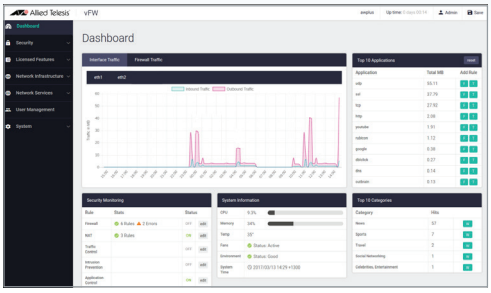
Advanced Virtual UTM Firewall

AR4000S-Cloud

Allied Telesis AR4000S-Cloud advanced virtual UTM firewall provides an ideal integrated security platform for businesses enabling cloud-first support for today's distributed work environments. Power inter-office SD-WAN connectivity, remote worker VPNs, and easy access to cloud-based applications, ensuring a high performance enterprise solution.



The AR4000S-Cloud virtual UTM firewall enables flexible deployment on your own local central office hardware, or fully cloud-based to meet today's fluid and flexible work environment. Best-of-breed security features provide up-to-the-minute threat protection, combined with an advanced firewall, SD-WAN inter-branch automation and optimization, and comprehensive networking capability.

Flexible performance

Choose the performance you need, by installing the virtual firewall on local server hardware to meet performance requirements - or alternately as Infrastructure as a Service (IaaS) in the cloud. This flexibility provides a high performing cost effective solution for security and distributed business WAN connectivity. See performance table for indicative values.

Cloud-based deployment

Support your distributed cloud-first environment by deploying the virtual UTM firewall on Amazon Web Services, Microsoft Azure, or Oracle Cloud IaaS platforms. Pay-as-you-go provides the ability to enjoy the performance you require today, and upgrade in the future.

Application-aware Firewall

The AR4000S-Cloud advanced virtual UTM firewall has 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)

The virtual firewall supports 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 virtual firewall runs the advanced AlliedWare Plus™ fully featured operating system, with an industry standard CLI.

The Device GUI provides an easy-to-use graphical interface with 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, provide a consistent approach to policy management.

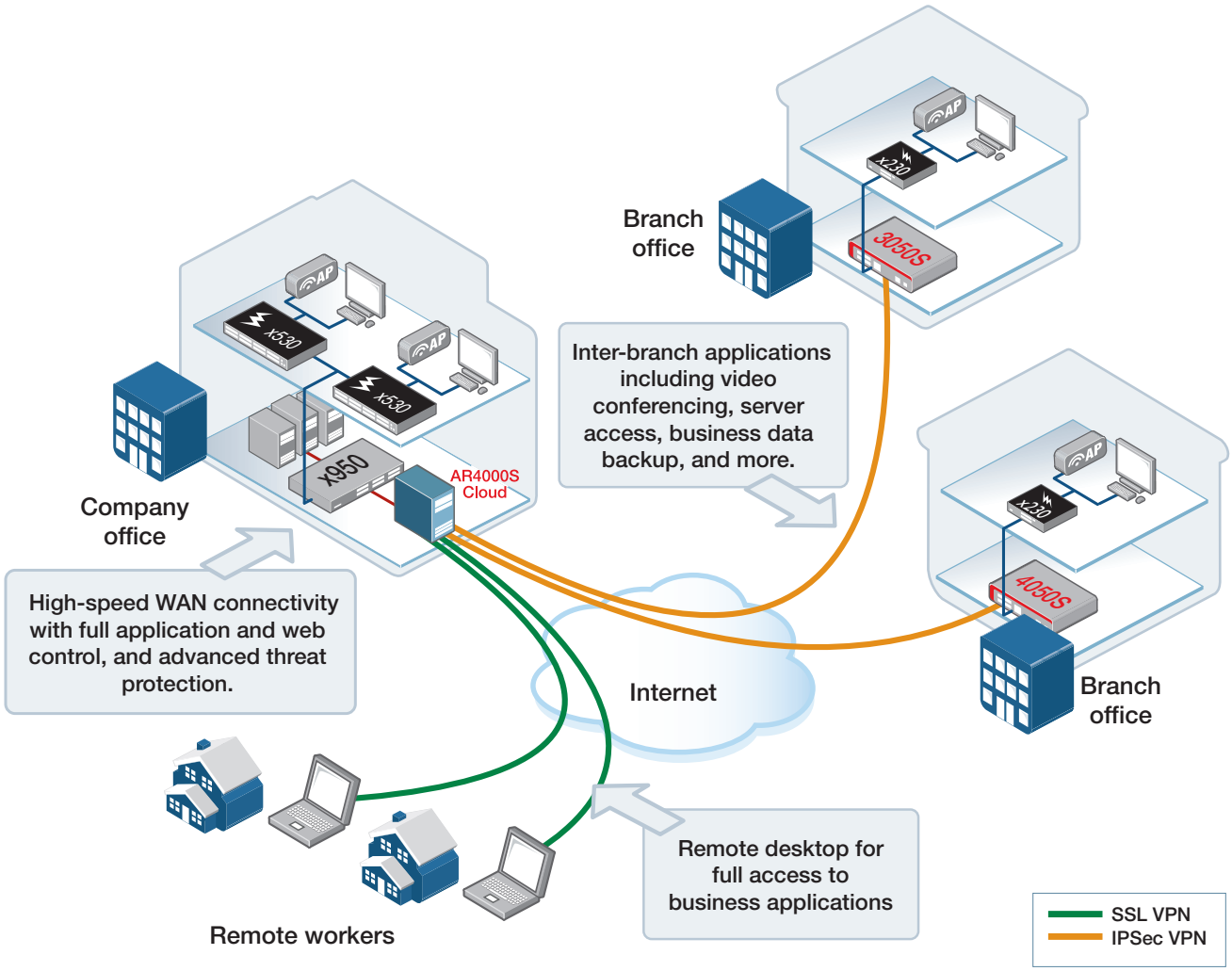
Performance

FEATURE	SERVER HARDWARE				
	vCPU	1	2	4	8
	MEMORY	4GB	8GB	16GB	32GB
Firewall throughput (Raw)		36 Gbps	80 Gbps	100 Gbps	108 Gbps
Firewall throughput (App Control)		3 Gbps	7 Gbps	18 Gbps	36 Gbps
Concurrent firewall sessions		300,000	1,000,000	1,000,000	1,000,000
Configurable firewall rules		3,000	5,000	5,000	5,000
Advanced Threat Protection throughput		3 Gbps	6 Gbps	12 Gbps	24 Gbps
VPN (IPSec) throughput		2 Gbps	4 Gbps	8 Gbps	16 Gbps
VPN (IPSec) connections		1,000	1,000	1,500	1,500

Note: All performance values are UDP maximums, and vary depending on system configuration.
Testing hardware: Dell PowerEdge R750xs with Intel® Xeon® Gold 6334 CPU (connected via an Intel E810-CQDA2 dual port QSFP28 100G adapter).

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 increased network 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	
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)	AMF-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 Prevention 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/TLSv1.3 for secure remote VPN 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.

Key Solution: 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 an AR4000S-Cloud advanced virtual UTM firewall installed on premise at the corporate head-office, providing site-to-site IPSec VPN connectivity to the 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.

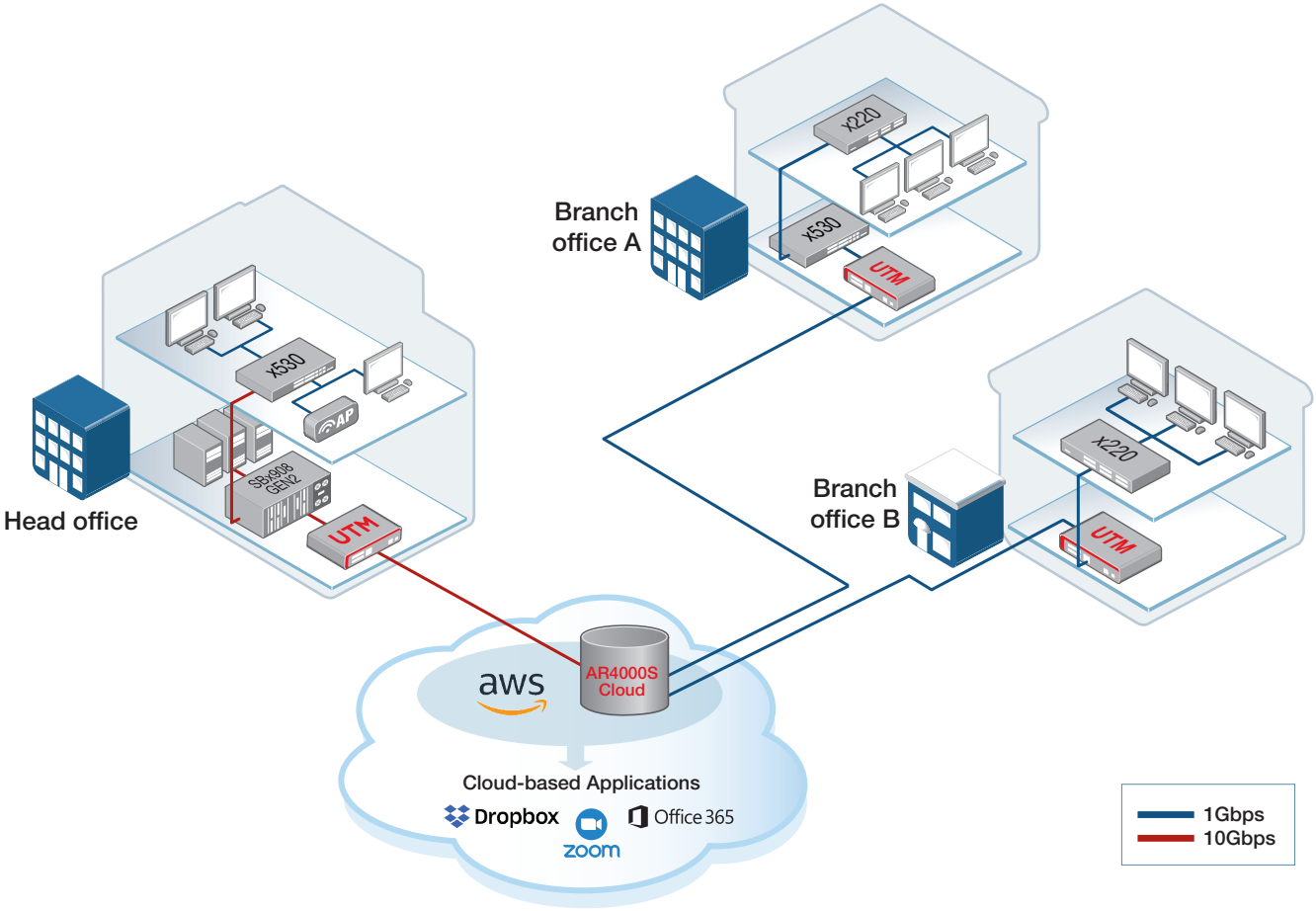
Flexible local performance

The AR4000S-Cloud allows fully flexible deployment either in the cloud or locally on premise. When deployed locally, businesses can utilize server hardware to meet their security and WAN connectivity performance requirements. Advanced automation and optimization features like SD-WAN can be used to maximize WAN connectivity and business operation.

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.

This powerful combination of features makes Allied Telesis advanced virtual UTM firewall an ideal one-stop integrated security platform for protecting today's online business activity.

Key Solution: Seamless cloud-first business operation



Cloud-first business security

Today's business relies on seamless access to online resources and applications for staff from any location at any time. With many SaaS (Software as a Service) applications hosted online, a cloud-first approach ensures that secure access to these important business tools supports smooth business operation.

In this solution, the AR4000S-Cloud advanced virtual UTM firewall is deployed on the Amazon Web Services IaaS (Infrastructure as a Service) platform. The flexibility of pay-as-you-go provides the ability to get the performance required today, and easily upgrade in the future.

Staff from all locations are assured of secure access to productivity and collaborative work cloud-based applications such as Office 365, Zoom, Dropbox and more. The virtual firewall provides centralized security and threat protection for the business ensuring a consistent approach to policy management for a secure online work environment.

The flexibility of a virtual firewall combined with local security appliances supports today's complex and distributed work situations, where working in different offices and locations and from home have become a common occurrence. Allied Telesis powerful and comprehensive LAN and WAN solutions provide seamless and essential operation for the modern enterprise.

Features

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 4 over 6, and MAP-E for connecting IPv4 networks over IPv6
- Dynamic routing (RIP, OSPF and BGP) for IPv4 and IPv6
- Flow-based Equal Cost Multi Path (ECMP) routing
- 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 SNMPv6, Telnetv6 and SSHv6
- Logging to IPv6 hosts with Syslog v6
- Web redirection allows service providers to direct users to a specified web address
- sFlow packet sampling for network monitoring
- Virtual Router Redundancy Protocol (VRRPv2/v3)

Management

- Allied Telesis Autonomous Management Framework Plus (AMF Plus) enables powerful centralized management and zero-touch device installation and recovery
- 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
- The wireless controller, built-in to the Device GUI, enables visual management and monitoring of a wireless network
- 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 SNMPv1/v2c/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

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
- RADIUS group selection
- TACACS+ Authentication, Accounting and Authorization (AAA)
- Local or server-based RADIUS user database
- 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 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)
- Redundant VPN gateway
- SSL/TLSv1.3 for secure remote VPN access using OpenVPN
- Two-factor authentication and LDAP authentication options ensure secure OpenVPN login
- IPv6 tunneling

Specifications

	AR4000S-CLOUD
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
Tunneling and encryption	
Site-to-site VPN tunnels (IPsec)	Dependant on hardware/cloud deployment
Client-to-site VPN tunnels (OpenVPN)	Dependant on hardware/cloud deployment
Encrypted VPN	IPsec, SHA-1, SHA-256, SHA-512, IKEv2, SSL/TLS VPN
Encryption	3DES, AES/AES-GCM (128, 192, 256 bit encryption), TLS-Crypt (OpenVPN)
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 & 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™ Plus (AMF Plus) member
User authentication	RADIUS, TACACS+, internal user database
Command authorization	TACACS+ AAA (Authentication, Accounting and Authorization)
Networking	
Routing (IPv4)	Static, Dynamic (BGP4, OSPF, RIPv1/v2), source-based routing, policy-based routing, SD-WAN
Routing (IPv6)	Static, Dynamic (BGP4+, OSPFv3, RIPng), policy-based routing, SD-WAN
Multicasting	IGMPv1/v2/v3, 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, Dynamic & Static ENAT, Double NAT, subnet-based NAT
VLANs	802.1Q tagging
Discovery	sFlow
Virtual Environment	
Microsoft Hyper-V	
Public Cloud	
Amazon Web Services	
Microsoft Azure	
Oracle Cloud	

Security Licenses

LICENSE NAME	INCLUDES	1 YR SUBSCRIPTION	3 YR SUBSCRIPTION	5 YR 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-AR4-VPN10S-xYR
AT-AR4-VPN10H-xYR

The VPN10S "Standard speed" base license supports deploying on local hardware or in the cloud with 1/2.5/5G interface connectivity.

The VPN10H "High speed" base license supports deploying on local hardware or in the cloud with 10/25/40/100G interface connectivity.

Both the VPN10S and VPN10H base licenses include VPN connectivity for 10 branch office locations, as well as advanced firewall and routing functionality.

AT-AR4-VPN10ADD-xYR
Purchase one VPN10ADD license per 10 extra VPN connections to branch office locations.

Where x = 1 for a one year subscription
5 for a five year subscription

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

Related Products

AT-VISTA Manager EX
Unified network management and monitoring platform supporting wired, wireless, and third-party devices across the LAN and WAN.

AT-VST-APL-10
Network Appliance based firewall with 6 x 10/100/1000T, and 4 x 100/1000T/10G copper ports

AT-VST-APL-06
Network Appliance based firewall with 6 x 10/100/1000T copper ports

AT-ARX200S-GTX
UTM Firewall with 1 x 1/2.5/5/10G WAN, 2 x 1/2.5/5/10G LAN, and 2 x 10/100/1000 LAN ports

AT-ARX200-GT
UTM Firewall with 1 x 10/100/1000 WAN, and 4 x 10/100/1000 LAN ports

AT-AR4050S-5G
UTM Firewall with 2 x GE WAN and 8 x 10/100/1000 LAN ports, and dual SIM slots for 5G mobile broadband access

AT-AR4050S
UTM Firewall with 2 x GE WAN and 8 x 10/100/1000 LAN ports

AT-AR3050S
UTM Firewall with 2 x GE WAN and 8 x 10/100/1000 LAN ports

AT-AR1050V
Secure VPN Router with 1 x GE WAN and 4 x 10/100/1000 LAN ports

AT-TQ7403-R
Enterprise-Class Wi-Fi 6E Wireless AP Router with 3 radios (2x2 2.4GHZ and 2x2 5GHz and 2x2 6GHz), an embedded and external antenna, and 2 multi-gigabit Ethernet ports

AT-TQ6702 GEN2-R
Enterprise-Class Wi-Fi 6 Wireless AP Router with 2 wireless radios (4x4 2.4GHZ and 8x8 5GHz), an embedded antenna, and 2 multi-gigabit Ethernet ports

617-000706 RevJ