



Three blue squares and one red square are positioned in the upper left corner of the image.

# NXGATE

Controllo totale della rete  
In un ambiente sicuro

**NEXTWORKS**  
HEADING THE FUTURE

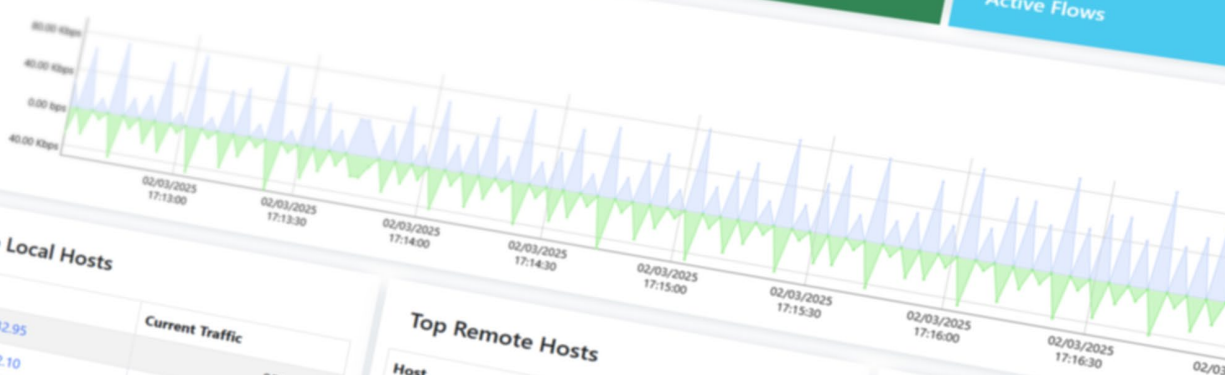


Engaged Alerts

32 Active Hosts

113 Active Flows

### Interfaces Traffic



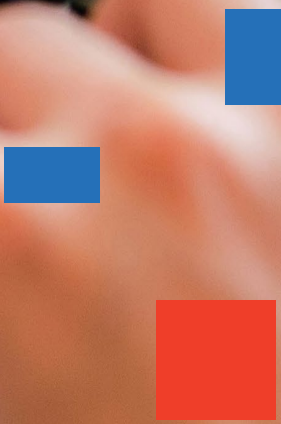
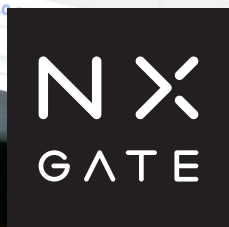
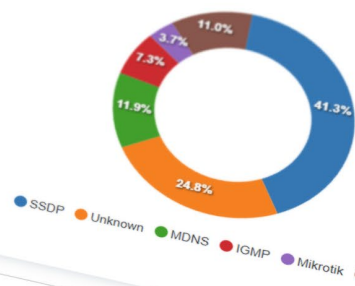
### Top Local Hosts

Host	Current Traffic
192.168.32.95	858.90 bps
192.168.32.10	700.10 bps
192.168.33.253	265.30 bps
192.168.20.253	255.80 bps
192.168.40.253	255.80 bps
192.168.30.253	255.80 bps

### Top Remote Hosts

Host	Current Traffic
10.0.4.50	37.20 Kbps
10.0.2.185	28.70 Kbps
8.8.8.8	8.40 Kbps
10.0.4.255	304.50 bps
10.0.4.19	132.60 bps
10.0.4.1	105.60 bps

### Top Applications





# Più controllo, meno problemi. La tua rete, come dovrebbe essere.

I tuoi asset digitali e le tue operazioni online potranno contare su strumenti avanzati per una rete più sicura, controllata ed efficiente:

- **Controllo Totale in un Ambiente Sicuro**
- **Gestione e Supervisione delle Policy**
- **Analisi del Traffico e dei Flussi**
- **Multi-WAN, Failover & Bonding**
- **Monitoraggio Avanzato dei Dispositivi Attivi e Latenti**
- **Suddivisione in Sezioni per Servizio e Classi di Utenti profilate**
- **Gestione e Controllo del Traffico tra le Diverse Applicazioni e Servizi (Layer 7)**
- **Filtro avanzato del traffico multicast**

**NXGate** fornisce protezione alla tua LAN, garantendo un accesso sicuro e controllato alle risorse digitali. La comunicazione tra dispositivi e asset avviene in un ambiente sicuro.

**NXGate** supervisiona il flusso di dati, prevenendo minacce, ottimizzando la connettività e assicurando un utilizzo efficiente della rete.



NXGate può operare come:

## BRIDGE

NXGate crea un bridge trasparente tra la rete locale (LAN) e la rete esterna (WAN), consentendo al traffico di transitare senza alterare la configurazione esistente. Le policy di rete configurate vengono applicate direttamente sul traffico che attraversa il bridge, garantendo sicurezza e controllo senza impattare l'infrastruttura.

**Questa è la modalità ideale se hai bisogno di un metodo rapido e trasparente per proteggere e monitorare le comunicazioni LAN-WAN senza dover riconfigurare dispositivi o indirizzi IP.**

## ROUTER

NXGate opera come un router, instradando il traffico di rete e applicando regole di gestione per decidere quali connessioni inoltrare e quali bloccare. Inoltre NXGate può controllare interfacce WAN Multiple, scegliere quale attivare o disattivare, distribuire il traffico in modo dinamico e ottimizzare l'utilizzo delle risorse di rete.

**Questa è la modalità ideale se si vuole configurare un router (multi-WAN) con instradamento basato sui singoli dispositivi, VLAN, utenti o su applicazioni Layer-7 per gruppi di utente con funzionalità captive portal.**

## Controllo totale in un ambiente sicuro



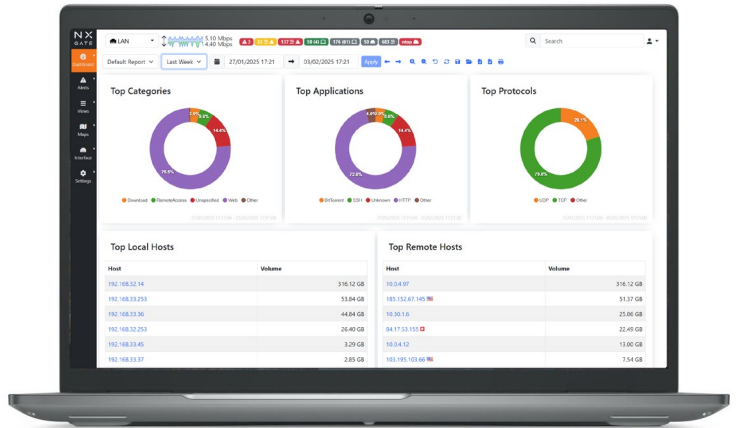
Supporta gli amministratori di rete nella gestione efficiente di infrastrutture complesse, offrendo un'interfaccia web intuitiva per monitorare l'utilizzo della banda e controllare i dispositivi connessi.

**NXGate consente di impostare facilmente limiti di download e upload, garantendo un funzionamento stabile e ottimizzato della rete.**

### ESEMPI D'USO

*"Consenti agli ospiti di navigare senza restrizioni fino al raggiungimento di 10 GB di consumo giornaliero, dopodiché limita la velocità"*

*"Assegna una quota fissa di banda del 20% per il personale."*



## Sicurezza avanzata



NXGate integra un **sistema di DNS sicuro con liste di IP e domini per garantire una protezione continua.**

Se un dispositivo tenta di connettersi a un host malevolo o se un host malevolo prova a raggiungere la rete, NXGate genererà automaticamente un avviso di sicurezza, segnalando una potenziale violazione dei dati in corso.

### ESEMPI D'USO

*"Quando un numero anomalo di richieste improvvise inizia a sovraccaricare i server, NXGate riconosce un tentativo di attacco e genera un avviso automatico, bloccando il traffico sospetto prima che causi una interruzione del servizio."*

Serial	Application	Proto	Client	Server	First Seen	Duration	Score	Breakdown	Actual Thpt	Total Bytes	Info
1	HTTP	TCP	10.0.4.97	192.168.32.16	02/03/2025 14:20:10	03:15:12	100	Green	5.80 Mbps	7.11 GB	
2	? Unknown	UDP	84.17.53.155	192.168.32.253	02/03/2025 16:50:10	45:12	10	Yellow	269.20 Kbps	118.19 MB	
3	? Unknown	TCP	10.0.4.12	80006	02/03/2025 16:18:26	01:16:56	10	Green	344.50 Kbps	54.88 MB	
4	? Unknown	UDP	192.168.33.253	84.17.53.155	02/03/2025 14:20:06	03:15:16	10	Yellow	14.90 Kbps	40.53 MB	
5	QUIC.GoogleD	UDP	192.168.33.36	74.125.8.160	02/03/2025 17:32:42	01:32	100	Green	4.30 Mbps	15.06 MB	r11-sm-SF
6	ICMP	ICMP	8.8.8.8	10.0.4.51	02/03/2025 14:34:18	03:01:04	10	Green	1.70 Kbps	7.69 MB	Echo reply
7	? Unknown	UDP	216.128.11.190	192.168.32.253	02/03/2025 15:56:34	01:38:44	10	Green	10.50 Kbps	5.91 MB	
8	QUIC.GoogleD	UDP	192.168.33.36	74.125.8.160	02/03/2025 17:34:48	00:24 sec	100	Green	4.30 Mbps	5.06 MB	r11-sm-SF
9	QUIC.GoogleD	UDP	192.168.33.36	173.194.188.9	02/03/2025 17:33:12	01:02	100	Green	1.00 Mbps	1.96 MB	r4-sm-SF
10	Telegram	TCP	149.154.167.89	192.168.33.37	02/03/2025 16:24:36	01:10:46	100	Green	1.50 Kbps	1.32 MB	
11	? Unknown	UDP	10.0.3.197	393004	02/03/2025 17:05:23	29:59	100	Green	3.00 Kbps	1010.69 KB	
12	Telegram	TCP	149.154.167.89	192.168.33.37	02/03/2025 16:24:36	01:10:46	100	Green	1.60 Kbps	838.01 KB	
13	QUIC.GoogleD	UDP	192.168.33.36	142.250.203.106	02/03/2025 17:15:53	19:29	100	Green	7.00 Kbps	757.03 KB	signal-p
14	? Unknown	UDP	103.195.103.66	10.0.4.51	02/03/2025 17:33:18	02:04	10	Yellow	117.60 Kbps	758.21 KB	



# Gestione e controllo del traffico Layer-7



Gestire le policy sui protocolli Layer-7 significa avere il **pieno controllo su quali servizi e applicazioni possono essere utilizzati all'interno della rete**. È possibile definire regole precise per stabilire chi può accedere a determinati contenuti, come bloccare l'accesso a siti di streaming video per tutti gli utenti connessi alla rete, utilizzare specifiche categorie o inviare dati, garantendo sicurezza e conformità alle esigenze operative. NXGate permette di farlo senza alterare la topologia di rete, evitando costi aggiuntivi e conflitti con l'infrastruttura esistente.

## ESEMPI D'USO

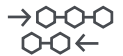
*"Limita l'accesso a YouTube, Facebook e ad altri social network, in base alle tue policy di rete"*

*"Limita la velocità di download per i servizi di file sharing (Google Drive, Dropbox, WeTransfer)"*



# Segmentazione granulare del servizio

Nel **modello zero-trust** usato da NXGate, nessun dispositivo è considerato affidabile a priori: ogni connessione deve essere verificata. **Decidi esattamente cosa ogni dispositivo è autorizzato a fare nella tua rete**: invece di aprire la rete a qualsiasi accesso e utente, definisci regole specifiche per ogni tipo di servizio, in base alle sue reali necessità. Un sensore, ad esempio, non ha bisogno di navigare in Internet, ma solo di inviare dati a un sistema centrale. Un sistema di prenotazione può mostrare una pagina web al pubblico, ma non accedere ai dati interni.



Con NXGate, **ogni funzione è isolata, controllata e protetta**, senza interferenze o accessi indesiderati. Il risultato è **una rete più sicura, più leggera e più ordinata**, dove ogni elemento opera esclusivamente nell'ambito delle autorizzazioni assegnate.

## ESEMPI D'USO

*"Permetti ai terminali dei sistemi di pagamento elettronico di trasmettere dati solo ai gateway di pagamento certificati, impedendo connessioni non autorizzate."*

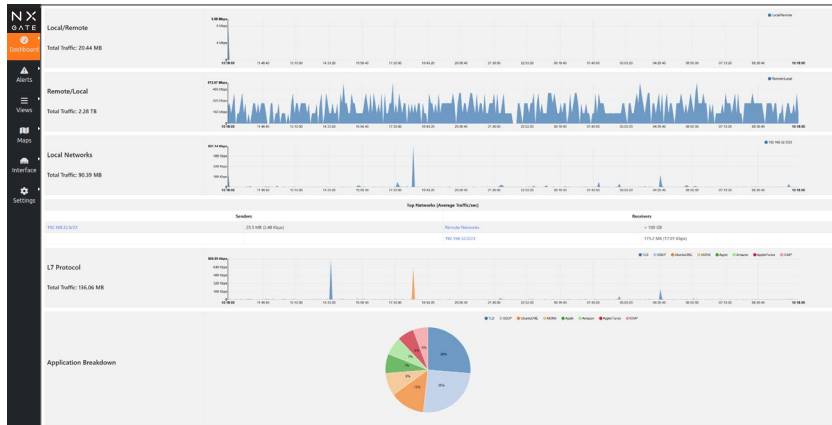
*"Consenti alle videocamere di sorveglianza di comunicare solo con il server del sistema di registrazione video, bloccando qualsiasi altro tipo di connessione in uscita"*





## Monitoraggio avanzato dei dispositivi

**NXGate monitora e classifica tutti i dispositivi connessi alla rete, inclusi quelli inattivi**, identificando tipologia, categoria, modello e sistema operativo quando possibile, con la possibilità di scaricare **report dettagliati sull'attività dei dispositivi per un'analisi e una gestione avanzata della rete**. Inoltre, rileva i nuovi accessi in tempo reale e invia notifiche per dispositivi sconosciuti, garantendo un controllo costante e una maggiore sicurezza della rete.



## Multi-WAN, Failover & Bonding

**La gestione multi-WAN è la soluzione ideale per garantire una connettività stabile e continua**, indipendentemente dalle condizioni della rete, l'intuitiva interfaccia di NXGate offre un metodo semplice per attuarla.

Un sistema avanzato di **Failover** consente di **passare automaticamente tra diverse connessioni Internet** - da Starlink al 5G fino ai Gateway WiFi - **assicurando una rete sempre disponibile e performante**.

Il **Bonding** di rete di NXGate permette inoltre di **aggregare più interfacce di rete in un'unica interfaccia WAN**. Questa configurazione determina l'**aumento della velocità della connessione media**, il **bilanciamento del carico di traffico** tra le interfacce e garantisce **stabilità e tolleranza agli errori** (es. in caso di guasto di un link, il traffico viene reindirizzato automaticamente).



# Suddivi la tua rete in sezioni dedicate per servizio e classi di utenti, ciascuna gestita tramite VLAN

**Garantisci a ogni categoria di utenti un ambiente digitale separato, con livelli di accesso e privilegi personalizzati.**

Separare le reti per utenti amministrativi, ospiti e personale operativo migliora la sicurezza, riduce il rischio di interferenze tra dispositivi e previene la condivisione accidentale o indesiderata di contenuti multimediali.

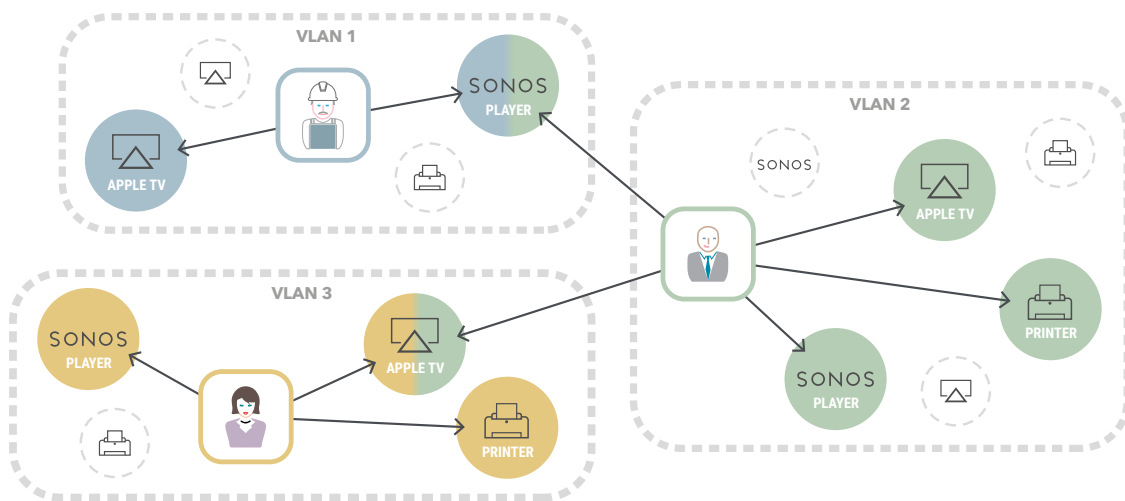
## FILTRO AVANZATO TRAFFICO MULTICAST

La nuova funzionalità di filtro avanzato del traffico multicast consente all'amministratore di rete di gestire in modo molto semplice il flusso dei dati tra una VLAN e l'altra, **specificando, per ciascuno utente, quale traffico e servizio multicast rendere disponibile e "visibile" e quale, invece no.**

NXGate permette inoltre di bloccare il traffico multicast in modo monodirezionale.

### ESEMPI D'USO

*"Impedisci che un utente connesso alla rete possa inviare contenuti a dispositivi AirPlay o vedere speaker audio non autorizzati, evitando errori e violazioni di privacy."*



## VELOCIZZA LA MANUTENZIONE

La manutenzione dell'infrastruttura IT diventa notevolmente più snella ed efficiente, consentendo interventi su singole sezioni della rete senza influenzare le altre. Gli aggiornamenti e le riparazioni diventano così un processo rapido e mirato.



<b>Web GUI</b>	<ul style="list-style-type: none"> <li>• Accesso disponibile tramite qualsiasi browser web compatibile con HTML5</li> <li>• Supporto TLS/HTTPS</li> </ul>
<b>Protocolli</b>	<ul style="list-style-type: none"> <li>• Ethernet</li> <li>• IPv4/IPv6</li> <li>• TCP/UDP/ICMP</li> <li>• GRE</li> <li>• DHCP/BOOTP/NetBIOS/DNS...</li> <li>• 250+ Layer-7 protocolli applicativi supportati da nDPI</li> <li>• ...e molti altri</li> </ul>
<b>Caratteristiche aggiuntive</b>	<ul style="list-style-type: none"> <li>• Dominio Internet, AS, StatisticheVLAN</li> <li>• Gestione protocolli per tutti gli applicativi supportati da nDPI</li> </ul>

## CARATTERISTICHE PRINCIPALI

Tra i criteri di selezione del traffico di rete vi sono l'indirizzo IP, la porta, i protocolli applicativi Layer-7 (L7), throughput e gli Autonomous Systems (ASs)

Visualizza il traffico di rete in tempo reale e gli host attivi

Produzione di report a lungo termine per diverse metriche di rete, tra cui il throughput e i protocolli applicativi L7.

Top talkers (trasmissione/ricezione), top ASs, top protocolli applicativi L7

Monitoraggio e segnalazione in tempo reale del throughput, delle latenze di rete e delle applicazioni, Round Trip Time (RTT), statistiche TCP (ritrasmissioni, pacchetti fuori ordine, pacchetti persi), byte e pacchetti trasmessi.

Memorizzazione su disco delle statistiche di traffico persistenti per consentire interrogazioni future e analisi post-mortem.

Geolocalizzazione e sovrapposizione degli host in una mappa geografica

Individuazione dei protocolli applicativi Layer-7 (Facebook, YouTube, BitTorrent, ecc.) sfruttando la tecnologia nDPI, Deep Packet Inspection (DPI).

Analisi del traffico IP e smistamento in base alla sorgente/destinazione.

Rapporti sull'utilizzo del protocollo IP ordinati per tipo di protocollo

Produzione statistiche sul traffico di rete

Supporto completo del Layer-2 (comprese le statistiche ARP)

Esplorazione interattiva dei dati storici monitorati

Gestione flessibile degli allarmi

Supporto SNMP v1/v2c e monitoraggio continuo dei dispositivi SNMP

Focalizzazione sulla visibilità del traffico e sulla sicurezza informatica.

Analisi comportamentale del traffico e rilevamento periodico del traffico.

REST API per facilitare le integrazioni con terze parti.

## CARATTERISTICHE PRINCIPALI

---

Identificazione dei protocolli applicativi (Facebook, Youtube, BitTorrent, ecc.) nella rete.
Registrazione e visualizzazione dell'utilizzo storico dei protocolli applicativi degli host (timeseries)
Individuazione dei dispositivi collegati alla rete locale (Network Discovery)
Accesso a tutti i Behavioural Check
Identificazione dei top talkers (mittenti e destinatari) host con risoluzione al minuto
Visualizzazione dei principali siti HTTP contattati da un host
Generazione di avvisi (per Flussi, Host, Interfacce, ...) quando vengono rilevate determinate condizioni (superamento di una soglia, comportamento sospetto, ...)
Ricezione di notifiche di allarme come e-mail, Discord, Telegram, WebHook, Slack, messaggi Syslog o Shell Scripts
Limitazione o blocco del traffico degli host con criteri personalizzati per applicazione.
Visualizzazione e storicizzazione di altri dati (Interface Score Anomalie, Top Talkers, ...)
Generazione di report grafici dei principali host, protocolli applicativi, paesi, reti e sistemi autonomi in qualsiasi intervallo di tempo configurabile.
Consultazione dei dati dei dispositivi SNMP, come lo stato delle porte, il traffico e le informazioni sull'indirizzo MAC.
Rapporti sul traffico totale e sulle attività per qualsiasi host, rete o interfaccia.
Identificazione di attacchi e vittime attraverso un dashboard di allerta in tempo reale ed elenco attività passate
Esplorazione e filtro degli avvisi di flusso nelle attività passate
Attivazione di avvisi in caso di comportamento SNMP anomalo
Applicazione di quote giornaliere di traffico e di tempo per protocollo
Mappa degli host

---

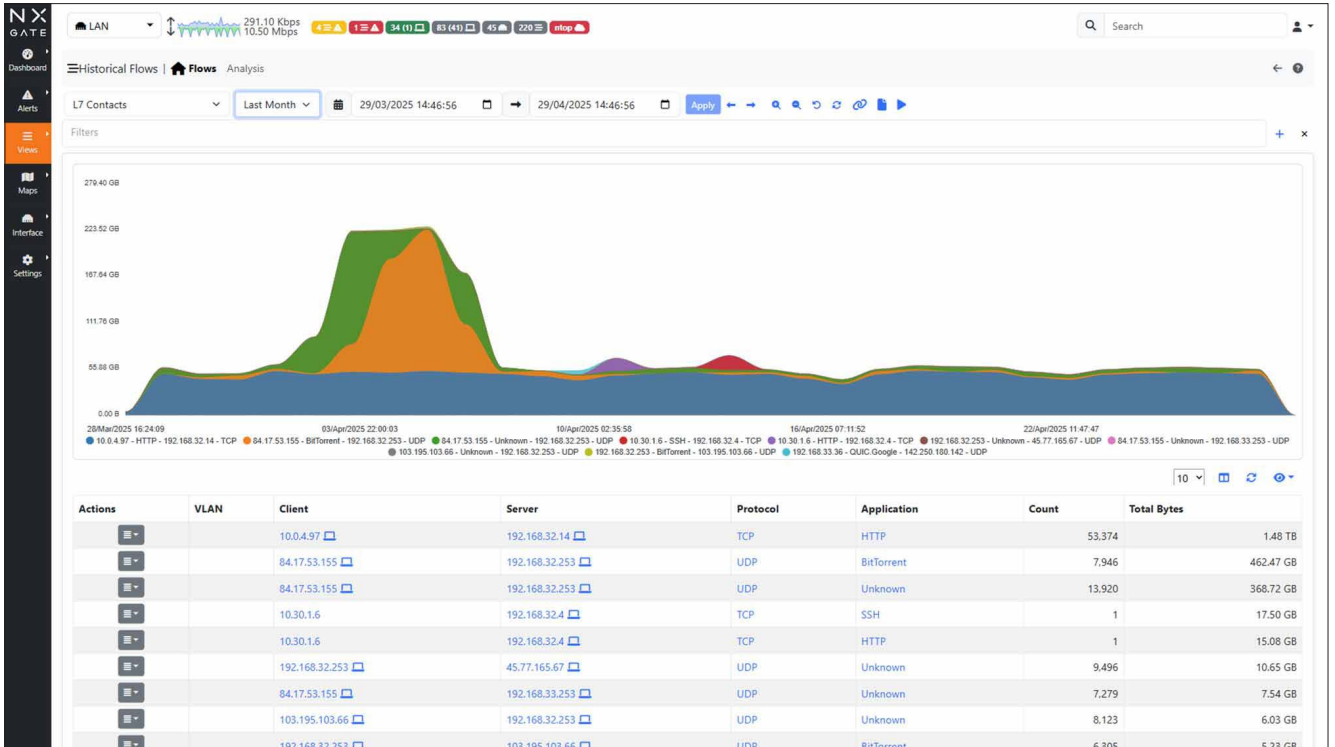
## SPECIFICHE MODELLO

---

Modello	W340	W3800
		
<b>Scheda principale</b>	Scheda industriale IPC	Scheda industriale IPC
<b>NIC</b>	4 x 2.5GbE (max 3 WAN)	8 x 1GbE (max 7 WAN)
<b>Telaio</b>	Lega di alluminio	Lega di alluminio
<b>Alimentazione</b>	Alimentatore esterno 12V	Alimentatore esterno 12V
<b>Consumi</b>	5 Watt (min) - 16 Watt max (a pieno carico)	10 Watt (min) - 14 Watt max (a pieno carico)
<b>Dimensioni</b>	60 X 109 X 43.5mm (WDH)	480 x 229 x 43mm (WDH, 1U rackmount)
<b>Temperatura d'esercizio</b>	-20 / 60° C	-20 / 60° C

---

# USER INTERFACE



Name	Family	Interface	Category	Severity	Description	Values	Action
Binary File/Data Transfer (Attempt)	Flow			Warning	Binary File/Data Transfer (Attempt)		
Possible Exploit	Flow			Error	Trigger an alert when a possible exploit is detected (e.g. Log4j/Log4Shell)		
TLS Fatal Alert	Flow			Notice	Trigger an alert when a fatal alert is detected in a TLS flow		
HTTP Susp. Header	Flow			Error	HTTP Susp. Header		
HTTP Susp. User-Agent	Flow			Error	HTTP Susp. User-Agent		
Blacklisted Server Contact	Flow			Critical	Trigger an alert when a localhost contacts a remote blacklisted host		
TCP With No Answer	Flow			Warning	Trigger an alert when detecting a TCP connection with no server answer		
Susp. Entropy	Flow			Notice	Detect suspicious data carried in ICMP packets whose entropy is suspicious and thus that it can indicate a data leak.		
Broadcast Non-UDP Traffic	Flow			Error	Trigger an alert when an host contacts a Broadcast address using a non-UDP protocol		
HTTP Obsolete Server	Flow			Warning	Trigger an alert when an obsolete HTTP server is contacted		

Showing 1 to 10 of 84 rows

**NOTES**

- Categories
  - Active Monitoring: Active monitoring alerting system (e.g., host unreachable).
  - Intrusion Detection and Prevention: Checks that evaluate the behavior of hosts and add them to the jailed hosts pool when deemed to be suspicious. When ntopng is used in combination with nProbe IPS, suspicious hosts are actually blocked and prevented from generating traffic.
  - Internals: Internal functionalities of NXGate (e.g., memory management and host and flows lifecycles)
  - Network: Network behaviors and anomalies (e.g., traffic above a certain threshold, TCP not working as expected)
  - Other: Default category for uncategorized scripts or for those that cannot be included in any of the other categories
  - Cybersecurity: Security behaviors and anomalies (e.g. contacts from or to a blacklisted host, TCP and UDP scans)
  - SNMP: SNMP devices status (e.g., Interface duplex status changes, SNMP device restart).
  - System: Functionalities of the system on top of which NXGate is running (e.g. disk space full, load too high)
- Interface
  - Check available for packet interfaces



**NXGATE**

**NEXTWORKS**  
HEADING THE FUTURE

[info@nextworks.it](mailto:info@nextworks.it)  
[www.nextworks.it](http://www.nextworks.it)

**HQ: via Livornese, 1027-29**  
**56122 Pisa (Italy)**

**Tel: +39-050-3871600**  
**Fax: +39-050-3871601**