Compact VPN Firewall

AR2010V

Allied Telesis Virtual Private Network (VPN) Firewalls are the ideal secure gateway for modern network applications. Powerful VPN functionality is combined with comprehensive routing, to provide an innovative high performance solution that is easy to use and very secure.

With the advent of the Internet of Things (IoT) and the development of Smart Cities, connected infrastructure that is easy to install and manage has become a critical requirement.

The Allied Telesis AR2010V is the ideal choice for applications that require reliable, high-capacity data transfer in demanding scenarios—including IP video surveillance, outdoor digital signage, kiosks, remote office VPN back-up, as well as critical Machine-to-Machine (M2M) telemetry in remote or mobile environments.

The AR2010V features comprehensive security and advanced networking capabilities, including connectivity over 3G/4G, to easily meet the high data transmission demands of today's distributed infrastructure networks.

High performance

By harnessing the power of multi-core processors and hardware acceleration engines, the AR2010V guarantees high performance, dramatically increases throughput, and enables sustained low latency traffic inspection. You can enjoy maximum throughput, while still protecting your important data and business information.

Intrusion Detection and Prevention Systems (IDS/IPS)

IDS/IPS is an intrusion detection and prevention system that protects your network from malicious traffic. When using the firewall as a business network gateway, IDS/IPS adds an additional layer of security by monitoring inbound and outbound traffic, and identifying threats which may not be detected by the firewall alone.

Flexible deployment

With its compact size, operation up to 50°C, and the ability to run on AC or DC power, the AR2010V VPN firewall is easy to deploy in all environments, including business, outdoor, surveillance, and M2M telemetry. A DIN rail mounting option supports industrial applications, and silent operation allows use in office spaces.

Secure Remote Virtual Private Networks (VPN)

The firewall supports IPSec site-to-site VPN connectivity, to ensure secure data retrieval from remote locations in distributed Smart City networks that connect multiple devices. This ensures up-to-the-minute information is available, despite long distances and a variety of connected devices, and enhances the quality and interactivity of urban services.

Comprehensive routing support

Strong security features are complemented by advanced routing capability. Full IPv6 routing and protocol implementation ensures today's networks are fully connectable, both internally and externally, with other leading edge equipment. Powerful multicasting features support streaming video, ideal for modern surveillance solutions.

Easy to manage

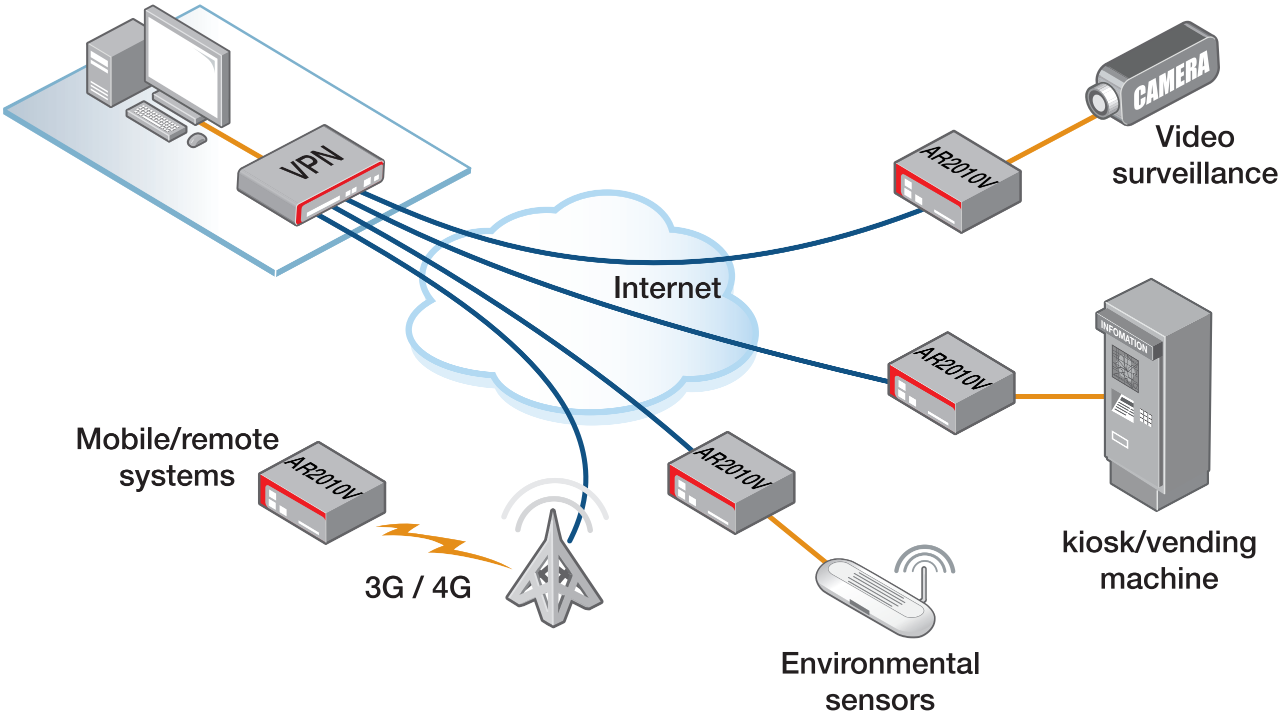
The AR2010V runs the AlliedWare Plus™ fully featured operating system, with an industry standard CLI. The Graphical User Interface (GUI) provides a dashboard for monitoring, showing traffic throughput, security status, and application use at a glance. Configuration of security zones, networks and hosts, and rules to limit and manage traffic, provides a consistent approach to policy management.

Support for Allied Telesis Management Framework™ (AMF) allows the AR2010V VPN Firewall to integrate with Allied Telesis switching products to from a network able to be managed as a single virtual entity. A powerful 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 connectivity and services.

Performance	
Firewall throughput	750 Mbps
Concurrent sessions	100,000
New sessions per second	3,600
IPS throughput	200 Mbps
VPN throughput	400 Mbps

DPI FIREWALL ENGINE	
Bidirectional inspection engine	All traffic flowing in and out of the firewall is inspected and categorized, so it can be managed in line with business policies.
DoS attack protection	Protection against Denial of Service (DoS) attacks, which are designed to consume resources and therefore deny users network and application access.
Intrusion Detection & Prevention (IDS/IPS)	An Intrusion Detection and Prevention System (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 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 Allied Telesis AR2010V 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.
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 all VPN sessions.
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.
QUALITY OF SERVICE (QOS)	
Traffic control	Traffic control allows the amount of bandwidth to be restricted for different traffic classes. RED curves can be defined to predictably drop traffic if congestion occurs.
Bandwidth management	Protect your business-critical traffic by limiting the bandwidth available to non-essential traffic. During peak times, the non-essential traffic will be limited allowing the critical traffic through unhindered.
NETWORKING	
3G/4G/LTE USB modem	The 3G/4G/LTE modem offers an additional secure data connection for critical services that can automatically switch to a 3G network whenever a primary data connection becomes unavailable.
Layer 2 Tunnelling Protocol (L2TP)	L2TP provides site-to-site connectivity, which can also be protected by IPSec encryption.
IPv6 support	Full support for IPv6 routing, multicasting and security is provided.
Dual Stack	Dual Stack enables IPv4 and IPv6 traffic to be processed simultaneously.
Policy-based routing	Policy-based routing enables traffic forwarding decisions to be based on where the traffic is coming from, rather than where it is going to.
AMF management	AMF enables new devices to be pre-provisioned for zero-touch deployment. This simplifies installation and guarantees a consistent configuration reducing setup time and cost.
Flexible deployment options	The Allied Telesis AR2010V can be deployed in traditional NAT, Layer 2 Bridge, Wire Mode and Network Tap modes.
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.

Key Solution



Secure connectivity for remote infrastructure

All over the world, smart cities are looking to increase information availability, security, and transport efficiency, while still reducing pollution and waste. Access to real-time data from a variety of sources gives cities the ability to enhance the quality of urban services, while increasing the safety of citizens.

The AR2010V is the ideal solution for applications with data sensors in remote locations, including traffic monitoring systems, video surveillance, flood and pollution sensors, and industrial telemetry systems. In addition, the compact and easy to install AR2010V is ideal for M2M communication—such as kiosks, vending and gaming machines, weather stations, and 3G/4G connectivity for mobile applications.

The above solution shows how a network of AR2010V firewalls can provide connectivity for a number of different types of remote devices. A compact chassis, wide operating temperature, plus AC and DC power options, make the AR2010V easy to deploy in multiple locations.

With Allied Telesis Management Framework (AMF), private or public cloud-based management of the entire network makes keeping the environment secure and up to date simple. Centralized control, automated provisioning, back-up, upgrade and replacement all ensure simplified management for large distributed networks.

Features

Firewall

- Multi zone firewall with bidirectional inspection engine
- Application Layer Gateway (ALG) for FTP, TFTP and SIP
- Application layer proxies for SMTP and HTTP
- Bandwidth limiting control
- Firewall session limiting per user
- Bridging between LAN and WAN interfaces
- Intrusion Detection and Prevention System (IDS/IPS)
- User-defined URL filtering
- DoS and DDoS attack detection and protection
- Maximum and guaranteed bandwidth control
- Per-host session limits
- Static NAT (port forwarding)
- 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
- 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 route redistribution (OSPF, BGP, RIP)
- Virtual Routing and Forwarding (VRF-Lite)
- Traffic control for bandwidth shaping and congestion avoidance
- Policy-based routing
- PPPoE client with PADT support
- 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
- 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

- Policy-based storm protection

Diagnostic tools

- Ping polling for IPv4 and IPv6
- Port mirroring
- TraceRoute for IPv4 and IPv6

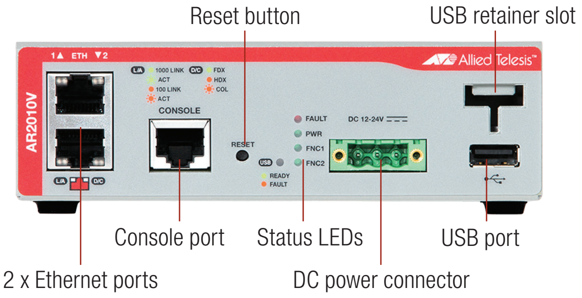
Authentication

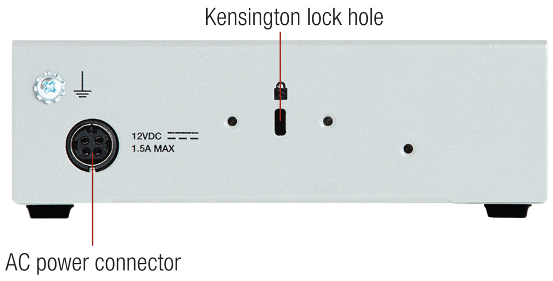
- RADIUS authentication and accounting
- TACACS+ Authentication, Accounting and Authorization (AAA)
- Local or server-based RADIUS user database
- Strong password security and encryption

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
- Dynamic routing through VPN tunnels (RIP, OSPF, BGP)
- Generic Routing Encapsulation (GRE) over IPv6
- L2TPv2 virtual tunnels
- Redundant VPN gateway
- SSL/TLS VPN for secure remote access

AR2010V VPN FIREWALL

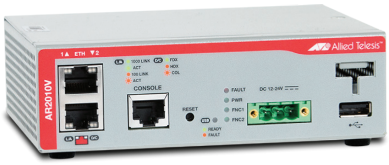




Specifications

	AR2010V
Processor & memory	
Security processor	800MHz dual-core
Memory (RAM)	512MB
Memory (Flash)	4GB
Security features	
Firewall	Stateful multi-zone packet inspection firewall
Application proxies	FTP, TFTP, SIP
Threat protection	DoS attacks, fragmented & malformed packets, blended threats & more
Tunneling & encryption	
IPsec site-to-site VPN tunnels	50
SSL VPN users	100
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 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, SNMPv2 & v3
User interfaces	Scriptable industry-standard CLI, Web-based GUI
Secure management	SSHv1/v2, strong passwords
Management	Allied Telesis Management Framework™ (AMF)
User authentication	RADIUS, TACACS+, internal user database
Command authorization	TACACS+ AAA (Authentication, Accounting and Authorization)
Networking	
Routing (IPv4)	Static, Dynamic (BGP4, OSPF, RIPv1/v2), source-based routing, VRF-Lite
Routing (IPv6)	Static, Dynamic (BGP4+, OSPFv3, RIPng)
Multicasting	IGMPv1/v2/v3, PIM-SM, PIM-DM, PIM-SSM, PIMv6
Resiliency	STP, RSTP
Traffic control	8 priority queues, DiffServ, HTB scheduling, RED curves
Quality of Service (QoS)	Premarking and remarking, taildrop queue congestion, strict priority, weighted round robin or mixed scheduling
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 Full environmental monitoring of temperature and internal voltages. SNMP traps alert network managers in case of any failure

	AR2010V
Hardware characteristics	
Rated input voltage	DC12-24V AC100-240V (with AC adapter)
Max power consumption	13 watts
LAN port	1 x 10/100/1000 RJ-45
WAN port	1 x 10/100/1000T RJ-45
Other ports	1 x USB, 1 x RJ-45 console
Product dimensions (H x W x D)	42.5mm (1.67 in) x 140mm (5.51 in) x 105mm (4.13 in)
Product weight	556 grams (1.2 lb)
Fanless	Silent operation
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-AR2010V-xx
2 x 10/100/1000T RJ-45

AT-DRMT-J02
Din rail mount kit

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

3G/4G USB Modems

For a list of supported USB modems visit
http://alliedtelesis.com/securityapps/AR2010V

Allied Telesis | NETWORK SMARTER