Security Appliances | Product Information

Allied Telesis™

Virtual UTM Firewall

Application for the Vista Manager Network Appliance

Allied Telesis Unified Threat Management (UTM) Firewalls are the ideal integrated security platform for modern businesses. A powerful 1/10G firewall and threat protection is combined with comprehensive VPN capability to provide an innovative high performance business solution.

The Allied Telesis Virtual 1/10G UTM Firewall is an ideal choice for high speed Enterprise gateway applications. Securely connect branch office locations, while the "best of breed" security platform enables up-to-the-minute threat detection, ensuring business continuity and corporate data protection.

High performance

1/10G interfaces and a high performance specification provide excellent central office connectivity.

FEATURE	PERFORMANCE
Firewall throughput (Raw)	20 Gbps
Firewall throughput (App Control)	18 Gbps
Concurrent sessions	1,000,000
IPS throughput	16 Gbps
IP Reputation throughput	18 Gbps
Malware protection throughput	13 Gbps
VPN throughput	5 Gbps

Note: All performance values are UDP maximums, and vary depending on system configuration.

Advanced feature licenses

Flexible subscription licensing options make it easy to choose the right combination of security features to best meet your business needs. The Next Generation Firewall (NGFW) license includes App Control, Web Control and URL Filtering. The Advanced Threat Protection (ATP) license includes IP Reputation, stream-based Malware Protection and proxy-based Antivirus. Standard Firewall, VPN connectivity, and all other security features are included in the base feature set.

Application-aware Firewall

Allied Telesis UTM Firewalls have a Deep Packet Inspection (DPI) engine that provides real-time, Layer 7 classification of network traffic. Rather than being limited to filtering packets based on protocols and ports, the firewall can determine the application associated with the packet. This allows Enterprises to differentiate business-critical from non-critical applications, and enforce security and acceptable use policies in ways that make sense for the business.

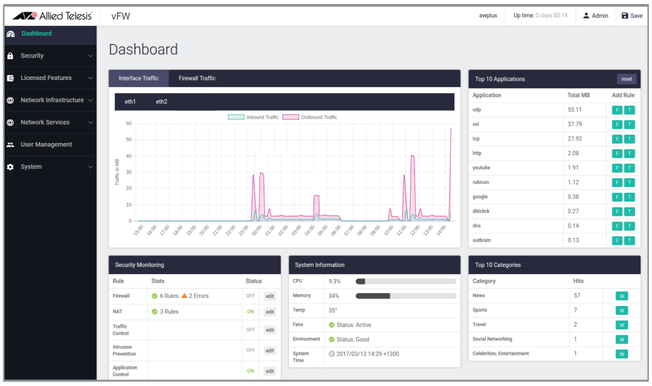
Secure Remote Virtual Private Networks (VPN)

Allied Telesis UTM Firewalls support IPSec site-to-site VPN connectivity to connect one or more branch offices to a central office, providing employees company-wide with consistent access to the corporate network. Multipoint VPN enables a single VPN to connect the central office to multiple branch offices.

Remote workers can utilize an SSL VPN connection to encrypt their business data over the Internet, allowing them to utilize all their business resources when working from home, travelling, or otherwise away from the company premises.

Easy to manage

The firewalls run the advanced AlliedWare Plus™ fully featured operating system, with an industry standard CLI. The Graphical User Interface (GUI) provides a dashboard for monitoring, showing traffic throughput, security status, and application use at a glance. Configuration of security zones, networks and hosts, and rules to limit and manage traffic, as well as management of advanced threat protection features and network services, provide a consistent approach to policy management.



Top 10 Applications

Application	Total MB	Add Rule
udp	55.11	F T
ssl	37.79	F T
tcp	27.92	F T
http	2.08	F T
youtube	1.91	F T
rubicon	1.12	F T
google	0.38	F T
dblclick	0.27	F T
dns	0.14	F T
outbrain	0.13	F T

Security Monitoring

Rule	Stats	Status	
Firewall	✓ 6 Rules ⚠ 2 Errors	OFF	edit
NAT	✓ 3 Rules	ON	edit
Traffic Control		OFF	edit
Intrusion Prevention		OFF	edit
Application Control		ON	edit

System Information

CPU	9.3%
Memory	34%
Temp	35°
Fans	✓ Status: Active
Environment	✓ Status: Good
System Time	2017/03/13 14:29 +1300

Top 10 Categories

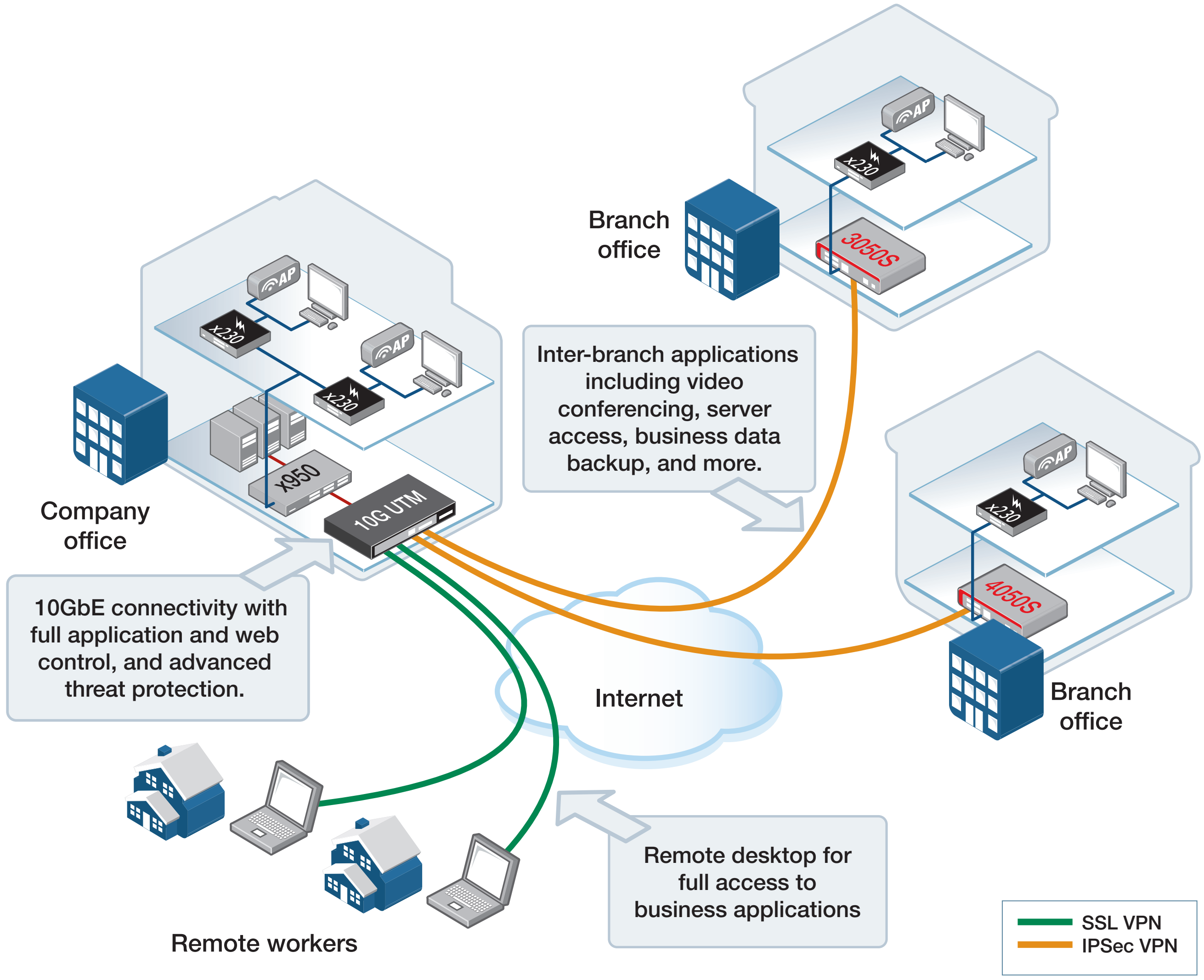
Category	Hits	
News	57	W
Sports	7	W
Travel	2	W
Social Networking	1	W
Celebrities, Entertainment	1	W

Deployment

The Virtual UTM Firewall application runs on an Allied Telesis Vista Manager Network Appliance. To use the firewall, follow the install guide instructions to download, install and operate the application.

DPI FIREWALL ENGINE	
Deep Packet Inspection engine	The high-performance inspection engine performs stream-based bi-directional traffic analysis, identifying individual applications, while blocking intrusion attempts and malware.
Bi-directional inspection	Protects your network by scanning for threats in inbound traffic, while also protecting your business reputation by scanning for threats in outbound traffic.
Single-pass inspection	Multiple threat detection and protection capabilities are integrated within a purpose-built solution that provides single-pass low-latency inspection and protection for all network traffic.
APPLICATION AND WEB CONTROL	
Application control	The visibility provided by the application-aware firewall allows fine-grained application, content and user control. Use either the free built-in application list, or the subscription-based Sandvine database of application signatures which is regularly updated.
Application bandwidth management	Manage application bandwidth to support business requirements, while limiting non-essential applications.
Web control	Digital Arts$^{\text{TM}}$ web categorization enables easy control of web content by selecting which of the 100 content categories to allow or deny globally, or per user or group. URL categories are cached locally so the response time for access to frequently visited sites is not delayed. Any URL can be checked to view its web control category, to ensure website management aligns with business policies.
URL filtering	Enables HTTP or HTTPS access to particular websites to be allowed (whitelist) or blocked (blacklist) with user-defined lists. A subscription service can also be employed, utilizing a frequently updated blacklist from Kaspersky.
FIREWALL AND NETWORKING	
Flexible deployment options	The Allied Telesis UTM Firewalls can be deployed in traditional NAT, Layer 2 Bridge, Wire Mode and Network Tap modes.
IPv6 transition technologies	DS (Dual Stack) Lite, Lightweight 4over6, and MAP-E support connecting IPv4 networks over an IPv6 Internet connection.
AMF-WAN (Allied Telesis SD-WAN)	Software-Defined Wide Area Networking (SD-WAN) enables users to measure the quality of their WAN links and send real-time and other applications over the most suitable connection. Users can also load-balance an application over multiple WAN links, prioritize the delivery of business-critical applications, and send traffic directly to Cloud-based services from the branch office.
sFlow	sFlow is an industry-standard technology for monitoring networks. It provides complete visibility into network use, enabling performance optimization, usage accounting/billing, and defense against security threats. Sampled packets sent to a collector (up to 5 collectors can be configured) ensure it always has a real-time view of network traffic.
UNIFIED THREAT MANAGEMENT	
Malware protection	All inbound, outbound and intra-zone traffic is scanned for viruses, Trojans, and other malware to protect business information.
DoS attack protection	Protection against Denial of Service (DoS) attacks, which are designed to consume resources and therefore deny users network and application access.
Automatic security updates	Security is kept up-to-the-minute without requiring user intervention or network disruption. UTM Firewalls with active security subscriptions automatically receive new threat signature and database updates, which have been tested by Allied Telesis.
Zone-based protection	Internal security is increased with the network segmented into multiple security zones, with boundaries that block the propagation of threats.
Bot activity detection	Kaspersky$^{\text{TM}}$ malware protection identifies and blocks command and control traffic originating from bots on the local network to IPs and domains that are identified as propagating malware.
Intrusion Detection and Prevention Systems (IDS/IPS)	IDS/IPS is an intrusion detection and prevention system that protects your network from malicious traffic. IDS/IPS monitors inbound and outbound traffic, and identifies threats which may not be detected by the firewall alone.
Protocol anomaly detection	Identifies and blocks attacks that abuse protocols in an attempt to circumvent the IDS/IPS.
VIRTUAL PRIVATE NETWORKING	
IPSec VPN for site-to-site and multi-site connectivity	High-performance IPSec VPN allows an Allied Telesis UTM Firewalls to act as a VPN concentrator for other large sites, branch offices or home offices. Multipoint VPN uses a single VPN to connect a head office to multiple branch offices.
SSL/TLS VPN for secure remote access	The OpenVPN® client allows easy access to corporate digital resources when away from the office. The TLS version for OpenVPN connections can be specified to encourage use of version 1.2 or 1.3, which are compliant with Information-technology Promotion Agency guidelines.
Redundant VPN gateway	Primary and secondary VPNs can be configured when using multiple WAN connections, for seamless failover of VPN connectivity to a remote site.
Dynamic routing through VPN tunnels	Dynamic routing over VPN links ensures no loss of connectivity, as traffic is routed through an alternate link in the event of a tunnel failure.

Key Solution: Integrated Security and Threat Protection



Inter-branch applications including video conferencing, server access, business data backup, and more.

10GbE connectivity with full application and web control, and advanced threat protection.

Remote desktop for full access to business applications

Integrated protection and secure remote access

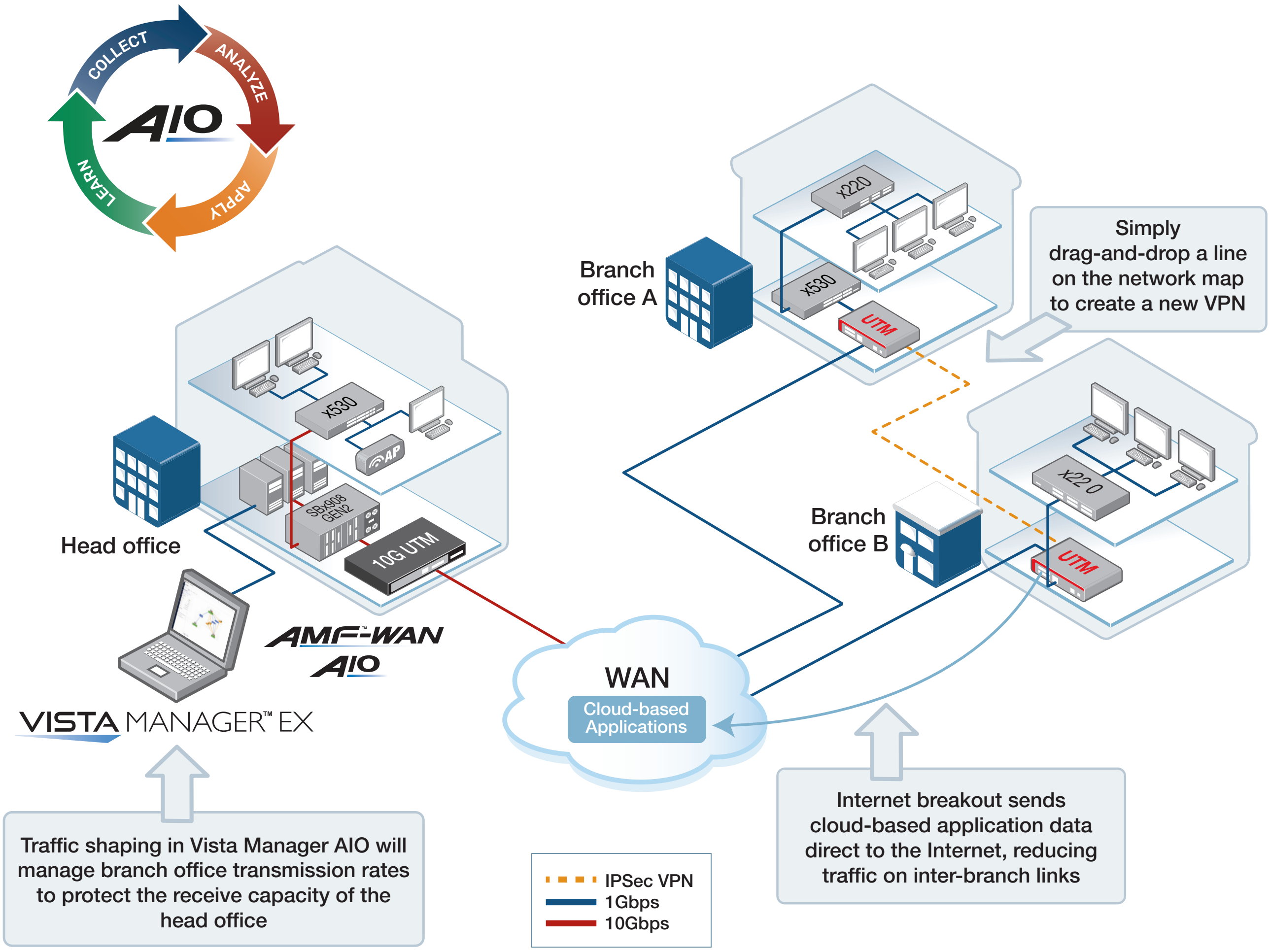
Allied Telesis UTM Firewalls are the ideal integrated security platform for modern businesses. The powerful combination of an application-aware firewall and integrated threat protection, along with secure remote access, provides a single platform able to connect and protect corporate data.

This solution shows a Virtual 10G UTM Firewall providing site-to-site IPSec VPN connectivity between the corporate office and branch offices, while also allowing secure SSL VPN access for remote workers, so they enjoy full access to digital company resources when away from the office.

As well as securing remote connectivity, the firewall will simultaneously ensure the security of inbound and outbound business data, with advanced threat protection features like IP reputation, malware protection and antivirus. Full application control allows this organization to control the applications their people use, and how they use them, so security and acceptable use policies can be enforced in ways that make sense for the business.

The powerful combination of features makes Allied Telesis UTM Firewalls the one-stop integrated security platform for protecting today's online business activity.

Key Solution: Intent-based WAN Management with AIO



Simply drag-and-drop a line on the network map to create a new VPN

Traffic shaping in Vista Manager AIO will manage branch office transmission rates to protect the receive capacity of the head office

Internet breakout sends cloud-based application data direct to the Internet, reducing traffic on inter-branch links

AIO enables intent-based WAN management

Allied Telesis Intent-based Orchestrator (AIO) provides todays businesses with intuitive GUI driven management of their business WAN infrastructure. This solution shows a Virtual 10G UTM Firewall providing VPN connectivity between the corporate office and branch offices.

AIO is integrated into Vista Manager EX, our powerful network management and monitoring tool. The AIO enables effortless translation of business intent into dynamic network change to meet requirements, and make network management easy.

The AIO graphical interface supports:

- Dynamic creation of VPNs between locations with graphical drag-and-drop simplicity
- Prioritizing business-critical applications between office locations
- Shaping inter-branch traffic for maximum performance
- Breaking out cloud-based applications directly from the branch
- Simple setting of security levels for multiple locations

Enjoy streamlined administration of WAN traffic between distributed office locations, with simple requirements input – and let the intelligence of the AIO manage your business network.

Features

Firewall

- Deep Packet Inspection (DPI) application aware firewall (built-in or Sandvine application lists) for granular control of apps and IM (chat, file transfer, video)
- Application Layer Gateway (ALG) for FTP, SIP and H.323
- Application layer proxies for SMTP and HTTP
- Bandwidth limiting control for applications and IM/P2P
- Firewall session limiting per user or entity (zone, network, host)
- Bridging between Ethernet ports
- Data leakage prevention
- Bidirectional single-pass inspection engine
- Maximum and guaranteed bandwidth control
- Multi zone firewall with stateful inspection
- Static NAT (port forwarding), double NAT and subnet-based NAT
- Masquerading (outbound NAT)
- Proxy-based web control by content categorisation (Digital Arts)
- Custom web control categories, match criteria and keyword blocking per entity
- Security for IPv6 traffic

Networking

- Routing mode / bridging mode / mixed mode
- Static unicast and multicast routing for IPv4 and IPv6
- DS-Lite, Lightweight 4over6, and MAP-E for connecting IPv4 networks over IPv6
- Dynamic routing (RIP, OSPF and BGP) for IPv4 and IPv6
- Dynamic multicasting support by IGMP and PIM
- Route maps and prefix redistribution (OSPF, BGP, RIP)
- Traffic control for bandwidth shaping and congestion avoidance
- Policy-based routing
- SD-WAN: performance measure and load balance WAN links
- PPPoE client
- DHCP client, relay and server for IPv4 and IPv6
- Dynamic DNS client
- IPv4 and IPv6 dual stack
- Device management over IPv6 networks with SNMP and SSH
- Logging to IPv6 hosts with Syslog
- Web redirection allows service providers to direct users to a specified web address
- sFlow packet sampling for network monitoring

Management

- Allied Telesis Autonomous Management Framework (AMF) member
- AMF secure mode increases network security with management traffic encryption, authorization, and monitoring
- Web-based Device GUI for firewall configuration and easy monitoring
- Industry-standard CLI with context-sensitive help
- Role-based administration with multiple CLI security levels
- Built-in text editor and powerful CLI scripting engine
- Comprehensive SNMPv2c/v3 support for standards-based device management
- Event-based triggers allow user-defined scripts to be executed upon selected system events
- Comprehensive logging to local memory and syslog
- Console management port on the front panel for ease of access

Diagnostic Tools

- Ping polling for IPv4 and IPv6
- TraceRoute for IPv4 and IPv6
- DPI statistics per entity (Zone, Network, Host), or per PBR rule for SD-WAN

Authentication

- RADIUS authentication and accounting
- TACACS+ Authentication, Accounting and Authorization (AAA)
- Local or server-based RADIUS user database
- RADIUS group selection
- Strong password security and encryption

Unified Threat Management (UTM)

- Proxy-based anti-virus scanning
- Auto-update of UTM signature files
- Bot activity detection (using Kaspersky malware protection)
- Intrusion Detection and Prevention System (IDS/IPS) (no license required)
- DoS and DDoS attack detection and protection
- IP reputation (Emerging Threats)
- Stream-based Malware protection (Kaspersky) from over 20,000 attacks
- Dynamic URL filtering (Kaspersky)
- URL blacklists and whitelists (block or allow HTTP and HTTPS access to specific Websites)
- Protocol anomaly detection and protection
- Zone-based UTM

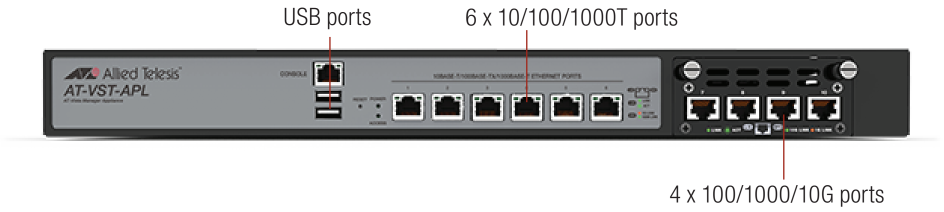
VPN Tunneling

- Diffie-Hellman key exchange (D-H groups 2, 5, 14, 15, 16, 18)
- Secure encryption algorithms: AES and 3DES
- Secure authentication: SHA-1 and SHA-256
- IKEv1 and IKEv2 key management
- IPsec Dead Peer Detection (DPD)
- IPsec NAT traversal
- IPsec VPN for site-to-site connectivity
- Multipoint VPN for connecting a single VPN to multiple end points
- Dynamic routing through VPN tunnels (RIP, OSPF, BGP)
- SSL/TLS VPN for secure remote access using OpenVPN
- IPv6 tunneling

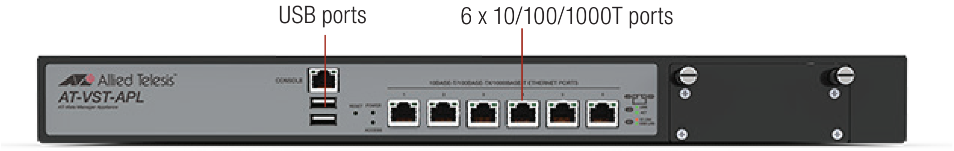
Virtual UTM Firewall

Running on the VST-APL-10 or VST-APL-06 Vista Manager Network Appliance

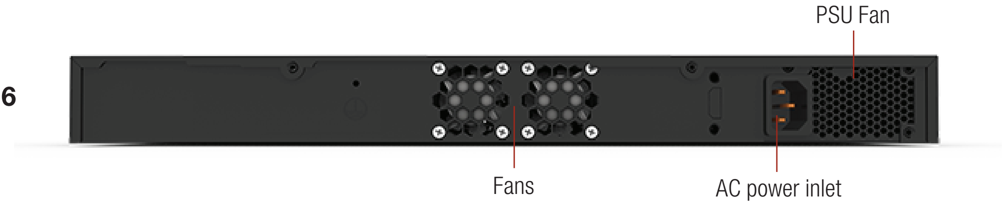
VST-APL-10



VST-APL-06



VST-APL-10/06



Specifications

	VIRTUAL UTM FIREWALL (RUNNING ON VST-APL)
Memory	
Memory (RAM)	32GB (shared)
Memory (Flash)	1TB (shared)
Security features	
Firewall	Stateful deep packet inspection application aware multi-zone firewall
Application proxies	FTP, TFTP, SIP
Threat protection	DoS attacks, fragmented & malformed packets, blended threats & more
Security subscriptions	Next-Gen Firewall, Advanced Threat Protection
Tunneling & encryption	
Site-to-site VPN tunnels (IPsec)	3,000
Client-to-site VPN tunnels (OpenVPN)	3,000
Encrypted VPN	IPsec, SHA-1, SHA-256, SHA-512, IKEv2, SSL/TLS VPN
Encryption	3DES, AES-128, AES-192, AES-256
Key exchange	Diffie-Hellman groups 2, 5, 14, 15, 16, 18
Dynamic routed VPN	RIP, OSPF, BGP, RIPng, OSPFv3, BGP4+
Point to point	Static PPP, L2TPv3 Ethernet pseudo-wires
Encapsulation	GRE for IPv4 and IPv6
Management & authentication	
Logging & notifications	Syslog (IPv4 and IPv6), SNMPv2c & v3
User interfaces	Web-based GUI, scriptable industry-standard CLI
Secure management	SSHv1/v2, strong passwords
Management tools	Allied Telesis Autonomous Management Framework™ (AMF), Vista Manager EX
User authentication	RADIUS, TACACS+, internal user database
Command authorization	TACACS+ AAA (Authentication, Accounting and Authorization)

	VIRTUAL UTM FIREWALL (RUNNING ON VST-APL)	
Networking		
Routing (IPv4)	Static, Dynamic (BGP4, OSPF, RIPv1/v2), source-based routing, policy-based routing, VRF-Lite, SD-WAN	
Routing (IPv6)	Static, Dynamic (BGP4+, OSPFv3, RIPng), policy-based routing, SD-WAN	
Multicasting	IGMPv1/v2/v3, MLD, PIM-SM, PIM-SSM, PIMv6	
Traffic control	8 priority queues, DiffServ, HTB scheduling, RED curves	
IP address management	Static v4/v6, DHCP v4/v6 (server, relay, client), PPPoE	
NAT	Static, IPsec traversal, Dynamic NAPT, Double NAT, subnet-based NAT	
Ethernet bonding	Static and LACP	
Hardware characteristics	**VST-APL-06**	**VST-APL-10**
Max power consumption	110 Watts	150 Watts
Max heat dissipation	375.4 BTU/h	511.9 BTU/h
Noise	29 dBA	29 dBA
10/100/1000T RJ45 copper ports	6	6
100/1000/10G RJ45 copper ports	-	4
Dimensions	438 x 292 x 44 mm	438 x 292 x 44 mm
Weight (unpackaged)	4.5 kg	4.9 kg
Weight (packaged)	7.5 kg	7.9 kg
Environmental specifications	**VST-APL-06/10**	
Operating temperature range	0°C to 40°C (32°F to 104°F)	
Storage temperature range	-25°C to 70°C (-13°F to 158°F)	
Operating relative humidity range	5% to 90% non-condensing	
Storage relative humidity range	5% to 95% non-condensing	
Operating altitude	2,000 meters maximum (6,561 ft)	
Regulations and compliances	**VST-APL-06/10**	
EMC	CISPR 32 class A, EN55032 class A, FCC class A, VCCI class A	
Immunity	EN55035, EN55024	
Safety Standards	UL62368, IEC60950-1, IEC62368, EN62368	
Safety Certifications	UL, TUV	
Reduction of Hazardous Substances (RoHS)	EU RoHS6 compliant	
IPv6 Ready	Phase 2 (Gold) Logo	

Security Licenses

LICENSE NAME	INCLUDES	1 YR SUBSCRIPTION	3 YR SUBSCRIPTION	5 YR SUBSCRIPTION
Advanced Firewall	Application Control Web Control URL Filtering	AT-FL-AR4-NGFW-1YR	AT-FL-AR4-NGFW-3YR	AT-FL-AR4-NGFW-5YR
Advanced Threat Protection	IP Reputation, Malware Protection Anti-virus	AT-FL-AR4-ATP-1YR	AT-FL-AR4-ATP-3YR	AT-FL-AR4-ATP-5YR

Ordering Information

AT-VST-APL-06[1]

AT-Vista Manager Network Appliance with 6 x 10/100/1000T copper ports

AT-VST-APL-10[1]

AT-Vista Manager Network Appliance with 6 x 10/100/1000T, and 4 x 100/1000T/10G copper ports

AT-FL-VFW-BASE[1]

Virtual firewall license to enable the UTM Firewall application on the AT-VST-APL-06 or AT-VST-APL-10 Vista Manager Network Appliance

[1] To use the Virtual UTM Firewall purchase a Vista Manager Network Appliance. Follow the install guide instructions to install and use the UTM Firewall application.