

	Base	Proxy	Qualità of Services	Intrusion detection System	Antispam e antivirus
[PORT FORWARDING (MULTI NAT)] Gestione grafica del port forwarding con possibilità di definire alias di IP.	✓				
[DMZ PINHOLES] Creazione di "tunnel" protetti dalla DMZ alla LAN per l'accesso a servizi.	✓				
[VPN] Possibilità di creare tunnel cifrati compatibili Microsoft® o con certificati pubblici/privati.	✓				
[HTTP SCAN] Scansione in tempo reale del traffico http per l'identificazione di possibili codici ostili (browser exploit , phishing, virus, ecc)	✓				
[HTTP TRAFFIC SCAN] Scansione in tempo reale del contenuto delle pagine visionate per l'identificazione di possibili contenuti ostili (ads, banners, jumping-windows, ecc)	✓				
[HTTP VIRUS SCANNER] Scansione in tempo reale del traffico http e proxy alla ricerca di possibili virus.	✓				
[FTP SCANNING] Scansione in tempo reale del traffico FTP in upload e download su tutte le interfacce.	✓				
[GESTIONE DELLA MEMORIA CACHE] Consente di variare i parametri di utilizzo dello spazio su disco e in memoria RAM degli oggetti tenuti in cache durante la navigazione Internet.		✓			
[ESCLUSIONE PER IP O MACADDRESS] Permette l'esclusione di alcuni host dal controllo e dalle statistiche del Proxy.		✓			
[BLOCCO PER IP O MAX ADDRESS] Gli host indicati non possono effettuare navigazione Internet.		✓			
[RESTRIZIONI PER GIORNI E ORARI] Consente di indicare un intervallo di orario e i giorni nei quali è possibile effettuare navigazione Internet.		✓			
[LIMITI SUL TRASFERIMENTO (UPLOAD E DOWNLOAD)] Permette di limitare la banda usata per le operazioni di Upload e di Download per interfaccia e per singolo host.		✓			
[LIMITAZIONI SUL CONTENUTO DEI DOWNLOAD] Effettua un controllo sulla tipologia dell'oggetto che si desidera scaricare ed eventualmente ne impedisce il download.		✓			
[FILTRO SUI TIPI MIME] Permette il blocco dei tipi MIME indicati.		✓			
[CONTROLLO SUI BROWSER] Controlla e permette l'inibizione alla navigazione dai browser indicati e degli add-on browser specificati.		✓			
[METODI DI AUTENTICAZIONE (LOCALE, IDENTDM, LDAP, WINDOWS, RADIUS)] Consente l'autenticazione degli utenti per l'accesso a Internet.		✓			
[ESCLUSIONE DOMINI DALL'AUTENTICAZIONE] Possibilità di accesso diretto ai domini indicati senza necessità di autenticazione.		✓			
[RESTRIZIONI BASATE SUI NOMI UTENTE (DOMINIO WINDOWS)] Utenti del dominio Windows a cui è consentita la navigazione.		✓			
[FILTRAGGIO DELLE URL E DEI DOMINI (PER CATEGORIE, BLACKLIST, WHITELIST)] Blocco della navigazione a siti per categoria di appartenenza, per black list e white list personalizzate.		✓			
[BLOCCO DEI FILES PER ESTENSIONE] Blocco del download/esecuzione di files per estensione.		✓			
[REINDIRIZZAMENTO DOWLOAD VERSO FILES LOCALI] Possibilità di reindirizzamento ad un repository locale automaticamente alla richiesta di download di un file.		✓			
[AGGIORNAMENTO AUTOMATICO DELLE BLACKLIST] Aggiornamento manuale o automatico della blacklist su cui si basa il filtraggio delle URL.		✓			
[QoS LAYER 7] Controllo della qualità del servizio a livello layer 7			✓		
[QoS PORT] Controllo della qualità del servizio per porta sorgente/destinazione.			✓		
[SISTEMA DI RILEVAMENTO INTRUSIONE (PER TUTTE LE INTERFACCE)] Controllo di accessi non autorizzate e possibili minacce/attacchi su tutte le interfacce presenti.				✓	
[AGGIORNAMENTO REGOLE] Possibilità di attivare l'autoaggiornamento delle regole IDS per l'apprendimento di nuovi exploit, vulnerabilità, ecc				✓	
[ANTISPAM SCANNING] Filtro antispam della posta in entrata ed in uscita.					✓

ML INFORMATICA SRL

UFFICI: Via Martiri di Nassirya, 18 – 23900 Lecco (LC)

Email: info@mlinformaticasrl.it

WEB: http://www.mlinformaticasrl.it

Telefono: 0341499590 Fax: 0341259684

P.IVA e CF 02861890131 C.C.I.A.A. Lecco n° 300331

[SPAM QUARANTINE] Possibilità di mettere in quarantena gli elementi di posta riscontrati come spam.					✓
[SPAM DELETE] Possibilità di eliminare gli elementi riconosciuti come spam.					✓
[SPAM MARK] Possibilità di marcare l'oggetto dei messaggi riconosciuti come spam.					✓
[MAIL ANTIVIRUS] Scansione in tempo reale della posta in ingresso ed in uscita con gestione della quarantena suddivisa.					✓
[RINOMINA ALLEGATI PERICOLOSI] Consente di ridenominare gli allegati riconosciuti potenzialmente pericoli per impedirne l'accidentale esecuzione.					✓
[INDIRIZZI MAIL USATI IN WHITE LIST] Possibilità di inserimento nella white list degli indirizzi usati per l'invio di posta.					✓
[WHITE LIST] Indirizzi in white list amministrabile via http.					✓
[BLACK LIST] Indirizzi in black list amministrabile via http.					✓
[WHITE LIST USER ADMIN] Possibilità da parte degli utenti di inserire autonomamente indirizzi in white list.					✓
[AUTO PULIZIA QUARANTENA] Gestione automatica della rimozione degli elementi in quarantena per un periodo superiore a quello indicato.					✓
[SPAM QUARANTINE / DELETE] Possibilità di quarantena, eliminazione o marchiatura dei messaggi riconosciuti come spam.					✓
[SPAM SCORE MODIFICABILE] Gestione della soglia di spam modificabile.					✓
[DAILY SPAM DIGEST] Invio di un report giornaliero via mail agli indirizzi indicati con il resoconto delle attività anti spam.					✓
[BAYESIAN SCORING] Processo anti spam basato sulle bayesiane e sull'autoapprendimento degli "errori" commessi.					✓
[RAZOR, DCC, DNSBL, RULES DU JUR, GERMAN RULES] Processi Antispam automatici.					✓
[LOG] Log grafici e testuali delle attività svolte dai processi. Possibilità di monitoraggio delle risorse di sistema e dei processi attivi.	✓	✓	✓	✓	✓

ALL-IN-ONE

L'appliance viene fornito munito di tutto quello che serve per il funzionamento e adeguato alla realtà ed al contesto in cui verrà introdotto.

MODULARITA'

Per la sua natura modulare, l'appliance è inseribile nella realtà senza produrre scompensi alla produttività del Sistema Informativo. I vari moduli sono infatti attivabili separatamente ed in momenti diversi consentendo di lasciare inalterate le configurazioni già presenti e di testare nel frattempo le nuove funzionalità offerte.

NOLEGGIO

La formula di noleggio garantisce il massimo risparmio e protezione degli investimenti. Non è necessario acquistare nessun hardware o software, è richiesto solo un contributo di attivazione ed un canone mensile che garantisce anche le parti hardware dello stesso.

ML INFORMATICA SRL

UFFICI: Via Martiri di Nassirya, 18 – 23900 Lecco (LC)

Email: info@mlinformaticasrl.it

WEB: <http://www.mlinformaticasrl.it>

Telefono: 0341499590 Fax: 0341259684

P.IVA e CF 02861890131 C.C.I.A.A. Lecco n° 300331