5G Mobile Broadband UTM Firewall

AR4050S-5G

Allied Telesis AR4050S-5G mobile broadband UTM Firewall is the ideal integrated security platform for modern distributed businesses. The power of 5G enables unprecedented mobile data speed with low latency to boost network performance, ideal for rural areas and remote office connectivity. The AR4050S-5G resolves the increased demand for access to business applications from anywhere across the corporate WAN.

Overview

The AR4050S-5G enables flexible business WAN deployment, with high-speed 5G mobile broadband used to link remote offices to the corporate network, or to back up a wired Ethernet Internet connection. 5G performance is integrated in a “best of breed” security platform for up-to-the-minute threat protection with advanced networking capabilities.

5G mobile broadband connectivity[1]

The 5th generation mobile communication system (5G) offers rich features, including high speed, large capacity, low latency, and connection of multiple devices. It supports the growing use of immersive-experience applications, video conferencing, and other online corporate resources. Businesses relying on mobile WAN connections can fully utilize these applications thanks to the performance of 5G on the AR4050S-5G. Dual SIM card slots support resilient mobile connectivity, with the ability to use SIM cards from two different carriers.

Easy to manage

The AR4050S-5G runs the advanced AlliedWare Plus™ operating system, with an industry standard CLI, while the Device GUI provides graphical monitoring and management of security, threat protection, and other key features.

Device and network management

Integrated into the Device GUI, Vista Manager mini supports visibility and management of AMF Plus 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.

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. The AMF Security mini license enables our state-of-the-art integrated solution that automatically protects the LAN from internal security threats.

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

Application-aware Firewall

The AR4050S-5G 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.

Secure Remote Virtual Private Networks (VPN)

The AR4050S-5G supports IPSec site-to-site VPN connectivity to connect 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.

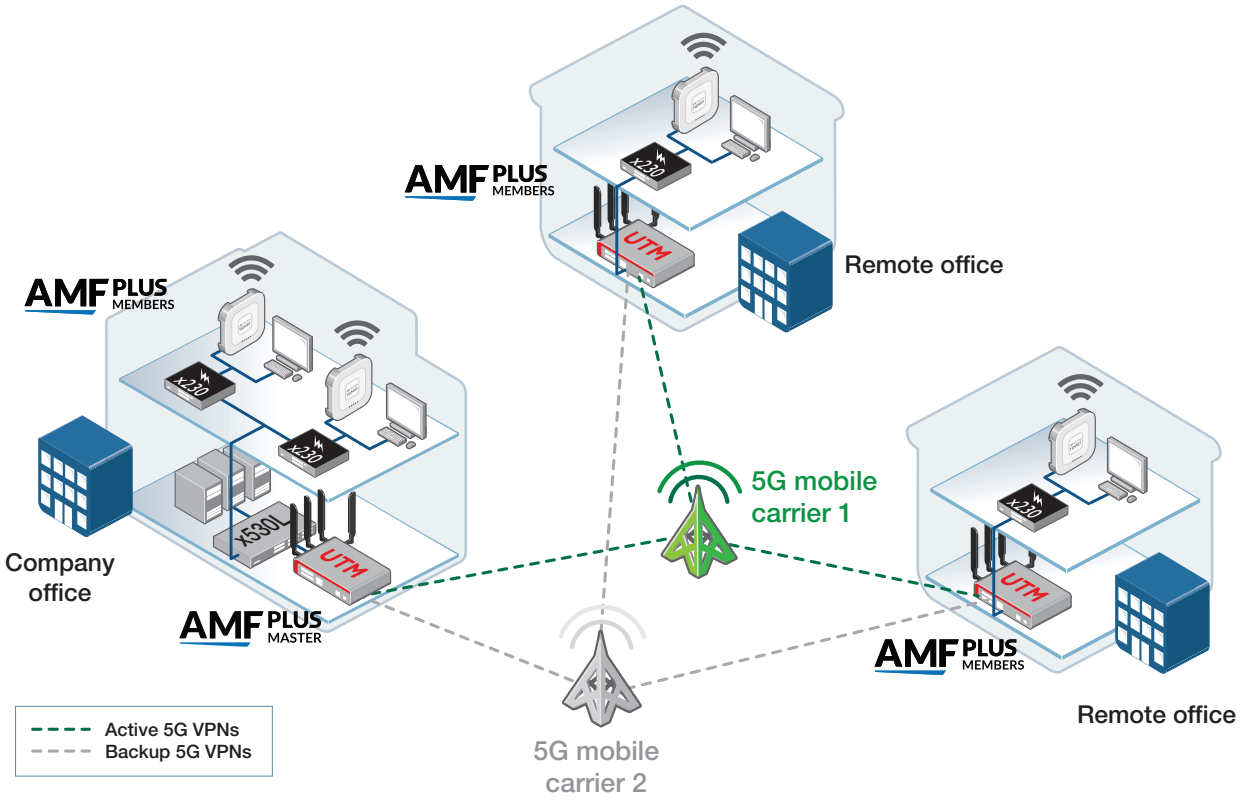
Remote workers can utilize an SSL VPN connection to encrypt their business data over the Internet, allowing them to utilize all their business resources when working from home, travelling, or otherwise away from the company premises.

Both inter-branch and remote worker VPNs are ably supported across the mobile network with the performance and capacity of 5G.

[1] 5G connectivity is not supported in Vietnam, but the AR4050S-5G can still be used at 3G or 4G speeds

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 application list 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, which are independent so the same or overlapping IP addresses can be used. VRF Lite supports IPv4 (unicast and multicast) and IPv6 (unicast) traffic. 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.
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.
UTM Offload	UTM Offload enables some security and threat protection features (for example, IPS and IP Reputation) to be offloaded to a secondary physical or virtual machine that is automatically managed by the AR4050S-5G. 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 feature.
Dual SIM card slots	Dual SIM card slots provide resilient 5G mobile connectivity by using different carriers, with the back-up mobile connection able to be automatically enabled if required.
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.
RESILIENCY	
VRRP triggers for router failover	Allied Telesis UTM Firewalls support event-based triggers to automatically change VRRP mastership if required. This simplifies WAN failover and reduces disruption to other network devices.
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.
VIRTUAL PRIVATE NETWORKING CONTINUED	
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: Resilient 5G WAN connectivity

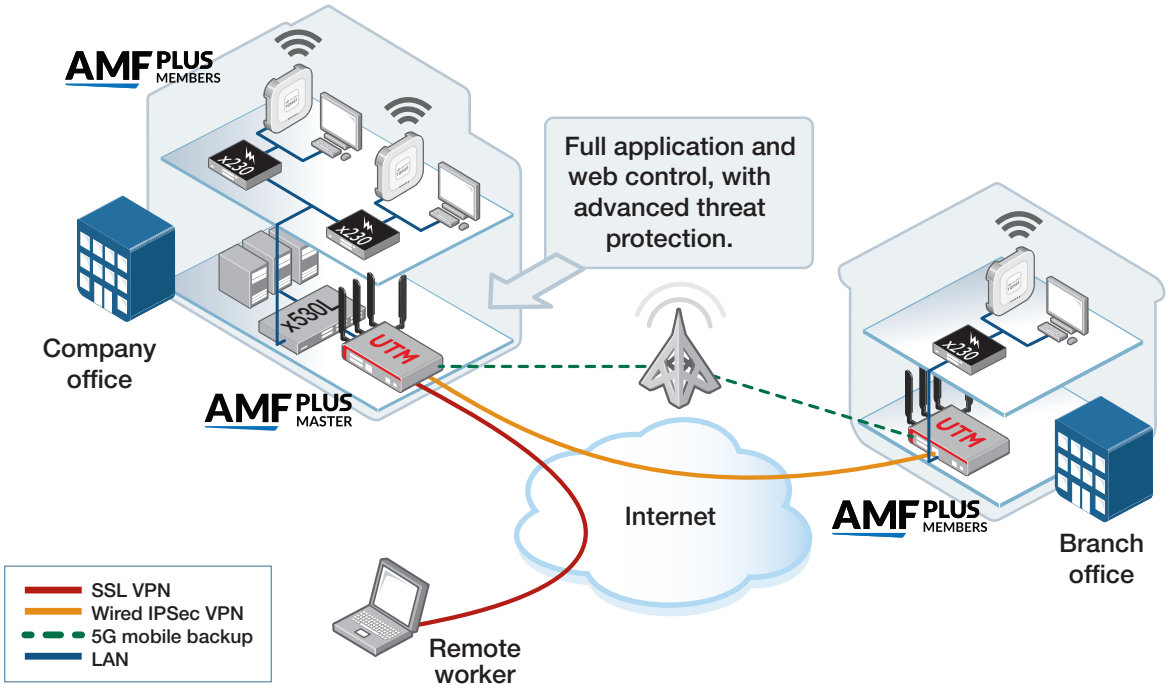


Resilient 5G WAN connectivity with the dual SIM AR4050S-5G

5G mobile broadband provides a high performance solution for connecting rural or remote offices to the corporate network - ensuring they enjoy the same full access to online company resources and applications as those connected locally or over wired networks.

Installing 5G SIM cards from two different carriers enables a resilient business solution, with backup of inter-branch links, as even if the 5G signal from one carrier fails, the device can automatically connect to the alternate carrier using the second SIM (note that only one SIM card can be active at a time). This ensures always-on access and connectivity right across all company locations.

Key Solution: Integrated Security with 5G WAN Backup



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 a wired site-to-site IPSec VPN connectivity between corporate offices, with 5G mobile network backup available if the wired VPN becomes unavailable. SSL VPNs allow 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.

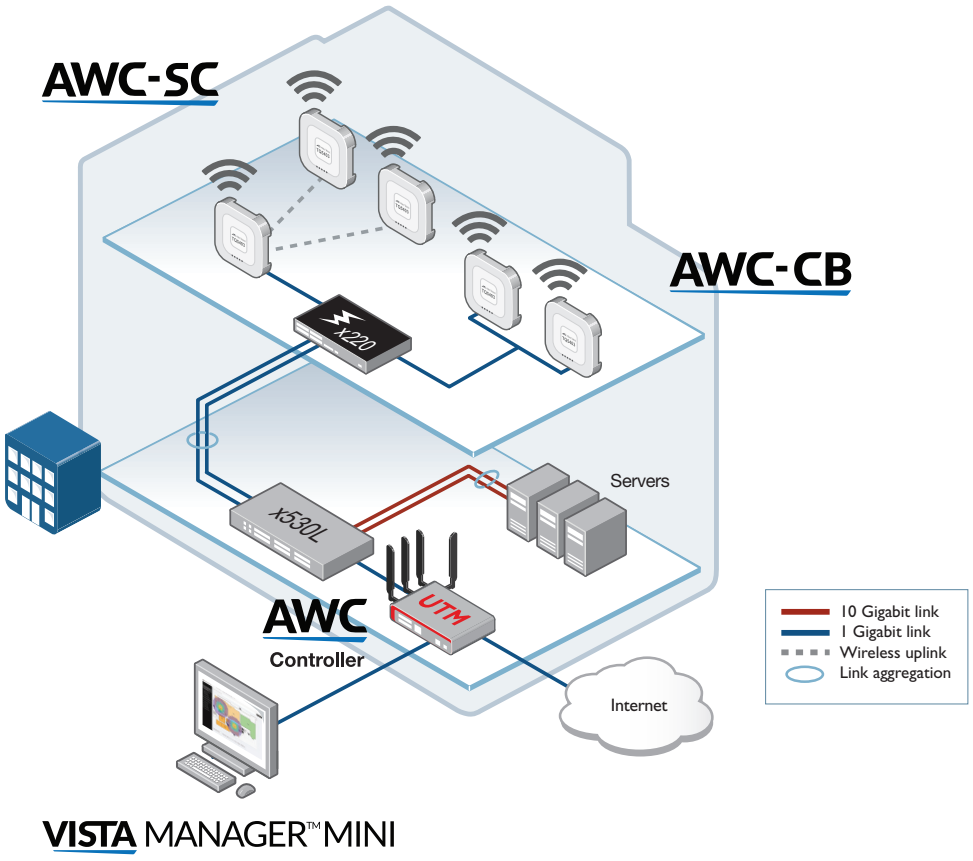
Automated network management

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 AR4050S-5G can operate as the AMF Plus 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 recalibrates the signal strength and radio channel of each AP for optimal WLAN performance.

When AWC is combined with the firewall functionality in the AR4050S-5G, 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.

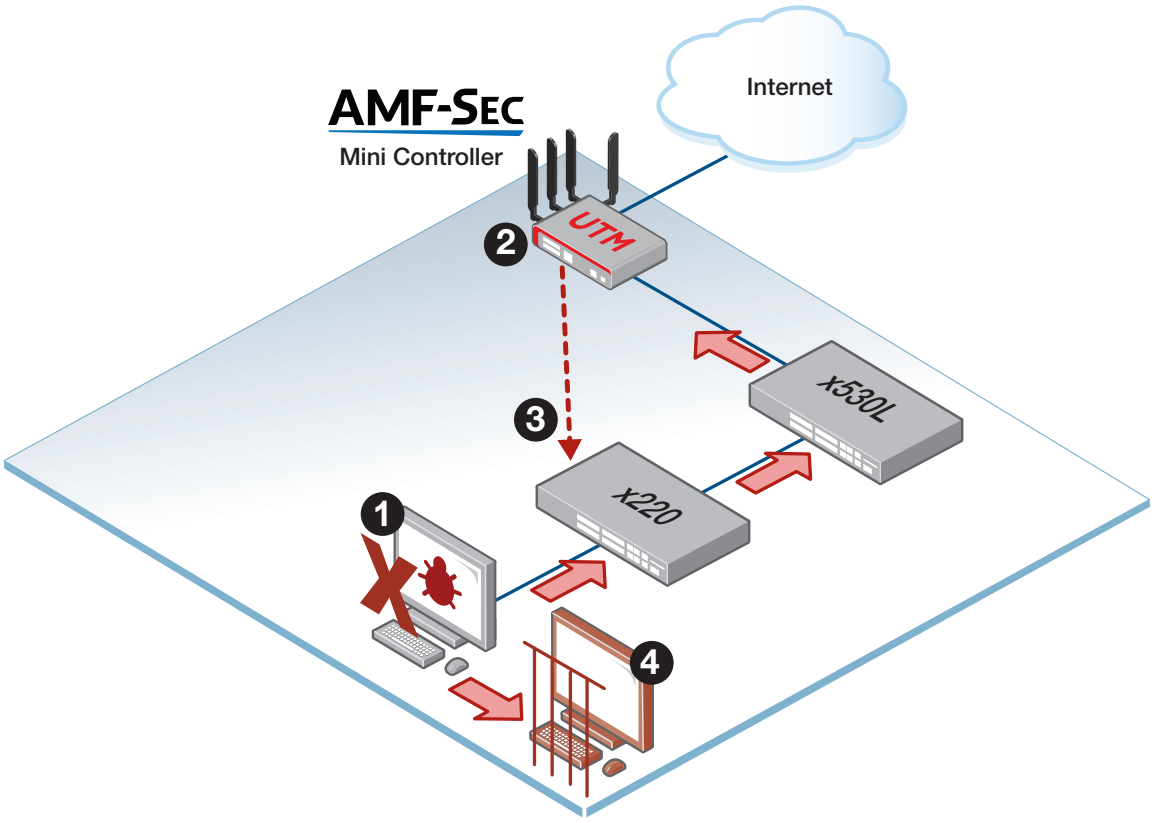
Vista Manager mini is integrated into the Device GUI of the AR4050S-5G and provides an ideal solution for modern networks, enabling management of both the wired (with AMF Plus) and wireless (with AWC) networks to be automated. This reduces both the time and cost of network administration, as well as 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-5G 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-5G 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-5G 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 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 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)
- 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
- Security for IPv6 traffic

Networking

- Routing mode / bridging mode / mixed mode
- MAC address filtering on switch ports to secure communication of IoT and other devices
- 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
- Secondary IP addresses per interface and subnet enable flexible deployment
- Device management over IPv6 networks with SNMP, Telnet, and SSH
- Logging to IPv6 hosts with Syslog
- 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
- 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
- Try AMF Plus for free with the built-in AMF Plus starter license
- 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 menu in Vista Manager EX (from version 3.10.1 onwards)
- Web-based Device GUI for firewall configuration and easy monitoring
- NETCONF/RESTCONF northbound interface with YANG data modelling
- 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 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
- Console management port on the front panel for ease of access
- USB interface for either removable file storage or external LTE/4G/5G allow software release files, configurations, and other files to be stored for backup and distribution to other devices.
- Two SIM Card slots are available that support standard size SIM cards. If two SIM cards are inserted, priority will be given to SIM 1 with SIM 2 acting as the backup.

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

- 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

- TACACS+ Authentication, Accounting and Authorization (AAA)
- RADIUS authentication and accounting
- Local or server-based RADIUS user database
- RADIUS group selection per VLAN or port
- RADIUS CoA (Change of Authorization)
- Strong password security and encryption
- MAC and 802.1x Port authentication on switch ports
- 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

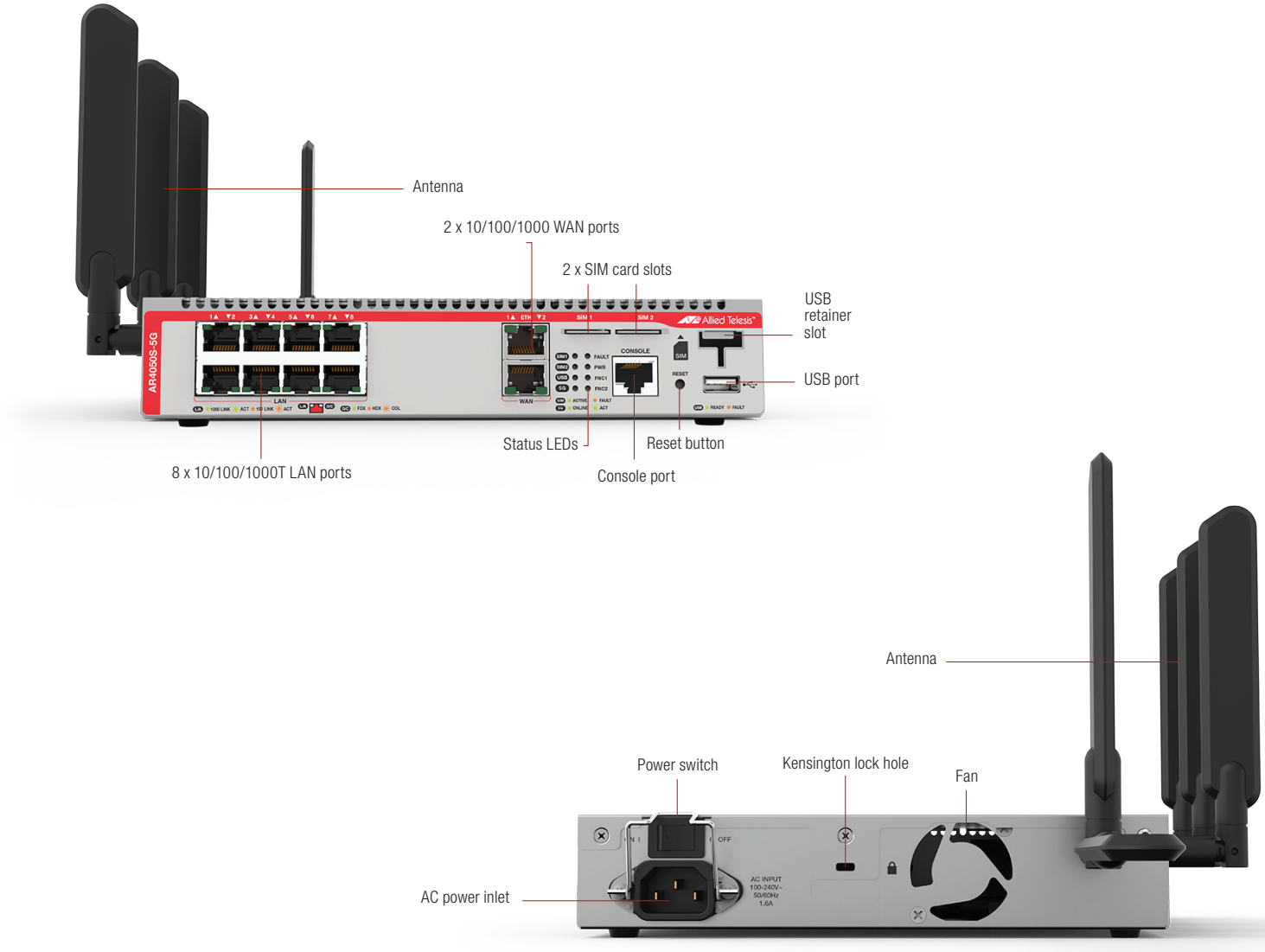
- Diffie-Hellman key exchange (D-H groups 2, 5, 14, 15, 16, 18)
- Secure encryption algorithms: AES/AES-GCM and 3DES
- Secure authentication: SHA-1, SHA-256, SHA-512
- IKEv1 and IKEv2 key management
- IPsec Dead Peer Detection (DPD)
- IPsec NAT traversal
- IPsec VPN for site-to-site connectivity
- Multipoint VPN for connecting a single VPN to multiple end points
- Dynamic routing through VPN tunnels (RIP, OSPF, BGP)
- 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

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
- 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-5G



Specifications

	AR4050S-5G
Processor and memory	
Security processor	1.5GHz quad-core
Memory (RAM)	2GB
Memory (Flash)	4GB
Frequency bands	
Sub 6GHz Bands	n1, n2, n3, n5, n28, n41, n66, n71, n77, n78, n79
LTE Bands	B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B29, B30, B32, B34, B38, B39, B40, B41, B42, B46, B48, B66, B71
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)	1,000
Client-to-site VPN tunnels (OpenVPN)	1,000
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, L2TPv2 virtual tunnels, L2TPv3 Ethernet pseudo-wires
Encapsulation	GRE for IPv4 and IPv6
Management & authentication	
Logging & notifications	Syslog & Syslog v6, SNMPv2c & v3
User interfaces	Web-based GUI, scriptable industry-standard CLI, NETCONF/RESTCONF
Secure management	SSHv1/v2, strong passwords
Management & authentication	
Management tools	Allied Telesis Autonomous Management Framework™ Plus (AMF Plus) 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)
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

	AR4050S-5G
Networking continued	
Multicasting	IGMPv1/v2/v3, PIM-SM, PIM-DM, PIM-SSM, PIMv6
Resiliency	STP, RSTP, MSTP
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, IPsec traversal, Dynamic NAPT, Double NAT, subnet-based NAT
Link aggregation	802.3ad static and dynamic (LACP)
VLANs	802.1Q tagging
Discovery	802.3ad static and dynamic (LACP)
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	28W
LAN ports	8x 10/100/1000BASE-T (RJ-45)
Hardware characteristics	
WAN ports	2x 10/100/1000BASE-T (RJ-45)
Other ports	1x USB port, 1x RJ-45 console port, 2x SIM slots
Product dimensions (W x D x H) (without antenna)	220 x 260 x 42.5 mm (8.66 x 10.23 x 1.67 in)
Packaged dimensions (W x D x H)	436 x 288 x 112 mm (17.16 x 11.33 x 4.41 in)
Product weight	2 kg (4.41 lb)
Typical / Max noise	35.1dB
Environmental specifications	
Operating temperature range	0° to 45°C (32°F to 113°F)
Storage temperature range	-20° 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, EN55035, EN61000-3-2, EN61000-3-3
Radio	EN301489-1, EN301489-52, EN301908-1, EN301908-2, EN301908-13, EN301908-25, 3GPPTS-38.521-3, TS134121-1, TS136521-1, EN50385, EN62311, EN62232
Safety standards	EN62368, UL62368-1, CSA-C22.2 NO. 62368-1, AS/NZS 62368.1
Safety certifications	UL, TUV
Reduction of Hazardous Substances (RoHS)	EU RoHS6 compliant, China RoHS compliant

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 security and threat protection feature processing for increased throughput.

PERFORMANCE	
Firewall Throughput (Raw)	1,900 Mbps
Firewall Throughput (APP Control)	1,800 Mbps
Concurrent sessions	300,000
New sessions per second	12,000
IPS throughput	750 Mbps
IP reputation throughput	1,000 Mbps
VPN throughput	1,000 Mbps

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

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[2]	AT-AR4-UTM-01-3YR[2]	AT-AR4-UTM-01-5YR[2]
Advanced Threat Protection	Advanced IPS IP Reputation	AT-AR4-UTM-02-1YR[2]	AT-AR4-UTM-02-3YR[2]	AT-AR4-UTM-02-5YR[2]

[2] The AT-AR4-UTM-01 and AT-AR4-UTM-02 licenses cannot be used together

Feature Licenses

NAME	DESCRIPTION	INCLUDES
AT-FL-UTM-OFFLOAD-1YR	UTM Offload license for 1 year	▸ UTM Offload license for 1 year
AT-FL-UTM-OFFLOAD-3YR	UTM Offload license for 3 years	▸ UTM Offload license for 3 years
AT-FL-UTM-OFFLOAD-5YR	UTM Offload license for 5 years	▸ UTM Offload license for 5 years
AT-RT-APM5-1YR[3, 4]	Cumulative AMF Plus Master license	▸ AMF Plus Master license for up to 5 nodes for 1 year
AT-RT-APM5-5YR[3, 4]	Cumulative AMF Plus Master license	▸ AMF Plus Master license for up to 5 nodes for 5 years
AT-RT-AWC5-1YR[5]	Cumulative AWC license	▸ Autonomous Wave Control (AWC) license for up to 5 access points for 1 year
AT-RT-AWC5-5YR[5]	Cumulative AWC license	▸ Autonomous Wave Control (AWC) license for up to 5 access points for 5 years
AT-RT-CB5-1YR-2022[6]	Cumulative AWC-CB and AWC-SC license	▸ AWC Channel Blanket and AWC Smart Connect license for up to 5 access points for 1 year
AT-RT-CB5-5YR-2022[6]	Cumulative AWC-CB and AWC-SC license	▸ AWC Channel Blanket and AWC Smart Connect license for up to 5 access points for 5 years
AT-FL-AR4-ASEC-1YR6[7]	AMF-Sec license	▸ AMF-Sec license for 1 year
AT-FL-AR4-ASEC-5YR[7]	AMF-Sec license	▸ AMF-Sec license for 5 years

[3] From AW+ version 5.5.2-2 onwards, AMF Plus licenses provide all standard AMF network management and automation features. They also enable the AMF Plus intent-based networking features menu in Vista Manager EX (from version 3.10.1 onwards)
[4] Purchase one license per 5 nodes (up to 20 nodes maximum)
[5] 5 APs can be managed for free. Purchase one license per 5 additional APs (up to 20 APs maximum)
[6] Channel Blanket and Smart Connect are not available as free services. Both an AWC-CB license and an AWC license are required for Channel Blanket and/or Smart Connect to operate. A maximum of 5 APs can use these features. (Channel Blanket is supported on TQ6702 GEN2, TQ6602 GEN2, and TQ6602 access points. Smart Connect is supported on TQ6702 GEN2 and TQ6602 GEN2)
[7] To use AMF-Sec in conjunction with either the Advanced Firewall (NGFW) or Advanced Threat Protection (ATP) licenses, you must have AMF-Sec mini version 2.2.1 or newer

Ordering information

AT-AR4050S-5G-xx
2x 10/100/1000 WAN and 8x 10/100/1000 LAN with 5G[8] mobile broadband access and dual SIM slots

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

AT-AR4050S-5G-Bxy
2x 10/100/1000 WAN and 8x 10/100/1000 LAN with 5G[1] mobile broadband access and dual SIM slots with Net cover support

Where y = 1 for one year Net Cover support
5 for five years Net Cover support

AT-BRKT-J24
Wall mount kit for AT-AR4050S-5G

VT-Kit3
USB Console Cable

AT-STND-J03
Stand Kit for AT-AR4050S-5G

Related Products

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-TQ6602
Enterprise-Class Wi-Fi 6 Wireless Access Point with 2 radios and embedded antenna

AT-TQm6602 GEN2
Enterprise-Class Wi-Fi 6 AP with 2 radios (4x4 2.4GHz and 4x4 5GHz) and embedded antenna

AT-TQm6702 GEN2
Enterprise-Class Wi-Fi 6 AP with 2 radios (4x4 2.4GHZ and 8x8 5GHz) and embedded antenna

AT-TQ6602 GEN2
Enterprise-Class hybrid Wi-Fi 6 AP with 2 radios (4x4 2.4GHz and 4x4 5GHz) and embedded antenna

AT-TQ6702 GEN2
Enterprise-Class hybrid Wi-Fi 6 AP with 2 radios (4x4 2.4GHZ and 8x8 5GHz) and embedded antenna

AT-TQ6702e GEN2-xx
Outdoor Wi-Fi 6 hybrid AP with 2 radios (4x4 2.4GHZ and 8x8 5GHz) and embedded antenna

[8] 5G connectivity is not supported in Vietnam, but the AR4050S-5G can still be used at 3G or 4G speeds

617-000693 RevL