



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

NXGATE

Total Network Control
In a Secure Environment

NEXTWORKS
HEADING THE FUTURE



NX
GATE

Engaged Alerts

32
Active Hosts

113
Active Flows

Interfaces Traffic



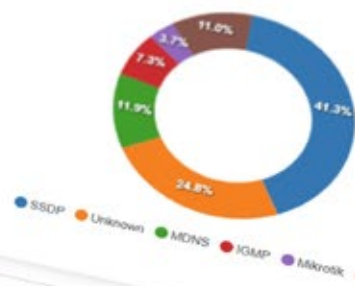
Top Local Hosts

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





More control, fewer issues. Your network, the way it should be.

Your digital assets and online operations can rely on advanced tools for a more secure, controlled, and efficient network:

- **Total Control in a Secure Environment**
- **Policy Management and Supervision**
- **Traffic and Flow Analysis**
- **Multi-WAN, Failover & Bonding**
- **Advanced Monitoring of Active and Idle Devices**
- **Segmentation by Service and User Class**
- **Application- and Service-Based Traffic Control (Layer 7)**
- **Advanced Multicast Traffic Filtering**

NXGate protects your LAN, ensuring secure and controlled access to digital resources. Device and asset communication take place in a secure environment.

NXGate oversees data flows, prevents threats, optimizes connectivity, and ensures efficient network usage.



NXGate can operate as:

BRIDGE

NXGate creates a transparent bridge between the local network (LAN) and the external network (WAN), allowing traffic to pass through without altering the existing configuration. Configured network policies are applied directly to the traffic passing through the bridge, providing security and control without impacting the infrastructure. **This mode is ideal if you need a quick and seamless way to protect and monitor LAN-WAN communication without reconfiguring devices or IP addresses.**

ROUTER

NXGate acts as a router, routing network traffic and applying management rules to determine which connections will be allowed and which will be blocked. It can also manage multiple WAN interfaces, activate or deactivate them as needed, dynamically distribute traffic and optimize resource usage. **This mode is ideal when you want to configure a (multi-WAN) router with routing based on specific devices, VLANs, users, or Layer-7 applications for user groups, complete with captive portal functionality.**

Total Control in a Secure Environment



NXGate supports network administrators in managing complex infrastructures efficiently, offering an intuitive web interface to monitor bandwidth usage and control connected devices.

NXGate lets you easily set download and upload limits, ensuring a stable and optimized network performance.

USE CASES

“Allow guests to browse freely until they reach 10 GB of daily usage, then apply a speed limit.”

“Assign a fixed 20% bandwidth quota to staff.”



Advanced Security

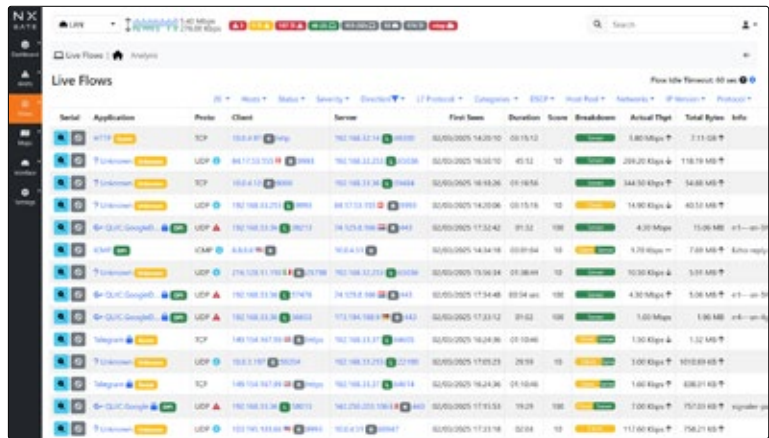


NXGate includes a **secure DNS system with IP and domain allowlists/denylists for continuous protection.**

If a device attempts to connect to a malicious host, or if a malicious host tries to access the network, NXGate will automatically generate a security alert, signaling a potential ongoing data breach.

USE CASES

“When an unusual number of sudden requests begins overloading the servers, NXGate detects a possible attack and automatically blocks suspicious traffic before it can disrupt the service.”





Layer-7 Traffic Management and Control



Managing policies for Layer-7 protocols means having **full control over which services and applications can be used within your network**. You can define detailed rules to specify who can access certain content, such as blocking video streaming sites for all users, applying category-based controls, or regulating data transfer to ensure operational compliance and security. NXGate allows all this without altering network topology, avoiding additional costs and conflicts with your existing infrastructure.

USE CASES

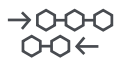
"Restrict access to YouTube, Facebook, and other social networks, according to your network policies."

"Limit download speeds for file sharing services (Google Drive, Dropbox, WeTransfer)."



Granular Service Segmentation

In NXGate's **zero-trust model**, no device is trusted by default: every connection must be verified. **You decide exactly what each device is allowed to do within your network**. Rather than opening access broadly, you define specific rules for each service based on actual needs. For example, a sensor only needs to send data to a central system, it doesn't need Internet access. A booking system may need to display a webpage to the public, but shouldn't access internal data.



With NXGate, **each function is isolated, controlled, and protected** from interference or unauthorized access. The result is **a network that's more secure, streamlined, and organized**, where each component operates strictly within its assigned permissions.

USE CASES

"Allow electronic payment terminals to transmit data only to certified payment gateways, blocking unauthorized connections."

"Allow surveillance cameras to communicate only with the video recording server, blocking all other outbound connections."





Advanced Device Monitoring

NXGate monitors and classifies all connected devices, including inactive ones, by identifying type, category, model, and OS where possible. It also provides downloadable **reports on device activity for advanced network analysis and management**.

Furthermore, it detects new connections in real time and sends alerts for unknown devices, ensuring constant control and enhanced network security.

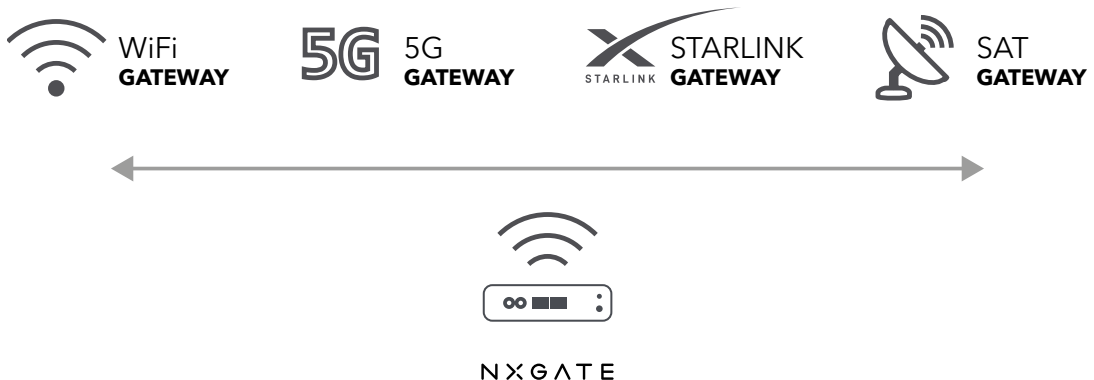


Multi-WAN, Failover & Bonding

Multi-WAN management is the ideal solution for ensuring stable, continuous connectivity, regardless of network conditions. NXGate’s intuitive interface makes this easy to implement.

An advanced **Failover** system enables **automatic switching between different Internet connections**, from Starlink to 5G and WiFi gateways, ensuring your **network is always available and high-performing**.

NXGate’s network **Bonding** feature **aggregates multiple interfaces into a single WAN interface**. This configuration **increases average connection speed, balances traffic load** across interfaces, and **ensures fault tolerance** (e.g., if a link fails, traffic is automatically rerouted).





Segment your network by service and user class, each managed through VLAN

Provide every user category with a dedicated digital environment, complete with customized access levels and privileges.

Separating networks for administrative staff, guests, and operational personnel improves security, reduces the risk of device interference, and prevents accidental or unauthorized media sharing.

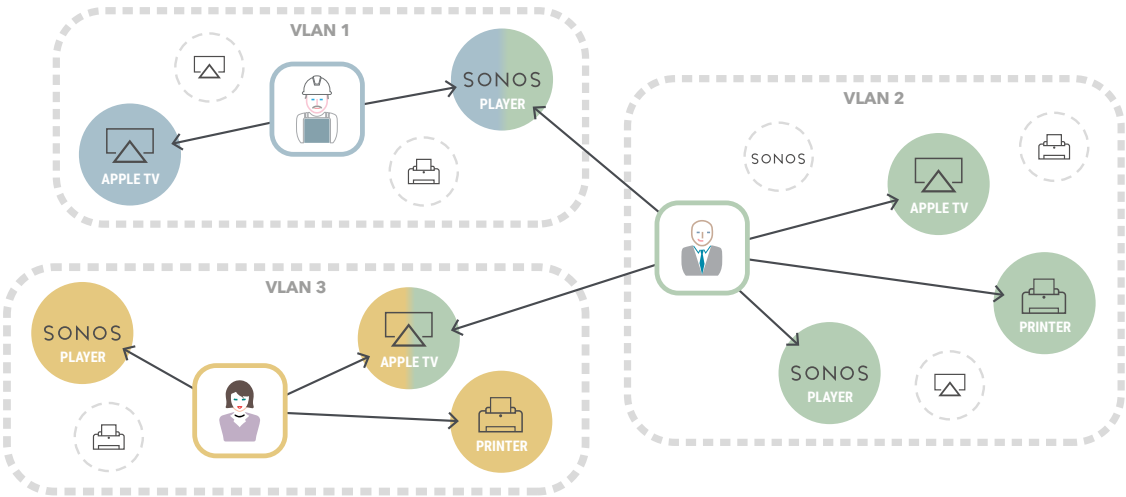
ADVANCED MULTICAST TRAFFIC FILTERING

The new advanced multicast traffic filtering feature allows network administrators to easily manage data flows between VLANs, **specifying for each user which multicast traffic and services should be available and "visible", and which should not.**

NXGate also allows one-way blocking of multicast traffic.

USE CASES

"Prevent a user on the network from sending content to AirPlay devices or seeing unauthorized audio speakers, avoiding mistakes and privacy violations."



FASTER MAINTENANCE

IT infrastructure maintenance becomes significantly more streamlined and efficient, allowing interventions on individual network segments without affecting others.

Updates and repairs thus become a fast, targeted process.



Web GUI	<ul style="list-style-type: none"> • Available through any HTML5-ready web browser • TLS/HTTPS support
Protocols	<ul style="list-style-type: none"> • Ethernet • IPv4/IPv6 • TCP/UDP/ICMP • GRE • DHCP/BOOTP/NetBIOS/DNS... • 250+ Layer-7 application protocols supported by nDPI • ...and many more
Additional Features	<ul style="list-style-type: none"> • Internet Domain, AS, VLAN (Virtual LAN) Statistics • Protocol decoders for all application protocols supported by nDPI

MAIN FEATURES

Sort network traffic according to many criteria including IP address, port, Layer-7 (L7) application protocols, throughput, Autonomous Systems (ASs)

Show realtime network traffic and active hosts

Produce long-term reports for several network metrics including throughput and L7 application protocols

Top talkers (senders/receivers), top ASs, top L7 application protocols

Monitor and report live throughput, network and application latencies, Round Trip Time (RTT), TCP statistics (retransmissions, out of order packets, packet lost), and bytes and packets transmitted

Store on disk persistent traffic statistics to allow future explorations and post-mortem analyses

Geolocate and overlay hosts in a geographical map

Discover Layer-7 application protocols (Facebook, YouTube, BitTorrent, etc) by leveraging on nDPI, Deep Packet Inspection (DPI) technology

Analyze IP traffic and sort it according to the source/destination

Report IP protocol usage sorted by protocol type

Produce network traffic statistics

Full Layer-2 support (including ARP statistics)

Interactive historical exploration of monitored data

Flexible alerts handling

SNMP v1/v2c support and continuous monitoring of SNMP devices

Focused on traffic visibility and cybersecurity.

Behavioral traffic analyses such as lateral movements and periodic traffic detection



REST API to ease integrations with third-parties.



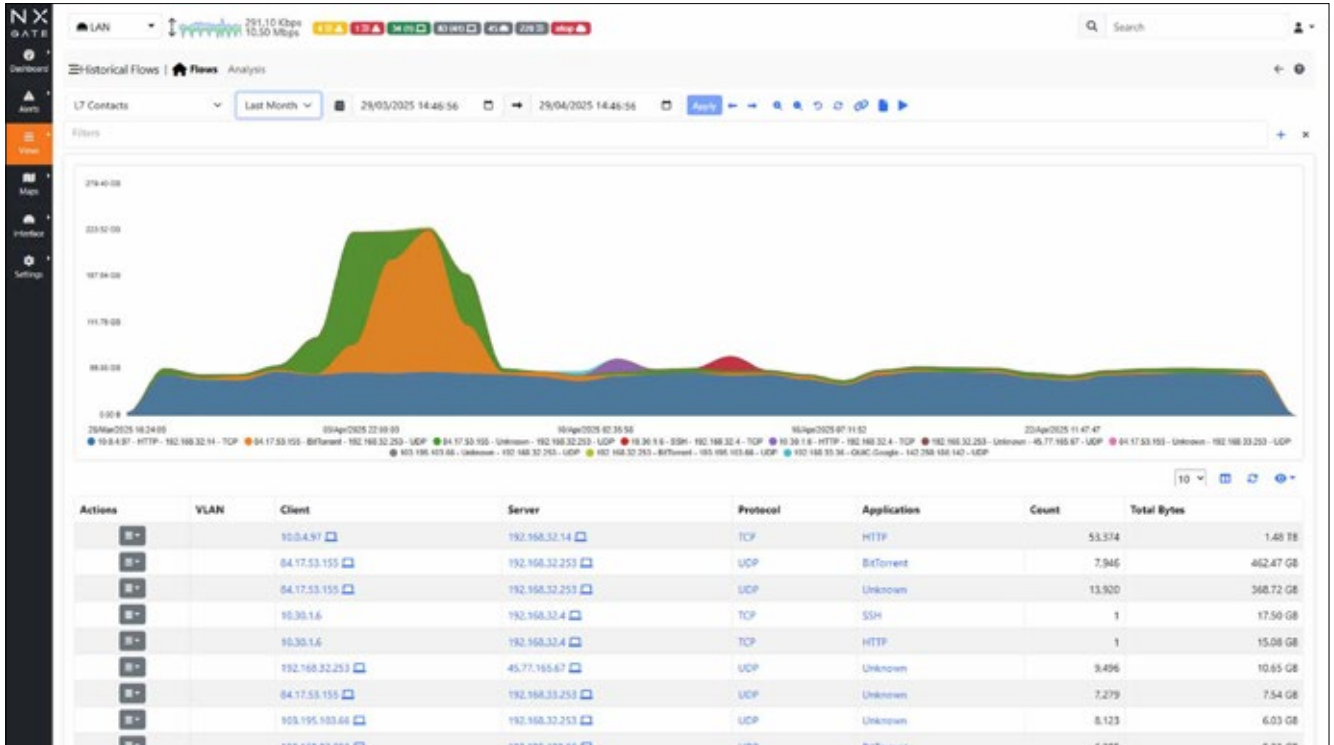
MAIN FEATURES

- Identify application protocols (Facebook, Youtube, BitTorrent, etc) in the network
- Record and Visualize hosts' historical application protocols usage (timeseries)
- Discover the devices connected to your Local Network (Network Discovery)
- Have access to all Behavioural Checks
- Identify top talkers (senders and receivers) hosts with minute resolution
- Visualise the top HTTP sites contacted by an host
- Generate alerts (for Flows, Hosts, Interfaces, ...) when certain conditions are detected (Threshold Crossed, Suspicious Behaviour, ...)
- Get alerts notifications as Email, Discord, Telegram, WebHook, Slack, Syslog messages or execute Shell Scripts
- Limit or block hosts' traffic with customized per-application policies
- Visualize and historicise other data (Interface Score Anomalies, Top Talkers, ...)
- Graphical reports with top hosts, application protocols, countries, networks, and autonomous systems within any configurable time frame
- Query SNMP devices data, such as port status, traffic and and MAC address information
- Get total traffic and activity reports for any given host, network, or interface
- Identify attackers and victims through an alerts dashboard in realtime and in the past
- Explore and filter flow alerts in the past
- Trigger alerts when SNMP unexpected behavior shows up
- Apply per-protocol daily traffic and time quotas to your clients
- Hosts Map (find the hosts outliers)

MODEL SPECIFICATIONS

Model	W340	W3800
		
Main board	Industrial IPC Board	Industrial IPC Board
NIC	4 x 2.5GbE (max 3 WAN)	8 x 1GbE (max 7 WAN)
Chassis	Aluminium alloy box	Aluminium alloy box
Power supply	External ac power adapter 12V	External ac power adapter 12V
Consumption	5 Watt (Idle) - 16 Watt Max (Full Load)	10 Watt (Idle) - 14 Watt Max (Full Load)
Dimensions	60 X 109 X 43.5mm (WDH)	480 x 229 x 43mm (WDH, 1U rackmount)
Operating temperature	-20 / 60° C	-20 / 60° C

USER INTERFACE



Behavioural Checks | All Host, Interface, Local Networks, SNMP, Flow, System, Active Monitoring, Syslog

All (121) Enabled (84) Disabled (37)

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

🛑 Disable All 🔄 Restore Checks Defaults

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 rtping 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 lifecycle)
 - 🏠 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
www.nextworks.it

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

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