

10G 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 1/10G UTM Firewall application is an ideal choice for high speed Enterprise gateway deployment.

High performance

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

Advanced feature licenses

Flexible subscription licensing options make it easy to choose features to best meet your business needs. The Advanced Firewall and Threat Protection licenses enable additional ways to manage website access, and protect your business from threats.

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.

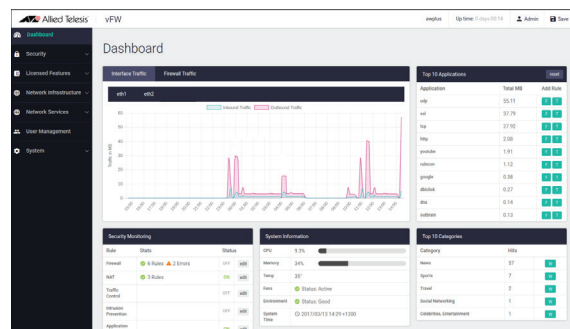
Deployment

The 10G 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.

Multiple firewall instances

Once the firewall application is installed on a Vista Manager Network Appliance, multiple 10G UTM firewall instances can be used at once. This allows managing and securing different parts of the network independently, and using overlapping IP addressing if required.

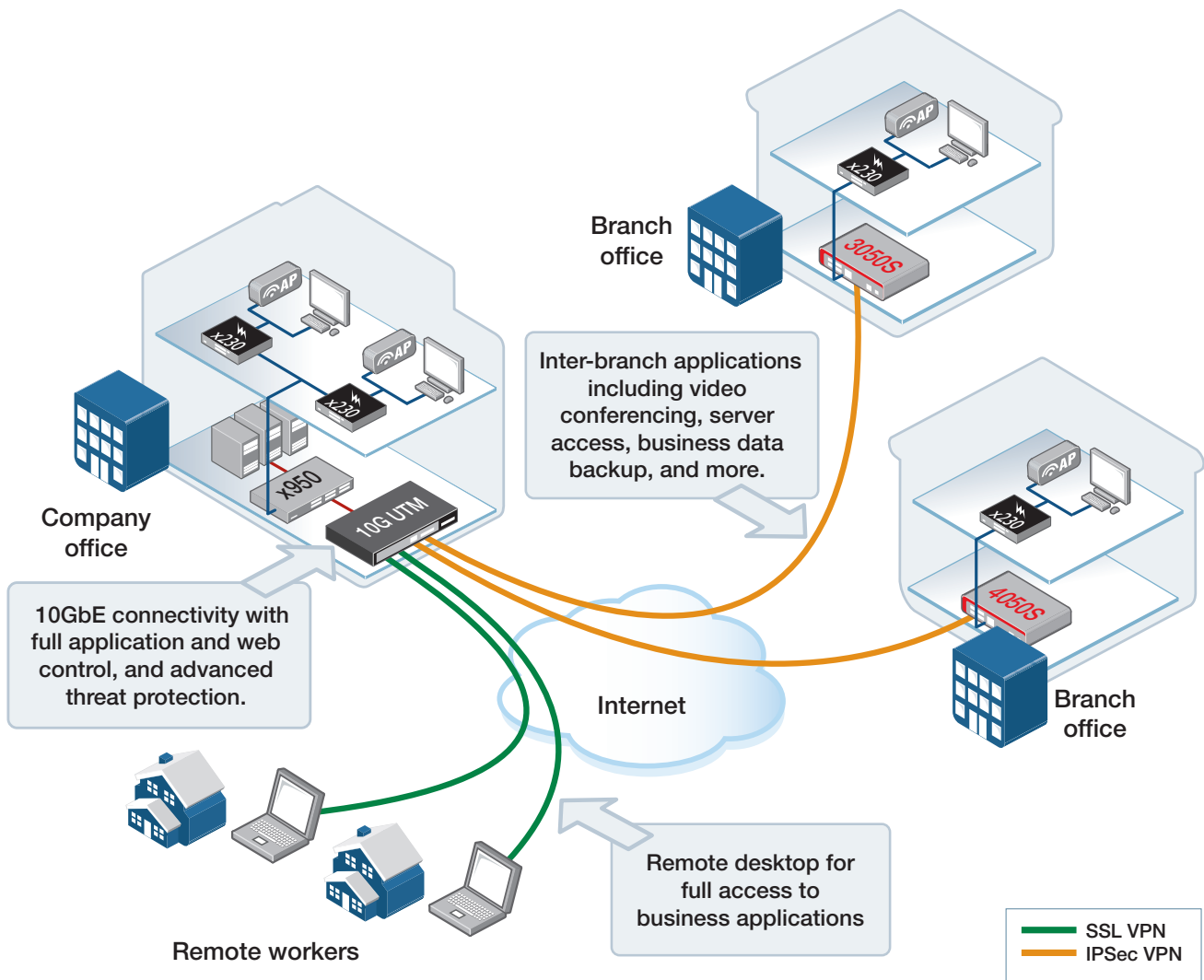
	Performance
Firewall Throughput (Raw)	20Gbps
Firewall throughput (App Control)	18Gbps
Concurrent sessions	1,000,000
IPS throughput	16Gbps
IPS Reputation throughput	18Gbps
VPN Throughput	5Gbps



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

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 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	Web categorization using the subscription-based Web Control feature enables easy management of user website access by selecting which content categories to allow or deny globally, or per user or group. Any URL can be checked to view its web control category, to ensure website management aligns with business policies. Proxy-based or Deep Packet Inspection (DPI) options provide flexibility.
URL filtering	Enables HTTP or HTTPS access to particular websites to be allowed or blocked with user-defined lists.
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	
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.
Advanced IPS (Intrusion Protection System)	Advanced IPS detects and blocks threats. The subscription-based service is updated daily, and protects against malware delivery, command and control, attack spread, in-the-wild exploits and vulnerabilities, and credential phishing. It also detects and blocks distributed denial-of-service attacks (DDoS), protocol and application anomalies, exploit kits and supervisory control and data acquisition (SCADA) attacks.
IP Reputation	The subscription-based IP Reputation uses regularly updated and comprehensive reputation lists which identify and categorize IP addresses that are sources of spam, viruses and other malicious activity, enabling strong local security policies to protect business networks.
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. Secure ways to login include LDAP authentication and two-factor authentication, with options to use a code, certificates, or a one-time password (OTP) via email. The TLS version for OpenVPN connections can be specified to encourage use of the latest and most secure version, and TLS Crypt provides ultimate security, with symmetric encryption including the key exchange for protection against TLS DoS attacks.
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.

Integrated Security and Threat Protection



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.

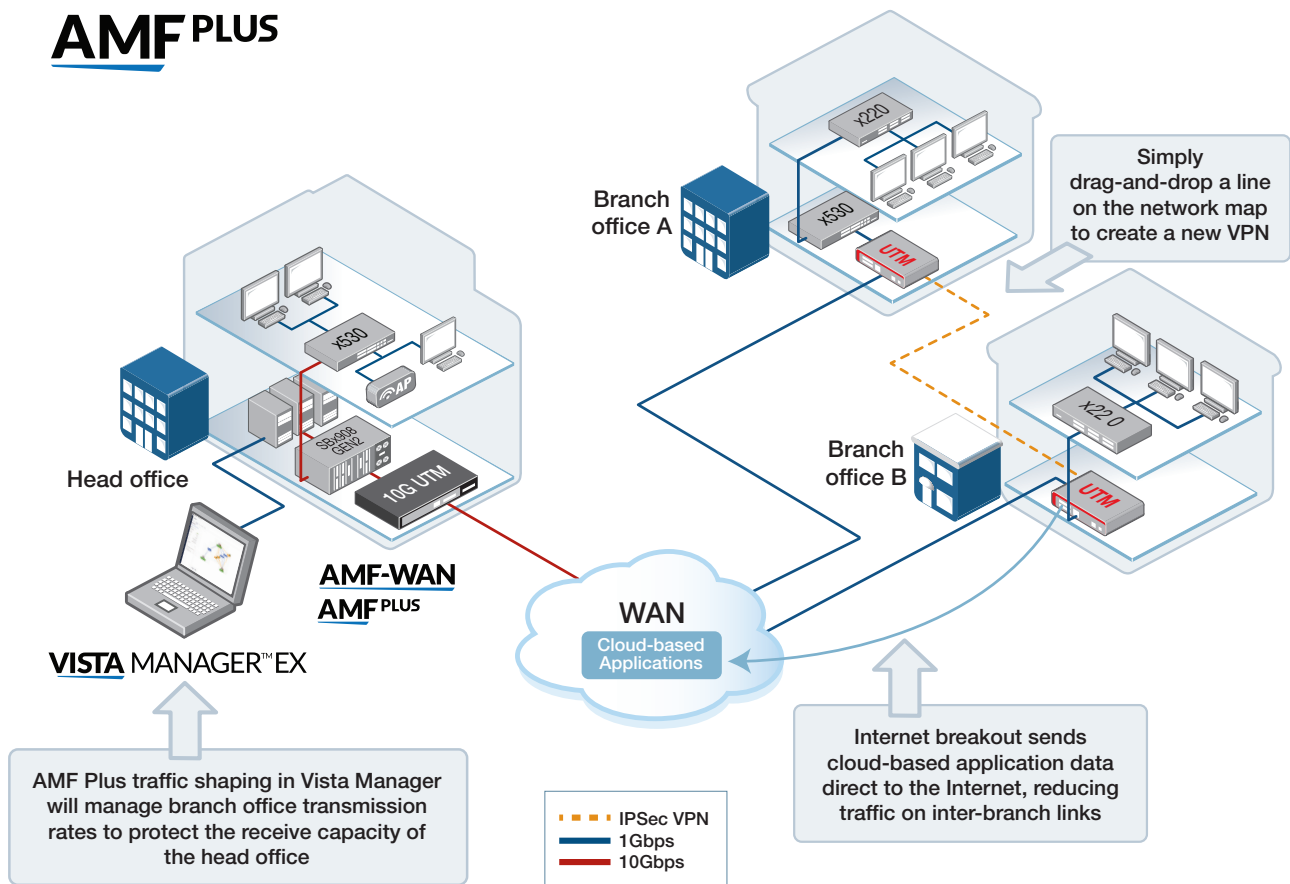
This solution shows a 10G UTM Firewall providing site-to-site IPSec VPN connectivity between the corporate office and branch offices, while also allowing secure SSL VPN access for remote workers, so they enjoy full access to digital company resources when away from the office.

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. 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.

Intent-based WAN Management with AMF Plus



AMF Plus enables intent-based WAN management

AMF Plus intent-based features are integrated into Vista Manager EX, our powerful network management and monitoring platform, for intuitive GUI driven management of business WAN infrastructure. This solution shows a 10G UTM Firewall providing VPN connectivity between the corporate office and branch offices.

AMF Plus provides effortless translation of business intent into dynamic network change to meet requirements, and make network management easy.

AMF Plus features enable:

- 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
- Managing traffic, and controlling the priority and performance of key applications right through the network, using centralized visual Quality of Service (QoS) administration
- Easily visualizing Access Control Lists (ACLs) in a matrix format to quickly and simply check for coverage inconsistencies, and ensure user data and different traffic types are managed in line with business policies

As well as easy WAN management, AMF Plus also provides:

- Health monitoring of key devices CPU, memory, storage, and temperature information. This allows visual at-a-glance network health status, trends, and simple fault resolution

FEATURES

Multiple firewall instances

- Multiple virtual firewall instances enable managing and securing different parts of the network independently
- Support for overlapping IP addressing if required
- Each firewall instance supports the comprehensive feature-set highlighted in the following feature sections

Firewall

- Deep Packet Inspection (DPI) application aware firewall (built-in or subscription 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)
- Web-Control uses subscription-based categories to manage user website access, with proxy-based and DPI options available
- Custom web control categories, match criteria and keyword blocking per entity
- Control network access and traffic regionally with GeoIP (Geographic IP)
- 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 Plus (AMF Plus) member
- AMF Plus secure mode increases network security with management traffic encryption, authorization, and monitoring
- From AW+ 5.5.2-2, an AMF Plus license operating in the network provides all standard AMF network management and automation features, and also enables the AMF Plus intent-based networking features in Vista Manager EX (from version 3.10.1 onwards)
- 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
- Backup and restore enables a snapshot of the current firewall to be saved. This can be used to configure a replacement device which can be deployed with plug-and-play simplicity if needed
- Simple Certificate Enrollment Protocol (SCEP) supports secure management

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

- Two-factor authentication using a code, certificates, or a one time password (OTP) via email for maximum security

Unified Threat Management (UTM)

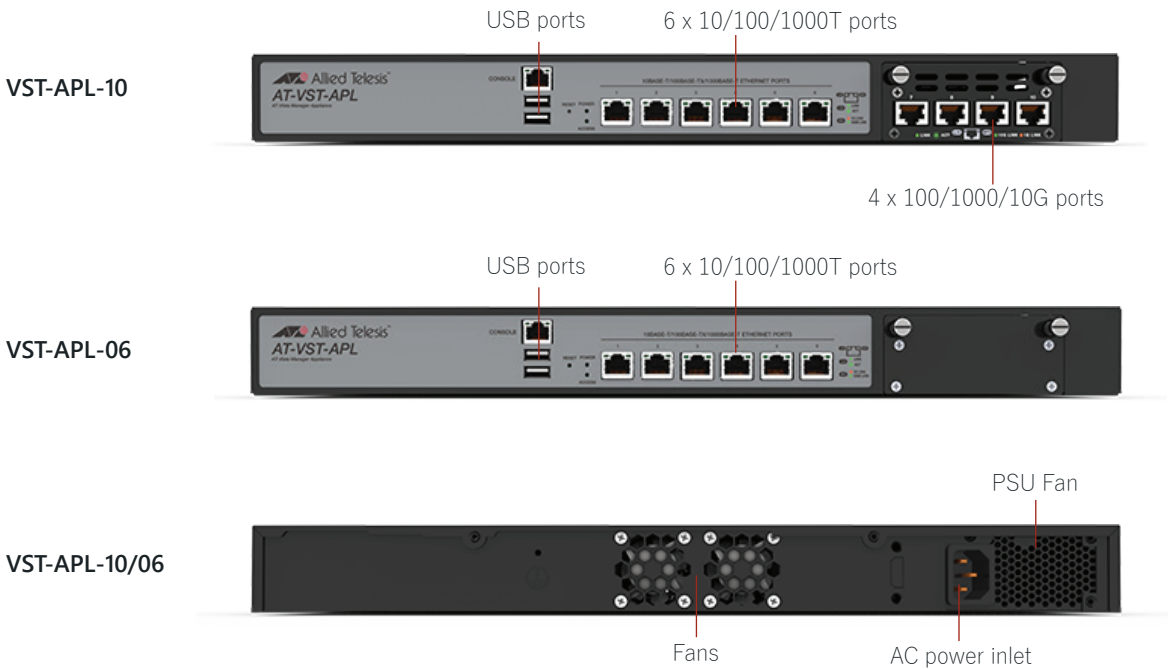
- Auto-update of UTM signature files
- Advanced IPS (Intrusion Prevention System) (subscription-based)
- IP Reputation protects against suspect websites (subscription-based)
- DoS and DDoS attack detection and protection
- URL access-control lists (block or allow HTTP and HTTPS access to specific Websites)
- Zone-based UTM

VPN Tunneling

- Diffie-Hellman key exchange (D-H groups 2, 5, 14, 15, 16, 18)
- Secure encryption algorithms: AES/AES-GCM and 3DES
- Secure authentication: SHA-1, SHA-256, SHA-512
- 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
- Two-factor authentication and LDAP authentication options ensure secure OpenVPN login
- IPv6 tunneling

UTM Firewall hardware

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



SPECIFICATIONS

UTM Firewall application (running on VST-APL)	
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 and malformed packets, blended threats and more
Security subscriptions	Next-Gen Firewall, Advanced Threat Protection
Tunneling and 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/AES-GCM (128, 192, 256 bit encryption)
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 and authentication	
Logging and notifications	Syslog (IPv4 and IPv6), SNMPv2c & v3
User interfaces	Web-based GUI, scriptable industry-standard CLI
Secure management	SSHv1/v2, strong passwords, SCEP
Management tools	Allied Telesis Autonomous Management Framework™ Plus (AMF Plus), Vista Manager EX
User authentication	RADIUS, TACACS+, internal user database
Command authorization	TACACS+ AAA (Authentication, Accounting and Authorization)

UTM FIREWALL APPLICATION (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 NAT, Double NAT, subnet-based NAT	
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
Product dimensions (W x D x H)	438 x 292 x 44 mm	438 x 292 x 44 mm
Unpackaged dimensions (W x D x H)	4.5 kg	4.9 kg
Packaged dimensions (W x D x H)	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

	Includes	1 Year subscription	3Year subscription	5 Year subscription
Advanced Firewall	Application Control Web Control	AT-AR4-UTM-01-1YR	AT-AR4-UTM-01-3YR	AT-AR4-UTM-01-5YR
Advanced Threat Protection	Advanced IPS IP Reputation	AT-AR4-UTM-02-1YR	AT-AR4-UTM-02-3YR	AT-AR4-UTM-02-5YR

ORDERING INFORMATION

AT-VST-APL-06¹	AT-Vista Manager Network Appliance with 6 x 10/100/1000T copper ports
AT-VST-APL-10¹	AT-Vista Manager Network Appliance with 6 x 10/100/1000T, and 4 x 100/1000T/10G copper ports
AT-FL-VFW-BASE¹	Firewall license to enable the UTM Firewall application on the AT-VST-APL-06 or AT-VST-APL-10 Vista Manager Network Appliance

¹ See the install guide for instructions on downloading and installing the AR4000S-Cloud software, and license to enable operation.