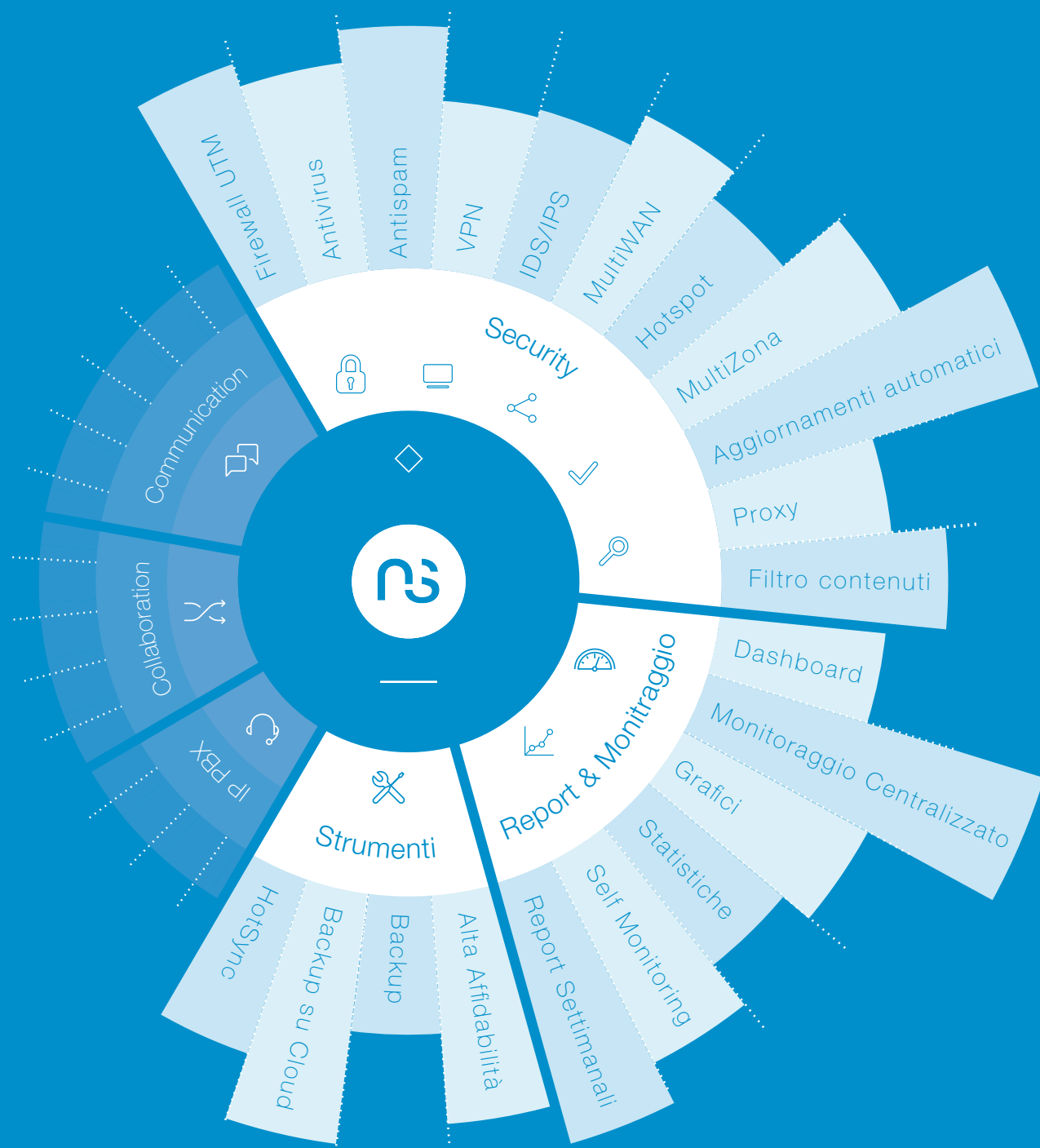




security

Firewall UTM





NethSecurity è un sistema completo ed affidabile per la gestione della sicurezza aziendale, la protezione della rete, il controllo dell'accesso a siti indesiderati e la creazione di collegamenti protetti via Internet (VPN) con utenti mobili o uffici remoti. Posto sull'unico punto di accesso ad Internet filtra all'ingresso tutti i tipi di attacchi da virus, tentativi di intrusione ad opera di hacker o utenti non autorizzati.

La versatilità dell'ambiente Linux e l'utilizzo di tecnologie OpenSource garantiscono elevata affidabilità e rapidità negli aggiornamenti.

NethSecurity è la versione enterprise del firewall UTM integrato nel progetto opensource nethserver (www.nethserver.org), avviato da Nethesis, animato e sviluppato da una fervente community.

Servizi di Base

Gestione utenti

Un pannello dedicato permette di definire le policy utente relative a diversi servizi: blocco totale della navigazione, assegnazione ad uno specifico profilo del filtro contenuti, abilitazione all'utilizzo di VPN.

Oltre alla gestione di utenti locali NethSecurity può integrarsi ad un Active Directory, ereditandone utenti e gruppi, per la definizione dei profili di utilizzo della rete.

Gestione MultiWAN

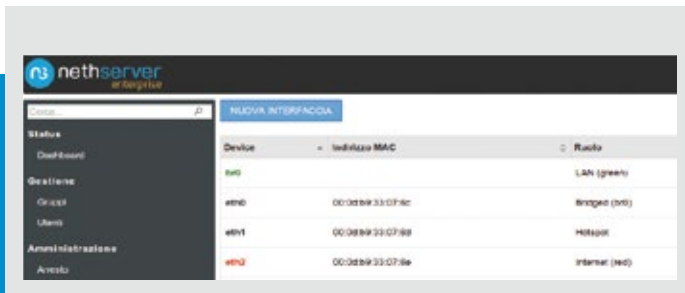
NethSecurity supporta connessioni multiple ad internet (fino a 15 differenti connettività) gestibili in base alle esigenze dell'amministratore: Load Balancing per sommare la banda delle connessioni, Fault Tolerance per spostare il traffico su connessioni di backup in caso di guasti della principale.

Fault Tolerance Dischi

Se installato su hw dotato di più dischi, NethSecurity attiva il miglior livello di fault tolerance possibile abilitando vari livelli di Raid (1,5,6 + hotspare). Lo storage così ottenuto, oltre ad avere alte prestazioni e fault tolerance, viene monitorato dal centro servizi che notifica eventuali fail sui singoli dischi.

Gestione reti

NethSecurity gestisce differenti tipi di zone pensate per compiti specifici (LAN, DMZ, HotSpot, VoIP, VPN, WAN..) ogni zona può essere associata a più interfacce fisiche o virtuali senza alcuna limitazione.



Protezione e Sicurezza Rete Interna

Scansione email: Antivirus/Antispam/Blocco degli allegati

Tutte le email che attraversano il firewall vengono sottoposte ad un attento filtro che verifica la presenza di minacce o contenuti pericolosi (Virus, Spam, Phishing, Malware...)

Il motore di scansione si basa su firme opensource, firme customizzate da Nethesis o direttamente su sistemi commerciali. L'antispam raggiunge percentuali altissime di riconoscimento spam grazie all'utilizzo di tre tipologie di analisi: regole euristiche, statistiche (Bayesiane) e blacklist esterne.

La scansione delle email è attivabile anche in modalità proxy, per proteggere le email dirette verso un mail server interno.

Backup su cloud

NethSecurity invia automaticamente il backup delle proprie configurazione sul Cloud Nethesis, consentendo restore sempre aggiornati ed immediatamente disponibili.

VPN

E' possibile stabilire connessioni cifrate per collegare tra loro sia sedi remote (VPN o Net2Net) che host remoti (VPN Host2Net). I differenti protocolli supportati (I2tp, OpenVPN, IPsec) assicurano l'interoperabilità con qualsiasi pc client (Linux, Windows, Mac), con smartphone/tablet (Android e iOS) e con apparati di rete di terze parti.

Firewall

NethSecurity integra un potente firewall ed un sistema IPS (Intrusion Protection System).

Grazie a questi servizi è possibile bloccare tutti gli accessi non autorizzati e tentativi di intrusione di hacker, spyware o software ostile.

Controllo Traffico in Uscita

Navigazione Web: Filtro contenuti, Antivirus, Antimalware

Impostare dei filtri sulla navigazione è ormai fondamentale per ottimizzare l'utilizzo della connessione Internet ed accrescere la sicurezza, prevenendo anche un uso improprio della rete (perdita di tempo, problemi di reputazione, virus, malware, spyware...).

NethSecurity garantisce questa protezione attraverso due strumenti fondamentali:

- L'antivirus web (con firme opensource o commerciali) che scansiona tutto il traffico relativo alla navigazione e blocca ogni download di contenuti infetti.
- Filtro Contenuti: cataloga i siti indesiderati in base alla categoria di appartenenza e associa gli utenti della rete ad un profilo di navigazione in base al gruppo di appartenenza o a regole su calendario settimanale.

L'autenticazione può essere sul db utenti locale o su Active Directory, mentre la definizione dei gruppi può essere fatta anche in base a gruppi di PC o subnet.

La categorizzazione dei siti avviene tramite liste locali fornite da vari progetti opensource, oppure liste Cloud ottenute dall'integrazione con il servizio Flashstart by Collini Consulting, che garantisce aggiornamenti giornalieri e oltre 50 categorie disponibili.

The image shows two screenshots from the NethServer web interface. The left screenshot displays the 'Active Flows' configuration page, where a rule named 'orari ufficio' is being configured. The right screenshot shows a table of 'Active Facebook Flows' with the following data:

Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thrt	Total Bytes	Info
Facebook	TCP	massimopc.50483	edge-star-eth-01-ita	2 h, 1 min, 43 sec	Client Server	0 bps	858.58 KB	
Facebook	TCP	andrea.nethsec.it.33044	edge-star-eth-01-cdg	1 h, 52 min, 10 sec	Client Server	0 bps	296.96 KB	
Facebook	TCP	alexis.nethsec.it.36916	edge-star-eth-01-cdg	1 h, 7 min, 15 sec	Client Server	0 bps	293.44 KB	
Facebook	TCP	stefano.nethsec.it.42026	edge-star-eth-01-cdg	2 min, 58 sec	Server	552.46 bps	223.47 KB	
Facebook	TCP	alexis.nethsec.it.41679	2.226.46.10	4 min, 49 sec	Client Server	210.78 bps	23.42 KB	
Facebook	TCP	alexis.nethsec.it.37306	edge-star-eth-01-cdg	1 min, 27 sec	Client Server	210.78 bps	11.44 KB	
Facebook	TCP	PC-DavidM.nethsec.it.33393	edge-star-eth-01-cdg	31 sec	Client Server	0 bps	8.18 KB	
Facebook	TCP	andrea.nethsec.it.34312	edge-star-eth-01-cdg	1 sec	Client Server	0 bps	7.96 KB	
Facebook	TCP	PC-DavidM.nethsec.it.30414	edge-star-eth-01-ita	1 sec	Client Server	0 bps	4.01 KB	
Facebook	TCP	stefano.nethsec.it.52150	2.226.46.10	2 min, 58 sec	Client Server	447.07 bps	2.48 KB	

Gestione del traffico

NethSecurity filtra tutto il traffico secondo regole impostate dall'amministratore, ogni regola utilizza a sua volta degli oggetti che permettono di mantenere una configurazione snella e di facile comprensione.

E' possibile regolamentare anche il traffico VPN, permettendo così l'accesso alle sole risorse strettamente necessarie per gli utenti che si connettono da remoto a tutto vantaggio della sicurezza della rete.

Il drag & drop delle regole, consente di modificarne rapidamente l'ordine di esecuzione (e quindi il comportamento del firewall).

E' possibile impostare priorità sul tipo di traffico o sulle sorgenti utili ad esempio per favorire il traffico VoIP rispetto all'email, o per dare sempre priorità massima o minima ad host specifici.

The image shows a screenshot of the 'Regole del traffico' (Traffic Rules) configuration page in NethServer. It displays a list of rules with the following details:

- Rule 1: ACCEPT, Action: ACCEPT, Direction: In, Protocol: TCP, Source: 192.168.1.0/24, Destination: 192.168.1.0/24, Action: ACCEPT.
- Rule 2: ACCEPT, Action: ACCEPT, Direction: In, Protocol: TCP, Source: 192.168.1.0/24, Destination: 192.168.1.0/24, Action: ACCEPT.
- Rule 3: ACCEPT, Action: ACCEPT, Direction: In, Protocol: UDP, Source: 192.168.1.0/24, Destination: 192.168.1.0/24, Action: ACCEPT.
- Rule 4: ACCEPT, Action: ACCEPT, Direction: In, Protocol: TCP, Source: 192.168.1.0/24, Destination: 192.168.1.0/24, Action: ACCEPT.
- Rule 5: ACCEPT, Action: ACCEPT, Direction: In, Protocol: TCP, Source: 192.168.1.0/24, Destination: 192.168.1.0/24, Action: ACCEPT.
- Rule 6: REJECT, Action: REJECT, Direction: In, Protocol: TCP, Source: 192.168.1.0/24, Destination: 192.168.1.0/24, Action: REJECT.

Reportistica e Monitoraggio

Report di Navigazione

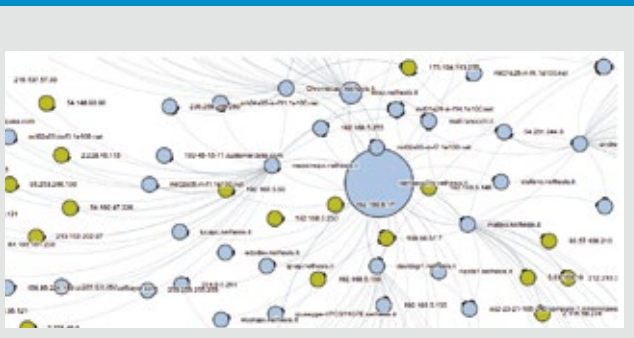
La reportistica di navigazione è dettagliata e semplice da consultare, anche da parte di personale non tecnico. Per ogni computer viene riportato l'elenco dei siti visitati, comprensivo del traffico scambiato e degli orari di navigazione. I dati sono archiviati all'interno del firewall e costituiscono uno storico completo sempre disponibile per la consultazione.

#	Total	Accessed site	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	Total
1	230.2	it.archive.ubuntu.com					230.2	565.7	114.9	239.7				21.7	1.3						
2	50.2	archive.canonical.com					50.2														
3	43.7	download.ubuntu.com						43.7													
4	40.8	repository.ubuntu.com											40.8								
5	27.5	security.ubuntu.com					0.7	0.2	27.5												
6	8.5	cdimage.ubuntu.com											8.5	10.8							
7	9.3	iso.ubuntu.com												9.3							
8	9.3	iso.ubuntu.com												9.3							
9	6.0	iso.ubuntu.com							6.0												
10		iso.ubuntu.com																			



Analisi Traffico

Il monitor della rete controlla tutto il traffico che attraversa il firewall consentendo di individuare l'utilizzo della banda e il tipo di traffico effettuato dai vari device aziendali. Tramite tabelle e grafici viene mostrato in tempo reale l'utilizzo della banda, consentendo all'amministratore di individuare sia gli host più attivi che il tipo di traffico effettuato. Sono disponibili anche dati aggregati che permettono di analizzare la situazione in diversi intervalli temporali.



Dettaglio Traffico L7

Il monitor di rete genera report dettagliati sull'utilizzo della banda da parte di ogni IP interno (LAN, DMZ, etc.). Tramite tabelle e grafici vengono mostrati i computer che fanno più traffico con dettaglio a livello applicativo (posta, facebook, skype, twitter...) permettendo, ad esempio, di individuare rapidamente un PC compromesso che sta inviando spam o una macchina che sta utilizzando software P2P.

Geolocalizzazione

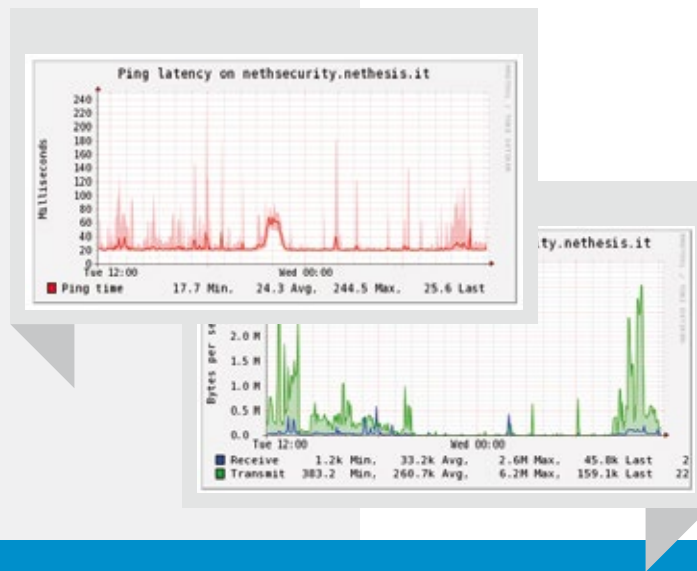
The geolocalization interface includes a map of Europe with several locations marked in red. Below the map is a detailed traffic log table with the following columns: Application, L4 Proto, Client, Server, Duration, Breakdown, Actual Tgbit, Total Bytes, and Info.

Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Tgbit	Total Bytes	Info
SMTP	TCP	giacomo.nethesis.135927	server-54-243-193-46...:1935	2 h, 19 min, 33 sec	Server	0 tbit	95.59 MB	
SMTP	TCP	filippo@th.nethesis...:54261	server-54-243-193-46...:1935	1 h, 2 min, 40 sec	Server	0 tbit	88.03 MB	
HTTP	TCP	giacomo.nethesis.149589	log2018.discoursefor...:80	2 h, 15 min, 47 sec	Server	0 tbit	50.45 MB	/?_id=1436289331822
ICMP	ICMP	diana.nethesis.8	nethsecurity.nethesis...	5 days, 1 h, 32 min, 12 sec	Server	3.06 Kbit	36.77 MB	
ICMP	ICMP	marco.nethesis.8	nethsecurity.nethesis...	5 days, 1 h, 32 min, 36 sec	Server	0 tbit	27.44 MB	
SSH	TCP	tom@15-136-46-35...:22	android.nethesis.8:4373	8 min, 45 sec	Client	3.67 Kbit	24.08 MB	
Tarzan	TCP	andrea.nethesis.103405	199.16.156.102:443	2 days, 2 h, 5 min, 24 sec	Server	0 tbit	22.58 MB	
ICMP	ICMP	imap.nethesis.1	nethsecurity.nethesis...	5 days, 1 h, 32 min, 51 sec	Server	376.85 tbit	19.7 MB	
ICMP	ICMP	ivan@lako.nethesis.8...	nethsecurity.nethesis...	5 days, 1 h, 32 min, 43 sec	Server	376.85 tbit	19.7 MB	
ICMP	ICMP	ivan@lako.nethesis...	nethsecurity.nethesis...	5 days, 1 h, 32 min, 35 sec	Server	376.85 tbit	19.69 MB	
SQL	TCP	alexis.nethesis.100242	ml.discourse.org:443	1 h, 48 min, 3 sec	Server	34.05 Kbit	12.69 MB	meta.discourse.org

Grafici Latenza

I grafici di latenza descrivono la qualità della connettività in termini di latenza e pacchetti persi ed è possibile ricevere allarmi via email se tali parametri superano determinate soglie personalizzabili.

È possibile calcolare la qualità non solo della connettività internet ma di qualsiasi interconnessione, ponti radio, VPN e collegamenti infrasede.



Report Firewall

Il firewall di NethSecurity produce una reportistica accurata e di semplice consultazione: è possibile risalire all'indirizzo IP da cui proviene l'attacco, sapere a chi è assegnato o capire la tipologia della "tentata intrusione".

Questi dati vengono archiviati all'interno di NethSecurity e possono essere esportati per eventuali indagini.

Backup fatto	Integrità sistema	SNMP striscia	RAID monitorato	Netbios monitorato	Funzionamento mail proxy	Server Backup (prevenzione dati mancanti)
	09-04-2015 11:22:09					
	07-04-2015 02:08:57					
28-02-2015 01:09:25 12-03-2015 02:01:02	01-04-2015 04:07:09				12-04-2015 01:16:36	
	02-02-2015 18:58:42					
						02-02-2015 01:28:46
12-03-2015 04:09:32	12-03-2015 05:15:38	12-03-2015 03:08:01				
12-03-2015 04:09:32	12-03-2015 04:10:27					

Aggiornamento Continuo e Monitoraggio

Un sistema di sicurezza non aggiornato e non monitorato, diventa inefficace dopo poco tempo; per questo motivo le soluzioni Nethesis sono caratterizzate da due elementi fondamentali:

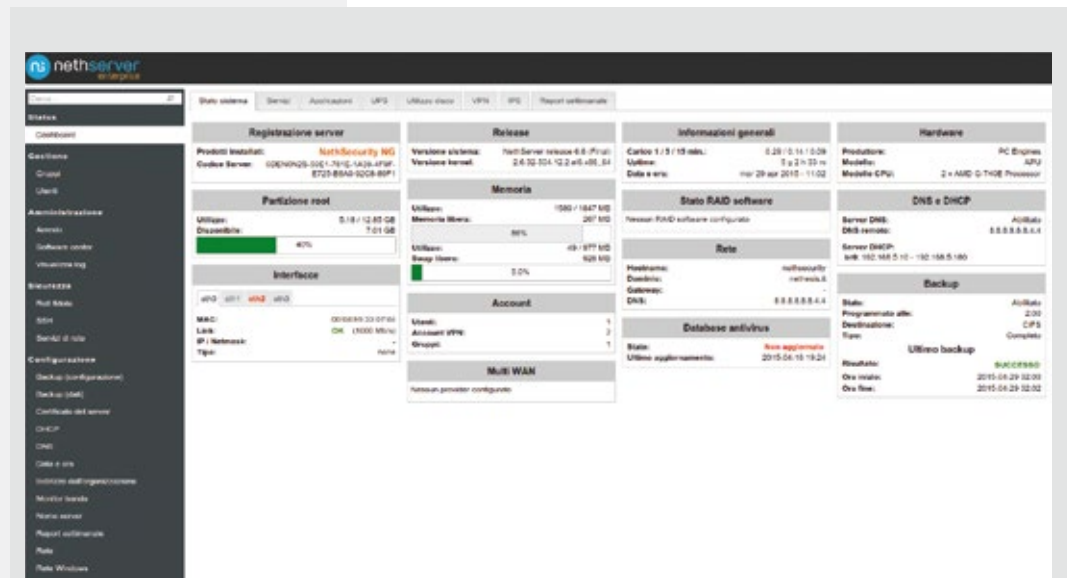
- Aggiornamento automatico di tutti i moduli critici (definizione dei virus, regole antispam, tabella intrusione hacker, etc.).
- Monitoraggio remoto tramite il centro servizi Nethesis: verifica il corretto funzionamento del sistema e avverte l'amministratore in caso di anomalie (aggiornamenti non effettuati, PC infetti, problemi di connettività, etc.).

Stato del Sistema

Attraverso una serie di tabelle e grafici, l'amministratore di rete può analizzare lo stato dei servizi, la configurazione e l'utilizzo delle risorse hardware del sistema, intervenendo tempestivamente (anche da remoto) in caso di necessità.

Dashboard

Permette di avere una panoramica sullo stato di funzionamento della macchina tramite widget di agevole consultazione. Tali report vengono generati a partire dalle statistiche di alcuni parametri di funzionamento come: utilizzo cpu, utilizzo dischi, carico medio, utilizzo memoria, qualità linea Internet, utilizzo partizioni.



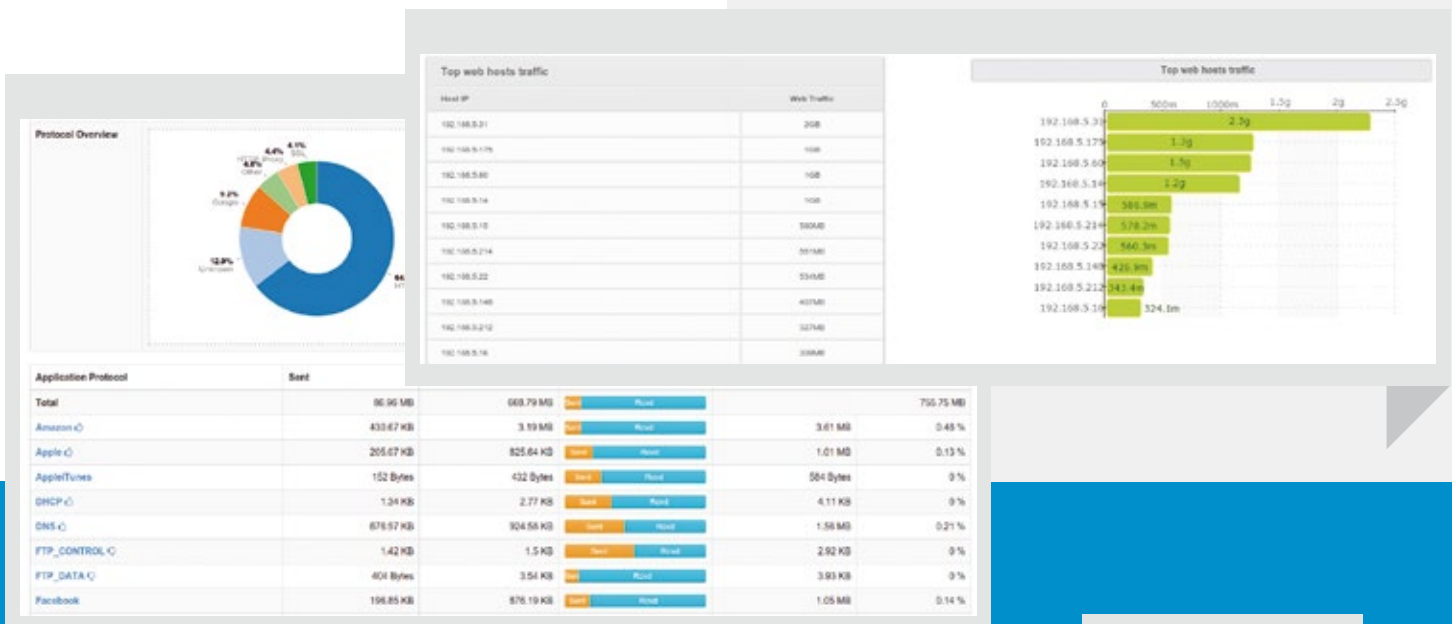
Report Settimanale

I tanti moduli di reportistica e monitoraggio di nethsecurity producono una grande quantità di informazioni con dettaglio tecnico particolarmente approfondito, normalmente indirizzate all'analisi e valutazione di personale tecnico.

In realtà il reale destinatario di queste informazioni non sempre deve essere il referente tecnico, ma può essere il titolare o il direttore che deve poter valutare in maniera semplice, accorpata e leggibile il corretto utilizzo dello strumento internet all'interno dell'azienda. Il taglio tecnico di certi report rende questa operazione difficile se non mediata da una elaborazione successiva da parte dei tecnici. Il report settimanale di nethsecurity risponde proprio a questa esigenza, in quanto accorpa, semplifica e rende leggibili le informazioni salienti relative all'utilizzo aziendale di internet.

Queste informazioni sono di facile reperimento per il manager in quanto è il firewall stesso che si preoccupa di inviare settimanalmente via email un cruscotto riepilogativo ai vari destinatari, inserendo per ciascuno i soli report assegnati al profilo di appartenenza (tecnico, commerciale, amministratore...)

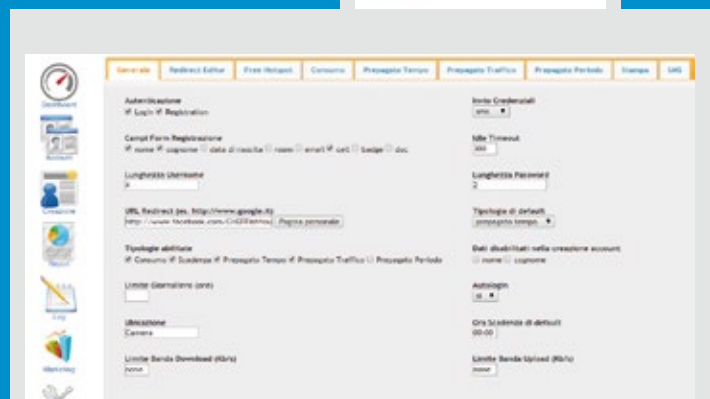
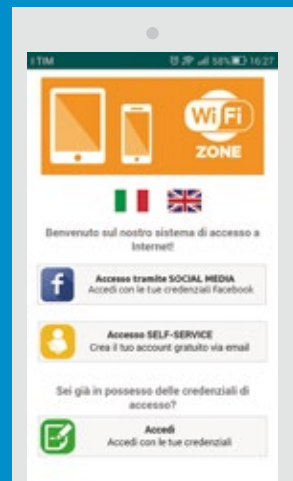
Questo rende NethSecurity non solo uno strumento particolarmente sicuro, ma anche in grado di relazionarsi adeguatamente con i vari referenti aziendali.



HotSpot

Permette di regolamentare, tracciare e tariffare l'accesso ad Internet nei luoghi pubblici (Internet point, hotel e fiere). Divide la rete aziendale dalla rete ospiti e regola in maniera sicura l'accesso ad Internet: la rete aziendale, protetta dal firewall, avrà libero accesso ad Internet, mentre la rete "ospiti" gestita dall'HotSpot, richiederà "utente" e "password", attivando una tariffazione a consumo, a scadenza, prepagata o libera.

Oltre alla possibilità di autenticarsi con tagliandini e credenziali fornite dall'amministratore del servizio, l'hotspot di Nethesis permette vari metodi di autenticazione selfservice tramite email, sms o integrando i più diffusi social network.



'nethesis

Strada degli Olmi, 12
61122 - Pesaro (PU)

Tel: +39 0721 1791157
Fax: +39 0721 268147
info@nethesis.it
www.nethesis.it