allo.com

UTM
(Unified Threat Manager)

- Intrusion Prevention based Snort 2.9.
- Support for signatures from Snort VRT and Emerging Threat.
- HTTP/SSL Web Proxy based on Squid 3.1.20
- URL Filtering with Internet DB from URLBlacklists.com
- L7 Application Control
- Open vpn based SSLVPN Gateway
- Site-to-Site VPN with IPSec

DESIGNED &
MANUFACTURED IN INDIA

UTM 1.0 Appliances provide the Advanced State full Firewall integrated with L7 Application Control, Intrusion Prevention, SSLVPN, IPSec VPN Web filtering, Users Authentication functionalities.

Firewall

- State full Firewall with connections tracking capabilities
- Dynamic/Static NAT, Port forwarding
- Prevention of DOS, DDOS & IP Spoofing
- Bandwidth control
- Multicast forwarding
- TCP syn cookies
- MAC filtering
- QOS/Diffserv marking
- Content Filtering - Blocking Java/ActiveX/Proxy/Cookies
- L7 Application Control with 70+ protocols support
- Transparent Firewall/Routed Firewall mode
- Use of Policy Objects for Firewall/NAT Policies Configuration
- Support for multiple firewall zones
- Zone based security policies

SSLVPN

- SSLVPN Solution - Access Gateway Mode
- SSLVPN Site-to-Site VPN tunnel support
- Locally managed SSLVPN Client Profiles
- Two factor Authentication enabling Password/Certificates based Authentication for SSLVPN Clients
- Use of Pre shared Keys/Certificates for P2P Authentication
- TCP/UDP Based Tunnels
- AES/DES/BF/CAST5/RC2 Encryption
- Traffic compression
- Tunnel All Traffic mode support on the client side.
- Supporting up to 25 VPN Clients
- Support for Mobile VPN Clients
- Easy to use VPN User Profiles/P2P Policies Configuration

Intrusion Prevention

- Intrusion Prevention enabling both Signature based Detection and Detailed Protocol Decoders.
- Support for Automatic Signature Updates
- Support for Custom Signatures with Intuitive signature configuration wizard
- Supporting the signatures from Emerging threats/Snort VRT

IP Sec

- Tunnel/Transport Mode
- IKE Exchange - Main/Aggressive/Base mode
- DES/3DES/Blowfish/Cast128/AES Encryptio
- MD5/SHA Digest Authentication
- Pre shared Keys/Certificates/Password Authentication
- IKE/Diffe Hellman Group
- AH/ESP Support
- IPSec/PFS Group Support
- Traffic Compression
- Dead Peer Detection

Antivirus

- Onboard ClamAV Engine support
- AV Inspection of Web traffic

Network

- DHCP Server Support per Network Subnet/Vlan
- DNS
- Static routes
- Virtual IP
- DDNS
- VLAN/801.q
- Dual WAN with Wan Failover/Load Balancing (Only Available in SMB Model)
- Firewall zones/port mapping
- PPPoE Support

Web Filtering

- Web filtering with Squid Proxy – Support for URLs/Regular expression based Filtering
- Categories based Filtering with URL Blacklist service
- Users/User Groups based Web filtering Policies
- SSL Proxy
- Explicit/Transparent Proxy mode support
- Limiting Http connections per Network/Users/User Groups
- Filtering based on Web request/response size
- SSL Control
- Digest Based Authentication for locally managed Users
- Web Caching with USB Based Storage
- Localization Support for Web filtering Blocking Pages
- Custom Webfilter Blocking Page support
- External Webproxy support

Device Management

- WebUI accessible via SSL
- SSH CLI access
- NTP
- SNMP v1/v2/v3 support
- Syslog
- Provision to update firmware via WebUI
- Factory Reset
- Diagnostic utilities
- Certificates management for web proxy/SSLVPN/IPSec services

Reports

- Log viewer for accessing Syslog logs/Security Alerts
- Firewall Connections Monitoring
- DHCL Clients Status
- VPN Connections Monitoring
- Graphical reports on System Resources Usage/FW Connections Monitoring/IPS Alerts
- Web filtering Reports
- Bandwidth usage report

Product Models

aUTM - Friewall througput 100Mbps+
aUTM2 - Friewall througput 300Mbps+

Warranty Info

1 Year hardware warranty

Operating Temperature : 10°C to 40 C (50 F to 104 F)
Operating Humidity : 10% to 90%, Non-condensing
Storage Temperature : 0°C to 50°C (32°F to 122°F)
Storage Humidity : 5% to 95%, Non-condensing
Power Input : 05V DC / 2.0 A

allo.com

For more information please contact
Canada: +1 778 892 2877 | andre@allo.com
India: +91 80 67080808

SBC
(Session Border Controller)

SBC is enabled with DPI packet inspection on VoIP traffic, supporting the signatures for key malwares/vulnerabilities observed in SIP deployments like extensions enumeration DoS and password cracking. Supporting open source PBXs like Asterisk™, FreeSwitch™, TrixBox™

Handles the SIP-NAT issues observed in the common VoIP deployments.

DESIGNED &
MANUFACTURED IN INDIA

A Session border controller(SBC) is used to control VoIP signaling and media streams. SBC is responsible for setting up, conducting, and tearing down calls. SBC allows owners to control the types of call that can be placed through the networks and also overcome some of the problems caused by firewalls and NAT for VoIP calls. A common location for a stand-alone SBC is a connection point, called a border, between a private local area network (LAN) and the Internet. SBC polices real-time voice traffic between IP network borders ensuring your private network is robustly secure and fully manageable.

Key Features

- SBC is enabled with DPI packet inspection on VoIP traffic, supporting the signatures for key malwares/vulnerabilities observed in SIP deployments like extensions enumeration DoS and password cracking. Supporting open source PBXs like Asterisk™, FreeSwitch™, TrixBox™.
- Handles the SIP-NAT issues observed in the common VoIP deployments.
- Topology-hiding function is to prevent customers or other service providers from learning details about how the internal network is configured, or how calls being placed through the SBC are routed.

Advanced Features

- Transcoding - SBCs can also allow VoIP calls to be set up between two phones by transcoding of the media stream, when different codecs are in use.
- TLS/SRTP - support for signaling and media encryption.
- Policy-based call routing, including crankback of call setup.

Basic Functions

- Eliminates bad VoIP signaling and media protocol at the network boundary.
- Built-in firewall which can controls IP addresses/port based filtering, DOS/DDOS attacks, IP blacklist & NAT. It opens pinhole in the firewall to allow VoIP signaling and media to pass through.
- Media bridging, which may include voice over IP and Fax over IP.
- Roaming extension for internal SIP PBX.
- Support for SIP outbound/inbound trunk and policies to route the calls.
- DTMF support for RFC2833/INBAND/SIP INFO
- Can handle simultaneous calls from 10 to 60 channels (Including media transcoding and encryption)
- Easy GUI configuration and call statistics.

Pricing Information

Unified Threat Manager

Sl. No.	Description	Reseller Pricing (USD)	MSRP Pricing (USD)
1	ALLO UTM	495	675

Contact Information

Andre Martin Strul
Chief Marketing Officer

Phone: +1 604 800 4363
Toll Free (US/Canada): 1 877 339 ALLO (2556)
Email: wholesales@allo.com andre@allo.com