security, VPN, etc. A report includes a statistic table, ranking grid, bar/line graphs, and pie charts. Provides analysis of debug, system performance, intrusion attempts, and tracking.
Virtual Server	Supports virtual server that data fiows can be transmitted to any of the other ports without using any switch or router
High Availability	Building a cluster and hot standby of two or more AADONA devices is available
Bulletin Board	Announcement can be made to employees in a very effective and proper way
Diagnostic Tools	Standard net tools such as Ping, Traceroute, DNS lookup, and port scanner are available to help users identify and fix connection problems.

Others	1. The network is divided in zones and a zone can by managed by SDN 2. Administrators can choose authorized users and assign access conditions 3. Automatic disk check can be scheduled 4. Supports SNMP 5. Supports VLAN 802.1Q 5. LCM display 6. Data backup and mount

SPECIFICATIONS

Model Name	INU-7184H
HARDWARE	
Dimensions W*H*D(mm)	438*292*44
Platform Size	1U
Recommended Users Numbers	Up to 600
LAN Bypass	Y
Reset Button	Y
USB 3.0	2
CAPACITY	
Ethernet Interfaces 10/100/1000	18 ports
UTM Throughput	9.6 Gbps
VPN Throughput	2 Gbps
IPS Throughput	1.2 Gbps
Anti-Virus Throughput	0.9 Gbps
Max. Concurrent Sessions	5,000,000
Mail Scan / Day	5,500,000
VPN TUNNELING	
IPSec VPN Tunnels	8,000
PPTP Tunnels	3,000
SSL VPN Tunnels	3,000
IP Tunnel Tunnels	1,500
NETWORK PROTECTION	
Security Gateway	Y
Kaspersky	1 year

HTTPS Filtering	Y
Spam Filtering	Y
IPS	Y
IPS Signature Database	Y
APP Access Control	Add network configuration, video, file transfer, remote contol, browser, software update
URL Database	Y
Dashboard	APP, Mail, IPS, Web, Defense, Dynamic Sessions Analysis
Reports	Y
Mail Audit	Y
Behavior Management	Y
Anomaly IP Analysis	Y
Load Balance (Out / In)	Y
QoS	Y
Bulletin Board	Y
Authentication	Y
Eye Cloud	Y
High Availability	Y
IPS Signatures	4,020
IPSec / PPTP / L2TP VPN	Y
SSL VPN	Y
Encryted IP Tunnel Mode	Y
Warranty	2 Year Default + 3 Year Warranty Pack, Total 5 Year

*ALL SPECIFICATIONS ARE SUBJECT TO CHANGE WITHOUT NOTICE.

*All specifications are subject to change without notice.

AADONA Communication Pvt Ltd

1st Floor, Phoenix Tech Tower, Plot No.
14/46, IDA - Uppal, Hyderabad,
Telangana 500039

Phone : 1800-202-6599

www.aadona.com

contact@aadona.com

AADONA Communication Pvt Ltd

7, SBI Colony, Mohaba Bazar, Hirapur
Road, Raipur Chhattisgarh 492099

Phone : 1800-202-6599

www.aadona.com

contact@aadona.com