

Leistungsbeschreibung

Netkom Managed SD-WAN

Präambel

Die Thüringer Netkom GmbH (nachfolgend „Netkom“) stellt dem Kunden im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten eine von Netkom gemanagte Lösung zur Verfügung, mit der der Kunde seine IT-Standorte vernetzen und gegen unerwünschte Netzzugriffe von außen absichern kann. Hierzu überlässt Netkom dem Kunden für einen einzelnen Standort eine Firewall mit SD-WAN-Funktionalität. Das System wird zwischen dem Internet-Anschluss des Kunden und seinem lokalen Netz (LAN) geschaltet. Die Systeme verbinden die IT-Standorte des Kunden zu einem virtuellen Netz, das verschiedene darunter liegende physikalische Netze als Ressourcen für die Übertragung der Daten nutzen kann. Die Daten werden gesichert durch IPsec VPN-Tunnel übertragen.

Konfiguration und Einstellungen des Netzes und der einzelnen Systeme werden individuell mit dem Kunden abgestimmt. Ein Anschluss an das Internet ist nicht Bestandteil des Produktes. Das Produkt setzt nicht den Anschluss an das Glasfaser-Netz der Netkom voraus und ist deshalb auch außerhalb des Netzgebietes der Netkom verfügbar.

1) Lokale Firewall

Netkom überlässt dem Kunden für die Dauer des Vertrags eine Firewall mit SD-WAN-Funktionalität zur Installation im lokalen Netz des Kunden. Die Firewall wird von Netkom betrieben und gemäß den Anforderungen des Kunden konfiguriert. Der Kunde erhält keinen Zugriff auf das System zur Veränderung der Konfiguration.

Netkom stellt den Dienst auf Systemen der Firma Fortinet zur Verfügung. Dem Kunden stehen zwei Geräte-Modelle mit der folgenden Leistung zur Auswahl:

Fortinet FortiGate 50G (Business Firewall)

- Bis zu 2 × 1 Gbit/s RJ45 WAN-Ports und bis zu 4 × 1 Gbit/s RJ45 LAN-Ports
- 1.250 Mbit/s NGFW-Durchsatz
- 1.100 Mbit/s Threat Protection

Fortinet FortiGate 90G (Extended Firewall)

- 2 × 1/10 Gbit/s WAN via RJ45 oder SFP+ Modul (Glasfaser oder RJ45 möglich)
- 8 × 1 Gbit/s RJ45 LAN-Ports
- 2,5 Gbit/s NGFW-Durchsatz
- 2,1 Gbit/s Threat-Protection

Der Leistungsumfang des Systems hängt von den aktivierten Funktionen in der Software ab. Diese werden vom Kunden gemeinsam mit Netkom festgelegt. Es sind verschiedene Architekturen des Kundennetzes möglich: Zentralisierung auf einen Standort (Hub-Spoke), Teilvermaschung, Vollvermaschung, Local Internet Breakout etc. Die lokalen Firewalls können WAN-seitig mit Internet-Anschlüssen der Netkom oder anderer Internet-Provider angeschlossen werden, auch mehrere Anschlüsse in Kombination. So kann beispielsweise ein DSL-Anschluss als Backup genutzt werden oder zwei Glasfaser-Anschlüsse zur Lastverteilung. Der Verkehr kann hierbei einer bestimmten Verbindung fest zugewiesen werden oder es kann der aktuell leistungsfähigere Internet-Anschluss genutzt werden (Dynamic Path Selection). Hierzu überprüft das System permanent Latenz, Paketverlust und Jitter der Routen im Netz (Path Quality Monitoring). Es können auch applikationsspezifisch unterschiedliche Vorgaben konfiguriert werden (Application Monitoring). Die Routen zwischen den WAN-Anschlüssen der einzelnen lokalen Firewalls im Kundennetz werden über IPsec-Tunnel geführt, die vom System automatisch entsprechend ihrer Konfiguration eingerichtet werden.

Zur Sicherung des lokalen Netzes wird das System als NGFW (Next Generation Firewall) mit den Funktionen Firewall, Intrusion Prevention und Applikationskontrolle betrieben. Hierbei werden Angriffe von außen gefiltert sowie die Datenpakete auf mögliche Angriffsmuster geprüft. Im Threat Protection Modus läuft die Firewall mit den gleichen Funktionen wie im NGFW-Modus. Zusätzlich ist hier aber die Malware Protection aktiv. Die Firewall prüft damit alle Datenpakete zusätzlich und blockiert sie, sofern sie sie als systemgefährdend erkennt. Systemgefährdende Inhalte werden im Konfigurationsworkshop mit dem Kunden gemeinsam definiert.

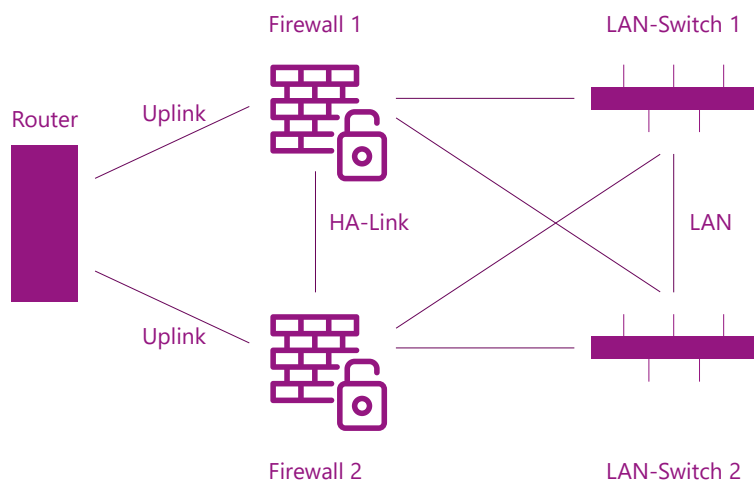
Die zur Verfügung gestellte lokale Firewall bleibt im Eigentum von Netkom. Für die fachgerechte Handhabung des Geräts, insbesondere der kundeneigenen Steckverbinder, ist der Kunde verantwortlich. Die Kosten für die zum Betrieb der lokalen Firewall notwendige Energie trägt der Kunde.

Der Kunde verbindet seine Geräte bzw. die ihm von seinem Internet-Provider überlassenen Netzendgeräte über entsprechende Anschlusskabel mit den von Netkom bereitgestellten Schnittstellen. Kundeneigene Geräte inklusive der Anschlusskabel liegen in der Verfügungsgewalt und im Verantwortungsbereich des Kunden. An den Produkten/Diensten dürfen nur Endeinrichtungen angeschlossen werden, die mit den angegebenen Schnittstellenbedingungen im Einklang stehen.

2) Hardware-Redundanz

Auf Wunsch des Kunden kann eine Hochverfügbarkeitslösung realisiert werden (High Availability, HA). Hierzu müssen zwei Geräte desselben Modells am Standort aufgebaut und über Switches miteinander verbunden werden. Diese Switches werden im Active-Passive-Modus betrieben, so dass beim Ausfall eines Geräts sofort das andere Gerät die Funktion übernimmt. Hierbei ist eine Firewall als primäres Gerät für den Transfer der Daten zuständig. Die zweite Firewall bleibt im passiven Modus und überwacht permanent den Status des aktiven Systems. Sollte ein Problem auf der primären Einheit erkannt werden, übernimmt das passive System automatisch alle Aufgaben des ausgefallenen Systems (HA Failover). Die Erreichbarkeit wird somit über das zweite Firewall-System sichergestellt.

Der HA-Modus erfordert eine entsprechende Verkabelung auf der Kundenseite. Beide Systeme müssen per LAN über Switches miteinander verbunden sein und alle Verbindungen müssen über LAN-Verkabelungen an beide Firewalls herangeführt werden, um eine vollständige Funktionsübernahme zu gewährleisten. WAN-seitig muss von beiden Firewalls eine Verbindung zum Router hergestellt werden. Dies ist in folgender Grafik dargestellt. Bei Verwendung mehrerer WAN-Anschlüsse müssen beide Firewalls an die jeweiligen Router angeschlossen werden.



Die vollständige Verkabelung und die Layer-2-Infrastruktur inklusive der Switches sind nicht Produktbestandteil und müssen vom Kunden bereitgestellt werden. Die Konfiguration der Redundanz wird vom Kunden gemeinsam mit Netkom festgelegt.

3) Konfiguration und Betrieb der Firewall

Die Konfiguration des Kundennetzes und der einzelnen lokale Firewall erfolgt durch Netkom in Abstimmung mit dem Kunden. Sofern nicht vorab anders besprochen, erfolgt die Auslieferung mit einer Standardkonfiguration. Hierbei sind noch keine Routen eingerichtet und alle eingehenden Verbindungen verboten und ausgehende Verbindungen erlaubt.

Vor der Bereitstellung werden in einem gemeinsamen Konfigurations-Workshop mit dem Kunden Abweichungen von der Standardkonfiguration gemäß den Anforderungen des Kunden festgelegt und dokumentiert. Die Dokumentation ist die Basis für die Bereitstellung der lokalen Firewall. Die Übernahme der Konfiguration von einer bestehenden Firewall ist nur in Ausnahmefällen möglich.

In diesem Workshop werden auch Informationen über WAN/LAN des Kunden abgefragt, die für die Konfiguration des Dienstes notwendig sind. Der Kunde ist verantwortlich, technisch entsprechend qualifizierte Mitarbeiter teilnehmen zu lassen. Der Workshop findet online statt. Auf Wunsch kann er auch vor Ort beim Kunden stattfinden. Hierfür fallen jedoch Kosten für die Beratung nach Stunden und Anfahrt an.

Netkom konfiguriert und betreibt die lokale Firewall über eine zentrale Management-Plattform (FortiManager), die im Netkom-Rechenzentrum in Thüringen installiert ist. Jede lokale Firewall ist über gesicherte Internet-Verbindungen mit der zentralen Plattform gekoppelt. Die lokale Firewall erhält ihre aktuelle Konfiguration von der Plattform. Die Plattform überwacht den Betriebszustand und den aktuellen Durchsatz der lokalen Firewall und die Qualität der Verbindungen im Kundennetz. Der Kunde erhält auf Wunsch bis zu fünf leseberechtigte, benannte Accounts für seine lokale Firewall auf der zentralen Plattform. Dies ermöglicht dem Kunden eine Sicht auf die aktuelle Konfiguration, den Betriebsstatus der lokalen Firewall und die aktuelle Qualität der Routen in seinem Netz. Letzteres auch je nach Konfiguration bis zur Applikationsebene. Eine Änderung von Konfigurationen hierüber ist nicht möglich.

Änderungen der festgelegten Konfiguration kann der Kunde jederzeit innerhalb der Vertragslaufzeit beauftragen. Die zentrale Management-Plattform erstellt bei einer Änderung der Konfiguration ein Backup der aktuellen Konfiguration einer lokalen Firewall. Es werden die letzten 20 Backups vorrätig gehalten.

Alle Hardware- und Software-Komponenten werden von Netkom durch regelmäßige Updates auf dem aktuellen Stand gehalten. Außer bei sicherheitskritischen Updates/Fixes geschieht dies innerhalb von vorher angekündigten Wartungsfenstern. Hierfür gelten die im Dokument „Netkom Service Level Agreement (SLA)“ genannten Bedingungen. In Einzelfällen kann es zu Einschränkungen des Dienstes kommen, sofern bestimmte Funktionen vom Hersteller Fortinet im neuen Release/Patchlevel nicht mehr angeboten werden. Dann wird Netkom Alternativen vorschlagen. Zusätzliche Leistungsmerkmale sind mit einem Update nur dann verfügbar, wenn sie vom Hersteller Fortinet innerhalb der für den Kunden verwendeten Lizenz angeboten werden.

4) Features von SD-WAN

Die lokale Firewall unterstützt zusammen mit der zentralen Administrationsplattform (FortiManager) eine Vielzahl von Vernetzungsfunktionen. Dies sind unter anderem:

- Policy Based Routing, das ermöglicht, den Datenverkehr abhängig von vordefinierten Regeln zu leiten. So können beispielsweise bestimmte Applikationen immer auf festgelegten Routen zu einem zentralen Standort geleitet werden, andere können vor Ort ins Internet ausgeleitet werden. Auch Mobilfunkverbindungen über 5G oder LTE können genutzt werden.
- Dynamic Path Selection, durch die für den gesamten Verkehr oder eine einzelne Applikation die WAN-Verbindung mit der besten Qualität genutzt wird. Hierfür überwacht die lokale Firewall die Verkehrsqualität all ihrer WAN-Verbindungen (Latenz, Paketverlust, Jitter).

- Load Balancing: Über eine dynamische Lastverteilung zwischen verschiedenen WAN-Anschlüssen kann die gesamte zur Verfügung stehende Bandbreite genutzt und die Ausfallsicherheit erhöht werden.
- Advanced Mesh VPN / Local Internet Breakout: Neben der klassischen Anbindung von Außenstandorten an einen zentralen Standort können Außenstandorte auch direkt miteinander kommunizieren und der externe Verkehr eines Außenstandortes kann direkt vom Außenstandort ins Internet geführt werden. Über die Sicherheitsfunktionen der Firewall ist der Außenstandort gegenüber dem Internet geschützt.
- Application Monitoring, das dem Kunden ermöglicht, die Verwendung einer einzelnen Applikation und deren Datenübertragung im Netz gezielt zu beobachten. Hierdurch kann er die Leistungsfähigkeit seines Netzes optimieren.

5) Features der Firewall

Die Firewall verfügt über alle Sicherheitsfeatures des Unified Threat Protection Bundles der Firma Fortinet. Dies sind insbesondere:

- Intrusion Prevention System (IPS) Identifizierung und Blockierung von böartigem Datenverkehr durch signaturbasierte Erkennung und Protokollanalyse.
- Advanced Malware Protection (AMP) Antivirus, Botnet Domains, Mobile Malware, Virus Outbreak Protection, Content Disarm 2, AI-based Heuristic AV, FortiGate Cloud Sandbox.
- URL, DNS und Video Filtering Blockieren von Malware und Durchsetzung von Internetnutzungsrichtlinien mit URL-Filterung, DNS-Filterung, Videofilterung 2, Malicious Certificate.
- Anti-Spam Identifizierung von Spammer-IPs und -E-Mails, bekannten Phishing- und Spam-URLs, bekannten Spam-E-Mail-Prüfsummen und anderen.

6) Analysefunktionen

Über das Tool FortiAnalyzer stehen dem Kunden Analysefunktionen zur Verfügung, die auf den Logfiles und protokollierten Events der lokalen Firewall beruhen. Die Daten stehen 30 Tage zur Verfügung. Die Daten werden dem Kunden auch über Reports zur Verfügung gestellt. Die Reports werden dem Kunden event- oder zeitgesteuert per Mail zugeschickt oder können von einem gesicherten Ort heruntergeladen werden. Standardmäßig werden folgende Reports bereitgestellt:

- FortiView Sources
Auflistung aller Geräte im Netzwerk, welche über die Firewall Daten austauschen.
- FortiView Destinations
Auflistung aller aufgerufenen Zieladressen.
- FortiView Applications
Anzeige aller aufgerufenen Dienste (Gmail, Instagram, Facebook, etc.).
- FortiView WebSites
Anzeige aller aufgerufenen Webseiten.
- FortiView Policies
Anzeige aller Trafficdaten sortiert nach zutreffender Firewallregel.
- FortiView Sessions
Anzeige aller Trafficdaten sortiert nach Quelle und Ziel, sowie Ports und dazugehöriger Applikation.
- FortiView VPN
Auflistung aller verbundener VPN-Benutzer.
- LogView Traffic
enthält alle ein und ausgehenden Trafficdaten in tabellarischer Form mit dazu gehöriger Firewall Aktion (accept/deny/etc)
- LogView Security
enthält alle ein und ausgehenden Trafficdaten in tabellarischer Form nach Applikation mit dazu gehöriger Firewall Aktion (accept/deny/etc).
- LogView Events
zeigt alle Firewall relevanten Systemevents an wie Logins von Benutzern, Überlastung, Überhitzung, Störungen von Systemdiensten, Konfigurationsänderungen etc. an.

Welche Daten die Reports im Detail enthalten und ob weitere Reports eingerichtet werden, wird gemeinsam mit dem Kunden festgelegt.

7) VPN-Einwahl

Endgeräte des Kunden können sich über eine mit SSL-VPN-gesicherte Internet-Verbindung von außerhalb in das lokale Netz des Kunden einwählen. Die Kommunikation des Clients ist über SSL oder IPSec VPN abgesichert. Als Zugangssoftware wird der Fortinet-VPN-Client genutzt, den der Kunde von der Download-Seite von Fortinet oder seinem App-Store herunterladen muss.

Es können nur solche Endgeräte genutzt werden, auf denen sich der Fortinet-VPN-Client in der aktuellen Version installieren lässt. Der Forticlient-VPN-Client ist für alle gängigen Systeme wie Windows, Mac, Android, IOS und Linux verfügbar. Die Verwendung von MFA (Multi-Faktor-Authentifizierung) ist möglich.

Zur Konfiguration des Dienstes auf dem Endgerät stellt Netkom eine Konfigurationsdatei mit Installationsanleitung zur Verfügung. Je Endgerät wird hierfür ein einmaliges Entgelt erhoben. Die Einrichtung auf dem Endgerät erfolgt durch den Kunden. Ein Support hierzu ist nicht Produktbestandteil.

8) Bereitstellung

Die lokale Firewall wird als Tischgerät bereitgestellt. Gegen Aufpreis wird das Modell 90G als 19“-Gerät bereitgestellt, das im Rack montiert werden kann. Die Aufstellung, die Montage und der Anschluss an WAN und LAN erfolgen durch den Kunden. Das Gerät wird mit einem Patchkabel und einer Montageanleitung ausgeliefert. Weitere notwendige Patchkabel werden vom Kunden bereitgestellt. Sie können, ebenso wie ggf. notwendige SFP-Module, gegen Aufpreis von Netkom bezogen werden.

Die lokale Firewall wird zwischen dem Router, der den WAN-Zugang bereitstellt, und dem lokalen Netz aufgestellt. Bei FortiGate 90G ist auch der direkte Anschluss an eine Glasfaser möglich. Hierzu ist ein gesondert zu bestellendes SFP-Modul notwendig. Es können mehrere WAN-Anschlüsse konfiguriert werden. Über einen FortiExtender kann auch gegen gesondertes monatliches Entgelt ein 5G-Mobilfunk-Anschluss als Backup konfiguriert werden (abwärtskompatibel zu LTE). Der Anschluss an ein Mobilfunknetz (SIM-Karte, eSIM) ist nicht Bestandteil des Produktes und wird vom Kunden bereitgestellt.

Für die Anbindung der lokalen Firewall an das Kundennetz und an die zentrale Administrationsplattform ist eine öffentliche feste IP-Adresse notwendig, die vom Kunden bereitgestellt wird.

Für Standorte in Thüringen kann auch gegen gesondertes Entgelt eine Installation der Firewall durch Netkom beauftragt werden. Diese wird von Netkom selbst oder einer von Netkom beauftragten Firma ausgeführt.

Der verbindliche Bereitstellungstermin wird dem Kunden nach der gemeinsamen Festlegung und Dokumentation der Konfiguration der Firewall im Konfigurationsworkshop mitgeteilt.

9) Services

Autorisierte Mitarbeiter des Kunden können jederzeit Services beauftragen. Dies umfasst Leistungen wie etwa eine Änderung der Firewall-Konfiguration, Anpassungen der Analyse- oder Reporting-Funktionalität, Änderung der Redundanzkonfiguration, Einrichten und Austragen von Leseberechtigungen oder Beratungsleistungen, beispielsweise bei einem Sicherheits-Incident. Netkom setzt die Service-Aufträge im Rahmen ihrer bestehenden technischen und betrieblichen Möglichkeiten um. Für die Beauftragung gelten die im Dokument „Netkom Service Level Agreement (SLA)“ unter dem Abschnitt „Zusätzliche Leistungen“ genannten Bedingungen.

Nach erstmaliger Bereitstellung des Dienstes werden Aufträge für Serviceleistungen nach zeitlichem Aufwand abgerechnet (je angefangener Viertelstunde). Im Monatsentgelt für den Dienst ist eine Stunde an Serviceleistungen enthalten. Nicht in Anspruch genommene Serviceleistungen verfallen zum Monatsende.

10) Verfügbarkeit, Entstörung, Service Level, geplante Arbeiten, Wartungen

Sofern nicht einzelvertraglich anders geregelt, gelten insoweit die Angaben der Leistungsbeschreibung „Netkom Service Level Agreement (SLA)“. Der dort aufgeführte Servicelevel „Komfort“ ist bereits kostenfrei in das Produkt integriert. Als kostenpflichtige Zusatzleistung für das vorliegende Produkt wird der Servicelevel „Premium“ angeboten. Sollte im Störfall ein Austausch eines Firewallgerätes erforderlich sein, wird Netkom das Gerät vor Ort austauschen. Die für den jeweiligen Servicelevel geltende maximale Entstörzeit verlängert sich in diesem Fall um die Anreisezeit.

11) Preise

Netkom berechnet dem Kunden einen einmaligen Einrichtungspreis, einen monatlichen Nutzungspreis, einen Stundenpreis sowie ggf. gesondert vereinbarte Preise für zusätzliche Leistungen. Es gilt die jeweils gültige Preisliste bzw. die individuell vereinbarten Preise.

12) Sonstige Verantwortlichkeiten des Kunden

Der Dienst Managed SD-WAN der Netkom dient ausschließlich für die Versorgung des Kunden. Die Nutzung durch Dritte bzw. eine Weitergabe an Dritte durch den Kunden ist nicht gestattet. Verstößt der Kunde gegen diese Vereinbarungen, behält sich Netkom das Recht vor, den Dienst ohne vorherige Ankündigung zu sperren.

Der Kunde wird Netkom von jeglicher Haftung Dritten gegenüber freistellen, die darauf beruht, dass die Nutzung des von Netkom bereitgestellten Dienstes Managed SD-WAN durch den Kunden Rechte Dritter oder gesetzliche Vorschriften verletzt.

13) Vertragsende

Bei Vertragsende (Kündigung/Ablauf/Aufhebung etc.) ist der Kunde verpflichtet, die von Netkom für diesen Dienst überlassenen Geräte innerhalb einer Frist von vier Wochen nach Vertragsende an Netkom oder ein von Netkom benanntes Unternehmen zurückzugeben (nachweisbarer Versand oder Abgabe in den Geschäftsräumen der Netkom).

14) Allgemeine Bestimmungen

Im Übrigen gelten die Allgemeinen Geschäftsbedingungen der Netkom in ihrer jeweils aktuell gültigen Fassung.

gültig ab 21. September 2026