Next-Generation Firewalls

AT-AR3050S and AT-AR4050S

Allied Telesis Next-Generation Firewalls (NGFWs) are the ideal integrated security platform for modern businesses. Next generation firewall and threat protection is combined with routing and switching, to provide an innovative high performance solution.

The AT-AR3050S and AT-AR4050S are the ideal choice for high speed Enterprise gateway applications. The NGFWs feature an integrated 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.

"Best of breed" security

Allied Telesis integrated security platforms utilize "best of breed" security providers, for the ultimate in up-to-the-minute protection — from all known threats. Powerful features like Malware ptotection, Web control and Antivirus ensure the safety of business data.

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 NGFW license includes App Control and Web Control. The Advanced Threat Protection (ATP) license includes IP Reputation, Malware Protection and Antivirus.* All other features are included in the base feature set.

Deep Packet Inspection (DPI) Firewall

The Allied Telesis firewall is a next-generation, 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.

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.

Secure Remote Virtual Private Networks (VPN)

Allied Telesis NGFWs 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 NGFWs run the advanced AlliedWare Plus™ fully featured operating system, with an industry standard CLI. The Graphical User Interface (GUI) provides a dashboard for monitoring and visual quick-start configuration. Dashboard widgets show status, traffic and system information at a glance. Graphical configuration of security zones, networks and hosts, as well as firewall rules to control traffic, and management of advanced threat protection features, provides a consistent approach to policy management.

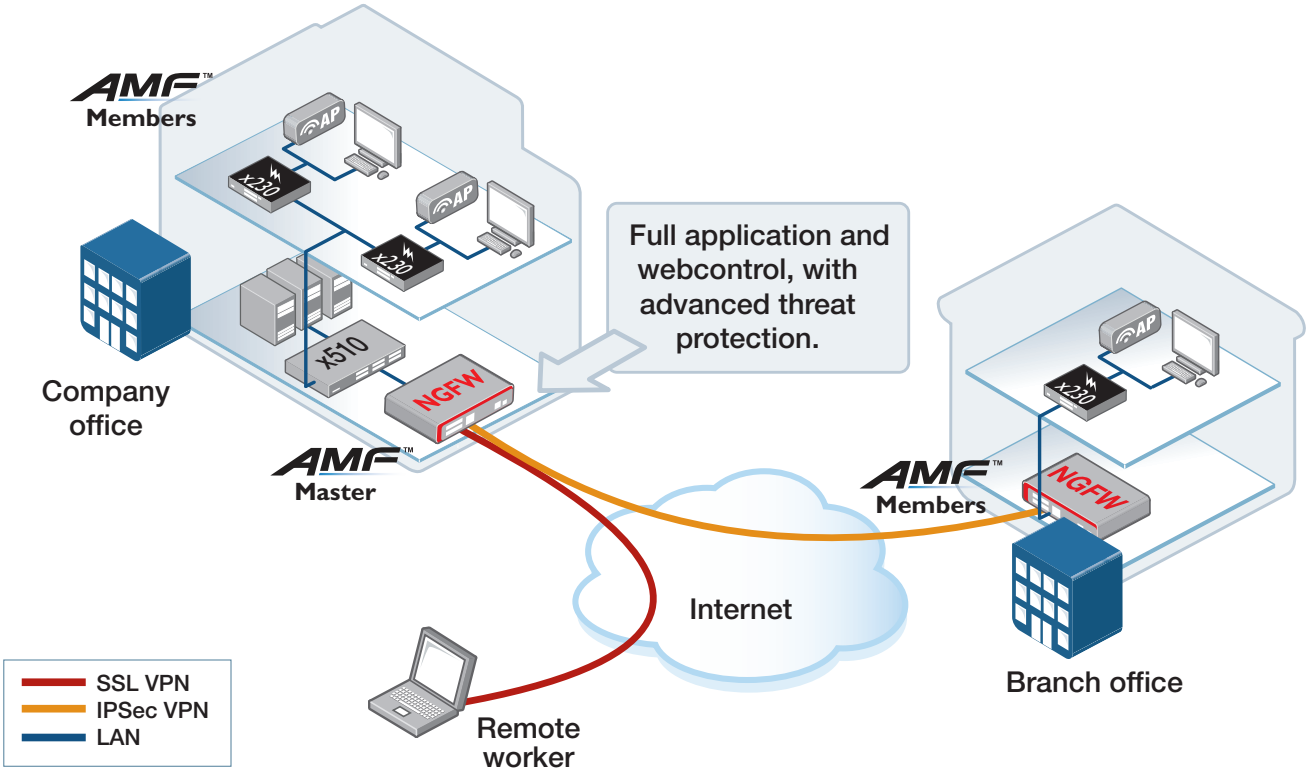
Full support for Allied Telesis Management Framework (AMF) allows Allied Telesis firewalls to integrate with Allied Telesis switching products to from a network able to be managed as a single virtual entity. A full suite of automated tools ensures that the firewall configuration is backed up, and able to be recovered with no user intervention, maximizing the availability of online services.

	AT-AR3050S	AT-AR4050S
Performance		
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

* Antivirus is only available on the AT-AR4050S

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.
Web control caching	URL categories are cached locally on the NGFW so that the response time for subsequent access to frequently visited sites is not delayed
URL filtering	Enables access to particular websites to be allowed (whitelist) or blocked (blacklist) with user-defined lists.
FIREWALL AND NETWORKING	
DoS attack protection	Protection against Denial of Service (DoS) attacks, which are designed to consume resources and therefore deny users network and application access
IPv6 support	Full support for IPv6 routing, multicasting and security is provided
Flexible deployment options	The Allied Telesis NGFWs 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.
VRRP triggers for bypass port failover	The Allied Telesis NGFWs 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 by the DPI engine for viruses, Trojans, and other malware to protect business information.
Automatic security updates	Security is kept up-to-the-minute without requiring user intervention or network disruption. NGFWs 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.
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 NGFWs 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 NGFWs 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 NGFW 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 NGFW 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 makew sense for the business.

The powerful combination of features make Allied Telesis NGFWs 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 NGFWs are fully supported by the Allied Telesis 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 AT-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)
- Masquerading (outbound NAT)
- Web control by content categorisation (Digital Arts)
- Custom web control categories, match criteria and keyword blocking
- URL Filtering with user defined lists
- 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)
- Traffic shaping for bandwidth control
- PPPoE client
- DHCP client, relay and server for IPv4 and IPv6
- DNS client and relay for IPv4 and IPv6
- 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 Management Framework (AMF) enables powerful centralized management and zero-touch device installation and recovery
- Try AMF for free with the built-in AMF starter license (AR4050S only)
- Web-based GUI for quick-start 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

- Authentication, Authorisation and Accounting (AAA)
- RADIUS and TACACS+ authentication and accounting
- Local or server-based RADIUS user database
- RADIUS group selection per VLAN or port
- Strong password security and encryption

Unified Threat Management (UTM)

- Stream-based anti-virus scanning
- 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)
- Malware protection (Kaspersky) protection from over 20,000 attacks
- Protocol anomaly detection and protection
- Zone-based UTM

VPN Tunneling

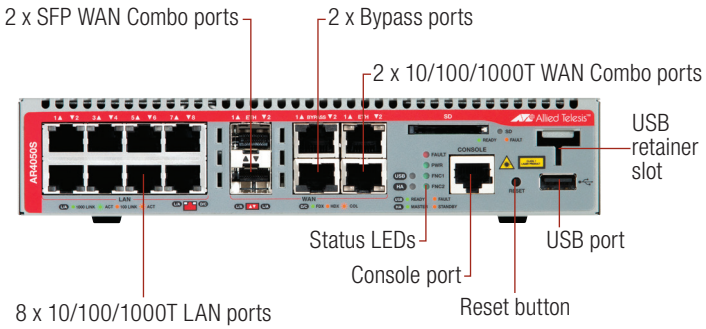
- Diffie-Hellman key exchange (D-H groups 5, 14, 16)
- Secure encryption algorithms: AES and 3DES
- Secure authentication: SHA-1 and SHA-256
- IKEv1 and IKEv2 key management
- IPsec Dead Peer Detection (DPD)
- IPsec NAT traversal
- IPsec VPN for site-to-site connectivity
- Dynamic routing through VPN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

Security Providers

Allied Telesis NGFWs utilize “best of breed” threat signatures and databases from the security industry’s leading providers.

Application Control	PROCERA EMPOWERING INTELLIGENCE
Web Control	DigitalArts.
Malware Protection	POWERED BY KASPERSKY
Antivirus	POWERED BY KASPERSKY
IP Reputation	EMERGING THREATS now part of proofpoint

AT-AR4050S



Specifications

	AT-AR3050S	AT-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		
IPsec site-to-site VPN tunnels	50	200
SSL VPN users	100	200
Encrypted VPN	IPsec, SHA-1, SHA-256, 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, 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	Allied Telesis Management Framework™ (AMF)	
User authentication	RADIUS, TACACS+, internal user database, web authentication	

	AT-AR3050S	AT-AR4050S
Networking		
Routing (IPv4)	Static, Dynamic (BGP4, OSPF, RIPv1/v2), source-based routing, policy-based routing	
Routing (IPv6)	Static, Dynamic (BGP4+, OSPFv3, RIPng), policy-based routing	
Multicasting	IGMPv1/v2/v3, PIM-SM, PIM-DM, PIM-SSM, PIMv6	
Resiliency	STP, RSTP, MSTP	
High availability	VRRP, VRRPv3, hardware controlled bypass ports	
Traffic shaping	8 priority queues, DiffServ, HTB scheduling	
IP address management	Static v4/v6, DHCP v4/v6 (server, relay, client), PPPoE	
NAT	Static, IPsec traversal, Dynamic NAPT	
Link aggregation	802.3ad static and dynamic (LACP)	
VLANs	802.1Q tagging	
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)	42.5mm (1.67 in) x 210mm (8.26 in) x 220mm (8.66 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	-25°C to 70°C (-13°F to 158°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	EN55022 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	
RoHS Compliance		
	EU RoHS6 compliant, China RoHS compliant	
Country of origin		
	China	

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
Rackmount shelf

AT-RKMT-J14
Rackmount brackets

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

Security Subscription Licenses

LICENSE NAME	INCLUDES	1 YR SUBSCRIPTION	3 YR SUBSCRIPTION	5 YR SUBSCRIPTION
AT-AR3050S				
Next-Gen Firewall	Application Control Web Control	AT-FL-AR3-NGFW1	AT-FL-AR3-NGFW3	AT-FL-AR3-NGFW5
Advanced Threat Protection	IP Reputation, Malware Protection	AT-FL-AR3-ATP1	AT-FL-AR3-ATP3	AT-FL-AR3-ATP5
AT-AR4050S				
Next-Gen Firewall	Application Control Web Control	AT-FL-AR4-NGFW1	AT-FL-AR4-NGFW3	AT-FL-AR4-NGFW5
Advanced Threat Protection	IP Reputation, Malware Protection, Anti-virus	AT-FL-AR4-ATP1	AT-FL-AR4-ATP3	AT-FL-AR4-ATP5

Feature Licenses

PRODUCT	NAME	DESCRIPTION
AT-AR4050S	AT-FL-AR4-AM20	AMF Master license for up to 20 nodes

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

3G/4G USB Modems

For a list of supported USB modems visit alliedtelesis.com

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com

617-000567 Rev H