Secure 1G Branch Office Firewall

ARX200s-GT

Allied Telesis ARX firewalls are the ideal choice for businesses, requiring Unified Threat Management (UTM) and secure WAN connectivity. For the branch office, a powerful 1G firewall and threat protection is combined with routing and switching, comprehensive VPN support, and SD-WAN capability to provide an innovative high performance business solution.

Overview

The ARX200S-GT is the ideal choice for 1G WAN performance at the branch office to enable cloud-first support for today's distributed work environments. The advanced UTM firewall features an integrated "best of breed" security platform to provide up-to-the-minute threat protection, an application-aware firewall, SD-WAN inter-branch automation and optimization, and remote worker VPNs. A fanless design provides silent operation and enables flexible deployment to support modern WAN solutions.

High performance with flexible connectivity

High performance is guaranteed by harnessing the power of multi-core processors and application wacceleration engines, with 1G WAN and LAN ports.

	ARX200S-GT
Firewall Throughput	2Gbps
Firewall Concurrent Sessions	600,000
VPN Throughput (AES-GCM)	1Gbps
VPN Throughput (AES256/SHA256)	1Gbps
UTM Throughput (Application Control/Web Control)[1]	1.2Gbps

Note:
Actual values may vary considerably depending on network environment.

[1] UTM features require a license. See security licenses table on page 7.

Application-aware Firewall

The 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 (VPNs)

Allied Telesis UTM Firewalls support IPsec site-to-site VPNs 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, provide a consistent approach to policy management.

Device and network management

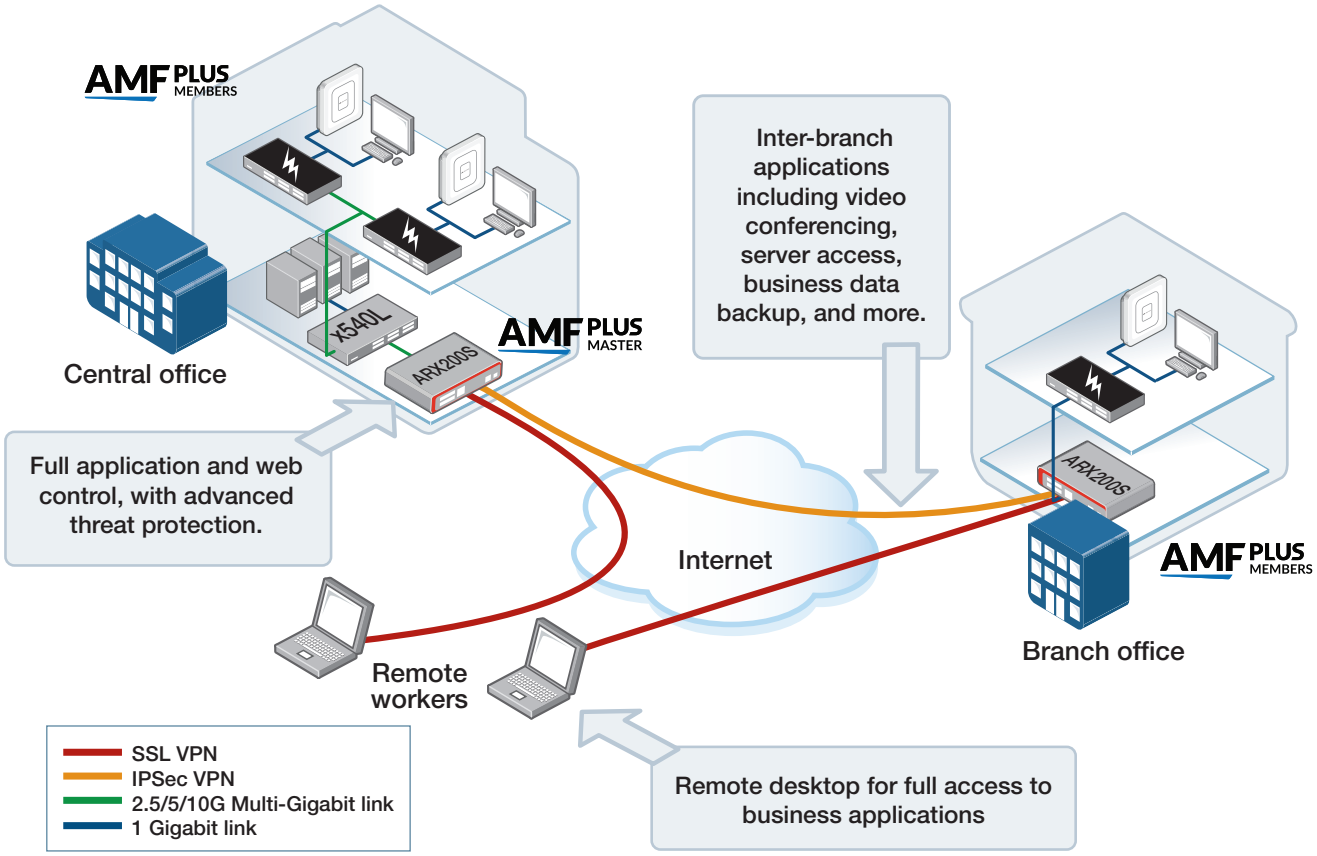
The Device GUI on the ARX200S-GT enables graphical monitoring of key firewall features to support easy management.

Integrated into the Device GUI, the wireless controller supports visibility and management of AWC wireless network devices, making it ideal as a one-stop solution for small to medium-sized networks.

AWC automatically maintains optimal wireless coverage, and the wireless controller includes floor and heat maps showing wireless coverage.

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	
VRF-Lite	Virtual Routing and Forwarding (VRF-Lite) allows multiple routing tables. As the routing instances are independent, the same or overlapping IPv4 addresses can be used. The built-in DHCP Server on the firewall is VRF aware, enabling the supply of IP addresses to clients across multiple isolated networks.
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.
WAN connectivity	By default the ARX200S-GT has a single gigabit WAN port. A gigabit LAN switch port can be configured as a second WAN port if dual Service Provider connections are desired for resiliency and higher performance.
AMF-WAN (Allied Telesis SD-WAN)	AMF-WAN measures WAN link quality and sends real-time and other applications over the most suitable inter-branch connection. Users can load-balance an application over multiple WAN links and prioritize the delivery of business-critical applications. Internet breakout sends cloud-based applications like Office 365 directly from the branch to the Internet, reducing inter-branch VPN traffic load and increasing performance.
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.
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



Intgrated protection and secure remote access

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

This solution shows a 1G ARX200S-GT UTM firewall at the branch office, and a 10G ARX200S-GTX UTM firewall at the central office with site-to-site IPSec VPN connectivity. SSL VPN access for remote workers enables them to 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. 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.

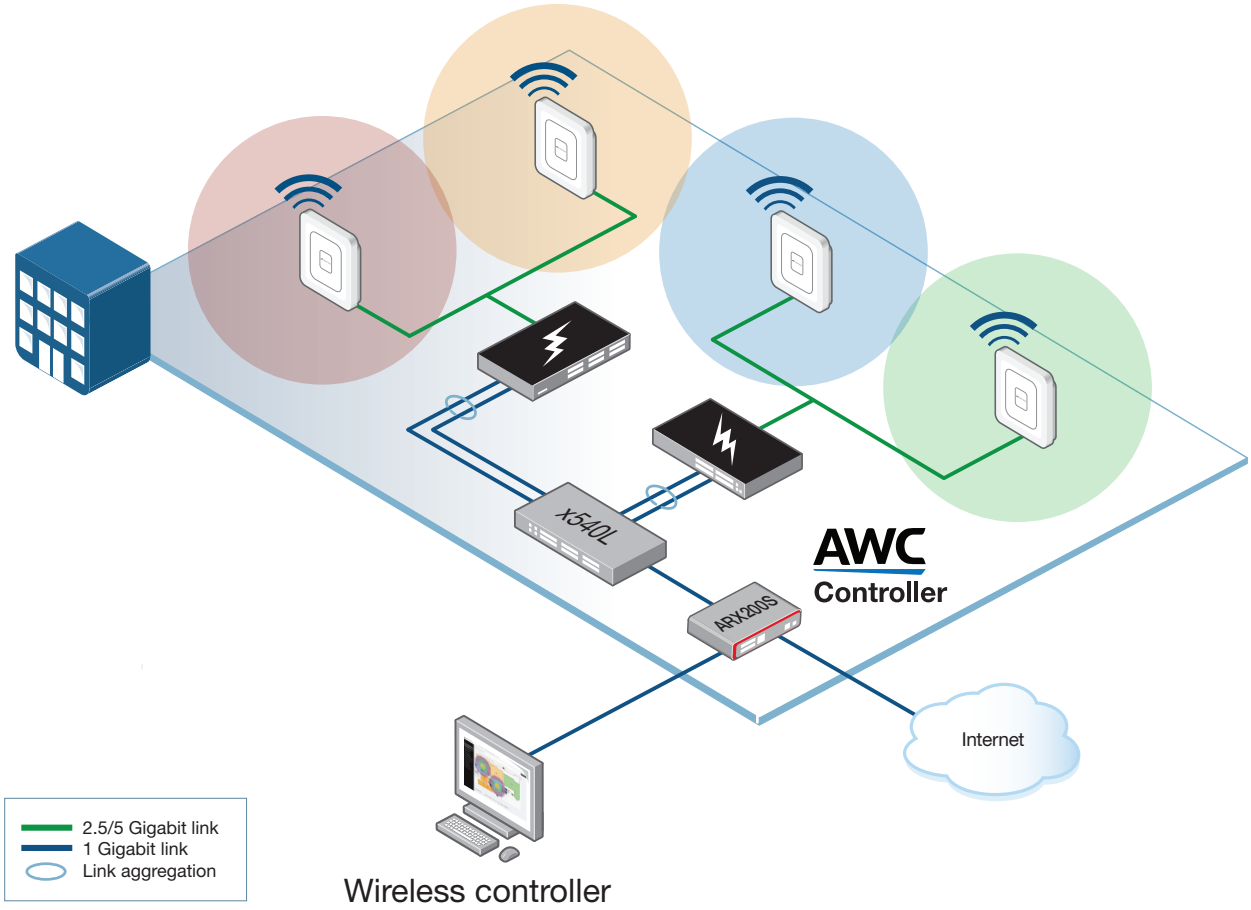
Automated network management

In addition to protecting and connecting modern networks, the firewalls are fully supported by Allied Telesis AMF Plus.

AMF Plus is a sophisticated suite of management tools that automate and simplify many day-to-day network administration tasks. Powerful features like centralized management, auto-backup, auto-upgrade, auto-provisioning and auto-recovery ensure streamlined networking. Growing the network can be accomplished with plug-and-play simplicity, and network node recovery is fully zero-touch.

The ARX200S-GT can operate as an AMF Plus member enjoying the full benefits of powerful management and automation.

Integrated Wireless Network Management



Autonomous Wireless LAN solution

Allied Telesis AWC offers solutions for two of the most common problems with Wireless LANs: initial setup complexity and on-going performance degradation.

Initial WLAN set-up usually requires a site survey to achieve the best coverage, and performance of WLANs can often change over time as external sources of radio interference reduce coverage and bandwidth. These issues can be time consuming to identify and resolve.

The auto-setup option simplifies wireless deployment by creating wireless profiles and associating discovered Access Points (APs) with them automatically, while AWC features an intelligent process that automatically recalibrates the signal strength and radio channel of each AP for optimal WLAN performance.

When AWC is combined with the firewall functionality in the ARX200S-GT, it becomes an ideal solution for branch offices and small businesses to both protect and manage the office network. AWC is an essential tool for busy network administrators to save time and money when deploying and managing WLANs.

The wireless controller is integrated into the Device GUI of the ARX200S-GT and provides an ideal solution for modern networks, enabling management of both the wired (with AMF) and wireless (with AWC) networks to be automated. This reduces both the time and cost of network administration, as well as maximizing network performance for a superior user experience.

Up to 10 TQ Series wireless APs can be managed for free.

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 categorization (Opentext)
- 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

- A gigabit LAN switch port can be configured as a second WAN port for resiliency and higher performance
- 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)
- Virtual Routing and Forwarding (VRF-Lite)
- Traffic control for bandwidth shaping and congestion avoidance
- Policy-based routing
- SD-WAN: performance measure and load balance WAN links
- PPPoE client with PADT support
- DHCP client, relay and server for IPv4 and IPv6
- Dynamic DNS client
- IPv4 and IPv6 dual stack
- Device management over IPv6 networks with SNMP, Telnet and SSH
- Logging to IPv6 hosts with Syslog v6
- Web redirection allows service providers to direct users to a specified web address
- LLDP and LLDP-MED for network discovery
- sFlow packet sampling for network monitoring

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
- 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 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
- USB interface allows software release files, configurations and other files to be stored for backup and distribution to other devices.
- Simple Certificate Enrollment Protocol (SCEP) supports secure management

Diagnostic Tools

- Automatic link flap detection and port shutdown
- Ping polling for IPv4 and IPv6
- Port mirroring
- 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 per VLAN or port
- TACACS+ Authentication, Accounting and Authorization (AAA)
- Local or server-based RADIUS user database
- Strong password security and encryption
- RADIUS CoA (Change of Authorization)
- MAC and 802.1x Port authentication on switch ports
- Web Authentication
- 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
- DoS and DDoS attack detection and protection
- URL blacklists and whitelists (block or allow HTTP and HTTPS access to specific Websites)
- Zone-based UTM

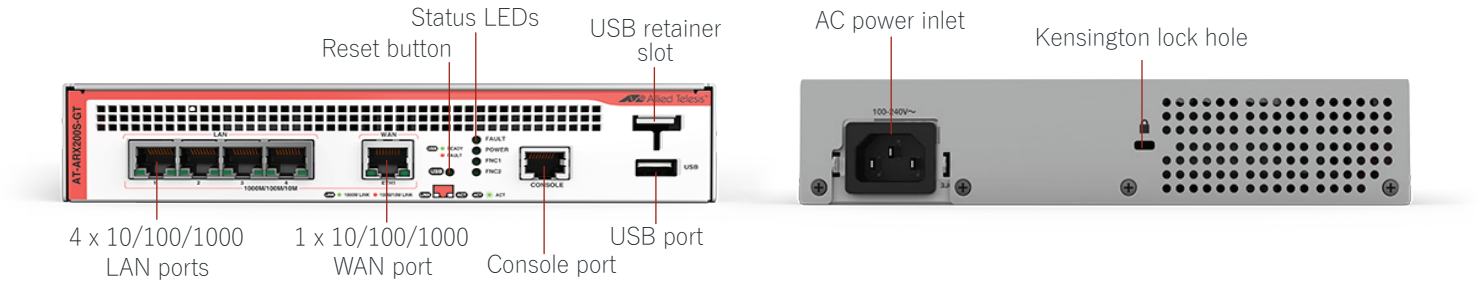
VPN Tunneling

- Diffie-Hellman key exchange (D-H groups 2, 5, 14, 15, 16, 18)
- Secure encryption algorithms: AES 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/TLS VPN for secure remote access using OpenVPN
- Two-factor authentication and LDAP authentication options ensure secure OpenVPN login
- IPv6 tunneling

Wireless Controller AWC

- Allied Telesis AWC is an intelligent WLAN controller that automatically maintains optimal wireless coverage
- Up to ten access points (APs) can be managed for free
- Auto-setup simplifies wireless network deployment
- Rogue AP detection for increased WLAN security
- WEP/WPA personal or WPA enterprise, pre-shared key (WEP/WPA personal), RADIUS server (WPA enterprise)
- Wireless networks can have separate SSIDs, VLANs, security settings, etc.
- APs can belong to multiple networks each with different wireless settings, and can broadcast multiple SSIDs (Virtual AP)
- APs can be defined individually or in bulk using a common profile
- AP radio settings can be configured automatically (default) or manually
- AP functions such as updating firmware, executing AWC calculations and applying calculation results can be run automatically based on a user-defined schedule
- AWC supports Allied Telesis TQ Series wireless access points

ARX200S-GT



SPECIFICATIONS

Processor and memory	
Security processor	1.6GHz 4-core
Memory (RAM)	2GB
Memory (Flash)	4GB
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	Advanced Firewall
Tunneling and encryption	
Site-to-site VPN tunnels (IPsec)	500
Client-to-site VPN tunnels (OpenVPN)	500
Encrypted VPN	IPsec, SHA-1, SHA-256, SHA-512, IKEv2, SSL/TLS VPN
Encryption	3DES, AES-128, AES-192, AES-256, AES-GCM, TLS-Crypt(OpenVPN)
Key exchange	Diffie-Hellman groups 5, 14, 16
Dynamic routed VPN	RIP, OSPF, BGP, RIPng, OSPFv3, BGP4+
Point to point	Static PPP, L2TPv2 virtual tunnels, 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, NETCONF/RESTCONF
Secure management	SSHv1/v2, strong passwords, SCEP
Management tools	Allied Telesis Autonomous Management Framework™ Plus (AMF Plus) Autonomous Wave Control for wireless LAN APs (AWC), Vista Manager EX
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, VRF-Lite, SD-WAN
Routing (IPv6)	Static, Dynamic (BGP4+, OSPFv3, RIPng), policy-based routing, SD-WAN
Multicasting	IGMPv1/v2/v3, PIM-SM, PIM-DM, PIM-SSM, PIMv6
High availability	VRRP, VRRPv3
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
Link aggregation	802.3ad static and dynamic (LACP)
VLANs	802.1Q tagging
Discovery	LLDP, LLDP-MED, sFlow

Reliability features	
	Modular AlliedWare Plus operating system. Full environmental monitoring of PSU, fan, temperature and internal voltages. SNMP traps alert network managers in case of any failure. Variable fan speed control
Hardware characteristics	
Input power	90V to 264V AC (47 to 63HZ)
Max power consumption	17W
LAN ports[2]	4 x 10/100/1000T RJ-45
WAN port	1 x 10/100/1000T RJ-45
Other ports	1 x USB port (3.0), 1 x RJ-45 console port
Product dimensions (W x D x H)	210 mm (8.26 in) x 220 mm (8.66 in) x 42.5 mm (1.67 in)
Packaged dimensions (W x D x H)	560 mm (22.04 in) x 331 mm (13.03 in) x 321 mm (12.63 in)
Product weight	1.4 kg
Typical / Max noise	Fanless/Silent Operation
Environmental specifications	
Operating temperature range	0°C to 50°C (32°F to 122°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	Up to 3000 meters (9,843 ft)
Regulations and compliances	
EMC	CISPR 32 class A, EN55032 class A, FCC class A, VCCI class A, ICES class A, UKCA class A
Immunity	EN55035
Safety Standards	UL 62368-1, IEC 62368-1, EN 62368-1
Safety Certifications	UL, TuV
Reduction of Hazardous Substances (RoHS)	EU RoHS10 compliant, China RoHS compliant

[2] A LAN switch port can be configured as a second WAN port for resilience and higher performance

Security Licenses

	Description	Includes
AT-ARX2-UTM-01-1YR	Advanced Firewall license (1 year)	■ Application Control (Sandvine) ■ Web Control (Opentext)
AT-ARX2-UTM-01-5YR	Advanced Firewall license (5 years)	■ Application Control (Sandvine) ■ Web Control (Opentext)

ORDERING INFORMATION

AT-ARX200S-GT-xx	1 x 10/100/1000 WAN, 4 x 10/100/1000 LAN

Where xx = 10 for US power cord
30 for UK power cord
40 for Australian power cord
50 for European power cord

AT-RKMT-J15	Rack mount kit to install two devices side by side in a 19-inch equipment rack[3]
AT-RKMT-J14	Rack mount kit to install one device in a 19-inch equipment rack
AT-BRKT-J24	Wall mount kit for AT-ARX200S
AT-STND-J03	Stand-kit for AT-ARX200S
AT-VT-Kit3	USB console Cable

[3] Requires 1.5U height space in the rack