nethesis

nethsecurity

Firewall UTM

Affidabile

La versatilità dell'ambiente Linux e l'utilizzo di tecnologie Open Source garantiscono elevata affidabilità e rapidità negli aggiornamenti.
NethSecurity è la versione enterprise del firewall UTM integrato nel progetto Open Source Nethserver (www.nethserver.org), avviato da Nethesis ed ora animato e sviluppato da una fervente community.

Sicuro

Per Nethesis la sicurezza è di primaria importanza e NethSecurity ha in sè tutte le funzioni del firewall UTM:

- Antivirus/Antispam su email
- Filtro Contenuti, Antivirus, Antimalware
- IDS/IPS
- VPN IPSec, Openvpn, L2TP
- Filtri su Applicazioni e Geolocalizzati

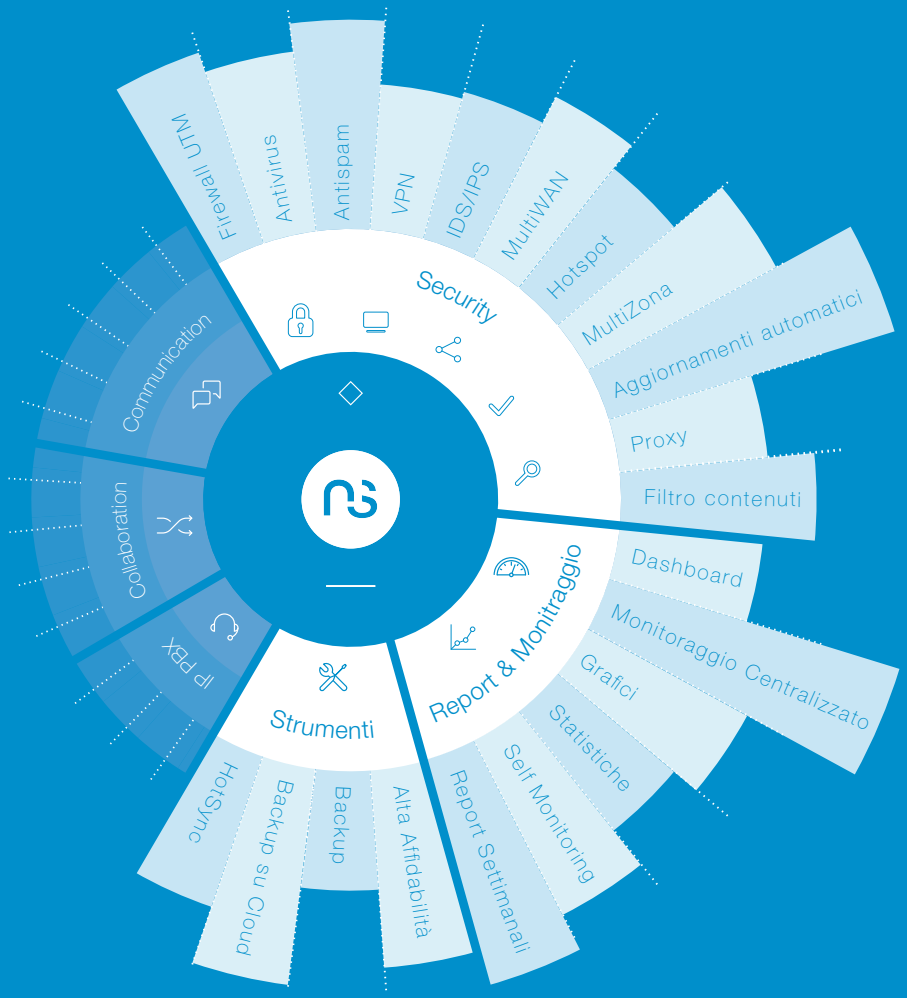
Analisi approfondita

NethSecurity è dotato di una ricca reportistica che permette di avere un'ampia panoramica sullo stato del sistema e del traffico della rete. Nello specifico:

- Monitoraggio Centralizzato
- Analisi Proattiva Eventi/Stati
- Geolocalizzazione traffico
- Report Navigazione e Traffico Applicativo

Completo

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.



Alcuni servizi base:

- Multiwan: Balance Failover
- QoS, Priorità Traffico
- Gestione Rete: vlan, bonding, bridge, alias...
- Multizona: Interna, Wan, DMZ, Ospiti, VoIP...
- Backup in Cloud
- Utenti Locali e AD
- NAT/Routing
- Fault Tolerance Storage

Protezione e Sicurezza Rete Interna

Firewall

NethSecurity evolve da semplice firewall UTM a coordinatore del processo di sicurezza: Content Filtering, AntiVirus, AntiSpam, AntiMalware, Monitoring, IDS/IPS, Deep Packet Inspection, Filtri per Applicazione (L7), VPN,... tutti elementi fondamentali, che NethSecurity integra e gestisce in maniera semplice e organica

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 (l2tp, 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.

Scansione email: Antivirus Antispam e 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…). 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.

Navigazione web: Antivirus/Antispam/Blocco degli allegati

La regolamentazione della navigazione è fondamentale per accrescere la sicurezza e prevenire un uso improprio della rete: perdita di tempo, problemi di reputazione, virus, malware, spyware...
NethSecurity risponde con il Filtro Contenuti Cloud: cataloga i siti visitati in base alla categoria di appartenenza e definisce profili di navigazione secondo vari criteri: tipologia sito, gruppo di lavoro, orari, calendario settimanale...
La categorizzazione dei siti è realizzata grazie all'integrazione del servizio Cloud Flashstart by Collini Consulting, che garantisce:

- blacklist ottimizzate per il mercato italiano, grazie agli strumenti di analisi semantica basati su pattern nazionali
- filtro nativo sulle ricerche di Google e Bing: per filtri su immagini e video
- filtro per area geografica, particolarmente utile contro le crescenti minacce di Ransomware. E' fondamentale bloccare su richiesta il traffico verso Paesi a rischio cyber-informatico
- filtri per Malware: blocca all'origine tutti i server compromessi e sorgenti di Malware

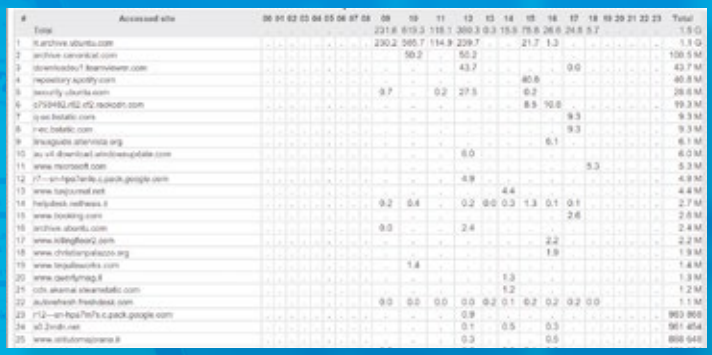
Gestione Traffico per Applicazione (L7)

NethSecurity è in grado di riconoscere diverse centinaia di tipologie di traffico, in base alle applicazioni che lo stanno generando (social network, p2p, chat, streaming, voip…)
Il traffico riconosciuto può essere facilmente gestito, con le varie regole di blocco, gestione priorità, limitazione banda o indirizzamento su specifiche connettività.

Reportistica e Monitoraggio

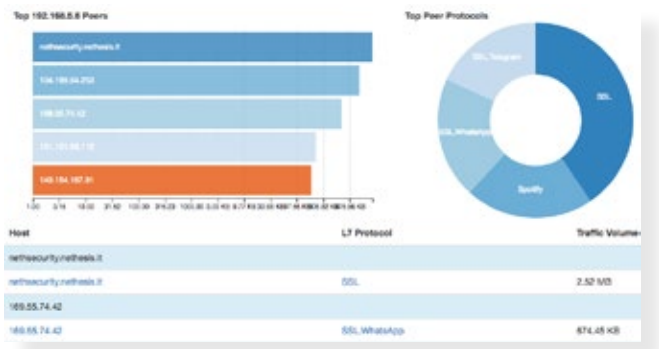
Report di Navigazione

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.



Analisi Traffico

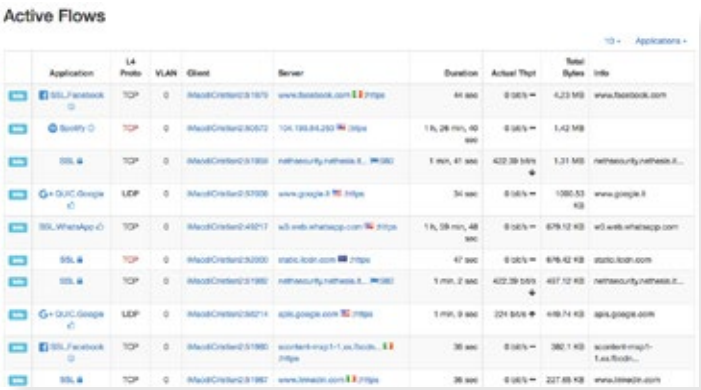
Il monitor della rete controlla tutto il traffico che attraversa il firewall consentendo di individuare l'utilizzo della banda e il tipo di traffico effettuato dai vari device aziendali.
Tramite tabelle e grafici viene mostrato in tempo reale l'utilizzo della banda, consentendo all'amministratore di 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.

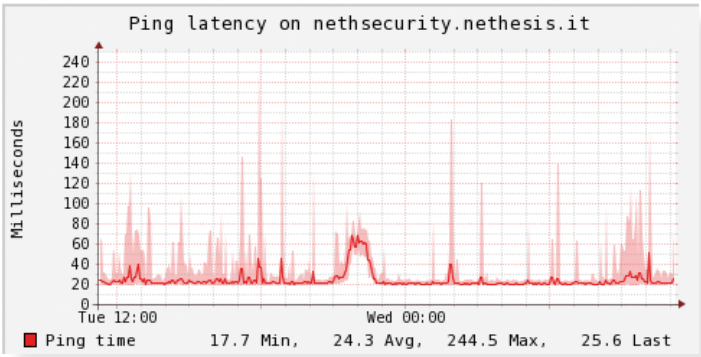


Controllo traffico L7

Il monitor di rete genera report dettagliati sull'utilizzo della banda da parte di ogni IP interno (LAN, DMZ...).
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



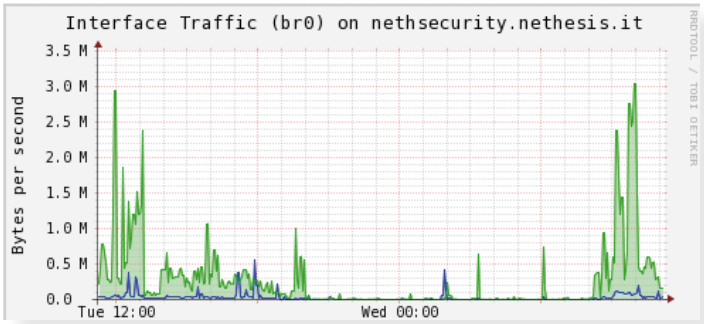


Grafici Latenza

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.



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.

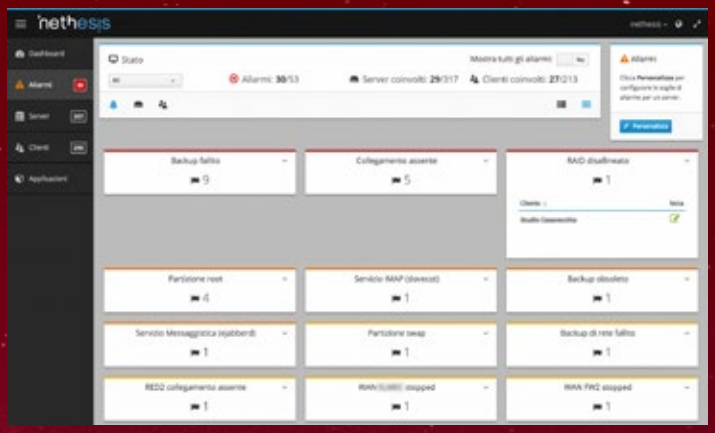
Dashboard

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.

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...).
- 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...).



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.

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.

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.

Backup su cloud

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

High Availability

NethSecurity, grazie al modulo HA attivabile sugli appliance S150, può lavorare in alta affidabilità Attiva/Passiva, azzerando così l'interruzione di servizio in caso di guasto.