

# 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, and advanced networking capabilities, meeting the needs of Enterprise networks.

### High performance

High performance is guaranteed by harnessing the power of multi-core processors and application acceleration engines, dramatically increasing throughput and enabling sustained low latency traffic inspection.

	AT-AR3050S	AT-AR4050S
<b>Firewall throughput (Raw)</b>	750 Mbps	1,900 Mbps
<b>Firewall throughput (App Control)</b>	700 Mbps	1,800 Mbps
<b>Concurrent sessions</b>	100,000	300,000
<b>New sessions per second</b>	3,600	12,000
<b>IPS throughput</b>	220 Mbps	750 Mbps
<b>IP Reputation throughput</b>	350 Mbps	1,000 Mbps
<b>Malware protection throughput</b>	300 Mbps	1,300 Mbps
<b>VPN throughput</b>	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.\* All other features are included in the base feature set.

\* Antivirus is only available on the AR4050S

### 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.

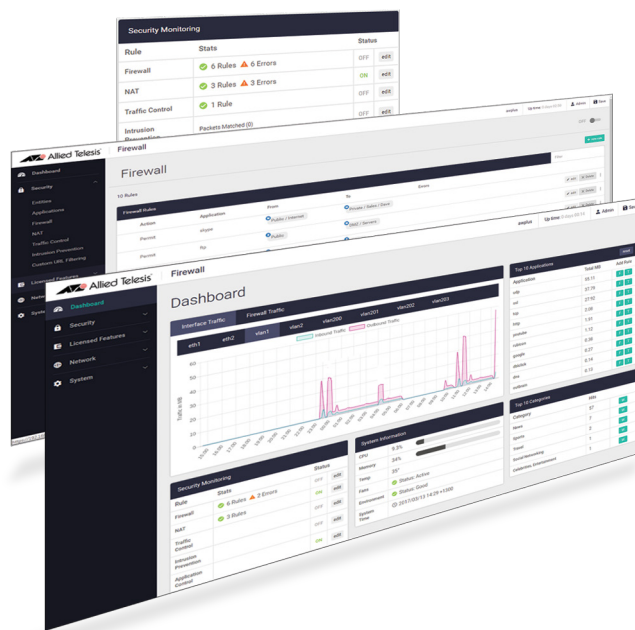
### Secure Remote Virtual Private Networks (VPN)

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.

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.

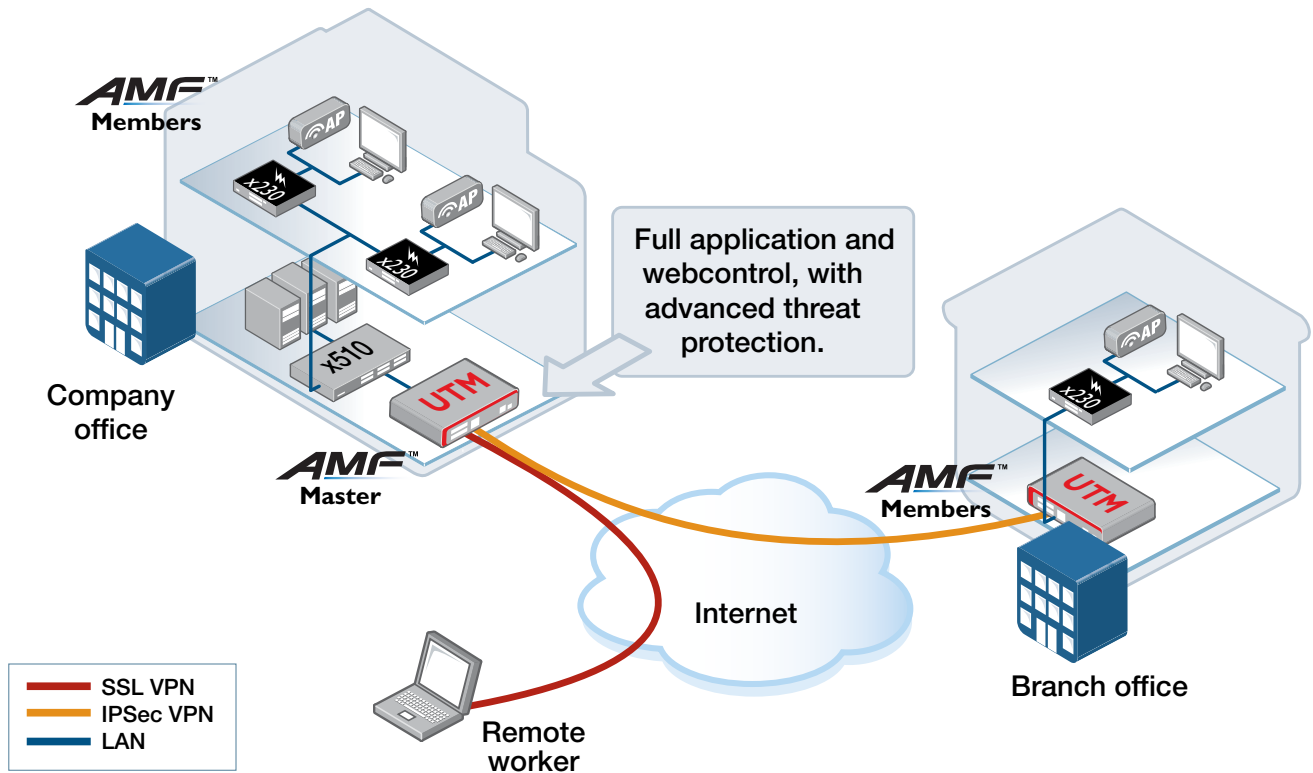
### Easy to manage

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, provides a consistent approach to policy management.



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. The ProCera™ DPI engine uses a regularly updated database of application signatures, to ensure business security and productivity.
Application bandwidth management	Manage application bandwidth to support business requirements, while limiting non-essential applications.
Web control	Digital Arts™ web categorisation enables easy control of web content by simply selecting which of the 100 content categories to allow or deny globally, or per user or group. URL categories are cached locally so that the response time for access to frequently visited sites is not delayed.
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 independent, 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.
3G/4G/LTE USB modem	A 3G/4G/LTE USB modem offers an additional secure 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.
VRPP triggers for bypass port failover	The Allied Telesis UTM Firewalls support event-based triggers to automatically change VRPP 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 by the DPI engine 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 connectivity	High-performance IPSec VPN allows the Allied Telesis UTM Firewalls to act as a VPN concentrator for other large sites, branch offices or home 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.

## Key Solution



### 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 make 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 the Allied Telesis Autonomous Management Framework (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.

## Features

### Firewall

- ▶ Deep Packet Inspection (DPI) application aware firewall (ProCera) 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
- ▶ 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

### Networking

- ▶ Routing mode / bridging mode / mixed mode
- ▶ Static unicast and multicast routing for IPv4 and 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
- ▶ 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

### 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 GUI for device configuration and easy monitoring
- ▶ Industry-standard CLI with context-sensitive help
- ▶ Role-based administration with multiple CLI security levels
- ▶ Built-in text editor and powerful CLI scripting engine
- ▶ Comprehensive SNMPv2c/v3 support for standards-based device management
- ▶ Event-based triggers allow user-defined scripts to be executed upon selected system events
- ▶ Comprehensive logging to local memory and syslog
- ▶ Console management port on the front panel for ease of access
- ▶ 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

### Resiliency

- ▶ High availability bypass ports
- ▶ Policy-based storm protection
- ▶ Spanning Tree (STP, RSTP, MSTP) with root guard
- ▶ Virtual Router Redundancy Protocol (VRRPv2/v3)
- ▶ VRRP triggers bypass port failover for v4 & v6 traffic

### 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

### 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

### Unified Threat Management (UTM)

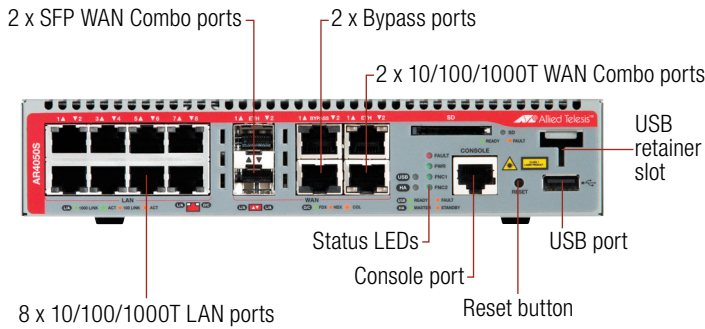
- ▶ Proxy-based anti-virus scanning (AR4050S only)
- ▶ No file size limitations
- ▶ Auto-update of UTM signature files
- ▶ Bot activity detection (using Kaspersky malware protection)
- ▶ Intrusion Detection and Prevention System (IDS/IPS) (no license required)
- ▶ DoS and DDoS attack detection and protection
- ▶ 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
- ▶ Dynamic routing through VPN tunnels (RIP, OSPF, BGP)
- ▶ Redundant VPN gateway
- ▶ SSL/TLS VPN for secure remote access using OpenVPN

SECURITY PROVIDERS	
Allied Telesis UTM Firewalls utilize “best of breed” threat signatures and databases for up-to-the-minute protection from the security industry’s leading providers.	
Application Control	
Web Control	
URL Filtering, Malware Protection, Antivirus	
IP Reputation	

AR4050S



Specifications

	AR3050S	AR4050S
<b>Processor and memory</b>		
Security processor	800MHz dual-core	1.5GHz quad-core
Memory (RAM)	1GB	2GB
Memory (Flash)	4GB	4GB
<b>Security features</b>		
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	
<b>Tunneling &amp; encryption</b>		
Site-to-site VPN tunnels (IPsec)	50	200
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	
<b>Management &amp; authentication</b>		
Logging & notifications	Syslog & Syslog v6, SNMPv2 & v3	
User interfaces	Web-based GUI, scriptable industry-standard CLI	
Secure management	SSHv1/v2, strong passwords	
Management	Allied Telesis Autonomous Management Framework™ (AMF)	
User authentication	RADIUS, TACACS+, internal user database, web authentication	
Command authorization	TACACS+ AAA (Authentication, Accounting and Authorization)	

	AR3050S	AR4050S
<b>Networking</b>		
<b>Routing (IPv4)</b>	Static, Dynamic (BGP4, OSPF, RIPv1/v2), source-based routing, policy-based routing, VRF-Lite	
<b>Routing (IPv6)</b>	Static, Dynamic (BGP4+, OSPFv3, RIPng), policy-based routing	
<b>Multicasting</b>	IGMPv1/v2/v3, PIM-SM, PIM-DM, PIM-SSM, PIMv6	
<b>Resiliency</b>	STP, RSTP, MSTP	
<b>High availability</b>	VRRP, VRRPv3, hardware controlled bypass ports	
<b>Traffic control</b>	8 priority queues, DiffServ, HTB scheduling, RED curves	
<b>IP address management</b>	Static v4/v6, DHCP v4/v6 (server, relay, client), PPPoE	
<b>NAT</b>	Static, IPsec traversal, Dynamic NAT, Double NAT, subnet-based NAT	
<b>Link aggregation</b>	802.3ad static and dynamic (LACP)	
<b>VLANs</b>	802.1Q tagging	
<b>Reliability features</b>		
	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	
<b>Hardware characteristics</b>		
<b>Input power</b>	90 to 260V AC (auto-ranging), 47 to 63Hz	
<b>Max power consumption</b>	23W	27W
<b>LAN ports</b>	8 x 10/100/1000T RJ-45	
<b>WAN ports</b>	2 x 1000X SFP / 2 x 10/100/1000T RJ-45 combo	
<b>High Availability bypass ports</b>	2 x 10/100/1000T RJ-45	
<b>Other ports</b>	1 x USB, 1 x RJ-45 console, 1 x SDHC slot	
<b>Product dimensions (H x W x D)</b>	42.5 mm (1.67 in) x 210 mm (8.26 in) x 220 mm (8.66 in)	
<b>Packaged dimensions (H x W x D)</b>	36.5 cm (14.37 in) x 26 cm (10.24 in) x 11.5 cm (4.53 in)	
<b>Product weight</b>	1.7 kg unpackaged, 2.6 kg packaged	
<b>Typical / Max noise</b>	28.4 dBA / 35.1 dBA	
<b>Environmental specifications</b>		
<b>Operating temperature range</b>	0°C to 50°C (32°F to 122°F). Derated by 1°C per 305 meters (1,000 ft)	
<b>Storage temperature range</b>	-25°C to 70°C (-13°F to 158°F)	
<b>Operating relative humidity range</b>	5% to 80% non-condensing	
<b>Storage relative humidity range</b>	5% to 95% non-condensing	
<b>Operating altitude</b>	2,000 meters maximum (6,600 ft)	
<b>Regulations and compliances</b>		
<b>EMC</b>	EN55022 class A, FCC class A, VCCI class A	
<b>Immunity</b>	EN55024, EN61000-3-levels 2 (Harmonics), and 3 (Flicker)	
<b>Safety Standards</b>	UL60950-1, CAN/CSA-C22.2 No. 60950-1-03, EN60950-1, EN60825-1, AS/NZS 60950.1	
<b>Safety Certifications</b>	UL, cUL, TuV	
<b>Reduction of Hazardous Substances (RoHS)</b>	EU RoHS6 compliant, China RoHS compliant	
<b>IPv6 Ready</b>	Phase 2 (Gold) Logo	
<b>Country of origin</b>		
	China	



# AR3050S and AR4050S | UTM Firewalls

## 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



### 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

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

## 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

## Security Subscription Licenses

LICENSE NAME	INCLUDES	1 YR SUBSCRIPTION	3 YR SUBSCRIPTION	5 YR SUBSCRIPTION
<b>AR3050S</b>				
Advanced Firewall	Application Control Web Control URL Filtering	AT-FL-AR3-NGFW1-YR	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
<b>AR4050S</b>				
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-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

### 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, 1550 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

## 3G/4G USB Modems

For a list of supported USB modems visit [alliedtelesis.com](http://alliedtelesis.com)