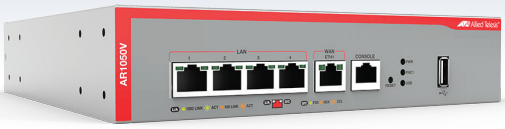
Secure VPN Router

AR1050V

Allied Telesis Secure Virtual Private Network (VPN) Routers are the ideal secure gateway for modern businesses. Integrated firewall and VPN functionality is combined with routing and switching, providing an innovative solution that is easy to use and very secure.



As businesses adapt to faster paced operations, with increasing amounts of data, and the need to access company resources from outside the office, the demand for high performance VPN connectivity becomes more urgent.

The AR1050V features comprehensive security and networking capabilities, meeting the demands of distributed businesses that require multi-site VPNs.

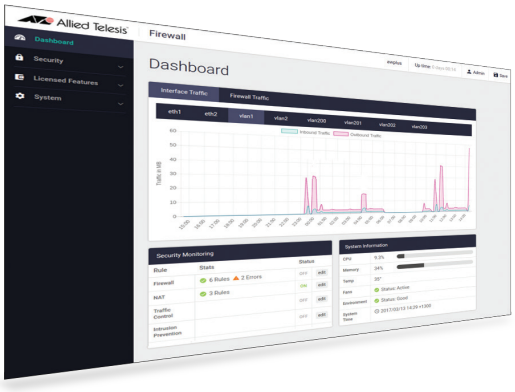
Secure Remote VPNs

The AR1050V supports IPSec site-to-site VPNs for connecting branch offices to a central office, providing employees company-wide with consistent access to the corporate network.

Performance	
Firewall throughput	480 Mbps
Concurrent sessions	100,000
New sessions per second	3,600
IPS throughput	135 Mbps
VPN throughput	180 Mbps

Easy to manage

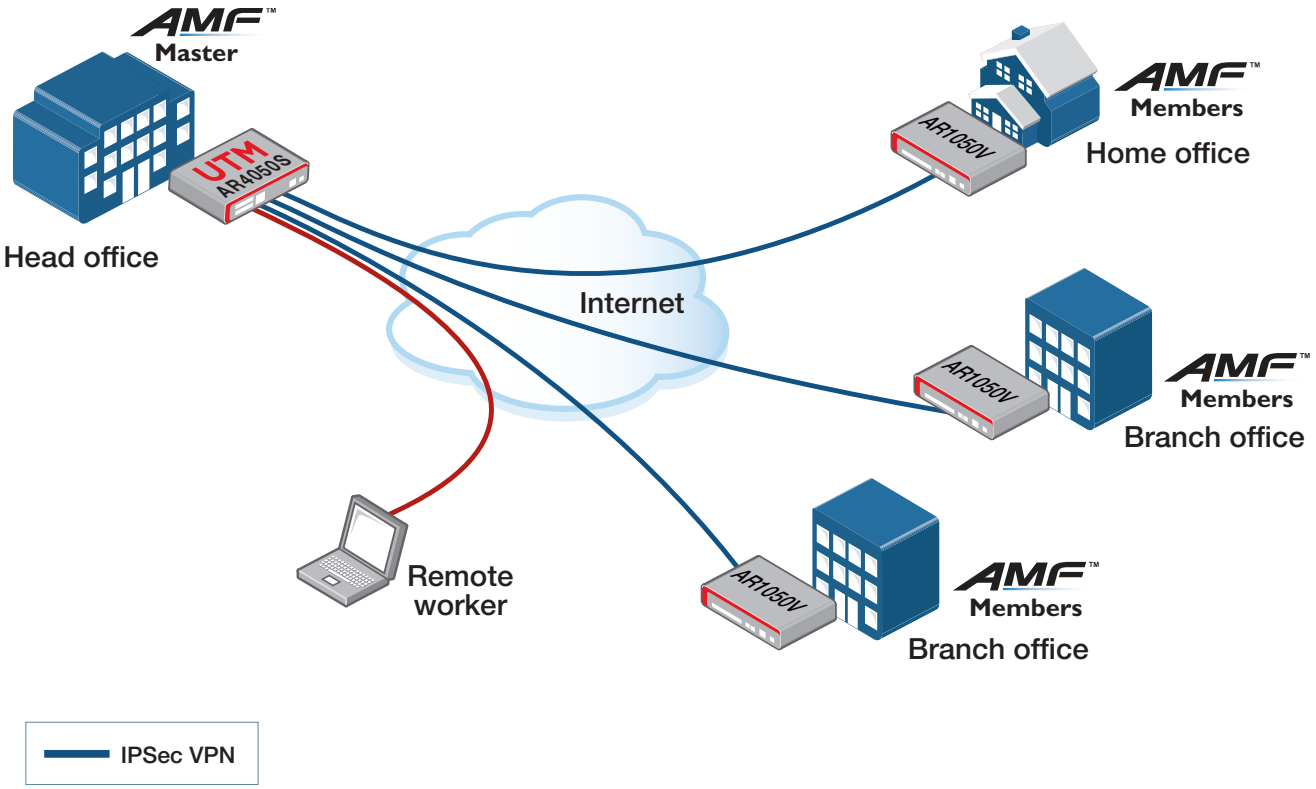
The AR1050V runs the advanced AlliedWare Plus™ fully featured operating system, with an industry standard CLI. The Graphical User Interface (GUI) includes wizards for easy Internet connectivity and VPN creation, while the dashboard enables monitoring of traffic throughput and security status. Configuration of security zones, networks and hosts, and rules to limit and manage traffic, provides a consistent approach to policy management.



FIREWALL ENGINE	
Intrusion Detection and Prevention System (IDS/IPS)	IDS/IPS provides monitoring, analysis and logging of suspicious events that occur on a network. It can also perform a variety of actions to prevent attacks.
URL filtering	Enables HTTP or HTTPS access to particular websites to be allowed (whitelist) or blocked (blacklist) with user-defined lists.
VIRTUAL PRIVATE NETWORKING (VPN)	
IPSec VPN for site-to-site connectivity	High-performance IPSec VPN allows the AR1050V to connect branch offices and other large sites, for secure sharing of business information.
SSL/TLS VPN for secure remote access	Users simply utilize the OpenVPN client on their computer, tablet, or other mobile device for easy access to email, files, and other corporate digital resources when away from the office.
VPN pass-through	Pass-through enables VPN clients to make outbound connections using L2TP, PPTP or IPsec.
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.
NETWORKING	
IPv6 support	Full support for IPv6 routing, multicasting and security is provided.
IPv6 transition technologies	DS (Dual Stack) Lite, Lightweight 4over6, and MAP-E support connecting IPv4 networks over an IPv6 Internet connection.
Autonomous Management Framework (AMF)	AMF enables new devices to be pre-provisioned for zero-touch deployment. This simplifies installation, guarantees consistent configuration, and reduces setup time and cost.
AMF backup/recovery	As an AMF member, the AR1050V is automatically backed up, and can be recovered with plug-and-play simplicity.
Flexible deployment options	The AR1050V can be deployed in traditional NAT, Wire Mode and Network Tap modes.
3G/4G/LTE USB modem[1]	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 available.

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

Key solution



Multi-site VPN connectivity

Allied Telesis Secure VPN Routers are the ideal integrated security platform for modern businesses. The powerful combination of VPN connectivity, secure remote access, and routing and switching, provides a single platform to connect and protect corporate data.

This example shows how the AR1050V can provide multisite connectivity back to a head office. IPSec VPNs to an Allied Telesis Unified Threat Management (UTM) Firewall ensure that all staff have full access to digital resources.

Automated network management

In addition to protecting and connecting modern networks, the AR1050V is fully supported by AMF.

Autonomous Management Framework (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.

As part of an AMF network, along with all of the network switches, the UTM Firewall and VPN Routers are automatically backed up, ensuring seamless recovery if required.

Features

Firewall

- Multi zone firewall
- Application Layer Gateway (ALG) for FTP, SIP and TFTP
- Bandwidth limiting control
- Firewall session limiting per user or entity (zone, network, host)
- Bridging between LAN and WAN interfaces
- Intrusion Detection and Prevention System (IDS/IPS)
- User-defined URL blacklists and whitelists (block or allow HTTP and HTTPS access to specific Websites)
- DoS and DDoS attack detection and protection
- Static NAT (port forwarding), double NAT and subnet-based NAT
- Masquerading (outbound NAT)
- Enhanced NAT (static and dynamic)
- Security for IPv6 traffic

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
- Policy-based routing
- 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
- Web-based GUI for device configuration and monitoring, with easy-start wizards for Internet connectivity and VPN creation.
- Industry-standard CLI with context-sensitive help
- Role-based administration with multiple CLI security levels
- Built-in text editor and powerful CLI scripting engine
- Comprehensive SNMPv2c/v3 support for standards-based device management
- Event-based triggers allow user-defined scripts to be executed upon selected system events
- Comprehensive logging to local memory and syslog
- Console management port on the front panel for ease of access
- USB interface allows software release files, configurations and other files to be stored for backup and distribution to other devices

Diagnostic Tools

- Automatic link flap detection and port shutdown
- Ping polling for IPv4 and IPv6
- TraceRoute for IPv4 and IPv6

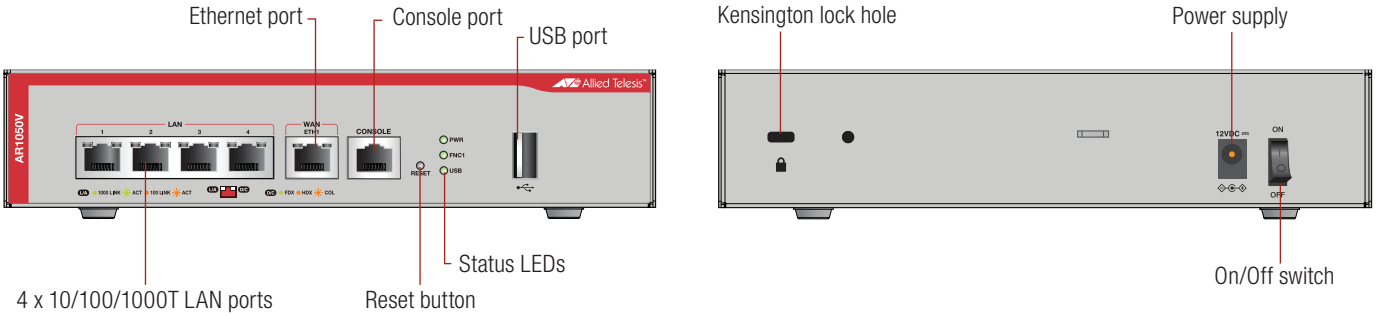
Authentication

- Strong password security and encryption

VPN Tunneling

- Diffie-Hellman key exchange
- Secure encryption algorithms: AES and 3DES
- Secure authentication: SHA-1, SHA-256, SHA-512
- IKEv2 key management
- IPsec Dead Peer Detection (DPD)
- IPsec NAT traversal
- IPsec VPN for site-to-site connectivity
- VPN pass-through
- Redundant VPN gateway
- IPv6 tunneling

AR1050V SECURE VPN ROUTER



Specifications

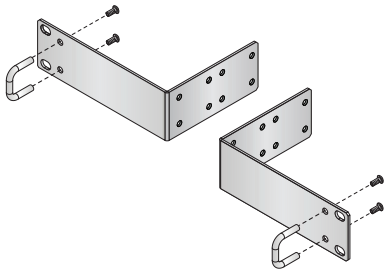
	AR1050V
Processor & memory	
Security processor	1GHz single-core
Memory (RAM)	512MB
Memory (Flash)	128MB
Security features	
Application proxies	FTP, TFTP, SIP
Threat protection	Intrusion Detection/Prevention (IDS/IPS) (Suricata basic rules)
Tunneling & encryption	
IPsec site-to-site VPN tunnels	30 (Recommended)
Encrypted VPN	IPsec, SHA-1, SHA-256, IKEv2
Encryption	3DES, AES-128, AES-192, AES-256
Key exchange	Diffie-Hellman groups 2, 5, 14, 15, 16, 18
Point to point	Static PPP, L2TPv2 virtual tunnels
Management & authentication	
Logging & notifications	Syslog & Syslog v6, SNMPv2 & v3
User interfaces	Scriptable industry-standard CLI, Web-based GUI
Secure management	SSHv1/v2, strong passwords
Management tools	Allied Telesis Autonomous Management Framework™ (AMF) Vista Manager EX
User authentication	Internal user database
Networking	
Routing (IPv4)	Static
Routing (IPv6)	Static
IP address management	Static v4/v6, DHCP v4/v6 (server, relay, client), PPPoE
NAT	Static, IPsec traversal, Dynamic NAPT
Reliability features	
	Modular AlliedWare Plus operating system SNMP traps alert network managers of any issues
Hardware characteristics	
Input power	90 to 264V AC, 47 to 63Hz
Max power consumption	13 Watts
LAN ports	4 x 10/100/1000T RJ-45
WAN ports	1 x 10/100/1000T RJ-45
Other ports	1 x USB, 1 x RJ-45 console
Product dimensions (H x W x D)	44 mm (1.73 in) x 210 mm (8.26 in) x 210 mm (8.26 in)
Packaged dimensions (H x W x D)	109 mm (4.29 in) x 265 mm (10.43 in) x 256 mm (10.08 in)
Product weight	1.3 kg (2.87 lb) unpackaged, 1.9 kg (4.19 lb) packaged
Fanless	Silent operation
Environmental specifications	
Operating temperature range	0°C - 40°C (32°F – 104°F)
Storage temperature range	-25°C to 70°C (-13°F - 158°F)
Operating relative humidity range	5% to 90% non-condensing
Storage relative humidity range	5% to 95% non-condensing
Operating altitude	3,000 meters maximum (9,843 ft)

	AR1050V
Regulations and compliances	
EMC	EN55032 class B, FCC class B, VCCI Class B
Immunity	EN55024, EN61000-3-2, EN61000-3-3
Safety Standards	UL62368-1, EN60950-1, CAN/CSA-C22.2 No.60950-1, AS/NZS 60950-1
Safety Certifications	UL, UL EU, CE
Reduction of Hazardous Substances (RoHS)	EU RoHS compliant, China RoHS compliant
IPv6 Ready	Phase 2 (Gold) Logo

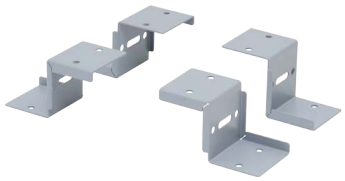
Ordering information

AT-AR1050V-xx
1 x GE WAN and 4 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-J14
Rack mount kit to install one device in a 19-inch equipment rack



AT-RKMT-J22
Wall mount brackets

617-000662 Revi