AlliedWare Plus™

UTM FIREWALL OVERVIEW

Allied Telesis Unified Threat Management (UTM) Firewalls provide advanced threat protection in a fully integrated security solution for today's networks.

AMF™ **Allied**Ware Plus™ OPERATING SYSTEM

The AlliedWare Plus Operating System from Allied Telesis is well proven on our advanced switching platforms. It provides a fully-featured network infrastructure experience, for powerful customer solutions.

The new range of Allied Telesis UTM Firewalls have an integrated architecture built on AlliedWare Plus, bringing its verified and superior operation to the security needs of today's networks. As well as Allied Telesis' industry leading key features, our UTM Firewalls utilize best of breed security providers, for up-to-the-minute protection from all known threats.

A fully integrated solution

Today's online experience revolves around applications, content, and user interaction. As network access has advanced, cyber threats have become more sophisticated.Targeted and tailored attacks are increasingly beating established defenses. Traditional routers and firewalls are no longer capable of protecting Enterprise networks from the host of external and internal threats that endanger corporate security.

To meet these challenges, a new breed of products have consolidated threat management capabilities into a single device to increase the security of business communications. Multiple threat detection and protection capabilities are now integrated within a purpose-built solution that provides protection for all network traffic.

Complete network security

Comprehensive application and content identification provides visibility into network activity, to allow intelligent control of network traffic. This visibility and control, partnered with advanced threat protection, together provide comprehensive online security for Enterprise businesses. With Allied Telesis advanced routing functionality, powerful VPN capabilities for remote access, and a cohesive single-pane-of-glass management console, our UTM Firewalls are a complete network security solution.

Key features

Sophisticated application and web control
- » Deep Packet Inspection (DPI) firewall
- » Application control
- » Web control
- » URL filtering

Comprehensive threat protection
- » Intrusion Detection/Prevention System (IDS/IPS)
- » IP reputation services
- » Malware protection
- » Anti-virus

Advanced user connectivity
- » Secure remote VPN access
- » Site-to-site VPN connectivity
- » Advanced routing capabilities
- » Resilient WAN connectivity

Powerful centralized management
- » Management and monitoring
- » Allied Telesis Autonomous Management Framework™ (AMF)
- » Flexible licensing options

Key features

Sophisticated application and web control

The Internet has evolved immensely. Whereas once it simply provided pages to be browsed, it now offers applications that enable people to interact, with Web 2.0 services such as collaborative document creation, social networking, video conferencing, cloud-based storage, banking and much more.

Organizations must be able to control the applications that their people use, and how they use them, as well as managing website traffic. Allied Telesis UTM Firewalls provide the visibility and control that are necessary to safely navigate the increase in online applications and web traffic that are used for effective business today.

Deep Packet Inspection (DPI) firewall

The AlliedWare Plus firewall is a Deep Packet Inspection (DPI) engine that provides real-time, Layer 7 classification of network traffic. It inspects every packet that passes through, and accurately identifies in use applications, for example social networking, instant messaging, file sharing, and streaming, whilst still maximizing throughput and reducing latency.

The AlliedWare Plus DPI firewall utilizes Procera Networks' Network Application Visibility Library (NAVL) to identify thousands of individual applications. Highly accurate real-time detection, and up-to-the-minute classification additions and updates, ensure precise identification of network traffic.

The AlliedWare Plus DPI firewall also supports filtering based on hierarchical entities, such as zones (logical groupings of networks), networks and hosts, to empower organizations to accurately apply and manage security policies at company, department or individual level.

Application control

The increased network visibility provided by the application-aware firewall allows fine-grained application, content and user control. Reliable identification of the individual applications means that rules can be established to govern not only which are allowed, but under what circumstances, and by whom. This allows Enterprises to differentiate business-critical from non-critical applications, and to enforce security and acceptable use policies in ways that make sense for the business. For example, Skype chat may be allowed company wide, while Skype video calls can only be made by sales and marketing.

Application control

Sales and Marketing Department

Other Departments

Internet
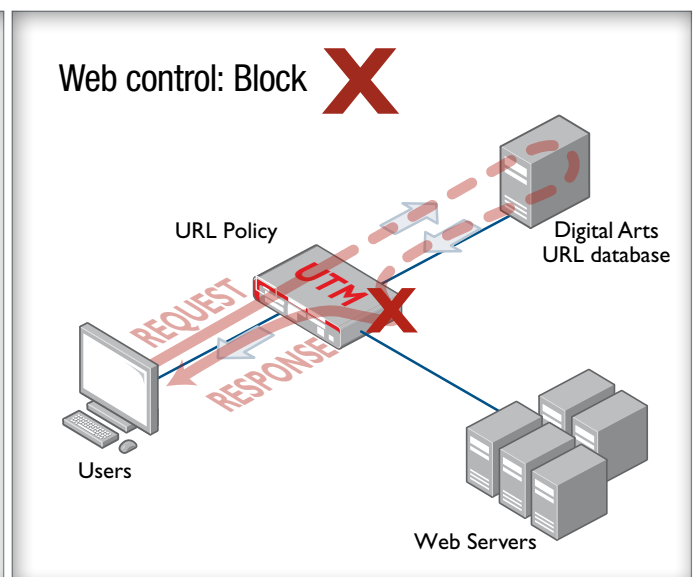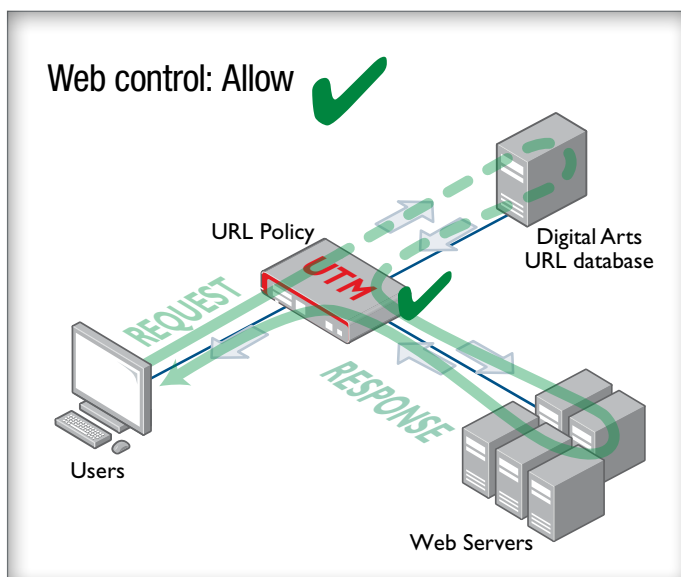
ALLOWED

BLOCKED

UTM Firewall
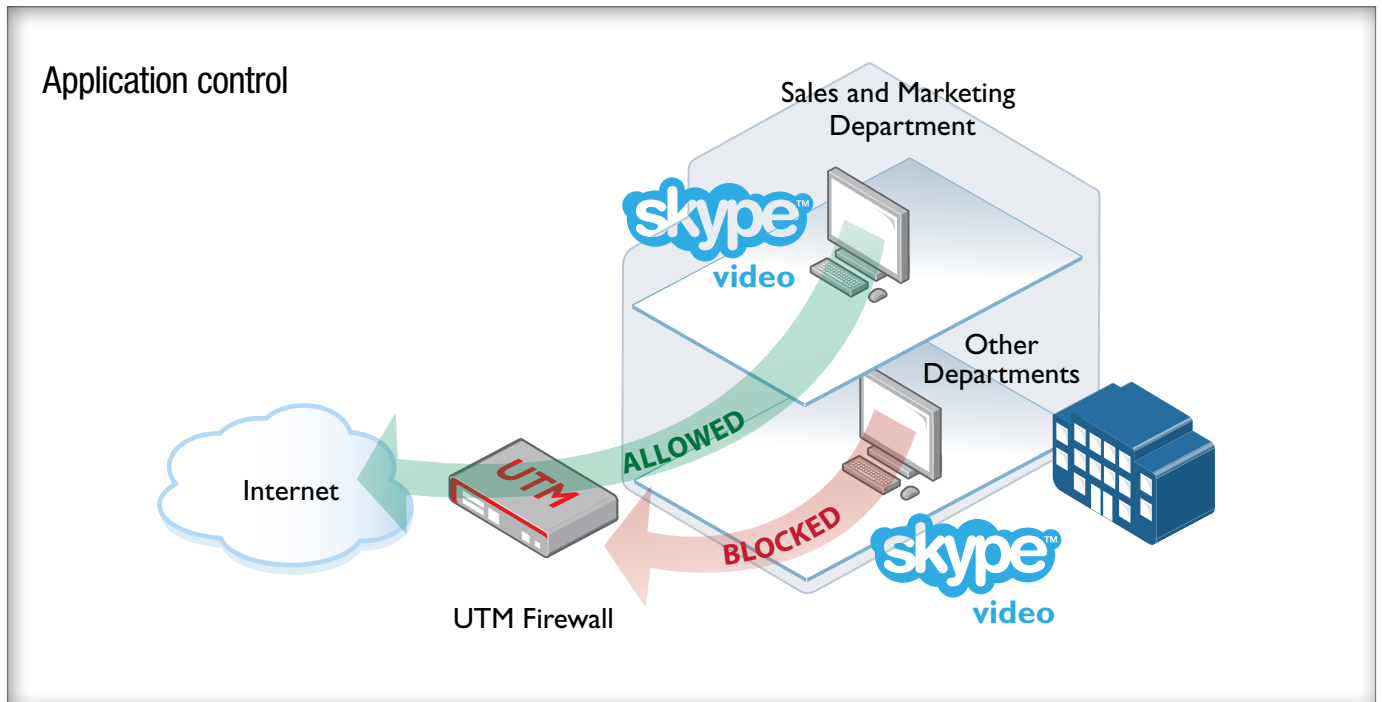
Web control

Web control provides Enterprises with an easy means to monitor and control their employees' web traffic for productivity, legal and security purposes. Utilizing Digital Arts' active rating system, AlliedWare Plus web control provides comprehensive and dynamic URL coverage, accurately assigning websites or pages into around 100 categories, and allowing or blocking website access in real-time.

Once a particular URL has been categorized, the result is cached in the firewall so that any subsequent web requests with the same URL can be immediately processed according to the policy in place.

Allied Telesis web control boosts user productivity, ensures compliance, and saves bandwidth, while preventing web-based threats from infecting your business.

Web control: Allow

URL Policy

Digital Arts URL database

REQUEST

RESPONSE

Users

Web Servers

Web control: Block

URL Policy

Digital Arts URL database

REQUEST

RESPONSE

Users

Web Servers

URL filtering

Alongside web control, URL filtering provides another option for controlling web traffic. HTTP or HTTPS access to particular websites can be allowed (whitelist) or blocked (blacklist) with user-defined lists, providing businesses with simple website access management.

A subscription service can also be employed, utilizing a frequently updated comprehensive blacklist from industry leading security vendor Kaspersky.

URL filtering offers high-performance website control across all users, and protection against known malicious websites.

Comprehensive threat protection

The fundamental shift to sophisticated application usage has provided an online experience that businesses can greatly profit from. There is now increased efficiency, improved collaboration, along with new ways to manage customer interaction. However, this has also opened the door for greater security concerns. Business data is potentially vulnerable, and the rapid development of new services has introduced new types of cyber threats.

An organization needs a security solution that can recognize and mitigate the ever-increasing range of threats. Allied Telesis UTM Firewalls provide comprehensive threat protection in a fully integrated security platform, using specialized multi-core CPUs optimized for single-pass low-latency performance. They utilize security engines, and threat signature databases from the industry's leading vendors, with regular updates to ensure up-to-the-minute protection against cyber attacks.
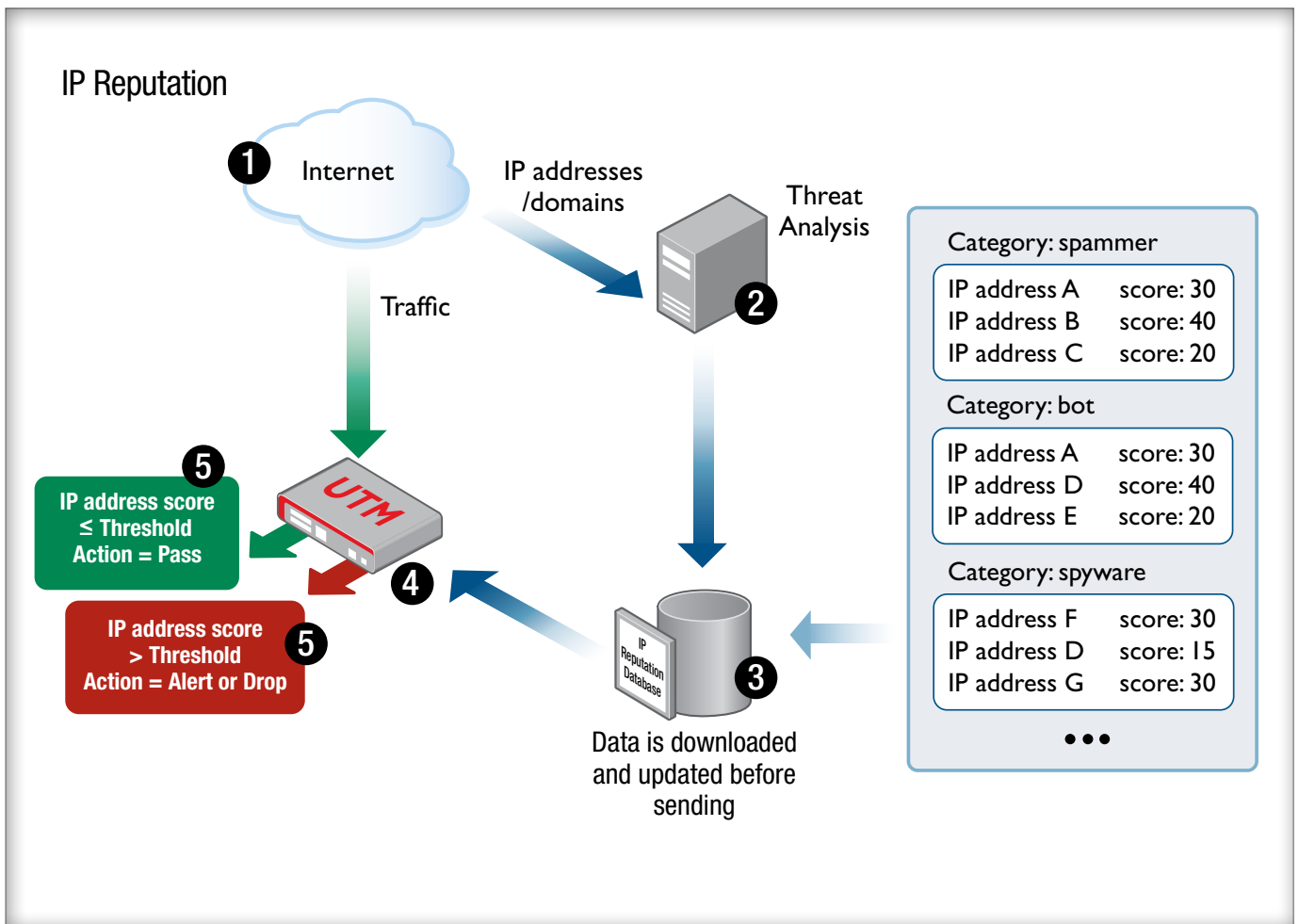
Intrusion Detection/Prevention System (IDS/IPS)

The AlliedWare Plus IDS/IPS protects businesses from attack through extensive threat coverage. IDS/IPS inspects inbound and outbound traffic; identifies and logs suspicious network activity; and proactively counteracts malicious threats. The Suricata high performance IDS/IPS engine monitors real-time network traffic and detects malicious activity by comparing threats against an IDS known threat signature database.

IP reputation

IP reputation improves the success of Intrusion Prevention by reducing false positives. It provides an extra variable to the prevention decision, which allows rules to be crafted to drop packets only if the reputation exceeds a chosen threshold.

AlliedWare Plus IP Reputation provides comprehensive IP reputation lists through Emerging Threats' ET Intelligence, which identifies and categorizes IP addresses that are sources of spam, viruses and other malicious activity. With real-time threat analysis, and regular updates to reputation lists, IP Reputation delivers accurate and robust scoring, ensuring strong local policies can be carried out with surgical precision.

IP Reputation

1 Internet

IP addresses /domains

Threat Analysis **2**

Traffic

5

UTM

IP address score ≤ Threshold Action = Pass

4

IP address score > Threshold Action = Alert or Drop **5**

3

IP Reputation Database

Data is downloaded and updated before sending

Category: spammer

IP address A	score: 30
IP address B	score: 40
IP address C	score: 20

Category: bot

IP address A	score: 30
IP address D	score: 40
IP address E	score: 20

Category: spyware

IP address F	score: 30
IP address D	score: 15
IP address G	score: 30

● ● ●

POWERED BY KASPERSKY

Malware protection

AlliedWare Plus uses stream-based high performance anti-malware technology to protect against the most dangerous cyber threats. By considering threat characteristics and patterns with heuristics analysis, unknown zero-day attacks can be prevented, along with server-side malware, web-borne malware, and other attack types. Detection covers all types of traffic including web, email and instant messaging.

The Kaspersky anti-malware signature database is updated regularly to keep on top of the latest attack mechanisms, to bring leading threat protection to modern business networks.

Antivirus

Proxy-based antivirus provides the first line of defense against a wide range of malicious content, guarding against threats, such as viruses, Trojans, worms, spyware and adware. In addition to protecting the local network by blocking threats in inbound traffic, it also prevents compromised hosts or malicious users from launching attacks. This is essential for protecting business reputation, and minimizing business disruption.

Using the Kaspersky Anti-Virus engine, the signature database containing known threat patterns is regularly updated. Scans performed on web traffic protect network users and devices.

Advanced user connectivity

Allied Telesis UTM Firewalls are a powerful and fully integrated solution that inspect and protect business data to ensure a secure online experience. Furthermore, they also provide comprehensive user connectivity through remote Virtual Private Network (VPN) access, advanced routing capabilities for Internet gateway applications, and powerful resiliency features for "always-on" Internet connectivity.

This broad and comprehensive feature set makes our firewalls a complete integrated solution for secure Internet connectivity.

Secure remote VPN access
Allied Telesis UTM Firewalls provide secure remote access, so employees can utilize all their business resources whether they are physically inside or outside their company premises. Staff members have the ability to work securely from remote locations.

An SSL VPN creates a secure tunnel over the untrusted and insecure Internet, by encrypting traffic. Users simply utilize the OpenVPN client on their computer, tablet or other mobile device. SSL VPNs are compatible with the security policies of almost all network installations, making them an ideal option for travelling staff that may need to connect to the corporate network from a variety of public-space networks.

Site-to-site VPN connectivity
An IPsec site-to-site VPN can securely connect one or more branch offices to a central office, which saves the cost of expensive leased lines, and provides workers company-wide with the same access to the corporate network.

Head office

Remote worker

UTM

3G/4G backup

Internet

Branch office

SSL VPN
IPSec VPN
LAN
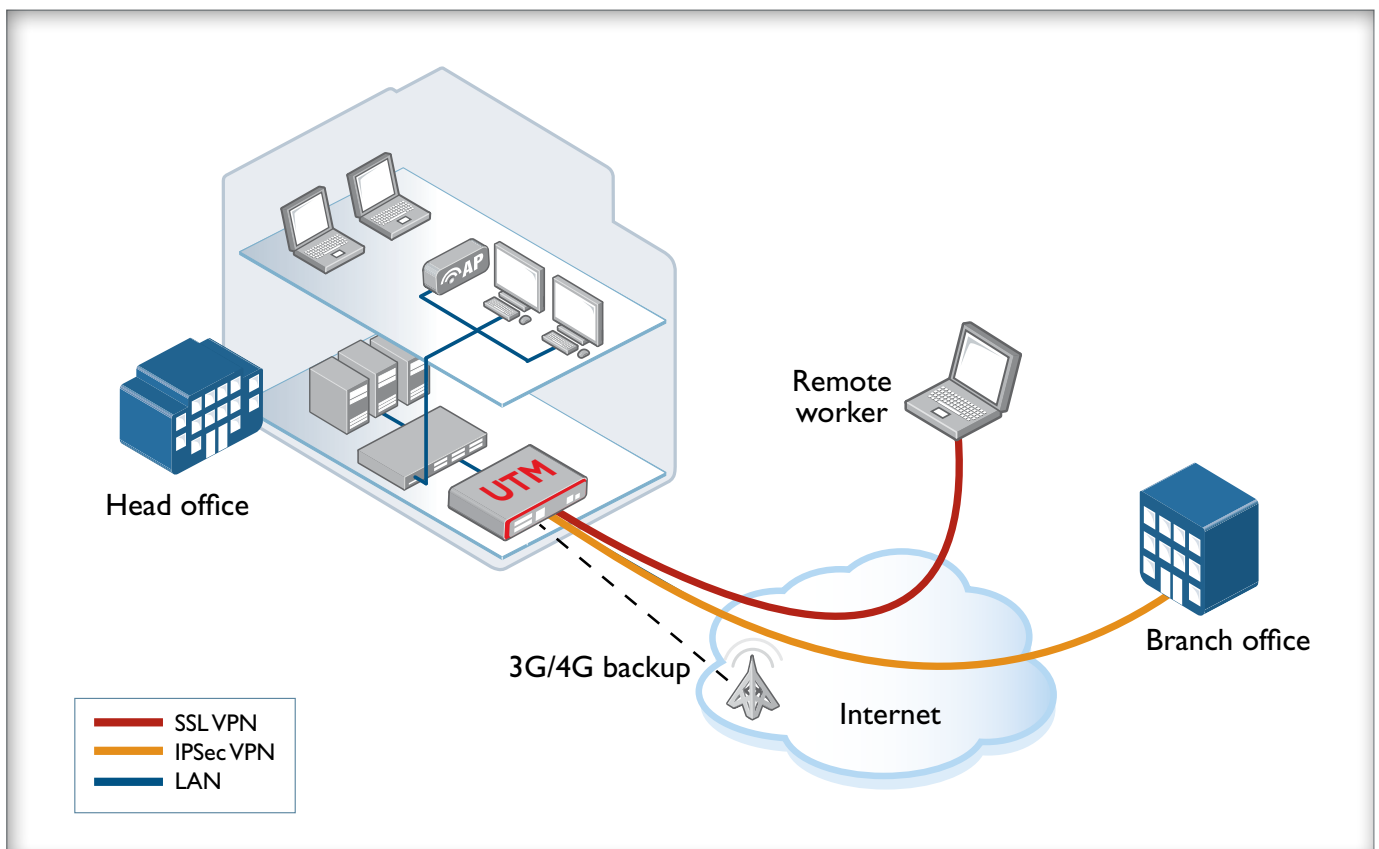
Advanced routing capabilities

Allied Telesis integrated security platforms include advanced routing and switching capabilities. With support for dynamic routing protocols, and business WAN connectivity, the firewalls provide a single-box platform for connecting and protecting modern Enterprise data communications. Comprehensive routing capability includes full IPv4/IPv6 unicast and multicast support, VRF-Lite, traffic shaping, email proxy, application layer gateways and more.

By concentrating all the security and connectivity operations into a single device, modern businesses gain all of the performance, support, and value of a fully integrated solution from a single vendor .

Resilient WAN connectivity

The UTM Firewalls have a high-availability bypass port, which allows device redundancy with only a single WAN link, reducing ongoing ISP fees. If the Master firewall loses power, traffic is automatically forwarded to the backup device, keeping Enterprises online and connected to their business partners and customers.

Powerful centralized management

Allied Telesis UTM Firewalls provide a full suite of security and connectivity features, that work cohesively to protect business networks and users. As well as visual dashboard monitoring and response, our firewalls also support fully automated configuration, backup and recovery, to ensure Enterprise businesses are never without connection to their online resources and applications.

Management and monitoring

The firewalls provide an industry standard Command Line Interface (CLI), and a Graphical User Interface (GUI).

The 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.
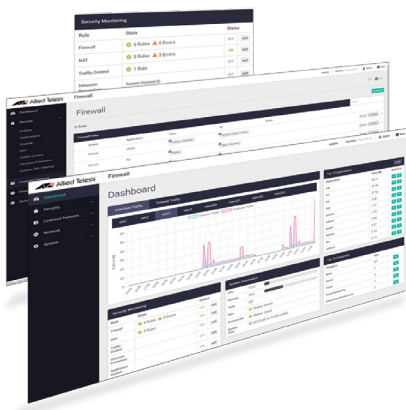
Allied Telesis Autonomous Management Framework (AMF)

Allied Telesis Autonomous Management Framework (AMF) is a sophisticated suite of management tools that provide a simplified approach to network management. Common tasks are automated and every-day running of the network made extremely simple. Powerful features like centralized management, auto-backup, auto-upgrade, auto-provisioning and auto-recovery, enable plug-and-play networking and zero-touch management.

Allied Telesis UTM Firewalls support AMF, so they can integrate with our switching products to form a network able to be managed as a single virtual device. A full suite of automated tools ensure that the firewall configuration is backed up, and able to be recovered with no user intervention, maximizing availability of online services.

Flexible licensing options

The Allied Telesis integrated security platforms utilize best-of-breed security providers for the ultimate in up-to-the-minute protection from all known threats. Flexible licensing options make it easy to choose the right combination of firewall and Intrusion Detection/Protection security features to best meet your business security needs.

Allied Telesis UTM Firewall products

The Allied Telesis AR3050S and AR4050S combine firewall and threat protection with routing and switching in a single, high-performance integrated security platform. An ideal choice for high-speed Internet gateway applications, the Allied Telesis integrated security platforms meet the needs of modern Enterprise networks.

For product datasheets, and more information, visit us online at:
alliedtelesis.com/products/securityapps

PERFORMANCE LIMITS	AR3050S	AR4050S
	Dual core 800Mhz CPU, 1Gb RAM	Quad core 1.5Ghz CPU, 2Gb RAM
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
Site-to-site VPN tunnels (IPsec)	50	200
Client-to-site VPN tunnels (OpenVPN)	100	1000

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

AlliedWare Plus UTM Firewall features

FEATURES	DESCRIPTION	AR3050S	AR4050S
FORM FACTOR		Desktop / rackmount	Desktop / rackmount
WAN PORTS	10/100/1000T	2 combo	2 combo
	1000X (SFP)	2 combo	2 combo
	WAN bypass	2	2
LAN PORTS	10/100/1000T	8	8
MEDIA SUPPORT	USB port	1	1
	SDHC slot	1	1
POWER SUPPLY		Fixed internal	Fixed internal
ENVIRONMENTAL	Temperature range	0C to 45C	0C to 45C
	Cooling	Speed controlled fan	Speed controlled fan
PERFORMANCE	CPU	Dual-core 800MHz	Quad-core 1.5GHz
	RAM	1 GB	2 GB
	Throughput	See previous table	
MANAGEMENT	Console port	RJ-45	RJ-45
	Web-based GUI	■	■
	CLI	■	■
	SNMP	■	■
	Telnet / SSH	■	■
	AMF	■	■
NETWORK RESILIENCE	VRRP and VRRPv3	■	■
	Spanning Tree	■	■
THREAT PROTECTION	Anti-virus		■
	Anti-malware	■	■
	IDS/IPS	■	■
	IP reputation	■	■
	Automatic threat updates	■	■
SECURITY	IEEE 802.1Q VLANs	■	■
	RADIUS / TACACS+	■	■
	Command authorisation	■	■
FIREWALL	DPI firewall	■	■
	Application control	■	■
	Web control	■	■
	Traffic shaping	■	■
	DMZ	■	■
	Port forwarding	■	■
	Dynamic NAPT	■	■

FEATURES	DESCRIPTION	AR3050S	AR4050S
TUNNELLING	IPsec site-to-site VPN	■	■
	SSL VPN	■	■
	L2TPv3	■	■
	GRE	■	■
ROUTING	Static routing	■	■
	RIP and RIPng	■	■
	OSPFv2 and OSPFv3	■	■
	BGP4 and BGP4+	■	■
	IGMP	■	■
	PIMv4 and PIMv6	■	■
	Bridging (LAN / WAN)	■	■
	PPPoE	■	■
	DHCPv4/v6 client, server, relay	■	■
	VRF-Lite	■	■

AlliedWare Plus UTM Firewall Licensing

Security licenses for AlliedWare Plus 5.4.5

LICENSE NAME	INCLUDES	1 YR SUBSCRIPTION	3 YR SUBSCRIPTION	5 YR SUBSCRIPTION
AR3050S				
Advanced Firewall	Application Control Web Control URL Filtering	AT-FL-AR3-NGFW-1YR	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
AR4050S				
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

Allied Telesis™

NETWORK SMARTER