

Haftungsausschluss

Rechtlicher Hinweis

Dieser Leitfaden und seine Inhalte (der „Leitfaden“) werden von NXGEN bereitgestellt. Alle Rechte am Leitfaden und am darin verkörperten geistigen Eigentum — einschließlich, aber nicht beschränkt auf Marken, Handelsnamen, Logos und ähnliche Kennzeichen im oder am Leitfaden — sind gesetzlich geschützt. Sämtliche Rechte, Ansprüche und Anteile am Leitfaden und an damit verbundenen Schutzrechten verbleiben bei NXGEN und seinen Lizenzgebern.

Der Leitfaden wird unentgeltlich, „wie besehen“ und ausschließlich zu Informationszwecken bereitgestellt, ohne jegliche Gewährleistung. Er ist weder dazu bestimmt noch geeignet, ein Rechtsverhältnis zwischen dem Leser und NXGEN oder seinen verbundenen Unternehmen zu begründen, einschließlich, aber nicht beschränkt auf Verpflichtungen von NXGEN oder seinen verbundenen Unternehmen gegenüber dem Leser.

Die Verpflichtungen von NXGEN und seinen verbundenen Unternehmen in Bezug auf von einem Kunden erworbene NXGEN-Produkte oder -Dienstleistungen richten sich ausschließlich nach den Bedingungen des Vertrags, unter dem diese Produkte oder Dienstleistungen erworben wurden.

Zur Klarstellung

Der Leser trägt das gesamte Risiko hinsichtlich der Nutzung, der Ergebnisse und der Leistung des Leitfadens. Soweit gesetzlich zulässig, schließt NXGEN alle Gewährleistungen aus, ob gesetzlich, ausdrücklich oder stillschweigend — einschließlich, aber nicht beschränkt auf stillschweigende Gewährleistungen der Marktgängigkeit, der Eignung für einen bestimmten Zweck, des Rechtsbestands und der Nichtverletzung von Rechten Dritter — sowie jegliche Haftung oder Gewährleistung aus Vorschlägen, Spezifikationen oder Mustern im Zusammenhang mit dem Leitfaden.

VPN-Datenblatt

Updated 11 August 2026

Produktübersicht

NXGEN VPN ist eine vollständig verwaltete Lösung für sichere Verbindungen, die die Überwachungsumgebungen Ihrer Kunden – NVRs, Kameras, Aufzeichnungsgeräte und Edge-Geräte – mit der Cloud- und Betriebsinfrastruktur von NXGEN verbindet. Die Lösung wurde speziell für Überwachungsintegratoren und MSPs entwickelt und beseitigt die Komplexität bei der Konzeption, dem Betrieb und der Fehlerbehebung der VPN-Infrastruktur, sodass sich Ihr Team auf die Bereitstellung von Dienstleistungen konzentrieren kann, anstatt sich um die Verwaltung der Netzwerkinfrastruktur kümmern zu müssen.

Die wichtigsten Vorteile

- Keine Belastung der Infrastruktur – NXGEN verwaltet den gesamten VPN-Betrieb zentral
- Ständiger Fernzugriff auf NVRs, Kameras und Edge-Geräte der Kunden
- Schnellere Reaktion auf Vorfälle – autorisierte Mitarbeiter können sich sofort mit jedem Standort verbinden
- Optimiert für Videodatenverkehr mit geringer Latenz in Überwachungsumgebungen
- Flexible Bereitstellung in Cloud-, Zweigstellen- und lokalen Umgebungen
- Die Unterstützung mehrerer Protokolle passt sich der bestehenden Infrastruktur des Kunden an
- Die NAT-Unterstützung bewältigt überlappende oder kundenspezifische IP-Adressierung
- Die skalierbare Architektur unterstützt groß angelegte Multi-Kunden-Implementierungen

Hauptanwendungsfälle

- Kunden-NVRs und -Recorder mit von NXGEN verwalteten Umgebungen verbinden
- Sichere Kommunikation mit Kameras und Edge-Geräten innerhalb von Kundennetzwerken
- Fernwartung und Supportzugriff durch autorisierte NXGEN-Mitarbeiter
- Zentraler Zugriff auf mehrere Kundenstandorte über einen einzigen VPN-Client
- Hybride Vernetzung zwischen Cloud, Zweigstellen und lokalen Überwachungsstandorten
- Managed VPN für MSPs und Integratoren in mandantenfähigen Umgebungen

Leistung auf einen Blick

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

VPN-Verbindung – Primäre Protokolle

OpenVPN (Primärprotokoll)

- VPN auf Basis von SSL/TLS nach Industriestandard
- Split-Tunnel – reduziert unnötigen Backhaul
- Zugriff auf den Operator-PC-Client (CloudConnexa)
- Ideal für Fernzugriff und die Vernetzung mehrerer Standorte
- Flexible Portkonfiguration (TCP/UDP)

IPsec (Primärprotokoll)

- Leistungsstarkes Site-to-Site-Tunneling
- Unterstützung für routenbasierte VPNs und AWS Site-to-Site-VPNs
- Kompatibel mit BGP und statischem Routing
- Hardwarebeschleunigte AES-256-Verschlüsselung
- Ideal für Filial- und Vor-Ort-Integrationen

Ebenfalls unterstützt

- WireGuard — Ein extrem leichtes, modernes VPN-Protokoll, ideal für Edge-Geräte mit begrenzter Rechenleistung
- Meraki VPN — Native Integration für Meraki-basierte Kundenimplementierungen

VPN-Zugang für Betreiber – Integrierte Fernzugriffsfunktion

NXGEN stellt autorisierten Betreibern OpenVPN-Client-Konten zur Verfügung, die Ihrem Team von jedem Standort aus sicheren Zugriff auf die NVRs, Rekorder und Kameras Ihrer Kunden ermöglichen – ohne diese Systeme dem öffentlichen Internet auszusetzen. Das bedeutet eine schnellere Problemlösung, geringere Supportkosten und ein besseres Serviceerlebnis für Ihre Kunden – alles über eine einzige, zentral verwaltete Zugriffsebene.

Technische Daten

Leistung & Geschwindigkeit

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

Unterstützte VPN-Protokolle und Konnektivität

SPECIFICATION	DETAILS
VPN Protocols	OpenVPN
Connectivity Types	OpenVPN CloudConnexa
Operator Access	OpenVPN client-based PC accounts for authorized NXGEN personnel

Authentifizierung und Sicherheit

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 & Verkehr

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

Verfügbarkeit und Ausfallsicherheit

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

Bereitstellung & Infrastruktur

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

INTEGRATIONEN

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

Verwaltung, Überwachung und Betrieb

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

Erste Schritte – Typischer Einarbeitungsprozess

Die meisten Implementierungen sind innerhalb von 2 bis 5 Werktagen betriebsbereit. NXGEN übernimmt die gesamte Planung und Konfiguration des VPN – die Kunden müssen lediglich ihre Netzwerkdaten bereitstellen.

1. Erkundung und Umfangsbestimmung — NXGEN prüft die Netzwerktopologie des Kunden, die Anzahl der Standorte und die Geräteanforderungen
2. Entwurf und Konfiguration — VPN-Architektur entworfen und konfiguriert — Protokolle, Routing, NAT und Authentifizierung ausgewählt
3. Prüfung und Validierung — Tunnel durchgängig getestet; Latenz, Durchsatz und Ausfallsicherheit bestätigt
4. Inbetriebnahme & Überwachung — Überwachung und Support aktiviert

Bereitstellung und Architektur

INFRASTRUCTURE	AWS-BASED VPN GATEWAY
Deployment Models	Cloud VPN Gateway
Connected Environments	NVRs
Onboarding Timeline	Typical deployment within 2–5 business days; complex multi-site rollouts scoped individually

Kontakt

Kontaktieren Sie uns, um die Bereitstellungsoptionen für Ihre Umgebung zu besprechen.

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