

Disclaimer

Legal disclaimer

This guide and its contents (the "Guide") are provided by NXGEN. All rights to the Guide and to the intellectual property embodied in it — including, without limitation, trademarks, trade names, logos and similar marks appearing in or on it — are protected by law. All right, title and interest in the Guide and in any related intellectual property rights belong to and remain with NXGEN and its licensors.

The Guide is provided free of charge, "as is" and for informational purposes only, without warranty of any kind. It is neither intended nor suitable to establish any legal relationship between the reader and NXGEN or its affiliates, including, without limitation, any obligation of NXGEN or its affiliates toward the reader.

The obligations of NXGEN and its affiliates in respect of NXGEN products or services purchased by a customer are governed exclusively by the terms of the agreement under which those products or services were purchased.

For clarification

The reader bears the entire risk as to the use, results and performance of the Guide. To the fullest extent permitted by applicable law, NXGEN disclaims and excludes all warranties, whether statutory, express or implied — including, without limitation, implied warranties of merchantability, fitness for a particular purpose, title and non-infringement of third-party rights — as well as any liability or warranty arising from suggestions, specifications or samples related to the Guide.

VPN Datasheet

Updated 11 August 2026

Product Overview

NXGEN VPN is a fully managed secure connectivity solution that bridges your customers' surveillance environments — NVRs, cameras, recorders, and edge devices — with NXGEN's cloud and operations infrastructure. Purpose-built for surveillance integrators and MSPs, it eliminates the complexity of designing, operating, and troubleshooting VPN infrastructure, so your team can focus on delivering service rather than managing network plumbing.

Key Benefits

- Zero infrastructure burden — NXGEN manages all VPN operations centrally
- Always-on remote access to customer NVRs, cameras, and edge devices
- Faster incident response — authorized operators connect instantly to any site
- Optimized for low-latency video traffic across surveillance environments
- Flexible deployment across cloud, branch, and on-premise environments
- Multi-protocol support adapts to existing customer infrastructure
- NAT support handles overlapping or customer-specific IP addressing
- Scalable architecture supports high-volume multi-customer deployments

Primary Use Cases

- Connect customer NVRs and recorders to NXGEN-managed environments
- Secure communication with cameras and edge devices inside customer networks
- Remote troubleshooting and support access by authorized NXGEN operators

- Centralized access to multiple customer sites via a single VPN client
- Hybrid networking across cloud, branch, and on-premise surveillance sites
- Managed VPN for MSPs and integrators serving multi-tenant environments

Performance at a Glance

METRIC	VALUE
Uptime SLA	99.95% (AWS IPsec)
Typical Tunnel Latency	< 70ms
VPN Throughput	1 Gbps+ per tunnel
Encryption Standard	AES-256

VPN Connectivity — Primary Protocols

OpenVPN (Primary Protocol)

- Industry-standard SSL/TLS-based VPN
- Split tunnel — reduces unnecessary backhaul
- Operator PC client access (CloudConnexa)
- Ideal for remote access & multi-site connectivity
- Flexible port configuration (TCP/UDP)

IPsec (Primary Protocol)

- High-performance site-to-site tunnelling
- Route-based & AWS Site-to-Site VPN support
- BGP and static routing compatible
- Hardware-accelerated AES-256 encryption
- Best for branch and on-premise integrations

Also Supported

- WireGuard — Ultra-lightweight modern VPN protocol, ideal for performance-constrained edge devices
- Meraki VPN — Native integration for Meraki-based customer deployments

Operator VPN Access — Built-In Remote Reach

NXGEN provides OpenVPN client accounts for authorized operators, giving your team secure access to customer NVRs, recorders, and cameras from any location — without exposing those systems to the public internet. This means faster issue resolution, lower support costs, and a better service experience for your customers — all through a single, centrally controlled access layer.

Technical Specifications

Performance & Speed

SPECIFICATION	DETAILS
VPN Throughput	Up to 1 Gbps+ per tunnel (protocol and infrastructure dependent)
Encryption Overhead	Minimal — hardware-accelerated AES-256 via AWS infrastructure
Tunnel Latency	Typically < 70ms; varies by customer site geography
Concurrent Tunnels	Scalable — multiple concurrent site-to-site and operator tunnels supported
Video Traffic Handling	Optimized for continuous H.264/H.265 surveillance streams; split tunnel reduces unnecessary backhaul
Packet Loss	< 0.5% target under normal operating conditions

Supported VPN Protocols & Connectivity

SPECIFICATION	DETAILS
VPN Protocols	OpenVPN
Connectivity Types	OpenVPN CloudConnexa

Operator Access

OpenVPN client-based PC accounts for authorized NXGEN personnel

Authentication & Security

SPECIFICATION	DETAILS
Authentication Methods	Pre-Shared Keys (PSK)
Encryption Standard	AES-256 across all supported VPN technologies
Access Control	Centrally managed by NXGEN — no customer systems exposed directly to the internet
Audit & Logging	Full access logs maintained — who accessed which device and when

Routing & Traffic

SPECIFICATION	DETAILS
Routing Models	Static Routing
Tunneling	Split Tunnel (OpenVPN) to minimize bandwidth usage; Full Tunnel available
NAT Support	Available — handles overlapping or customer-specific IP addressing
QoS / Prioritization	Traffic prioritization for surveillance streams configurable per deployment

Availability & Resilience

SPECIFICATION	DETAILS
Uptime SLA	99.95% monthly uptime; higher resilience available for IPsec HA configurations
High Availability	IPsec Active/Passive HA and failover options supported — aligned with deployment design
Redundancy	Dual-tunnel configurations supported for automatic failover
Maintenance Windows	Planned maintenance conducted with minimal disruption; short windows designed to stay within SLA

Deployment & Infrastructure

SPECIFICATION	DETAILS
Infrastructure	AWS-based VPN gateway
Deployment Models	Cloud VPN Gateway
Connected Environments	NVRs
Onboarding Timeline	Typical deployment completed within 2–5 business days from engagement; complex multi-site rollouts scoped individually

Integrations

SPECIFICATION	DETAILS
Cloud Platform	AWS Networking Environment
Vendor Integrations	Meraki-Based Deployments

Management, Monitoring & Operations

SPECIFICATION	DETAILS
Management Model	Fully managed by NXGEN operations team
Monitoring	Centrally operated — tunnel health
Reporting	Operational status reports available as part of managed service engagement
Support Model	NXGEN team handles ongoing operations

Getting Started — Typical Onboarding Process

Most deployments are live within 2–5 business days. NXGEN handles all VPN design and configuration — customers simply provide their network details.

1. Discovery & Scoping — NXGEN reviews customer network topology, site count, and device requirements
2. Design & Configuration — VPN architecture designed and configured — protocols, routing, NAT, and auth selected

3. Testing & Validation — Tunnels tested end-to-end; latency, throughput, and failover confirmed
4. Go-Live & Monitoring — Monitoring and support activated

Contact

Contact us to discuss deployment options for your environment.

- NXGEN Technologies AG
- Website: www.nxgen.io
- Email: info@nxgen.io