

Oneshield Next Generation UTM Security Appliance

la strumento completo, gestito e tele-aggiornato per la sicurezza delle aziende e delle organizzazioni



POWERED BY



Oneshield è una Unified Threat Management (UTM) Appliance che protegge la rete e il perimetro informatico di aziende e organizzazioni migliorando la connettività e offrendo tutti i servizi e i contenuti di sicurezza indispensabili alle organizzazioni moderne e sempre connesse ad Internet, in maniera semplice da configurare.

Il software di Oneshield comprende, tra le sue principali funzionalità un'ampia gamma di caratteristiche, fra cui Stateful Inspection Firewall, Enterprise IDS, Antivirus e Antispam HTTP, POP e SMTP, Antivirus HTTP e FTP, VPN Concentrator, Content Filter e Telegiustizia.

Oneshield Security Appliance: la famiglia prodotti

In ciascuna versione della famiglia Oneshield, contrariamente alle altre soluzioni sul mercato, sono attive tutte le funzionalità e i moduli del software. Inoltre non sono presenti "tasse" o limitazioni relative numero di utenti: il limite di connessioni è dato solo ed esclusivamente dalle capacità e dalle performance dell' hardware, e il vostro responsabile commerciale Oneshield è a disposizione per indicarvi il modello più adatto alle vostre esigenze di business.

Oneshield UTM NANO è la più piccola appliance, in formato tabletop, della famiglia Oneshield. Dedicata al mercato small business, agli uffici dove lo spazio o gli armadi di rack non sono disponibili o per le installazioni VPN in uffici remoti, la Oneshield in edizione NANO include tutti i moduli software disponibili sui prodotti hardware di fascia superiore.

Oneshield UTM BUSINESS è la soluzione Unified Threat Management (UTM) più completa della sua categoria, poichè integra application level filter, antivirus, antispam, filtro dei contenuti, VPN server e uno dei più aggiornati Intrusion Detection System (sistema contro le intrusioni informatiche) presenti sul mercato in un'unica appliance.

Queste funzionalità offrono una protezione di alto livello per il business contro gli attacchi di rete, i virus, lo spam e la maggior parte delle minacce informatiche provenienti da internet, senza sacrifici in performance.

Oneshield UTM PRO include tutte le funzionalità della modello Business, ma è potenziato a livello hardware per offrire performance migliori nella prevenzione delle intrusioni informatiche, nel filtro dei contenuti per la navigazione e per le e-mail e la massima disponibilità grazie presenza di un Gigabyte di RAM e alla tecnologia di mirroring degli Hard Disk.

Oneshield UTM ENTERPRISE comprende tutte le funzionalità e le caratteristiche di alta disponibilità della modello Pro, ma gestisce le massime performance grazie ai suoi 4 Core di computazione, alle sei porte Gigabit Ethernet e agli Hard Disk con capacità di sostituzione a caldo.

La versione Enterprise è indicata per le installazioni più complesse come quelle presso operatori di telecomunicazioni, large enterprise o datacenter in genere.

Stabilità e Scalabilità per la gestione unificata delle minacce (Unified Threat Management, UTM)

Oneshield offre una protezione completa: un “singolo scudo” che offre stateful inspection firewall, VPN Server, intrusion detection system aggiornato su base continuativa, web content filtering, web antivirus, e-mail antivirus/antispam, VOIP security e wireless hotspot security.

Grazie ad una interfaccia semplice da usare ed al sistema di aggiornamento di rete Oneshield Network, Oneshield assicura una sicurezza completa unita ad una grande stabilità e scalabilità per la reti informatiche di aziende e organizzazioni.

I moduli software Oneshield offrono inoltre una delle soluzioni più complete e aggiornate di Threat Management e Intrusion Detection per proteggere le reti informatiche dagli “Zero Day Attacks” (gli attacchi informatici non ancora di pubblico dominio).

Protezione contro gli attacchi “Zero Day”

Sfruttando la tecnologia Stateful Inspection, quella di Intrusion Detection System e uno dei database più aggiornati sulle vulnerabilità informatiche di classe “0Day”, Oneshield protegge contro intrusioni indesiderate e attacchi di malintenzionati con un'analisi del traffico alla ricerca di comportamenti sospetti. I moduli software Oneshield difendono la rete da virus, spam, phishing attacks e software exploits. L'Intrusion Detection System in particolare, rileva in maniera proattiva attacchi DoS/DDoS, exploits, hacks e minacce multiple.

L'Intrusion Detection System Oneshield, che consente la visualizzazione in tempo reale dei messaggi di allarme, è basato su di un Backend DBMS e un database SQL dove tutte le informazioni dei sensori “anti intrusione” vengono salvate per la semplice archiviazione e interrogazione successiva.

L'Intrusion Detection System Oneshield, permette al proprio amministratore la possibilità di visualizzare i dati delle intrusioni in modo dettagliato:

- * Data
- * Ora
- * IP Sorgente/Destinazione
- * Porta
- * Informazioni sul protocollo (TCP, UDP, ecc.)
- * Informazioni sulla signature
- * Payload del pacchetto (opzionale)

e include la funzionalità di ricerca delle intrusioni in base a:

- * Data/Ora (arco di tempo)
- * IP Sorgente/Destinazione
- * Porta Sorgente/Destinazione

Firewall con tecnologia “stateful inspection”

Oneshield è una piattaforma di sicurezza basata su tecnologia Stateful Inspection, che identifica singolarmente e qualitativamente ogni pacchetto in arrivo, ne determina l'origine e il contenuto, vigila contro intrusioni indesiderate o attacchi dall'esterno.

SSL VPN Server: Tecnologia Universale, Veloce e Sicura

Grazie al server OpenVPN integrato, Oneshield è in grado di offrire una soluzione per VPN su SSL/TLS. Con Oneshield SSL VPN è possibile in modo semplice e veloce impostare connessioni SSL criptate, bypassando i vari “proxy”, tra le diverse sedi delle aziende o tra i portatili dei lavoratori remoti e le sedi principali. Il client VPN di Oneshield permette poi di connettere il PC fisso o portatile alla rete aziendale da remoto.

Oneshield ha sviluppato un proprio client VPN per Windows, Linux e Mac OSX in grado di connettere l'utente remoto con assoluta sicurezza e semplicità.

Gateway Antivirus

Il motore dell'Antivirus Gateway di Oneshield è il più potente scanner antivirus nel mondo Open Source. Oneshield fa la scansione di tutto il traffico web e email in real-time, proteggendo la vostra rete da viruses, trojans, phishing attacks, worms e altri malware. Gli aggiornamenti delle definizioni dell' Antivirus vengono inviate all' appliance ogni giorno e sono configurabili attraverso l'interfaccia web di Oneshield.

Web Security

Fornendo la possibilità di gestire e filtrare l'accesso al web degli utenti e dei dipendenti, gli Application Proxies di Oneshield proteggono e controllano l' accesso ad internet per garantire l'applicazione delle politiche aziendali e migliorare la produttività interna.

Con il supporto di diverse tecnologie di autenticazione (LDAP, Active Directory, eDirectory, RADIUS e Windows Win NT/2003 e Samba) l'autenticazione per la navigazione internet può essere forzata a livello di dominio.

Il Web Content Filter inoltre, fa la scansione di tutto il traffico web alla ricerca di viruses, trojans, malicious code e “bad” URLs mettendo aziende, scuole, hotel, e le organizzazioni in genere di essere in linea con gli standard CIPA (children's internet protection act).

Il filtro dei contenuti di Oneshield inoltre, protegge la navigazione degli utenti da virus e contenuti indesiderati come siti su violenza, pornografia o software illegale.

Questo modulo spesso è utile nelle organizzazioni con utenza minorenni o con dipendenti che devono mantenere alta la propria produttività, impedendo la navigazione su siti con materiale riservato ad un pubblico adulto, o in generale con contenuti ambigui.

Email Security

Oneshield è in grado di ripulire in modo semplice e in tempo reale tutta il sistema di posta aziendale da email con viruses, spam e phishing attacks. Il modulo software opera la scansione di tutto il traffico mail in modo trasparente, di modo che sia i server (anche quelli "enterprise") che i vari client mail saranno automaticamente protetti da Oneshield.

Oneshield protegge qualsiasi mail server o client mail dai virus e dallo spam, grazie ai suoi proxy in modalità trasparente. Sia i mail server come Microsoft Exchange o Domino che programmi di posta come Microsoft Outlook e ThunderBird, sono protetti e "filtrati" dall' antivirus e dall' antispam di Oneshield, in tempo reale e senza modificare la loro configurazione e le loro impostazioni.

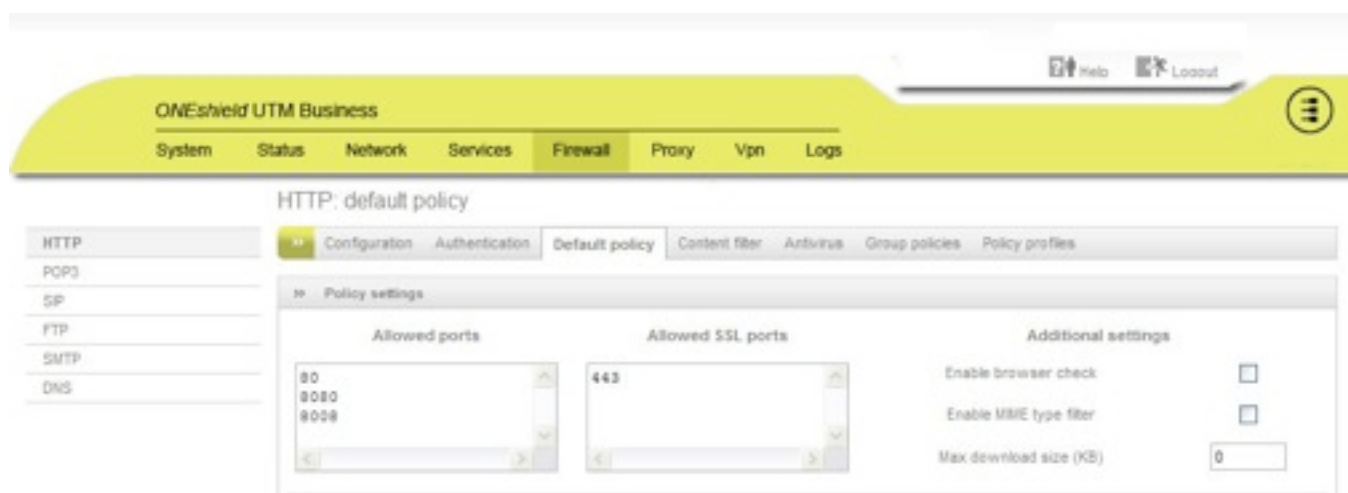
Sistema di Routing e Networking Avanzato

Oneshield offre funzionalità avanzate per le reti aziendali, assicurando oltre alla sicurezza, ridondanza e velocità. Il pannello di controllo di Network Setup permette di impostare in modo semplice e corretto tutti i parametri della rete, dando la possibilità di impostare zone separate al suo interno. Grazie al supporto per Multi-WAN, di load-balancing, high availability, VLAN, Interface Failover, e Traffic Shaping l'amministratore del sistema sarà in grado di gestire senza difficoltà le risorse della rete e di controllare al meglio il traffico sicuro in movimento al suo interno e attraverso essa.

Wireless Network Hotspot Security

La soluzione per la sicurezza delle reti Wireless di Oneshield rappresenta uno strumento flessibile per gestire gli accessi ad internet in luoghi aziendali pubblici e commerciali. Con Oneshield Hotspot Security le aziende, gli hotel, gli aeroporti e le banche possono offrire ai propri clienti in tutta semplicità una navigazione protetta e sicura, senza pericoli di attacchi dall'esterno ai propri sistemi critici.

Oneshield è in grado di gestire la navigazione a tempo (sia prepagata che post-pagata) e di registrare i dati dell'utente come previsto dalla recente legge antiterrorismo



Oneshield Instant Logs

Oneshield fa ampio uso dell' interfaccia web per le sue piattaforme di sicurezza, per renderle compatibili con qualsiasi sistema operativo, senza rinunciare alle funzionalità grafiche in real time tipiche di una GUI

tradizionale. L'Instant Log di Oneshield permette di conoscere in tempo reale, attraverso un browser con supporto Ajax, tutto ciò che succede all'interno della rete Oneshield.

OneShield Teleguardia

Oneshield è la prima famiglia di prodotti ad essere immessa sul mercato con la possibilità "ready in the box" di essere completamente "telecontrollata" dal centro servizi Oneshield.

Qualora si riscontrasse un problema sui servizi attivi o sull'hardware, il centro di guardia Oneshield informa il cliente attraverso un SMS o una e-mail, permettendo al cliente di venire a conoscenza in maniera tempestiva di un eventuale problema sulle Oneshield UTM appliances.

Utilizzando poi l'Organization and User Management del centro servizi Oneshield è possibile inoltre delegare completamente la gestione dei sistemi di sicurezza al centro stesso con pochi click di mouse.

Oneshield Teleguardia, una assicurazione per i perimetri informatici aziendali.

La gestione della sicurezza delle reti è oggi più che mai una necessità, ma spesso all'interno delle organizzazioni di business non ci sono le risorse o le competenze necessarie per mantenere alto il livello di guardia. Con l'accesso Internet "always on" infatti, e l'apertura delle porte informatiche verso l'esterno, si corre il rischio di lasciare libero accesso ai dati sensibili ad ospiti indesiderati.

Oneshield Teleguardia è un servizio (gestito da operatori esperti di sicurezza informatica) di difesa contro le minacce provenienti da Internet e protegge in modo completo e innovativo la rete aziendale.

Il servizio di protezione avviene completamente in outsourcing attivando il modulo "teleguardia" presente in ogni prodotto Oneshield (Nano, Business, Pro ed Enterprise), affidando così la responsabilità al centro stesso del controllo della sicurezza del flusso delle informazioni.

L'appliance Oneshield viene gestita dal centro operativo, il Security Operation Center (SOC), connesso ad Internet attraverso la più moderna e sicura tecnologia di trasporto.

Grazie ad un monitoraggio costante dello stato dell'apparato e alla supervisione di tecnici specializzati, Oneshield Teleguardia è in grado di intervenire in tempo reale nella gestione e risoluzione di ogni problema o variazione chiesta dal cliente.

L'analisi accurata delle necessità espresse dal cliente, e l'esperienza dei tecnici Oneshield nel valutare le minacce più ricorrenti, fanno di Oneshield Teleguardia un servizio tagliato su misura e interamente scalabile: può essere, infatti, ampliato e potenziato attraverso risorse aggiuntive, a seconda delle esigenze di sicurezza che di volta in volta emergono.

Navigazioni sicure: con Oneshield difende la navigazione dalle insidie di Internet e preserva le aziende dalle vulnerabilità delle reti.

Caratteristiche di base

- Telegestione delle policy e funzionalità del firewall (stateful inspection).
- Telecontrollo, teleconfigurazione e monitoraggio proattivo delle Funzionalità di Intrusion Detection (IDS/IPS), VPN Concentrator, Gateway, Proxy Applicativi.
- Teleconfigurazione delle funzionalità di Content Filtering (URL Filtering).

- Controllo e gestione remota in parallelo di ulteriori apparati e servizi presenti nella rete del Cliente, come Web server, DNS server, Mail relay, etc. .

- Call center proattivo e intervento di alerting telefonico in caso di attacchi, comportamenti sospetti o emergenze informatiche.

Management & Update Software: Oneshield Web Management

Oneshield Web Management è il sistema basato su portale che permette all'utente di gestire i propri sistemi Oneshield attraverso l'interfaccia web.

È la soluzione più semplice per tenere sotto controllo i propri sistemi. Alcune caratteristiche dell' Oneshield Management Software:

- Software Deployment indipendente dalle piattaforme per cui è utilizzato
- Gestione centralizzata degli aggiornamenti
- Sistema di Monitoring

OneShield Aggiornamenti di Sicurezza

L'acquisto di un pacchetto di Maintenance, Standard o Advanced, permette di ottenere un account in Oneshield Network, il portale di gestione e controllo di tutte le soluzioni Oneshield.

Con questo ausilio sia il Oneshield Business Partner che il cliente finale possono controllare lo stato della macchina, dell'aggiornamento dei software e dei servizi in pochi istanti, in modo semplice ed intuitivo, ovunque ci si trovi.

Oneshield Support & Maintenance

Oneshield offre ai propri clienti tutti gli strumenti per utilizzare e gestire al meglio i prodotti Oneshield.

Acquistando un prodotto Oneshield si può contare sull'aiuto di semplici strumenti online o di personale esperto per la risoluzione di eventuali problemi in fase di configurazione e utilizzo.

Un modello di licenza software “tutto incluso” e “senza tasse nascoste”

Tutti i moduli software di Oneshield, il supporto tecnico via mail, la sostituzione rapida dell'hardware, gli update di sistema, e i contenuti dell' Oneshield Network sono inclusi in un unico licensing model, con opzioni chiare e “senza tasse nascoste”.

Oneshield è una soluzione UTM completa, non esistono costi aggiuntivi per licenze e sottoscrizioni a singoli moduli o per numero di utenti.

Hardware Industriale e Scalabile

La famiglia di prodotti Oneshield è costituita di diverse piattaforme hardware adatte a reti di diverse dimensioni, per soddisfare il fabbisogno di tutte le realtà di mercato.

In particolare Oneshield UTM Pro ed Enterprise si configurano come sistemi ad alta affidabilità, in grado di funzionare in condizioni ambientali critiche e fornire un'elevata continuità di servizio.

Oneshield: la solidità di un hardware, riconosciuta nel mondo.

Le soluzioni di sicurezza Oneshield sono costruite sugli stessi microcomputer e HPC computers Eurotech che da anni sono utilizzati da grandi realtà internazionali, clienti industriali e organizzazioni governative e della difesa.

Oneshield, le caratteristiche tecniche in dettaglio

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

Oneshield, le caratteristiche tecniche innovative

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
- Isec 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

Managed Security Services *Descrizione del Servizio*

Il servizio Oneshield Managed Security Services sarà erogato a canone indipendentemente dal numero di richieste di change management o interventi in assistenza, con costi differenziati solo in base alle funzionalità attivate/richieste (FW,VPN Gateway, AV, ASP, CF, etc.).

Le funzionalità e i servizi erogati saranno i seguenti: Firewall, VPN Gateway (S-VPN L2L), VPN Concentrator (S-VPN L2C, S-VPN SSL), Content Filtering, Antivirus, Antispam, Traffic Shaping, IDS, High Availability.



a. Firewall.

Servizio di firewalling/NAT erogato senza limitazioni se non quelli propri dell'appliance.

b. VPN Gateway (S-VPN L2L).

Servizio di S-VPN LAN-to-LAN erogato senza limitazioni se non quelli propri dell'appliance.

c. VPN Concentrator IPSec/SSL VPN (S-VPN L2C).

Servizio di S-VPN LAN-to-Client erogato sia con Client (VPN IPSec) che Client-less (VPN SSL): è prevista l'autenticazione solo su piattaforme di autenticazione del cliente (Radius, AD). Il servizio viene erogato con due profili: Silver e Gold.

Profilo Silver. Clienti mono sede con autenticazione su Radius/AD, max. 25 utenti simultanei con solo una modalità di accesso (VPN IPSec o VPN SSL). Nel caso di VPN SSL, creazione di una sola homepage utente personalizzata con un massimo di 10 bookmark ad applicazioni interne.

Profilo Gold. Clienti mono sede con autenticazione su Radius/AD o clienti multi sede con installazione frontend Radius (MS IAS) a cura del Cliente sui controller di dominio della sede di installazione, max. 50 utenti

simultanei con possibilità di utilizzare sia VPN IPsec che VPN SSL. Nel caso di VPN SSL, creazione di massimo 5 homepage per gruppi di utenti, personalizzate ognuna con un massimo di 10 bookmark ad applicazioni interne.

Quanto non rientri nei profili sopraesposti, verrà valutato a Progetto.

d. Content Filtering.

Servizio di Content Filtering/URL Filtering. Blocciamo quanto selezionato dal Cliente: i siti non categorizzati vengono fatti passare di default, per non dover metter mano ogni giorno alle white list (p.e. per siti locali non categorizzati).

Quanto non rientri nei profili sopraesposti, verrà valutato a Progetto.

e. Antivirus.

Servizio di AV sui protocolli standard (p.e. http, smtp, pop3 e imap), erogato senza limitazioni se non quelli propri dell'appliance.

f. Antispam.

Servizio di ASPM erogato senza limitazioni se non quelli propri dell'appliance.

g. Traffic Shaping.

Profili di gestione banda per protocollo, IP, etc. fino a un massimo di 5 policy totali (WAN > LAN, DMZ > WAN, etc.).

Quanto non rientri nei profili sopraesposti, verrà valutato a Progetto.

h. IDS/IPS automatico.

Profili di gestione traffico anomalo con possibilità di inoltrare/scartare/loggare il traffico ritenuto malevolo, fino a un massimo di 5 protection profile e senza modifica dei valori proposti di default.

Quanto non rientri nei profili sopraesposti, verrà valutato a Progetto.

i. High Availability.

i. Servizio di alta affidabilità erogato senza limitazioni se non quelli propri dell'appliance: da verificare modalità di lavoro dell'appliance (active/standby o active/active).

j. Vulnerability Assessment.

Post-attivazione. Erogato al termine dell'attivazione quale validazione del servizio.

Periodico. Erogato con frequenza trimestrale: svolto di norma nei mesi Marzo, Giugno, Settembre e Dicembre, in modo da rilasciare l'ultimo VA nel mese di scadenza del servizio di assistenza).

k. Monitoring.

Profilo Silver. Monitoraggio standard con verifica disponibilità sistemi/servizi del Cliente con accesso a portale web dedicato per sinottico dei sistemi monitorati.

Profilo Gold. Monitoraggio proattivo con verifica disponibilità sistemi/servizi del Cliente con accesso a portale web dedicato per sinottico dei sistemi monitorati, con inoltro di avviso al Cliente (email o sms) in caso di mancata disponibilità dei sistemi/servizi monitorati.

l. Logging/Reporting.

Profilo Silver. Logging di base e invio via email di report statico sicurezza settimanale.

Profilo Gold. Logging di base, invio via email di report statico sicurezza settimanale, accesso a portale web con disponibilità in linea dei logs dell'ultima settimana e generazione report dinamici specifici in real-time.

I servizi erogati verranno suddivisi in servizi base, servizi avanzati e servizi extra:

a. Servizi base. Servizi compresi di default nell'attivazione, sia che vengano attivati o meno in base alle esigenze del Cliente. Il Cliente potrà scegliere di avvalersi del solo servizio di attivazione o attivazione/assistenza, ma non potrà attivare per conto proprio il sistema e poi chiedere di attivare il solo servizio di assistenza: I servizi base sono a loro volta suddivisi in profilo Basic e Advanced.

Profilo Basic: per clienti con max. 25 utenti complessivi (rete interna + VPN) e 3 interfacce attive (esclusa eventuale interfaccia di HA).

Profilo Advanced: per clienti con oltre 25 utenti e fino a 100 utenti complessivi (rete interna + VPN) e 4 interfacce attive (esclusa eventuale interfaccia di HA);

b. Servizi avanzati. Servizi non compresi di default nell'attivazione ma che vengono attivati su richiesta del Cliente. Il Cliente potrà scegliere di avvalersi del solo servizio di attivazione o attivazione/assistenza, ma non potrà attivare per conto proprio la nuova funzionalità e poi chiedere di attivare il solo servizio di assistenza: non possiamo gestire contesti attivati da altri senza effettuare la revisione degli stessi prima di prenderli in carico, e questo equivale comunque ad un'attivazione.

c. Servizi extra. Servizi specializzati usufruibili su richiesta del Cliente, da utilizzarsi come base per erogare consulenza specialistica sulle tematiche TLC/Sicurezza, con eventuale intervento on site per problematiche particolarmente complesse.

Quanto non rientri nei profili sopraesposti, verrà valutato a Progetto.

I servizi base comprendono di default le seguenti funzionalità/servizi:

FW, S-VPN L2L, Antivirus, Traffic Shaping, IDS/IPS automatico, Monitoring Silver, Logging/Reporting Silver, VA sistemi post attivazione.

I servizi avanzati vengono erogati individualmente e comprendono le seguenti funzionalità/servizi:

S-VPN L2C Silver o Gold, Content Filtering, Antispam, Monitoring Gold, Reporting Gold, VA sistemi one shot e periodico (trimestrale).

I servizi extra disponibili a richiesta sono i seguenti (spese trasferta escluse):

- a. Giornata Project Manager;*
- b. Giornata Sistemista Sicurezza Business Time;*
- c. Giornata Sistemista Sicurezza Extra Business Time;*
- d. Maggiorazione attivazione sistemi Extra Business Time;*
- e. VA applicativi one shot e periodico (trimestrale) secondo necessità fino a 10, 25, 50 e 100 IP.*

Tutti gli elementi della piattaforma dovranno essere dotati di indirizzi di management coerenti con il piano di indirizzamento del Cliente: per garantire il supporto da remoto, tali indirizzi dovranno essere accessibili dalle sedi del SOC Oneshield. Le modalità di accesso (VPN site-to-site, pubblicazione con IP pubblico, access-list, etc.) e l'elenco degli operatori autorizzati verranno concordati in fase di startup.

Nel caso si sottoscriva l'opzione Alta Affidabilità (HA) per clusterizzare gli apparati, tutti gli switch necessari a portare in Alta Affidabilità la piattaforma dovranno essere messi a disposizione dal Cliente: la configurazione da adottare dovrà essere concordata con il SOC.

Il servizio di attivazione verrà erogato solo dopo la verifica della visibilità IP tra le sedi oggetto dell'intervento o della disponibilità di accesso al backbone/Internet.

Secondo necessità, il SOC potrà inoltre prendere in carico anche contesti eterogenei (ovvero non esclusivamente con soluzioni hardware Oneshield Security) con prodotti basati su tecnologia Cisco, Stonesoft, Fortinet, SonicWALL, Astaro, Watchguard e altri (a progetto).

Modalità di erogazione del servizio

L'offerta prevede l'attivazione e la presa in carico degli appliance OneShield da parte del SOC di Oneshield Security e la successiva erogazione del servizio di sicurezza gestita.

Il processo di erogazione dei servizi sarà il seguente:

- a. Il processo di attivazione del Cliente inizia con l'analisi della sua attuale architettura di rete e delle policy di sicurezza attualmente implementate.
- b. Vengono quindi raccolte eventuali nuove esigenze, discussi scenari evolutivi di medio/lungo periodo, formulate proposte migliorative e definite modalità di accesso remoto agli apparati da parte del SOC.
- c. Sulla base di queste informazioni e dell'esperienza del nostro team, viene redatto un documento di progetto nel quale sono dettagliate le policy che verranno implementate al momento della presa in carico della piattaforma di sicurezza e le caratteristiche dei servizi erogati.
- d. Il documento di progetto viene quindi condiviso con il Cliente per approvazione.
- e. Conclusa la fase progettuale inizia l'implementazione dei servizi richiesti con implementazione delle politiche di sicurezza descritte nel documento di progetto approvato dal Cliente.
- f. Un nostro operatore si interfaccia con il Cliente per effettuare eventuali test e tuning delle configurazioni e per concordare l'orario del Vulnerability Assessment (effettuato dalla rete pubblica).
- g. Completato il VA e ricevuta conferma positiva dal Cliente, il documento di progetto viene validato e congelato: da questo momento in poi verrà definito "as built" e rispecchierà fedelmente le policy implementate negli apparati.
- h. Gli apparati sono quindi agganciati alla piattaforma di management collocata presso il SOC.
- i. Inizia la fase di Operation: da questo momento l'accesso esclusivo alla configurazione degli apparati è conferito al SOC che si occuperà delle attività di monitoraggio, aggiornamento della piattaforma, manutenzione ordinaria e straordinaria.
- j. Il Cliente tramite posta elettronica o chiamata al numero dedicato al servizio, può richiedere l'intervento del nostro SOC per consulenze o richieste di assistenza/manutenzione.
- k. Ad ogni richiesta è associato un numero di chiamata che consente al Cliente di tracciarne lo stato: gli interventi vengono effettuati nel rispetto dei Service Level Agreement contrattualizzati.

L'installazione "on site" degli apparati in oggetto verrà effettuata dal Partner Oneshield Security, mentre l'attività di attivazione dei servizi verrà effettuata dal ns. personale in modalità "remote", accedendo ai sistemi oggetto dell'intervento via Internet.

I servizi di presidio "10x5" e reperibilità tecnica "24x7" per attività di manutenzione correttiva verranno erogati da SOC in modalità "remota", facendo intervenire secondo necessità il Partner Oneshield Security locale con l'eventuale hardware di scorta messo a disposizione dal Partner stesso o da Oneshield Security. In particolare, il flusso classico della gestione di un evento è il seguente:

- a. Il Cliente segnala un problema con chiamata al SOC (in orario di presidio) o al ns. tecnico sistemista reperibile (in orario extra presidio), o il problema viene rilevato direttamente da SOC da allarme, se si tratta di perdita di connettività).
- b. SOC effettua la diagnosi sulla connettività e la raggiungibilità IP dei sistemi oggetto del disservizio (routing compreso).
- c. Se si tratta di un problema di connettività, SOC segnala al Cliente il problema affinché possa interessare il Partner Oneshield Security locale per il ripristino della stessa, rendendosi disponibile ad interfacciarsi con il Provider per eventuale supporto tecnico (se necessario).
- d. Qualora non sia un problema di connettività, SOC accede ai sistemi gestiti ed effettua la propria diagnosi per la parte competente.
- e. Se si tratta di un problema hardware, SOC segnala al Partner Oneshield Security locale per il ripristino delle funzionalità mediante sostituzione dell'hardware.
- f. Il Partner Oneshield Security pianifica un intervento per la sostituzione dell'hardware avvisando SOC, il quale si rende disponibile per monitorare l'esito dell'intervento e il ripristino dei servizi.
- g. Una volta ripristinata la connettività o sostituito l'appliance, SOC interviene di conseguenza sulle configurazioni, se necessario. Qualora venga riscontrato un problema hardware non identificato in precedenza, SOC avverte il Partner Eurotech della necessità di sostituzione dell'hardware.

Fermo restando il servizio di presidio e di eventuale reperibilità tecnica erogati secondo gli SLA definiti, i prodotti necessari per l'attivazione verranno acquisiti dal Cliente attraverso il Partner Oneshield Security locale di riferimento, al fine di poter erogare il supporto hardware con eventuale intervento "on site". L'interfaccia primaria di gestione e coordinamento sarà comunque sempre il SOC in orario di presidio o il tecnico sistemista in orario extra-presidio, i quali dopo aver appurato che il problema lamentato sia dovuto a malfunzionamenti hardware, si interfacceranno direttamente con il Partner Oneshield Security per gestire l'intervento fino alla chiusura del guasto.

Servizio di Assistenza Tecnica

Il servizio di assistenza tecnica prevede la disponibilità di un tecnico specializzato in ambiente TLC/Sicurezza da utilizzarsi per le attività di manutenzione ai sistemi installati presso i clienti e viene erogato secondo i seguenti profili:

- SAT 10x5 (Lun-Ven 9:00-19:00). Viene erogato avvalendosi del servizio di presidio dal Lunedì al Venerdì: si rimanda alla descrizione delle modalità di accesso al servizio per un maggior dettaglio.
- SAT 24x7 (Lun-Dom 0:00-24:00). Viene erogato avvalendosi del servizio di presidio dal Lunedì al

Venerdì e del servizio di reperibilità in orario extra-presidio: si rimanda alla descrizione delle modalità di accesso al servizio per un maggior dettaglio.

L'accesso al servizio con richiesta di intervento potrà essere effettuato come segue:

- In orario di presidio: a mezzo chiamata telefonica durante il normale orario di lavoro dal Lunedì al Venerdì dalle ore 9:00 alle 19:00, fatto salvo eventuali festività infrasettimanali per le quali opererà il servizio di reperibilità (verrà comunicato il numero di telefono del ns. SOC).
- In orario di reperibilità: a mezzo chiamata telefonica al di fuori del normale orario di lavoro (verrà comunicato il numero di telefono per il servizio di reperibilità).

In entrambi i casi, la richiesta dovrà comunque essere confermata inviando una email all'indirizzo mss@oneshieldsecurity.com e/o agli indirizzi specifici per la gestione del servizio che verranno comunicati.

Detti servizi verranno erogati in modalità "remote" con tempi di intervento dalla segnalazione di 4 (quattro) ore lavorative per gli interventi effettuati su guasti bloccanti, e 8 (otto) ore lavorative per interventi effettuati su guasti non bloccanti.

Per guasto bloccante si intende un'anomalia hardware/software che renda indisponibili servizi/risorse del cliente tali da non permettergli una normale operatività. In caso di necessità, sarà possibile richiedere un intervento da erogarsi in modalità "on site", in accordo con tariffe e modalità esposte. Nell'erogazione del servizio SAT, le eventuali variazioni a sistemi esistenti (change management) saranno gestite solamente in normale orario di presidio.