UTM Firewalls

AR3050S and AR4050S

Allied Telesis Unified Threat Management (UTM) Firewalls are the ideal integrated security platform for modern businesses. Powerful firewall and threat protection is combined with routing and switching, to provide an innovative high performance solution.

The AR3050S and AR4050S are the ideal choice for high speed Enterprise gateway applications. The UTM Firewalls feature an integrated "best of breed" security platform to provide up-to-the-minute threat protection with advanced networking capabilities, and the AR4050S is ICSA corporate firewall certified.

High performance

High performance is guaranteed by harnessing the power of multi-core processors and application acceleration engines, as well as the ability to offload[1] security and threat protection feature processing for increased throughput.

	AT-AR3050S	AT-AR4050S
Firewall throughput (Raw)	750 Mbps	1,900 Mbps
Firewall throughput (App Control)	700 Mbps	1,800 Mbps
Concurrent sessions	100,000	300,000
New sessions per second	3,600	12,000
IPS throughput	220 Mbps	750 Mbps
IP Reputation throughput	350 Mbps	1,000 Mbps
Malware protection throughput	300 Mbps	1,300 Mbps
VPN throughput	400 Mbps	1,000 Mbps

Note: All performance values are 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 Firewall 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[1]. The AMF-Security mini license[1, 2] enables our state-of-the-art integrated solution that automatically protects the LAN from internal security threats. All other security features are included in the base feature set.

The Allied Telesis Autonomous Management Framework™ (AMF) and AWC licenses[1] enable automated management of wired and wireless network nodes, while the UTM Offload license[1] supports increased WAN connection throughput.

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 (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.

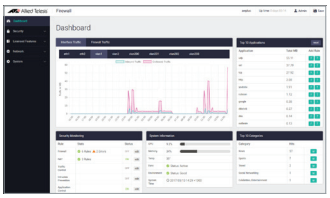
Remote workers can utilize an SSL VPN connection to encrypt their business data over the Internet, allowing them to utilize all their business resources when working from home, travelling, or otherwise away from the company premises.

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, provide a consistent approach to policy management.

Device and network management

The Device GUI on the AR4050S enables graphical monitoring of key switch features to support easy management.



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

AWC is an intelligent, easy to use Wireless LAN controller that automatically maintains optimal wireless coverage. Vista Manager mini includes AWC floor and heat maps showing wireless coverage. It also supports AWC Channel Blanket hybrid operation, providing maximum performance and seamless roaming, as well as AWC Smart Connect for simplified deployment, and a resilient Wi-Fi network solution using wireless uplink connectivity.

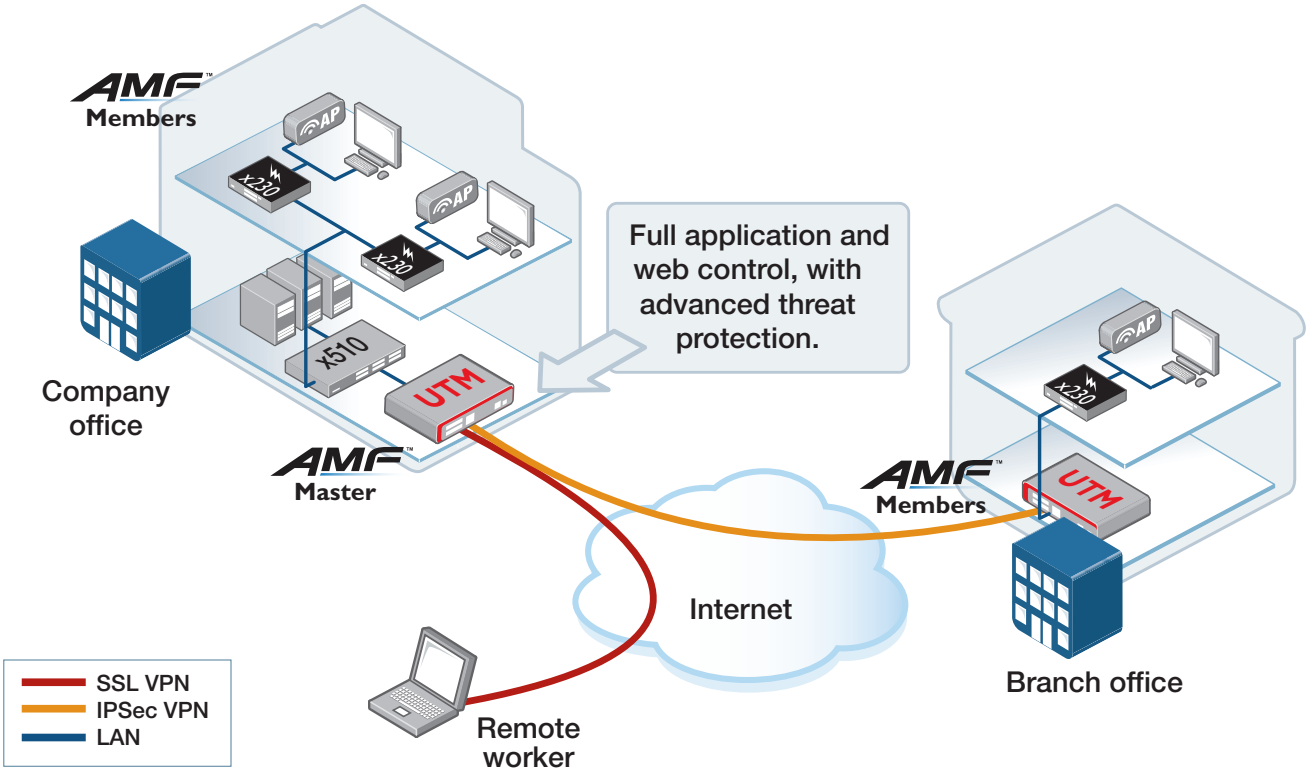
AMF Security (AMF-Sec) enables automatic protection from internal threats, to protect the LAN from malware by quarantining any suspect devices.

[1] Only available on the AR4050S
[2] The AMF-Sec license can not be used in conjunction with either the Advanced Firewall, or Advanced Threat Protection licenses

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 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™ 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	
VRF-Lite	Virtual Routing and Forwarding (VRF-Lite) allows multiple routing tables. As the routing instances are independant, the same or overlapping IPv4 addresses can be used.
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.
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, as well as send specific applications to different remote-site or Internet-based destinations.
UTM Offload	UTM Offload (AR4050S only) enables some security and threat protection features (IPS, IP-Reputation, Malware-Protection, and URL Filtering) to be offloaded to a secondary physical or virtual machine that is automatically managed by the AR4050S. UTM Offload can up to double WAN connection throughput when using these features for real-time threat protection, or in conjunction with Firewall, NAT, and Application Control to manage business application use.* *Note: it is recommended not to use UTM Offload when using the proxy-based Web-Control or Antivirus features.
3G/4G/LTE USB modem[3]	A 3G/4G/LTE USB modem offers an additional secure IPv4 or IPv6 data connection for critical services that can automatically switch to a mobile network whenever a primary data connection becomes unavailable.
RESILIENCY	
High availability bypass ports	Bypass ports allow a backup link to be formed to another device to act as a passive backup. In the event of a power failure, the WAN traffic is immediately transmitted to the backup device for an automatic failover of the WAN connection.
VRRP triggers for bypass port failover	The Allied Telesis UTM Firewalls support event-based triggers to automatically change VRRP mastership if a bypass port is activated. This simplifies WAN failover and reduces disruption to other network devices.
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™ 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	Users simply utilize the OpenVPN® client on their computer, tablet or other mobile device for easy access email, files, and other corporate digital resources when away from the office.
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.

[3] For a list of supported USB modems, please refer to the Allied Telesis USB Modem Compatibility List

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 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 UTM Firewall providing site-to-site IPSec VPN connectivity between corporate 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.

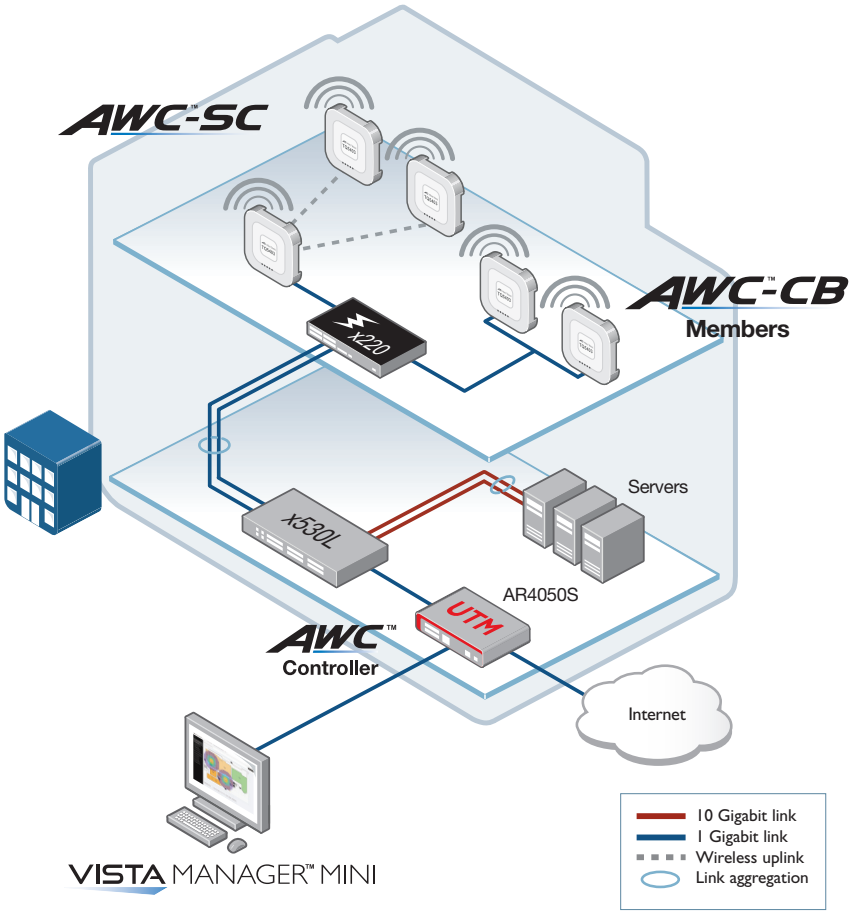
Automated network management

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

AMF 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 AR4050S can operate as the AMF network master, storing firmware and configuration backups for up to 20 other network nodes.

Key Solution: 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 re-calibrates the signal strength and radio channel of each AP for optimal WLAN performance.

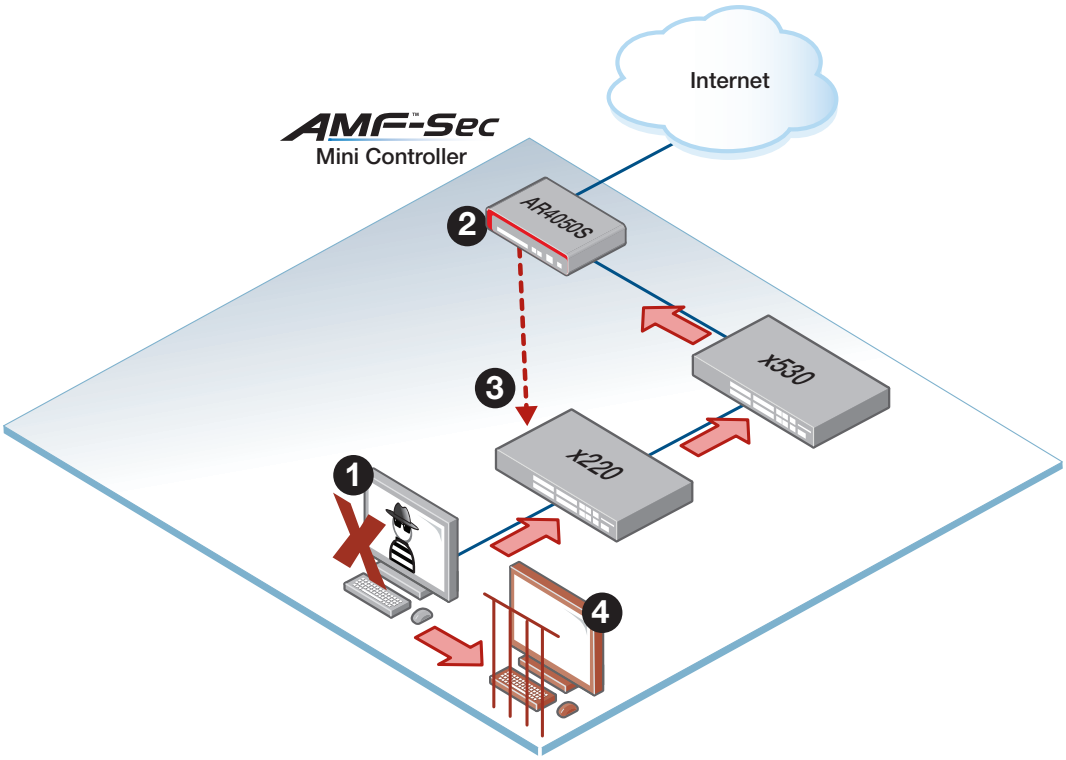
When AWC is combined with the firewall functionality in the AR4050S, it becomes an ideal solution for branch offices and small businesses to both protect and manage the office network. AWC is an essential tool for busy network administrators to save time and money when deploying and managing WLANs.

Vista Manager mini is integrated into the Device GUI of the AR4050S 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.

On some AP models, hybrid Channel Blanket enables multichannel and single-channel Wi-Fi operation simultaneously, which supports seamless roaming and maximum throughput. AWC Smart Connect uses wireless uplink connections between APs, so deployment is as easy as plugging in and powering on the new APs, which automatically extend the Wi-Fi network, creating a resilient solution.

Up to 5 TQ Series wireless APs can be managed for free, and up to a further 20 APs (max 25) with a feature license. Channel Blanket licenses are available for up to 5 APs. For plug-and-play wireless deployment Smart Connect licenses are available for up to 5 APs.

Key Solution: Automated Internal LAN Security



1. Targeted attack inside the network! Malware threat information is seen upline
2. AR4050S UTM Firewall passes threat notification to its integrated AMF-Sec mini security controller
3. AMF-Sec mini security controller instructs the x220 Series switch to block the threat source
4. Infected device is sent to quarantine to automatically stop the spread of infection

AMF Security mini

Most threat protection solutions are only capable of blocking suspicious external traffic arriving at the firewall from the Internet, so only those external threats can be detected and blocked—this is the traditional "secure border" model.

However, the AMF-Sec mini security controller integrated with the AR4050S UTM firewall can isolate traffic anywhere in the network, automatically blocking threats such as targeted attacks, or malware introduced inadvertently by staff with USB flash drives, BYOD and so on.

AMF Sec mini enables automatic protection from internal threats, to protect the LAN from malware by quarantining any suspect devices. Get easy and immediate edge security, so you can relax and enjoy your self-defending network.

AMF-Sec mini licenses for 1 year or 5 years are available for the AR4050S UTM firewall. Note that the AMF-Sec mini license cannot be used in conjunction with the Advanced Firewall or Advanced Threat protection licenses.

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 LAN and WAN interfaces
- 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
- ICSA corporate firewall certification (AR4050S only)

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
- 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
- UTM Offload improves WAN throughput when using multiple security features together, or when higher performance is required
- 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 SNMPv6, Telnetv6 and SSHv6
- Logging to IPv6 hosts with Syslog v6
- Web redirection allows service providers to direct users to a specified web address
- URL-offload enables cloud-based traffic (e.g. Office 365) to be sent directly to the Internet
- LLDP and LLDP-MED for network discovery

Management

- Allied Telesis Autonomous Management Framework (AMF) enables powerful centralized management and zero-touch device installation and recovery
- AMF secure mode increases network security with management traffic encryption, authorization, and monitoring
- Try AMF for free with the built-in AMF starter license (AR4050S only)
- Web-based Device GUI for firewall configuration and easy monitoring
- Vista Manager mini, 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 and SD/SDHC memory card socket allow software release files, configurations and other files to be stored for backup and distribution to other devices

AMF Security mini

- The built-in AMF-Sec mini security controller manages internal LAN protection
- Any internal security threats like malware are automatically blocked from spreading, and suspect network devices quarantined
- AMF-Sec mini enables a self-defending network solution

Resiliency

- High availability bypass ports
- Policy-based storm protection
- Spanning Tree (STP, RSTP, MSTP) with root guard
- Virtual Router Redundancy Protocol (VRRPv2/v3)

Diagnostic Tools

- Active Fiber Monitoring detects tampering on optical links
- Automatic link flap detection and port shutdown
- Optical Digital Diagnostic Monitoring (DDM)
- 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
- TACACS+ Authentication, Accounting and Authorization (AAA)
- Local or server-based RADIUS user database
- RADIUS group selection per VLAN or port
- Strong password security and encryption
- MAC and 802.1x Port authentication on switch ports

Unified Threat Management (UTM)

- Proxy-based anti-virus scanning (AR4050S only)
- No file size limitations
- 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

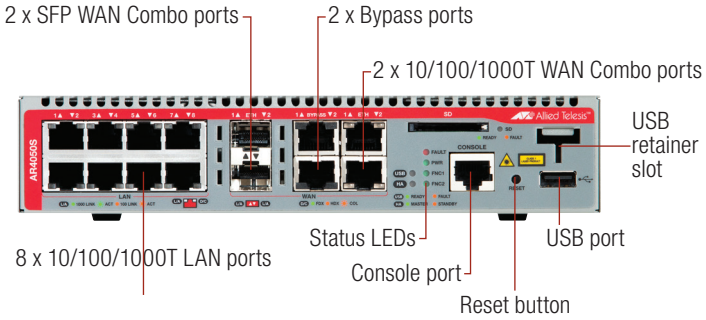
- Diffie-Hellman key exchange (D-H groups 5, 14, 16)
- Secure encryption algorithms: AES and 3DES
- Secure authentication: SHA-1 and SHA-256
- IKEv1 and IKEv2 key management
- IPsec Dead Peer Detection (DPD)
- IPsec NAT traversal
- IPsec VPN for site-to-site connectivity
- Multipoint VPN for connecting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

Wireless Controller AWC

- Allied Telesis AWC is an intelligent WLAN controller that automatically maintains optimal wireless coverage

- Up to five access points (APs) can be managed for free, with an additional 20 available via a separate software license (AR4050S only)
- 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
- AWC Channel Blanket hybrid operation provides maximum performance and seamless roaming
- AWC Smart Connect enables simplified deployment, and a resilient Wi-Fi network solution using wireless uplink connectivity

AR4050S



Specifications

	AR3050S	AR4050S
Processor and memory		
Security processor	800MHz dual-core	1.5GHz quad-core
Memory (RAM)	1GB	2GB
Memory (Flash)	4GB	4GB
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)	50	1,000
Client-to-site VPN tunnels (OpenVPN)	100	1,000
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 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 & authentication		
Logging & notifications	Syslog & Syslog v6, SNMPv2 & v3	
User interfaces	Web-based GUI, scriptable industry-standard CLI	
Secure management	SSHv1/v2, strong passwords	
Management tools	Allied Telesis Autonomous Management Framework™ (AMF) Autonomous Wave Control for wireless LAN APs (AWC) Vista Manager EX, AMF-Security mini	
User authentication	RADIUS, TACACS+, internal user database, web authentication, MAC authentication, 802.1x port authentication	
Command authorization	TACACS+ AAA (Authentication, Accounting and Authorization)	

	AR3050S	AR4050S
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	
Resiliency	STP, RSTP, MSTP	
High availability	VRRP, VRRPv3, hardware controlled bypass ports	
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	
Link aggregation	802.3ad static and dynamic (LACP)	
VLANs	802.1Q tagging	
Discovery	LLDP, LLDP-MED	
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	90 to 260V AC (auto-ranging), 47 to 63Hz	
Max power consumption	23W	27W
LAN ports	8 x 10/100/1000T RJ-45	
WAN ports	2 x 1000X SFP / 2 x 10/100/1000T RJ-45 combo	
High Availability bypass ports	2 x 10/100/1000T RJ-45	
Other ports	1 x USB, 1 x RJ-45 console, 1 x SDHC slot	
Product dimensions (H x W x D)	42.5 mm (1.67 in) x 210 mm (8.26 in) x 220 mm (8.66 in)	
Packaged dimensions (H x W x D)	36.5 cm (14.37 in) x 26 cm (10.24 in) x 11.5 cm (4.53 in)	
Product weight	1.7 kg unpackaged, 2.6 kg packaged	
Typical / Max noise	28.4 dBA / 35.1 dBA	
Environmental specifications		
Operating temperature range	0°C to 50°C (32°F to 122°F). Derated by 1°C per 305 meters (1,000 ft)	
Storage temperature range	-20°C to 60°C (-4°F to 140°F)	
Operating relative humidity range	5% to 80% non-condensing	
Storage relative humidity range	5% to 95% non-condensing	
Operating altitude	2,000 meters maximum (6,600 ft)	
Regulations and compliances		
EMC	EN55032 class A, FCC class A, VCCI class A	
Immunity	EN55024, EN61000-3-levels 2 (Harmonics), and 3 (Flicker)	
Safety Standards	UL60950-1, CAN/CSA-C22.2 No. 60950-1-03, EN60950-1, EN60825-1, AS/NZS 60950.1	
Safety Certifications	UL, cUL, TuV	
Reduction of Hazardous Substances (RoHS)	EU RoHS6 compliant, China RoHS compliant	
IPv6 Ready	Phase 2 (Gold) Logo	

Security Licenses

LICENSE NAME	INCLUDES	1 YR SUBSCRIPTION	3 YR SUBSCRIPTION	5 YR SUBSCRIPTION
AR3050S				
Advanced Firewall	Application Control Web Control URL Filtering	AT-FL-AR3-NGFW-1YR	AT-FL-AR3-NGFW-3YR	AT-FL-AR3-NGFW-5YR
Advanced Threat Protection	IP Reputation Malware Protection	AT-FL-AR3-ATP-1YR	AT-FL-AR3-ATP-3YR	AT-FL-AR3-ATP-5YR
AR4050S				
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

Feature Licenses

PRODUCT	NAME	DESCRIPTION
AR4050S	AT-FL-UTM-OFFLOAD-1YR	UTM Offload license for 1 year
AR4050S	AT-FL-UTM-OFFLOAD-3YR	UTM Offload license for 3 years
AR4050S	AT-FL-UTM-OFFLOAD-5YR	UTM Offload license for 5 years
AR4050S	AT-FL-AR4-AM20-1YR	AMF Master license for up to 20 nodes for 1 year
AR4050S	AT-FL-AR4-AM20-5YR	AMF Master license for up to 20 nodes for 5 years
AR4050S	AT-FL-AR4-AWC20-1YR[4]	WLAN Controller (AWC) license for up to 20 access points for 1 year
AR4050S	AT-FL-AR4-AWC20-5YR[4]	WLAN Controller (AWC) license for up to 20 access points for 5 years
AR4050S	AT-FL-AR4-CB5-1YR[5]	AWC-Channel Blanket license for up to 5 access points for 1 year
AR4050S	AT-FL-AR4-CB5-5YR[5]	AWC-Channel Blanket license for up to 5 access points for 5 years
AR4050S	AT-FL-AR4-SC5-1YR[6]	AWC-Smart Connect license for up to 5 access points for 1 year
AR4050S	AT-FL-AR4-SC5-5YR[6]	AWC-Smart Connect license for up to 5 access points for 5 years
AR4050S	AT-FL-AR4-ASEC-1YR[7]	AMF-Sec license for 1 year
AR4050S	AT-FL-AR4-ASEC-5YR[7]	AMF-Sec license for 5 years

[4] Five APs can be managed for free. Add an additional 20 APs with an AWC license
[5] Channel Blanket is not available as a free service. Both an AWC-CB license and an AWC license are required for Channel Blanket to operate. This features is supported on TQ5403 and TQ5403e access points
[5] Smart Connect is not available as a free service. Both an AWC-SC license and an AWC license are required for Smart Connect to operate. This feature is supported on TQ5403, TQ5403e and TQm5403 access points
[7] The AMF-Sec license can not be used in conjunction with either the Advanced Firewall (NGFW) or Advanced Threat Protection (ATP) licenses

Ordering information

AT-AR3050S-xx
2 x GE WAN and 8 x 10/100/1000 LAN

AT-AR4050S-xx
2 x GE WAN and 8 x 10/100/1000 LAN

Where xx = 10 for US power cord
20 for no power cord
30 for UK power cord
40 for Australian power cord
50 for European power cord
51 for encryption not enabled

AT-RKMT-J15
Rack mount kit to install two devices side by side in a 19-inch equipment rack

AT-RKMT-J14
Rack mount kit to install one device in a 19-inch equipment rack

1000Mbps SFP Modules

AT-SPTX
1000T 100 m copper

AT-SPSX
1000SX GbE multi-mode 850 nm fiber up to 550 m

AT-SPSX/I
1000SX GbE multi-mode 850 nm fiber up to 550 m industrial temperature

AT-SPEX
1000X GbE multi-mode 1310 nm fiber up to 2 km

AT-SPLX10
1000LX GbE single-mode 1310 nm fiber up to 10 km

AT-SPLX10/I
1000LX GbE single-mode 1310 nm fiber up to 10 km industrial temperature

AT-SPBD10-13
1000LX GbE Bi-Di (1310 nm Tx, 1490 nm Rx) fiber up to 10 km

AT-SPBD10-14
1000LX GbE Bi-Di (1490 nm Tx, 1310 nm Rx) fiber up to 10 km

AT-SPLX40
1000LX GbE single-mode 1310 nm fiber up to 40 km

AT-SPZX80
1000ZX GbE single-mode 1550 nm fiber up to 80 km

AT-SPBD20-13/I
1000BX GbE Bi-Di (1310 nm Tx, 1490 nm Rx) fiber up to 20 km

AT-SPBD20-14/I
1000BX GbE Bi-Di (1490 nm Tx, 1310 nm Rx) fiber up to 20 km

Related Products

AT-TQ4600-xx (Version 4.0.5)
Enterprise-Class Wireless Access Point with IEEE 802.11ac dual-band radio and embedded antenna

AT-TQ4400e-xx (Version 4.0.5)
Enterprise-Class Outdoor Wireless Access Point with IEEE 802.11ac dual-band radio

AT-TQm1402
Enterprise-Class 802.11ac Wave 2 Wireless Access Point with 2 radios and embedded antenna

AT-TQ1402
Enterprise-Class Advanced 802.11ac Wave 2 Wireless Access Point with 2 radios and embedded antenna

AT-TQm5403
Enterprise-Class 802.11ac Wave 2 Wireless Access Point with 3 radios and embedded antenna

AT-TQ5403
Enterprise-Class Advanced 802.11ac Wave 2 Wireless Access Point with 3 radios and embedded antenna

AT-TQ5403e
Enterprise-Class Outdoor Advanced 802.11ac Wave 2 Wireless Access Point with 3 radios with four omni-directional antennas

3G/4G USB Modems

For a list of supported USB modems visit alliedtelesis.com

617-000567 RevZi