

Oneshield Next Generation UTM Security Appliance

the complete UTM solution, remotely managed, for high end IT Corporate Security



POWERED BY



Oneshield is a Unified Threat Management (UTM) Network Appliance Device that protects the Network and the entire IT of mid-sized to large organization, improving the quality of connectivity while at the same time offering all the essential Security Services and contents suited to the modern, always on corporations, with an easy to use interface.

The Oneshield software incorporates, among its main features, a wide range of components including Stateful Inspection Firewall, Enterprise IDS, Antivirus e Antispam HTTP, POP e SMTP, Antivirus HTTP e FTP, VPN Concentrator, Content Filter and ready to use "in the box" Managed Security Services (Telemonitoring and Teleconfiguration Services provided by Oneshield certified partners).

Oneshield Security Appliance: the product family

In each version the the Oneshield product family, unlike the vast majority of the solution on the market, the entire security package and all the software modules are active and standard inside the box. No "per user taxes" included: the number of the concurrent IP connection is limited only by the capacity and the performance of each Oneshield Hardware, and your Oneshield certified partner is at your disposal to consult you on the best configuration for your organization size and business need.

Oneshield UTM NANO is the smallest, tabletop oriented, small business UTM appliance, best suited for small offices where no rack space is available of for multisite and remote branch hub and spoke VPN solutions. The Oneshield UTM NANO edition includes all the software modules of the higher end hardware products.

Oneshield UTM BUSINESS is the most complete Unified Threat Management (UTM) solution of the industry, integrating application level filtering, antivirus, antispam, content, filter VPN Server (VPN concentrator) and one of the most complete and up to date Intrusion Detection Systems on the market in one single network appliance

This features do guarantee a high degree of protection for business organizations against network attacks and intrusions, viruses and most of the IT threats presents on the Internet, with no compromise hardware performances.

Oneshield UTM PRO has all the features of the Business edition, but is based on a higher performance hardware to guarantee maximum scalability in protecting against IT threats, in the web content filtering management and for higher volume spam email processing. This particular hardware is equipped with 1 Gigabyte of Ram and with Hard Disk mirroring technology.

Oneshield UTM ENTERPRISE is again fully equipped with all the features and the high availability configuration of the Pro edition, but is capable to reach maximum performance thanks to its 4 computing Cores, 6 Gigabit Ethernet Ports, and Hot Swap Hard Disks. The Enterprise edition is best suited for the most complex installations like the ones collocated on telcos operators, large enterprises and datacentres.

Stability and Scalability for the unified management of IT threats (Unified Threat Management, UTM)

Oneshield means complete protection: a "single shield" that includes stateful inspection firewall, VPN Server (VPN Concentrator), intrusion detection system updated on a continuous base, web content filtering, web antivirus, e-mail antivirus/antispam, VOIP security and wireless hotspot security.

Thanks to its simple, clean and easy to use interface and to its network based, remote update service, Oneshield guarantees complete IT Security of business organizations in conjunction with a high degree of stability and performance scalability.

Oneshield software modules offer one of the most complete and updated Threat Management and Intrusion Detection solutions to protects IT Networks from "Zero Day Attacks" (IT Vulnerabilities not known or patched from the software and hardware vendors).

Prevention against "Zero Day" attacks.

Using Stateful Inspection and Intrusion Detection System technologies in conjunction to one of the largest vulnerability and "Zero Days" databases on the market, Oneshield protects against malicious intrusion with constant traffic analysis and scanning for suspicious patterns. Oneshield software modules protects business organization IT perimeters from viruses, spam, phishing attacks and software exploits. Intrusion Detection System in particular, detects proactively DoS/DDoS attacks, exploits, hacks and combined IT attacks.

The Oneshield IDS allows the network administrator to visualize in realtime alarm messages, and it is based on a DBMS backend and an SQL database where all relevant informations of "anti intrusion" sensor are saved for simple archiving and subsequent query and research.

The Oneshield IDS allows the network administrator to visualize intrusions data in a highly detailed way:

- * Date
- * Time
- * IP Source/Destination
- * Port
- * Protocol Information (TCP, UDP, etc.)
- * Signature Information
- * Packet Payload

and includes a query and research feature on the base of:

- * Date/Time (timeframe)
- * IP Source / Destinazion
- * Source Port/ Destinazion

Firewall with “stateful inspection” technology

Oneshield is a security platform based on Stateful Inspection technology capable of identifying each single incoming packet by quality, identifying its origin and its content, performing constant monitoring against external attacks.

SSL VPN Server: Universal Technology, Fast and Secure

Thanks to its OpenVPN integrated module, Oneshield is capable of offering a unique solution for VPN based on SSL/TLS. With Oneshield SSL VPN it is possible to setup in a simple and fast way encrypted SSL connections, capable of bypassing different levels of Proxies, among different companies or branches, or among remote workers and the headquarter. The Oneshield VPN client allows to connect a single PC to the corporate network remotely.

Oneshield developed its own VPN client for the Windows, Linux and the Mac OSX platform.

Antivirus Gateway

The Antivirus Gateway engine built by Oneshield is the most powerful open source antivirus scanner on the planet. Oneshield scans the entire web and email traffic in realtime, protecting from viruses, trojans, phishing attacks, worms and other malware. The Viruses Definition update of the antivirus engine are sent daily to the network appliance and are manageable through the Oneshield web interface.

Web Security

By allowing the network administrator to manage and filter web access for corporate users and employees, the Oneshield Application proxies protect and control the corporate internet access to guarantee compliancy with corporate politics and best practices, increasing business productivity.

With the support of different authentication technologies (LDAP, Active Directory, eDirectory, RADIUS and Windows Win NT/2003 and Samba) the authentication for web browsing can be forced at the domain level.

The Web Content Filter scans the whole network traffic for viruses, trojans, malicious code and "bad" URLs putting companies, schools, hotel and organization open to the public in line with international CIPA standards (children's internet protection act).

The Oneshield content filter, protects web browsing of corporate users from viruses and inappropriate content like violence, pornography or illegal software sites.

This module is often useful in organization with underage users or with employees that must maintain a high standard of productivity. banning the access to web sites with adult content or ambiguous content in general.

Email Security

Oneshield is capable of cleaning up in a simple way and in realtime the whole corporate mailing system from viruses, spam and phishing attacks. The software module scans the entire email traffic in a transparent way, automatically protecting mailing servers (also the enterprise class ones) and the email clients as well.

Mail Servers like Microsoft Exchange or Lotus Domino and clients like Microsoft Outlook and Thunderbird can be filtered and protected by the antivirus and antispam modules from Oneshield, without modifying their configurations and settings.

Advanced Networking and Routing system

Oneshield offers advanced networking features for corporate networks, combining performances and redundancy with high end security. The Network Setup control panel allows network administrators to set in a simple and straightforward way all the parameters, allowing to configure different network areas.

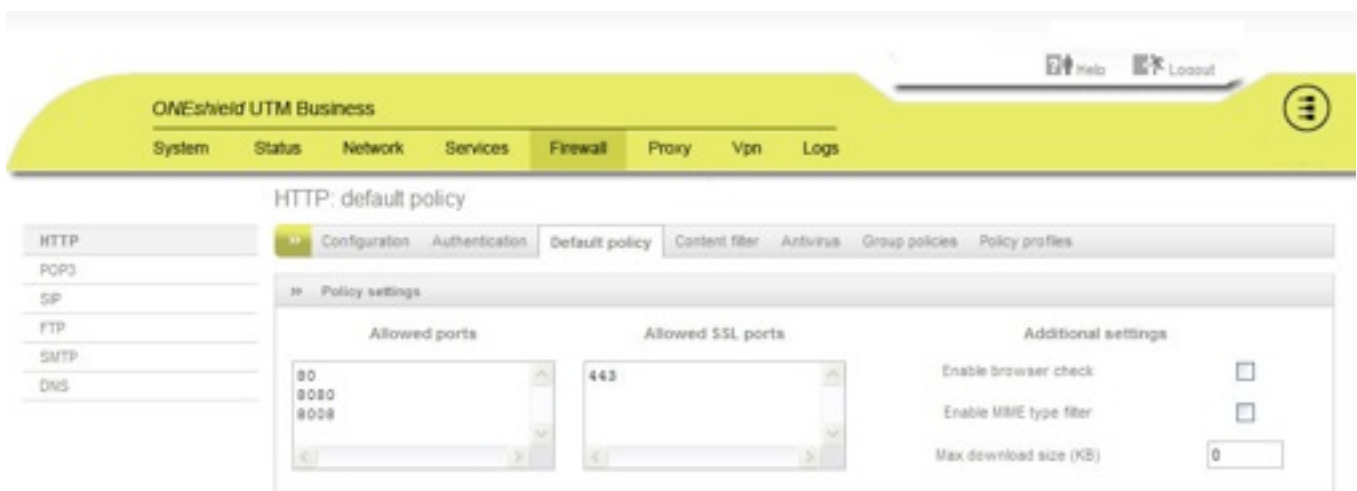
Thanks to the Multi-Wan support, load-balancing, high availability, VLAN, Interface Failover, and Traffic Shaping, the network administrator will be capable of managing without difficulties network resources and to control the internal and the internal/external traffic.

Wireless Network Hotspot Security

The Wireless Network security solution by Oneshield represent a flexible tool to manage wireless internet accesses in corporate or commercial areas. With Oneshield Hotspot Security, corporations, hotels, airports and banks can offer to their clients a protected and safe browsing access experience, without intrusion and external attacks problems to their critical IT systems.

Oneshield is capable of managing time based browsing (pre-paid - non pre-paid) and to log and register the users data, thus complying with the most recent anti terror and anti cyber terrorism laws.

Oneshield Instant Logs



Oneshield is highly web based for its managing interface, to be compatible and manageable from every operating system, without sacrificing real time graphical features typical of the traditional GUI.

The Oneshield Instant Log allows the Network Administrator to understand in real time, using an Ajax compatible web browser, everything that is happening inside the corporate network.

OneShield Managed Security Services, Remote Managing and Configuration System

Oneshield is the first family of IT Security Products to be capable “ready in the box” of being completely Tele Managed, Remotely Backed Up and Configured by an Oneshield Certified Security Operation Center (SOC).

Any problem that can happen on active software modules or on the hardware, can be tracked and resolved by the Oneshield Certified Security Operation Center (SOC). The end customer is automatically informed by the system via SMS or email, alerting internal corporate resources with minimal delay in case of an incident occurs.

By using the Organization and User Management of the Security Operation Center, it is possible to completely entrust to the SOC the complete managing of the corporate security system with a few mouse clicks.

Oneshield Remote Monitoring & Managing System, a complete insurance for the Corporate IT System.

IT Networks Security Managing is a high quality, human resource demanding, task but it is not always possible to dedicate quality personnel to such tasks in a highly flexible business environment to always maintain a "high guard" security level.

Oneshield Managed Security Services represent an innovative feature "inside the box" unique to the Oneshield product family, completely managed by an Oneshield Certified Security Operation Center (only highly skilled security professionals can be Certified by Oneshield).

The service is completely outsourced (thus entrusting the SOC of the responsibility of the Corporate IT Security), with a single monthly fee based on the service configurations required by the client.

Technical Highlights, Oneshield Managed Security Services:

- Remote management of firewall policies (stateful inspection) and change management policies
- Remote Control, Remote Configuration, Remote Backup and Proactive Monitoring (with operator intervention) of IDS-IPS, VPN Concentrator, Network Gateway, Application Proxies.
- Tele Configuration of Content Filtering (URL Filtering) policies.
- Remote control and management of other critical devices in the client network (Web server, DNS server, Mail relay, etc.)
- Proactive Call Center with 24*7 Security Professionals for remote intervention and customer alerting in case of attacks or suspicious events.

Management & Update Software: Oneshield Web Management

Oneshield Web Management is a system based on a Web Portal that allows the user to manage the status of its security systems using a web interface.

Oneshield Web Management represent the simplest interface to control multiple systems.

Some of the characteristics of Oneshield Management Software:

- Software Deployment
- Central Management of Software Updates
- Multiple Systems Monitoring

Oneshield Security Updates

By subscribing to a Maintenance Package (Standard or Advanced) an Oneshield customer can obtain an account to the Oneshield Network, the portal to maintain up to date the security contents of the Appliance.

Oneshield: An Industrial Strength and Scalable Platform

The Oneshield Security product family is based on different hardware platforms suited for different network sizing. The Oneshield UTM Pro and Enterprise in particular, are best fit for high availability installations even in critical environmental contexts.

Oneshield: An enterprise hardware, with a worldwide known brand.

Oneshield IT Security Solutions are built upon the same Eurotech microcomputers and HPC computers that are used worldwide by high end corporation, industrial organization, transportation companies and defense customers.

Oneshield, technical characteristics in detail:

Network Security:

- Stateful Packet Firewall
- Demilitarized Zone (DMZ)
- Intrusion Detection
- Multiple Public IPs
- Traffic Shaping
- VoIP/SIP support
- Malformed Packet Protection
- Portscan Detection
- DoS and DDoS Protection
- SYN/ICMP Flood Protection
- Anti-Spoofing Protection

Enterprise IDS:

- Fully Web Managed Intrusion Detection System
- Integrated with the largest Networks of 0Days Threats in the world
- Ajax Instant Log Web Interface for instant alerting of Intrusion Attempts

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 Access Control

Mail Security:

- SMTP & POP3 proxies

- Anti-spam with Bayes, Pattern, SPF, Heuristics, Black- and White-lists support
- Anti-virus (100.000+ patterns)
- Transparent Proxy support
- Spam Auto-Learning
- Transparent Mail Forwarding (BCC)
- Greylisting

VPN Concentrator:

- True SSL/TLS VPN (OpenVPN)
- IPSEC
- Encryption: DES, 3DES, AES 128-, 192-, 256-bit
- Authentication: Pre-Shared Key, X.509, Certification Authority, Local
- PPTP Passthrough
- Native VPN Client for MS Windows, MacOSX and Linux

Hotspot Security:

- Captive Portal
- Wired/Wireless support
- Pre-/Post-paid and free Tickets
- Integrated RADIUS service
- Connection Logging
- No additional software/hardware required

Management:

- Easy Web-based Administration (SSL)
- Secure Remote SSH/SCP Access
- Serial Console
- Centralized Management through Endian Network (SSL)

High Availability:

- Multi-Node Appliance Cluster
- Hot Standby (active/passive)
- Load Balancing (active/active)
- Node Data Synchronization

WAN Failover:

- Automatic WAN Uplink Failover
- Monitoring of WAN Uplinks
- VPN Failover

Network Address Translation:

- Static NAT (Port Translation)
- One-to-One NAT
- IPSec NAT Traversal

Routing:

- Static Routes
- Source Based Routing
- Destination Based Routing

Logging/Reporting:

- Instant Log Viewer (AJAX based)
- Detailed User Based Web Access Report
- Network/System/Performance Statistics
- Syslog (Local or Remote)

Updates and Backup:

- Centralized Updates through Oneshield Eurotech Network
- Anti-virus Definitions
- URL Blacklist Definitions
- Scheduled Automatic Backup
- Encrypted Backups via E-mail
- Instant Recovery/Backup to USB-Stick

Oneshield Security: technical innovations

Web Interface

- Completely redesigned web interface
- Many usability enhancements

Enhanced management of WAN/RED connections

- Support for multiple uplinks
- Multiple IPs/networks on each WAN/RED interface
- Uplink monitoring with automatic failover (ISP failover)
- Load balancing of multiple internet connections
- Easy editing/management of uplinks
- Support for new uplink types: UMTS, PPTP

Networking

- VLAN support (IEEE 802.1Q trunking)
- Policy Routing: routing based on user, interface, mac, protocol or port

Port Forwarding / NAT

- Multiple uplink support, allowing different rules per uplink
- Port Forwarding of traffic coming from VPN endpoints
- Source NAT management
- Option for rule based Logging

System Access

- External Access has now been enhanced and renamed to System Access
- Fine grained management of permissions regarding access to the system from LAN, WAN, DMZ and VPN endpoints
- Default policy for firewall/system access is now set to DENY
- Firewall services automatically define ports required for their proper function, but access can be restricted
- Support for ICMP protocol

Outgoing Firewall

- Support for ICMP protocol
- Handling of multiple sources/ports/protocols per Rule

Zone Firewall

- DMZ Pinholes has been enhanced and renamed to Zone Firewall
- Fine grained filtering of local network traffic
- Rules based on zones, physical interfaces, MAC addresses
- Support for ICMP protocol
- Handling of multiple sources/ports/protocols per rule

Intrusion Detection

- New version of High Performance IDS with reduced RAM usage and enhanced performance
- Support for inline intrusion detection

High Availability

- Multi-Node Appliance Cluster
- Hot Standby (active/passive)
- Automatic Node Data Synchronization
- Process monitoring/watchdog

HTTP Proxy

- Time based access control with multiple time intervals
- Group based web access policies
- Zone based operation mode: transparent, authentication or no authentication

Content Filter

- Better handling of content filter categories
- Enhanced performance

SMTP Proxy

- Enhanced performance
- Optional setting for Smarthost port
- Additionally secures SMTP traffic coming from VPNs (Roadwarrior and Gateway2Gateway)

DNS Proxy

- Route specific domains to a custom DNS

Hotspot

- Better account listing, with pagination, sorting and search
- 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)
- Enhanced user/client portal
- Generic JSON-API for external accounting and third party integration (like Hotel Management Software)
- Support for multiple network interfaces

OpenVPN

- X.509 and 2 factor based authentication
- Pushing of DNS settings to clients
- Pushing of global or per client routes
- Support for NATed VPN endpoints
- Support for VPN over HTTP Proxy
- Automatic connection failover
- Every VPN endpoint is resolvable through DNS (vpn.<username>.domain)

Oneshield VPN Client

- Downloadable from Oneshield Network
- Works with Windows (Vista, XP, 2000), MacOSX, Linux
- Multiple connections at once
- Encrypted configuration profiles
- PSK, X509 based and 2 factor authentication
- Runs as service and allows unprivileged users to start a connection
- Can start the connection automatically on boot / on user logon
- Supports openvpn server fallback, when primary server fails

IPSEC

- Rewrite of the base
- Added debugging possibilities
- Ipsec on orange
- Default MTU can be overridden
- Simplified GUI by removing Side (Left/Right) configuration and swapped completely to Local/Remote labeling
- added ID fields
- Added Dead Peer Detection options

Instant Log Viewer

- Realtime log viewer with filtering and highlighting
- Displays all the logfiles you are interested in at the same time

Logs

- Every service supports remote logging
- Daily log rotation

Backup

- Zero-configuration backups to USB stick: just plug in a USB stick to backup
- Restore a from any USB stick

Support

- One click to access to Oneshield Support Team and Managed Security Services
- Integrated ticketing support