

# ENDIAN UTM VIRTUAL APPLIANCE





## Endian UTM Virtual Appliance: Secure and Protect your Virtual Infrastructure

Whether you are securing your internal virtual business environment, running a world-class hosting or colocation facility, or providing cloud services - the Endian UTM Virtual Appliance can provide superior network security to protect your virtual infrastructure from any potential threats.

### Simple and Effective

By providing simple and effective network security solutions, Endian helps businesses leverage new virtual and cloud technologies to:

- Secure the entire virtual infrastructure (internally and externally)
- Seamlessly integrate with current virtual platform investments and their management tools
- Save time and effort (i.e. money) with Endian centralized management and support tools
- Securely connect all of the virtual or hosted infrastructure to the main office using VPN
- Monitor and prevent access to and from the virtual systems to the outside world
- Safeguard all inter-VM, internal, and external network connectivity

All of these objectives and more can be achieved using the Virtual Appliance.

### Endian Advantages

The Virtual Appliance offers the most intuitive and universally supported solution available by including things like:

- Support for three major virtual platforms including VMWare, Xen, and KVM
- Unified, intuitive user interface across all platforms - hardware, software, and virtual
- Extremely efficient and scalable resource requirements
- Native support included for available virtual infrastructure toolsets

In addition, you can utilize all of the great features that come with all flavors of the Endian UTM family including centralized management and monitoring via Endian Network, the simplest web interface available, best of breed open-source software, top-notch Endian support and much more.

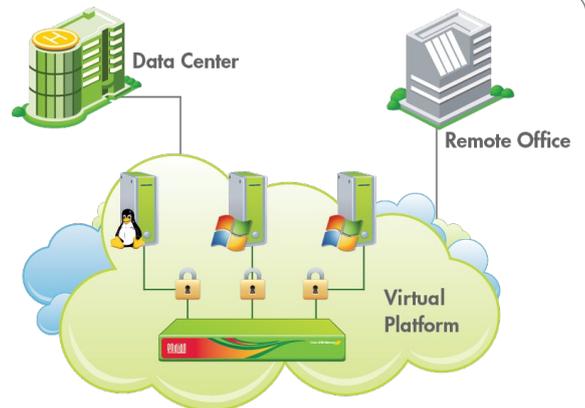
### Flexible Security

Endian offers a wide range of network security products to fit any requirement including hardware, software or virtual solutions. This means you can use the leading open source unified threat management product however and wherever you need.

## Endian UTM Virtual Appliance Use Cases

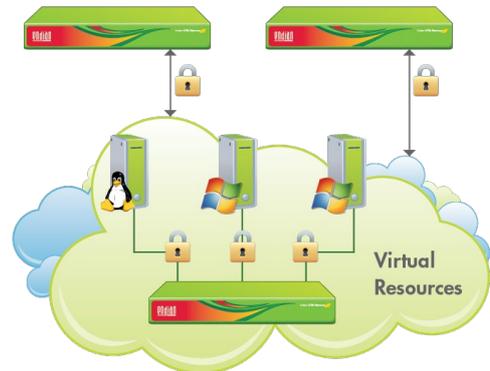
### Protect the Virtual Network

Most virtual networks are not much different from physical networks so the same networking and security principles should be applied. Whether you are running a virtualized platform in the data center or at remote offices, concepts like network separation are critical to safeguard various virtual resources from each other, protect and separate the virtual data and management networks, prevent the spread of malware, and provide containment against hackers and other threats.



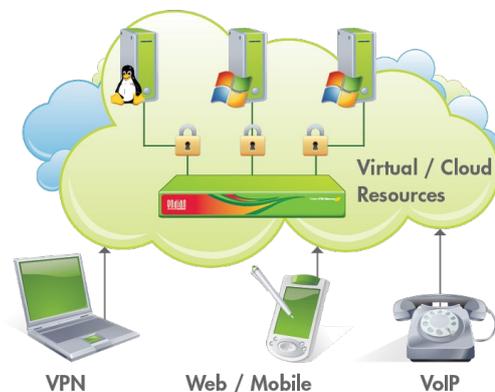
### Secure External Connectivity

All virtual networks require some form of physical connectivity which means you may want to securely connect virtual resources to the outside world. Endian provides this with both IPSec or SSL VPN (OpenVPN) and multiple connectivity options including network-to-network and individual remote access (roadwarrior). Whether you are using virtual platforms to connect remote offices, link up data centers, or just for disaster recovery, Endian has the solution for you.



### Hosted / Cloud Services

If you are providing some form of a hosted or cloud public service then you already recognize how important it is to ensure to your existing and potential customers that you implement maximum security processes and technology. Our virtual solution can enhance any hosted service from simple web and email services to more complex VoIP and VPN configurations. The Virtual Appliance makes securing your virtual platform simple, scalable, and best of all cost-effective.





## Firewall

Protect your network from Internet threats while providing appropriate access to resources inside and outside your network.



## Intrusion Prevention

Protect your virtual resources from malicious attacks, hackers, and most other internal or external threats using our deep packet inspection intrusion prevention system.



## Web Security

Take control over who can surf and where they can go on your network while protecting your employees from web threats. You'll also get peace of mind by retaining complete, historical web reports.



## Email Security

Eliminate spam, phishing, and other malicious email from your network and provide top-notch protection against email-based viruses and other malware.



## VPN (SSL & IPSec)

Whether you need to provide remote access to your employees or connect multiple offices together, we've got a solution that is simple and secure.



## Centralized Management

Centrally manage and support all of your Endian devices from one convenient place. You can one-click update and/or upgrade all your appliances as well as manage your Endian licenses.

## Virtual Appliance Highlights

- Optimized for Virtual Platforms
- VMware Prebuilt Appliance
- Xen Prebuilt Appliance\*
- KVM Prebuilt Appliance
- Centralized Management Included
- Robust Firewall
- IPS with Deep Packet Inspection
- IPSec and SSL VPN (OpenVPN)

\* Citrix XenServer & Xen are supported

## Feature Highlights

- Stateful Firewall
- Intrusion Prevention System
- Web Content & Antivirus Filtering
- Email Spam & Antivirus Filtering
- VPN (IPSec & SSL)
- Centralized Remote Management
- Load Balancing
- Routing (Static & Policy-Based)
- High Availability
- Multi-WAN with Failover
- Quality of Service (QoS)
- Logging & Reporting
- Network Address Translation (NAT)
- HotSpot with Captive

## Endian UTM Virtual Appliance Features

### Network Security

- Stateful Packet Firewall
- Demilitarized Zone (DMZ)
- Intrusion Prevention (Snort)
- Multiple Public IPs
- Quality of Service and Bandwidth Management
- SNMP support
- VoIP/SIP support
- Portscan Detection
- DoS and DDoS Protection
- SYN/ICMP Flood Protection
- VLAN support (IEEE 802.1Q trunking)
- DNS Proxy/Routing
- ntop (not in 4i, Mini)
- Anti-Spyware
- Phishing Protection

### Web Security

- HTTP & FTP proxies
- Anti-Virus (100.000+ patterns)
- Transparent Proxy support
- Content Analysis/Filtering
- URL Blacklist
- Authentication: Local, RADIUS, LDAP, Active Directory
- NTLM Single Sign-On
- Group-based web content filter
- Group-based web access policies
- Time-based access control with multiple time intervals
- Sophos Anti-Virus (optional)

### Mail Security

- SMTP & POP3 proxies
- Anti-Spam with Bayes, Pattern, and SPF
- Heuristics, Black- and White-lists support
- Anti-Virus (100.000+ patterns)
- Transparent Proxy support
- Spam Auto-Learning
- Transparent Mail Forwarding (BCC)
- Greylisting
- Commtouch RPD (optional)
- Sophos Anti-Virus (optional)

### Virtual Private Networking

- True SSL/TLS VPN (OpenVPN)
- IPsec
- Encryption; DES, 3DES, AES 128/192/256-bit
- Authentication: Pre-Shared Key, Certification Authority, and Local
- Support for VPN over HTTPS Proxy (OpenVPN)
- True SSL/TLS VPN (OpenVPN)
- Encryption; DES, 3DES, AES 128/192/256-bit
- Authentication: Pre-Shared Key, Certification Authority, and Local
- Support for VPN over HTTPS Proxy (OpenVPN)
- IPsec with L2TP and PSK/certificate support
- Unified VPN user management

### Hotspot

- Captive Portal
- Wired/Wireless support
- Pre-/Post-paid and free Tickets
- Traffic-based Tickets
- Integrated RADIUS service
- Connection Logging
- Per-user and global bandwidth limiting
- MAC-address-based user accounts
- User accounts import/export per CSV
- Single-click ticket generation (Quick ticket)
- Automatic client network configuration (support for DHCP and static IP)
- Generic JSON-API for external accounting and third party integration
- SmartConnect SMS user registration
- SmartConnect E-Mail user registration
- Password recovery
- Ticket validity
- Userless portal

### High Availability

- Hot Standby (active/passive)
- Node Data/Configuration Synchronization

### Multi-WAN with Failover

- Support for multiple Uplinks/WANs
- Automatic WAN Uplink Failover
- Monitoring of WAN Uplinks
- Uplink types: Ethernet (Static/DHCP), PPPoE, ADSL, ISDN, PPTP
- UMTS/GPRS/3G support
- Extended Support for GPRS/UMTS 3G devices

### Routing

- Static Routes; Source-based Routing
- Destination-based Routing
- Policy-based Routing (based on interface, MAC, protocol, or port)

### Network Address Translation (NAT)

- Destination NAT
- Incoming Routed Traffic
- One-to-One NAT
- Source NAT (SNAT)
- IPSec NAT Traversal

### Logging and Reporting

- Real-time Dashboard
- Event handling and notification
- Live Log Viewer (AJAX-based)
- Detailed User-based Web Access Report (not in 4i, Mini)
- Network/System/Performance Statistics
- Rule-based logging settings (Firewall Rules)
- Syslog: Local or Remote
- OpenTSA trusted timestamping

**Endian International**  
Tel: +39 0471 631 763  
E-mail: [sales@endian.com](mailto:sales@endian.com)

**Endian Italia**  
Tel: +39 0471 631 763  
E-mail: [italy@endian.com](mailto:italy@endian.com)

**Endian Deutschland**  
Tel: +49 (0) 8106 30750 - 13  
E-mail: [germany@endian.com](mailto:germany@endian.com)

**Endian US**  
Tel: +1 832 775 8795  
E-mail: [us@endian.com](mailto:us@endian.com)

**Endian Japan**  
Tel: +81 3 680 651 86  
E-mail: [japan@endian.com](mailto:japan@endian.com)

**Endian Turkey**  
Mobile +90 (0) 539 336 59 42  
E-mail: [turkey@endian.com](mailto:turkey@endian.com)