

Leistungsbeschreibung

Erneuerung, Implementierung und Migration einer Firewall- und Management-Infrastruktur (Palo Alto)

Anlage	Anlage 3 zu den Vergabeunterlagen
Gegenstand	Lieferung von Hardware, Lizenzen und Supportleistungen sowie Erbringung von Implementierungs-, Migrations- und Serviceleistungen
Vergabestelle	Vivantes Netzwerk für Gesundheit GmbH
Vergabenummer	VSG-SEK-2026-67

1 Gegenstand und Zielsetzung

Gegenstand dieser Leistungsbeschreibung ist die Lieferung der nachfolgend spezifizierten Hardware, Softwarelizenzen und Herstellersupportleistungen sowie die Erbringung der damit verbundenen Implementierungs-, Migrations- und Serviceleistungen durch den Auftragnehmer.

Der Auftraggeber betreibt eine bestehende Sicherheitsinfrastruktur auf Basis von Produkten der Palo Alto Networks Inc. Ziel dieser Beschaffung ist die Ablösung der eingesetzten Systeme durch die jeweiligen Nachfolgeprodukte des Herstellers sowie die Konsolidierung der bislang auf zwei getrennten Clustern betriebenen Funktionsbereiche Perimeter-Firewall und VPN-Gateway auf eine gemeinsame Plattform. Ergänzend wird ein weiterer Standort erstmals mit einem eigenen Firewall-System ausgestattet.

Die Festlegung auf die Produkte des genannten Herstellers ist erfolgt. Die technischen und funktionalen Anforderungen an den Leistungsgegenstand sind durch die Produktfestlegung in Abschnitt 4 abschließend bestimmt. Gegenstand der von den Bietern im Weiteren auszuführenden Leistungen sind daher die über die reine Lieferung der Produkte hinausgehenden Dienstleistungen gemäß den Abschnitten 5 bis 11 dieser Leistungsbeschreibung.

1.1 Leistungsziel

Leistungsziel ist ein vollständig implementiertes, konfiguriertes, migriertes und produktiv betriebsfähiges Gesamtsystem, das die Funktionen der abzulösenden Bestandsinfrastruktur vollumfänglich übernimmt und über die vereinbarte Vertragslaufzeit durch den Auftragnehmer gewartet und unterstützt wird. Das Leistungsziel in Bezug auf die Implementierung und Migration gilt als erreicht, wenn die in Abschnitt 8 definierten Abnahmekriterien erfüllt sind.

2 Beschreibung des Ist-Zustandes

Der Auftraggeber betreibt derzeit die nachfolgend aufgeführten Systeme im produktiven Einsatz:

Funktion	System	Betriebsform
Perimeter-Firewall	2x Palo Alto PA-5220	Hochverfügbarkeitsverbund. Konfiguration erfolgt direkt am System, nicht über Panorama
VPN-Gateway	2x Palo Alto PA-3250	Hochverfügbarkeitsverbund. Konfiguration erfolgt direkt am System, nicht über Panorama

Funktion	System	Betriebsform
Zentrales Management	1x Palo Alto Panorama M-600	Protokolldatensammlung für Perimeter und VPN. Vollständige Verwaltung der Firewalls an den Außenstandorten
Außenstandorte	Palo Alto Firewalls kleinerer Baureihen	Konfiguration und Verwaltung vollständig über Panorama M-600

Die Perimeter-Firewall kontrolliert und filtert den ein- und ausgehenden Netzwerkverkehr an der Außengrenze des Unternehmensnetzwerks. Das VPN-Gateway stellt Remote-Access-Zugänge für Mitarbeitende und externe Dienstleister sowie Site-to-Site-Verbindungen zu angebundenen Standorten und Partnernetzen bereit.

Für das Verständnis des Migrationsaufwands ist die derzeitige Rolle des Panorama M-600 von besonderer Bedeutung: Der Perimeter-Cluster und der VPN-Cluster sind an das Panorama ausschließlich zur Sammlung und Auswertung von Protokolldaten angebunden. Die Konfiguration dieser beiden Cluster erfolgt gegenwärtig direkt auf den jeweiligen Systemen und nicht über Panorama. Es bestehen für diese Systeme daher keine Templates, Template Stacks oder über Panorama gepflegten Device Groups.

Demgegenüber werden die an den Außenstandorten eingesetzten Palo Alto Firewalls kleinerer Baureihen vollständig über das Panorama M-600 konfiguriert und verwaltet. Für diese Systeme existiert eine gewachsene Panorama-Konfiguration mit Templates und Device Groups, die vollständig auf das neue Panorama M-700 zu übernehmen ist.

2.1 Betriebsumgebung und Systemvoraussetzungen

Die Systeme werden in den Rechenzentrumsflächen des Auftraggebers in Berlin betrieben. Für die Angebotskalkulation sind folgende Rahmenbedingungen maßgeblich:

- Netzerkennung: Anbindung über Multimode-Glasfaser mit den in Abschnitt 4 aufgeführten Transceiver-Typen (100 GbE, 25 GbE, 10 GbE)
- Aktuell eingesetzte PAN-OS-Version: 11.1
- Umfang der Bestandskonfiguration Perimeter und VPN: Sicherheitsrichtlinien Perimeter: ca. 750, VPN: ca. 300
- VPN-Nutzung: ca. 600 gleichzeitiger Remote-Access-Sitzungen im Spitzenlastbetrieb sowie ca. 100 Site-to-Site-Tunnel
- Über Panorama verwaltete Bestandssysteme an Außenstandorten: ca. 15 in der Anzahl und Baureihen von PA-210, PA-410 und PA-440
- Umfang der bestehenden Panorama-Konfiguration: ca. 15 Templates, 15 Template Stacks und 15 Device Groups
- Vorzuhaltendes Protokolldatenvolumen und Aufbewahrungsfrist: 90 Tage detailliert, 1 Jahr konsolidiert.

2.2 Anzubindende Schnittstellen und Umsysteme

Die neue Infrastruktur ist in die bestehende Systemlandschaft des Auftraggebers zu integrieren. Folgende Schnittstellen sind im Rahmen der Implementierung zu berücksichtigen:

- Verzeichnisdienst: Anbindung an Microsoft Active Directory zur benutzerbasierten Richtliniendurchsetzung (via User-ID Agent)
- Authentifizierung: Anbindung an SAML-IdP einschließlich Multi-Faktor-Authentifizierung für Remote-Access-Zugänge
- Protokollierung: Weiterleitung sicherheitsrelevanter Ereignisse an das zentrale SIEM via Syslog
- Monitoring: Einbindung in das bestehende Monitoring-System über SNMP
- Zeitsynchronisation: Anbindung an die internen NTP-Quellen des Auftraggebers

3 Beschreibung des Soll-Zustandes

Nach Abschluss der Leistungserbringung muss sich die Infrastruktur wie folgt darstellen:

Funktion	System	Betriebsform
Perimeter-Firewall und VPN-Gateway (konsolidiert)	2x Palo Alto PA-5540	Hochverfügbarkeitsverbund, logische Trennung der Funktionsbereiche über Virtual Systems
Firewall zweiter Standort	1x Palo Alto PA-1420	Einzelsystem, betriebsbereit und konfigurationsbereit zu übergeben
Zentrales Management	1x Palo Alto Panorama M-700	Konfiguration und Protokollierung für alle Systeme einschließlich der Bestandssysteme an den Außenstandorten

3.1 Konsolidierung der Funktionsbereiche

Die bislang auf zwei getrennten Clustern betriebenen Funktionsbereiche Perimeter-Firewall und VPN-Gateway werden auf dem neuen PA-5540-Cluster zusammengeführt. Die logische Trennung der beiden Funktionsbereiche ist über Virtual Systems zu realisieren. Dabei sind mindestens folgende Trennungsmerkmale sicherzustellen:

- Getrennte Sicherheitsrichtlinien und Regelwerke je Virtual System
- Getrennte virtuelle Router und Routing-Instanzen
- Getrennte Zuordnung physischer und logischer Schnittstellen
- Getrennte Administrationsrollen und Zugriffsberechtigungen in Panorama
- Getrennte Protokollierungsströme mit eigenständiger Auswertbarkeit
- Kein Datenverkehr zwischen den Virtual Systems ohne explizite Regelwerksfreigabe

Das konkrete Aufteilungskonzept der Virtual Systems, die Ressourcenzuteilung sowie die Schnittstellenzuordnung sind im Rahmen des Feinkonzepts gemäß Abschnitt 6 durch den Auftragnehmer auszuarbeiten und mit dem Auftraggeber abzustimmen.

3.2 Firewall am zweiten Standort

Der zweite Standort ist bereits an das Firmennetz des Auftraggebers angebunden. Die dort einzusetzende PA-1420 dient der Absicherung eines redundanten Netzwerkpfades für den Fall, dass die Anbindung am Hauptstandort ausfällt. Der Aufbau des Redundanzkonzepts selbst ist nicht Gegenstand dieser Leistungsbeschreibung.

Der Leistungsumfang für dieses System beschränkt sich auf die betriebsbereite Bereitstellung und die konfigurationsbereite Übergabe an den Auftraggeber. Im Einzelnen umfasst dies:

- Physische Installation im Rack am zweiten Standort einschließlich Anschluss der redundanten Stromversorgung
- Anschluss an die vom Auftraggeber bereitgestellte Netzwerkverkabelung
- Installation der zwischen den Vertragsparteien abgestimmten PAN-OS-Version einschließlich aktueller Wartungsstände
- Einrichtung der Management-Schnittstelle mit den vom Auftraggeber vorgegebenen Netzwerkparametern
- Aktivierung und Registrierung der Lizenzen und Subskriptionen
- Einbindung des Systems in das Panorama M-700 und Nachweis der Erreichbarkeit
- Übergabe an den Auftraggeber in konfigurationsbereitem Zustand

Die Erstellung der produktiven Sicherheitsrichtlinien sowie die Konfiguration der Routing- und Redundanzfunktionen für dieses System erfolgt durch den Auftraggeber und ist nicht Gegenstand des Auftrags.

3.3 Zentrales Management

Das neue Panorama M-700 löst das bestehende Panorama M-600 vollständig ab und übernimmt dessen sämtliche Funktionen. Über die im Ist-Zustand abgebildeten Funktionen hinaus muss das Panorama M-700 künftig auch die Konfiguration des neuen PA-5540-Clusters übernehmen. Die derzeit direkt auf den Systemen gepflegte Konfiguration des Perimeter- und des VPN-Funktionsbereichs ist somit im Zielbild in eine über Panorama verwaltete Struktur aus Templates, Template Stacks und Device Groups zu überführen.

Der Zielzustand des zentralen Managements umfasst:

- Übernahme der bestehenden Panorama-Konfiguration für die Bestandssysteme an den Außenstandorten einschließlich Templates, Template Stacks, Device Groups, Objekten und Richtlinienhierarchien
- Neuaufbau einer Panorama-basierten Konfigurationsstruktur für die beiden Virtual Systems des PA-5540-Clusters
- Überführung der bislang direkt auf den Bestandssystemen gepflegten Konfiguration in diese Struktur
- Einbindung der PA-1420 am zweiten Standort in das zentrale Management
- Fortführung der Protokolldatensammlung für alle angebundenen Systeme
- Abgestimmtes Rollen- und Berechtigungskonzept für die Administration über Panorama

Die Überführung der direkt gepflegten Konfiguration in eine Panorama-verwaltete Struktur stellt einen wesentlichen Leistungsbestandteil dar

Historische Protokolldaten der Bestandsumgebung sind zu übernehmen, soweit technisch möglich. Der Umfang der zu übernehmenden Protokolldaten ist im Angebotskonzept darzustellen und im Rahmen der Detaillierung nach Zuschlagserteilung verbindlich festzulegen.

4 Lieferumfang (Produktfestlegung)

Der Auftragnehmer liefert die nachfolgend abschließend spezifizierten Produkte. Die Angabe der Part Numbers ist verbindlich. Angebotene Positionen müssen den aufgeführten Part Numbers exakt entsprechen. Die Produkte sind über einen autorisierten Vertriebsweg des Herstellers zu beziehen; die Registrierung der Lizenzen und Supportverträge hat auf den Auftraggeber zu erfolgen.

Menge	Part Number	Beschreibung	Laufzeit / Art
2	PAN-PA-5540-AC	Palo Alto Networks PA-5540 mit redundanten AC-Netzteilen	Hardware
2	PAN-PA-5540-BND-PRECISIONAI-5YR	PA-5540, Precision AI Network Security Subscription Bundle (Advanced Threat Prevention, Advanced URL Filtering, Advanced WildFire, Advanced DNS Security, Advanced SD-WAN, Device Security)	60 Monate
2	PAN-PA-5540-PAA-5YR	PA-5540, Prisma Access Agent Subscription	60 Monate
2	PAN-SVC-BKLN-5540-5YR	PA-5540, Partner Enabled Premium Support	60 Monate
1	PAN-PA-1420	Palo Alto Networks PA-1420	Hardware
1	PAN-PA-1420-ATP-5YR	PA-1420, Advanced Threat Prevention	60 Monate
1	PAN-SVC-BKLN-1420-5YR	PA-1420, Partner Enabled Premium Support	60 Monate

Menge	Part Number	Beschreibung	Laufzeit / Art
1	PAN-M-700	Palo Alto Networks M-700 Chassis mit 16 TB Storage (4x 8 TB RAID-zertifizierte Laufwerke), redundante Netzteile, 4-Post-Rack-Mount-Schienen	Hardware
1	PAN-M-700-P-25	Panorama Central Management Software License, 25 Devices oder Log Collector für M-700	Lizenz
1	PAN-SVC-BKLN-M-700-P-25-5Y	Partner Enabled Premium Support, Panorama M-700 25 Devices, PAN-DB Private Cloud oder Log Collector	60 Monate
4	PAN-PWR-C19-EU	Netzkabel IEC-60320 C19 auf CEE 7/7 SCHUKO, 3 Meter (für PA-5540, 2 Stück je Appliance)	Zubehör
4	PAN-PWR-CORD-C15-EU	Netzkabel für Panorama M-700 und PA-1420	Zubehör
12	PAN-QSFP28-100GBASE-BIDI	QSFP+ Formfaktor, 100 Gb bidirektionaler optischer Transceiver, 70 m über OM3 MMF, 100 m über OM4 MMF, Duplex LC	Zubehör
16	PAN-SFP28-25GBASE-SR	SFP28 Formfaktor, SR 25 Gb optischer Transceiver, 100 m MMF, Duplex LC, IEEE 802.3ae 25GBASE-SR konform	Zubehör
12	PAN-SFP-PLUS-SR	SFP+ Formfaktor, SR 10 Gb optischer Transceiver, 300 m OM3 MMF, Duplex LC, IEEE 802.3ae 10GBASE-SR konform	Zubehör

Die Preise sind je Position einzeln im beigefügten Preisblatt auszuweisen. Sofern der Hersteller im Zeitraum zwischen Angebotsabgabe und Lieferung Produktnachfolger oder geänderte Part Numbers einführt, ist der Auftragnehmer verpflichtet, den Auftraggeber unverzüglich zu informieren und ein funktional mindestens gleichwertiges Nachfolgeprodukt ohne Mehrkosten anzubieten.

Sofern über die vorgenannten Mengen für Zubehör hinausgehende Bedarfe für die Inbetriebnahme des Gesamtsystems erforderlich werden, sind ohne gesonderte Vergütung vom Auftragnehmer zur Verfügung zu stellen.

4.1 Vertragslaufzeiten und Verlängerungsoptionen

Die Laufzeiten der Subskriptions- und Supportleistungen ergeben sich aus der Tabelle in Abschnitt 4. Die Laufzeit beginnt mit dem Datum der Gesamtabnahme gemäß Abschnitt 8.

4.2 Lieferbedingungen

- Lieferung frei Verwendungsstelle an die vom Auftraggeber benannten Standorte einschließlich Entladung und Transport zum Aufstellort
- Anlieferung ausschließlich nach vorheriger Terminvereinbarung innerhalb der Anlieferzeiten des Auftraggebers
- Lieferung in ungeöffneter Originalverpackung des Herstellers
- Sämtliche gelieferten Komponenten müssen zum Lieferzeitpunkt neu, ungebraucht und aus aktueller Herstellerproduktion stammen
- Beilage einer vollständigen Packliste mit Zuordnung von Seriennummern zu Part Numbers
- Fachgerechte Entsorgung des Verpackungsmaterials durch den Auftragnehmer

5 Implementierungs-, Integrations- und Migrationsleistungen sowie weitere Dienstleistungen

Die Implementierungs- und Integrationsleistungen nach Abschnitt 5.1 betreffen den Aufbau der neuen Systemumgebung bis zu dem Zustand, in dem diese betriebsbereit und für die Übernahme der produktiven Funktionen vorbereitet ist. Diese Leistungen werden an Systemen erbracht, die zu

diesem Zeitpunkt noch nicht produktiv sind, und können daher innerhalb der Regelarbeitszeit durchgeführt werden.

Die Migrationsleistungen nach Abschnitt 5.2 betreffen die Vorbereitung und Überführung der produktiven Funktionen aus der Bestandsumgebung in die neue Systemumgebung. Der Auftragnehmer trägt die Verantwortung für den vollständigen und fehlerfreien Übertrag der Bestandskonfiguration sowie für die Funktionsfähigkeit der migrierten Funktionsbereiche im Produktivbetrieb.

Der Auftragnehmer erbringt sämtliche Leistungen, die für die Herstellung eines produktiv betriebsfähigen Gesamtsystems erforderlich sind. Die nachfolgenden Aufzählungen beschreiben den Mindestumfang.

5.1 Implementierungs- und Integrationsleistungen

5.1.1 Bestandsaufnahme

Der Auftragnehmer führt eine vollständige Bestandsaufnahme der zu migrierenden Konfiguration durch. Die Ergebnisse fließen in das Feinkonzept ein. Die Bestandsaufnahme umfasst insbesondere:

- Erfassung und Analyse der Sicherheitsrichtlinien, Netzwerkobjekte, Zonen, Schnittstellen und Routing-Konfigurationen beider Bestandscluster
- Erfassung der bestehenden VPN-Konfiguration einschließlich Site-to-Site-Tunnel, Remote-Access-Profilen und Authentifizierungseinstellungen
- Erfassung der bestehenden Panorama-Konfiguration einschließlich Templates, Template Stacks, Device Groups und der zugeordneten Bestandssysteme an den Außenstandorten
- Identifikation nicht unmittelbar übertragbarer Konfigurationselemente sowie Vorschlag für deren Abbildung in der Zielumgebung
- Identifikation von Redundanzen und Konflikten, die sich aus der Zusammenführung der beiden bisher getrennten Regelwerke ergeben, sowie Vorschlag zu deren Auflösung
- Abstimmung der Ergebnisse mit dem Auftraggeber und Einholung der Freigabe des Zielregelwerks vor der Produktivschaltung

5.1.2 Physische Installation

- Montage der Appliances in den vom Auftraggeber bereitgestellten Racks einschließlich Rack-Mount-Kits
- Anschluss der redundanten Stromversorgung an die bereitgestellten Stromkreise unter Verkabelung sämtlicher Netzteile
- Bestückung der Systeme mit den gelieferten Transceivern gemäß abgestimmtem Portkonzept
- Anschluss und Beschriftung der Netzwerkverkabelung nach den Kennzeichnungsvorgaben des Auftraggebers
- Dokumentation der physischen Installation einschließlich Portbelegungsplan

5.1.3 Grundkonfiguration und Systemhärtung

- Installation der zwischen den Vertragsparteien abgestimmten PAN-OS-Version einschließlich aktueller Wartungsstände
- Einrichtung der Management-Schnittstellen und der administrativen Zugänge
- Aktivierung und Registrierung sämtlicher Lizenzen und Subskriptionen auf den Auftraggeber
- Konfiguration des Hochverfügbarkeitsverbundes der PA-5540 einschließlich HA-Links und Failover-Parametern
- Einrichtung und Konfiguration der Virtual Systems für die Funktionsbereiche Perimeter-Firewall und VPN-Gateway gemäß dem freigegebenen Feinkonzept

- Systemhärtung entsprechend den Härtungsvorgaben des Auftraggebers und den Empfehlungen des Herstellers
- Einrichtung des Konfigurationsbackups und Nachweis der Wiederherstellbarkeit
- Durchführung und Dokumentation eines kontrollierten Failover-Tests am noch nicht produktiven Cluster

5.1.4 Aufbau des zentralen Managements

Die nachfolgenden Leistungen betreffen den Neuaufbau des Panorama M-700. Die Ablösung des bestehenden Panorama M-600 und die Umstellung der bereits produktiv verwalteten Systeme sind demgegenüber Migrationsleistungen und in Abschnitt 5.2.4 geregelt.

- Inbetriebnahme des Panorama M-700 einschließlich Log-Collector-Konfiguration und Dimensionierung der Protokolldatenspeicherung
- Aufbau der Template-, Template-Stack- und Device-Group-Struktur für den PA-5540-Cluster gemäß dem freigegebenen Feinkonzept
- Einrichtung des Rollen- und Berechtigungskonzepts für die Administration
- Anbindung des PA-5540-Clusters und der PA-1420 an das Panorama M-700

5.1.5 Integrationsleistungen

Die in Abschnitt 2.2 aufgeführten Schnittstellen sind vollständig einzurichten, zu konfigurieren und funktional nachzuweisen. Der funktionale Nachweis ist zu dokumentieren und ist Voraussetzung für die Freigabe zur Migration nach Abschnitt 5.2.

- Einrichtung und Test der Verzeichnisdienstanbindung einschließlich User-ID-Mapping
- Einrichtung und Test der Authentifizierungsanbindung einschließlich Multi-Faktor-Authentifizierung für Remote-Access-Zugänge
- Konfiguration der Protokollweiterleitung an das SIEM-System einschließlich Abstimmung der zu übertragenden Ereignistypen
- Einbindung in das Monitoring-System einschließlich Definition der zu überwachenden Systemparameter
- Einbindung in die Zertifikatsinfrastruktur und die internen NTP-Quellen des Auftraggebers
- Konfiguration der Subskriptionsdienste gemäß dem gelieferten Leistungsumfang

5.1.6 Abschluss der Implementierungsphase

Die Implementierungsphase ist abgeschlossen, wenn die neue Systemumgebung betriebsbereit aufgebaut, konfiguriert, gehärtet und an alle Umsysteme angebunden ist und die Funktionsnachweise nach den Abschnitten 5.1.3 und 5.1.5 erbracht sind. Der Auftraggeber erteilt auf dieser Grundlage die Freigabe zum Beginn der Migration nach Abschnitt 5.2.

5.2 Migrationsleistungen

Die Migration umfasst die beiden Funktionsbereiche Perimeter-Firewall und VPN-Gateway, die Ablösung des bestehenden Panorama M-600 sowie die abschließende Freigabe zur Außerbetriebnahme der Altsysteme.

5.2.1 Grundsätze der Migration

- Die Verfügbarkeit der produktiven Netzwerkinfrastruktur ist während der gesamten Migrationsphase sicherzustellen. Unterbrechungen sind auf das technisch unvermeidbare Maß zu begrenzen.
- Migrationsschritte mit Auswirkung auf den Produktivbetrieb sind ausschließlich in abgestimmten Wartungsfenstern durchzuführen. Die Migration kann nicht innerhalb der Regelarbeitszeit erfolgen.
- Für jeden Migrationsschritt ist vor Beginn ein dokumentiertes Rückfallverfahren vorzuhalten, das die Wiederherstellung des Ausgangszustands innerhalb des jeweiligen Wartungsfensters ermöglicht.

- Vor jedem Migrationsschritt ist ein vollständiges Konfigurationsbackup des betroffenen Bestandssystems zu erstellen und zu sichern.
- Der Erfolg jedes Migrationsschritts ist anhand der im Testkonzept definierten Prüffälle nachzuweisen und zu protokollieren.
- Die Altsysteme sind bis zur Freigabe nach Abschnitt 5.2.6 in einem Zustand zu halten, der eine Rückkehr in den produktiven Betrieb ermöglicht.

5.2.2 Migration des Funktionsbereichs Perimeter-Firewall

- Übertragung der Sicherheitsrichtlinien, Netzwerkobjekte, Zonen und Schnittstellenkonfigurationen in das zugeordnete Virtual System des PA-5540-Clusters
- Übertragung der Routing-Konfiguration einschließlich statischer Routen und dynamischer Routing-Protokolle
- Übertragung der Konfiguration für SSL-Entschlüsselung und der zugehörigen Zertifikatszuordnungen
- Übernahme der Konfiguration der Sicherheitsprofile und Zuordnung zu den Subskriptionsdiensten des neuen Lizenzumfangs
- Durchführung der Prüffälle gemäß Testkonzept vor Produktivschaltung
- Produktivschaltung im abgestimmten Wartungsfenster einschließlich Funktionsnachweis unmittelbar nach der Umschaltung

5.2.3 Migration des Funktionsbereichs VPN-Gateway

- Übertragung der Site-to-Site-VPN-Konfiguration einschließlich aller bestehenden Tunnel, Verschlüsselungsparameter und Peer-Konfigurationen
- Abstimmung der Umschaltung mit den Betreibern der angebundenen Standorte und Partnernetze, soweit eine beidseitige Anpassung erforderlich ist
- Übertragung der Remote-Access-Konfiguration für Mitarbeitende und externe Dienstleister einschließlich Authentifizierungs- und Portalkonfiguration
- Übertragung und Prüfung der Konfiguration der Multi-Faktor-Authentifizierung
- Durchführung der Prüffälle gemäß Testkonzept vor Produktivschaltung, einschließlich Verbindungstests für Remote-Access und für jeden Site-to-Site-Tunnel
- Produktivschaltung im abgestimmten Wartungsfenster unter Minimierung der Unterbrechungszeiten für bestehende Verbindungen
- Unterstützung des Auftraggebers bei der Umstellung der Client-seitigen Konfiguration, soweit erforderlich

5.2.4 Migration des zentralen Managements

Die Ablösung des Panorama M-600 betrifft produktiv verwaltete Systeme an den Außenstandorten. Da Panorama ausschließlich als Managementebene wirkt und der Datenverkehr der verwalteten Systeme davon nicht berührt wird, können diese Leistungen innerhalb der Regelarbeitszeit erbracht werden.

- Vollständige und verlustfreie Übernahme der bestehenden Panorama-Konfiguration einschließlich Templates, Template Stacks, Device Groups, Objekten und Richtlinienhierarchien auf das Panorama M-700
- Umstellung der Bestandssysteme an den Außenstandorten auf das neue Panorama einschließlich Nachweis der Verwaltbarkeit jedes einzelnen Systems
- Überführung der bislang direkt auf den Bestandssystemen gepflegten Konfiguration des Perimeter- und des VPN-Funktionsbereichs in die nach Abschnitt 5.1.4 aufgebaute Panorama-Struktur
- Übernahme historischer Protokolldaten aus der Bestandsumgebung, soweit technisch möglich, in dem im Feinkonzept festgelegten Umfang
- Nachweis der vollständigen Protokolldatenerfassung und der Auswertbarkeit für alle angebundenen Systeme

5.2.5 Parallelbetrieb, Test und Stabilisierung

Nach der Produktivschaltung eines Funktionsbereichs erfolgt eine Stabilisierungsphase, während der die Altsysteme betriebsbereit vorgehalten werden. Der Auftragnehmer erbringt in dieser Phase:

- Begleitung des Betriebs mit erhöhter Aufmerksamkeit einschließlich erreichbarer Ansprechpartner während der ersten Betriebstage nach jeder Produktivschaltung
- Analyse und Behebung von Störungen, die auf die Migration zurückzuführen sind
- Nachjustierung der migrierten Konfiguration, soweit sich im Produktivbetrieb Abweichungen zum Verhalten der Bestandsumgebung zeigen
- Protokollierung aller Nacharbeiten und Übergabe an den Auftraggeber

Die Dauer der Stabilisierungsphase je Funktionsbereich ist im Feinkonzept festzulegen.

5.2.6 Abschluss der Migration und Freigabe zur Außerbetriebnahme der Altsysteme

Die Migration ist abgeschlossen, wenn beide Funktionsbereiche sowie das zentrale Management vollständig auf der neuen Umgebung betrieben werden, die Stabilisierungsphasen abgelaufen sind und keine offenen migrationsbedingten Störungen bestehen. Der Auftragnehmer legt dem Auftraggeber ein Migrationsprotokoll mit dem Nachweis aller durchgeführten Prüffälle vor.

Auf dieser Grundlage erteilt der Auftraggeber die Freigabe zur Außerbetriebnahme der Altsysteme. Der Rückbau und die weitere Behandlung der Altsysteme richten sich nach Abschnitt 12.

5.3 Wissenstransfer und Schulung

Der Auftragnehmer führt einen strukturierten Wissenstransfer für das Betriebspersonal des Auftraggebers durch. Der Wissenstransfer umfasst mindestens 5 Tage vor Ort oder Remote für bis zu 7 Teilnehmende und behandelt die spezifische Konfiguration der implementierten Umgebung, die Administration über Panorama, die Besonderheiten der Virtual-System-Aufteilung sowie die Verfahren für Backup, Wiederherstellung und Failover.

Schulungsunterlagen sind in bearbeitbarer Form zu übergeben. Herstellerzertifizierungskurse sind nicht Gegenstand dieser Leistung; ein optionales Angebot hierfür kann gesondert ausgewiesen werden.

6 Feinkonzept

Der Auftraggeber beabsichtigt, unmittelbar nach Zuschlagserteilung mit der Umsetzung zu beginnen. Aus diesem Grund ist das in Ziffer 9.5 der Bewerbungsbedingungen beschriebene Konzept bereits mit dem Angebot einzureichen. Eine erst nach Zuschlagserteilung beginnende Konzeptphase ist nicht vorgesehen.

Nach Zuschlagserteilung ist das Angebotskonzept innerhalb der in Abschnitt 7 genannten Frist zu einem Feinkonzept zu detaillieren. Gegenstand der Detaillierung sind ausschließlich die Konkretisierung auf Basis der dann verfügbaren Bestandsinformationen sowie die Abstimmung der konkreten Umsetzungsschritte. Eine grundlegende Neukonzeption ist nicht vorgesehen; das im Angebot dargestellte Lösungskonzept ist für den Auftragnehmer bindend.

7 Projektablauf, Terminplan und Zahlungsplan

Der Auftraggeber legt Wert auf einen zügigen Projektbeginn. Der Auftragnehmer hat sicherzustellen, dass die für den Projektstart erforderlichen personellen Ressourcen unmittelbar nach Zuschlagserteilung verfügbar sind. Da das Lösungskonzept bereits mit dem Angebot vorliegt, beginnen die Umsetzungsarbeiten unmittelbar nach dem Kickoff-Termin.

Der Auftragnehmer führt das Projekt eigenverantwortlich unter Einhaltung der nachfolgenden Meilensteine durch. Die Termine sind verbindlich und als zeitliche Mindestvorgaben in den Projektplan gemäß Ziffer 9.5 der Bewerbungsbedingungen zu überführen.

Nr.	Meilenstein	Termin
M1	Zuschlagserteilung und Projekt-Kickoff	T0, Kickoff innerhalb von 5 Werktagen
M2	Bestellung der Hardware beim Hersteller	T0 + 5 Werktage
M3	Vorlage des Feinkonzepts auf Basis des Angebotskonzepts	T0 + 2 Wochen
M4	Freigabe des Feinkonzepts durch den Auftraggeber	T0 + 3 Wochen
M5	Lieferung der Hardware an die Standorte	T0 + 8 Wochen
M6	Physische Installation und Inbetriebnahme Panorama M-700	T0 + 9 Wochen
M7	Übernahme der Panorama-Konfiguration für die Außenstandorte	T0 + 10 Wochen
M8	Aufbau und Konfiguration PA-5540-Cluster inkl. Virtual Systems	T0 + 10 Wochen
M9	Freigabe zum Beginn der Migration durch den Auftraggeber	T0 + 11 Wochen
M10	Migration Funktionsbereich Perimeter-Firewall	T0 + 12 Wochen
M11	Migration Funktionsbereich VPN-Gateway	T0 + 12 Wochen
M12	Abschluss Parallelbetrieb und Außerbetriebnahme Altsysteme	T0 + 13 Wochen
M13	Übergabe Dokumentation und Durchführung Wissenstransfer	T0 + 14 Wochen
M14	Teilabnahme des PA-5540-Clusters sowie Panorama M-700 durch Auftraggeber	T0 + 16 Wochen
M15	Installation und konfigurationsbereite Bereitstellung PA-1420	T0 + 16 Wochen
M16	Gesamtabnahme des funktionsfähigen Gesamtsystems durch Auftraggeber	T0 + 18 Wochen

Der Bieter hat im Angebot die zum Zeitpunkt der Angebotsabgabe beim Hersteller geltende Lieferzeit (Projektplanungskonzept) für die angebotenen Positionen anzugeben. Verlängert sich die Lieferzeit nach Zuschlagserteilung aus Gründen, die der Auftragnehmer nicht zu vertreten hat, ist der Auftraggeber unverzüglich zu informieren; die nachgelagerten Meilensteine verschieben sich in diesem Fall entsprechend.

Der Auftragnehmer benennt einen verantwortlichen Projektleiter als zentralen Ansprechpartner für den Auftraggeber. Statustermine finden in einem Turnus von 2 Wochen statt. Abweichungen vom Terminplan sind dem Auftraggeber unverzüglich unter Angabe der Ursache und der vorgesehenen Gegenmaßnahmen anzuzeigen.

7.1 Wartungsfenster

Arbeiten mit Auswirkungen auf den Produktivbetrieb sind ausschließlich in abgestimmten Wartungsfenstern durchzuführen.

7.2 Zahlungsplan

Termin-Nr.	Betrag	Art der Zahlung
M5	Positionen 1 bis 8 sowie 15 bis 17 des Preisblattes	Teilzahlung
M14	90 % der Position 13 des Preisblattes	Teilzahlung

Termin-Nr.	Betrag	Art der Zahlung
M16	Restliche Vergütung der Positionen 13 sowie Positionen 9 bis 12, 14 und 23	Schlusszahlung

8 Freigabe- und Abnahmekriterien

Die Leistung wird in zwei Stufen abgenommen. Die Abnahme erfolgt jeweils förmlich unter Erstellung eines von beiden Vertragsparteien zu unterzeichnenden Abnahmeprotokolls.

8.1 Freigaben

Nach Abschluss der jeweiligen Implementierungs- und Migrationsschritte je Funktionsbereich erfolgt eine Freigabe. Voraussetzung ist der Nachweis der vollständigen Funktionsfähigkeit des jeweiligen Funktionsbereichs anhand der im Testkonzept definierten Prüffälle.

8.2 Teilabnahme des PA-5540-Clusters sowie Panorama M-700 durch Auftraggeber

Die Teilabnahme erfolgt, wenn sämtliche der folgenden Kriterien erfüllt sind:

- Alle gelieferten Komponenten des PA-5540-Clusters sowie Panorama M-700 sind installiert, konfiguriert und produktiv in Betrieb
- Beide Funktionsbereiche sind vollständig migriert und über einen Zeitraum von mindestens einer Woche störungsfrei im Produktivbetrieb
- Die Firewall am zweiten Standort ist betriebsbereit installiert, in das zentrale Management eingebunden und wurde konfigurationsbereit übergeben
- Die Bestandssysteme an den Außenstandorten werden vollständig über das neue Panorama M-700 verwaltet und sind unbeeinträchtigt in Betrieb
- Die Konfiguration des PA-5540-Clusters wird über Panorama verwaltet und ist gemäß dem freigegebenen Konzept strukturiert
- Alle in Abschnitt 2.2 genannten Schnittstellen sind funktional nachgewiesen
- Der Hochverfügbarkeitsverbund wurde durch einen kontrollierten Failover-Test erfolgreich validiert
- Die Wiederherstellbarkeit aus dem Konfigurationsbackup wurde nachgewiesen
- Sämtliche Lizenzen und Supportverträge sind auf den Auftraggeber registriert und für einen rechtzeitigen Supportbeginn aktiv
- Die vollständige Dokumentation gemäß Abschnitt 10 wurde übergeben und vom Auftraggeber freigegeben
- Der Wissenstransfer gemäß Abschnitt 11.3 wurde durchgeführt
- Es bestehen keine betriebsverhindernden oder betriebsbehindernden Mängel

Mängel, die den Produktivbetrieb nicht beeinträchtigen, stehen der Teilabnahme nicht entgegen, sind jedoch im Abnahmeprotokoll mit verbindlicher Frist zur Beseitigung zu erfassen.

8.3 Gesamtabnahme

Die Gesamtabnahme erfolgt, wenn sämtliche der folgenden Kriterien erfüllt sind:

- Alle gelieferten Komponenten des PA-5540-Clusters sowie Panorama M-700 sind installiert, konfiguriert und produktiv in Betrieb (siehe 8.2)
- Alle gelieferten Komponenten des PA-1420 sind installiert, konfiguriert und produktiv in Betrieb (inklusive Anbindung PA-1420 an Panorama M-700)
- Sämtliche Lizenzen und Supportverträge sind auf den Auftraggeber registriert und für einen rechtzeitigen Supportbeginn aktiv

- Die vollständige Dokumentation gemäß Abschnitt 10 wurde übergeben und vom Auftraggeber freigegeben
- Der Wissenstransfer gemäß Abschnitt 11.3 wurde durchgeführt

Mängel, die den Produktivbetrieb nicht beeinträchtigen, stehen der Gesamtabnahme nicht entgegen, sind jedoch im Abnahmeprotokoll mit verbindlicher Frist zur Beseitigung zu erfassen.

9 Mitwirkungsleistungen des Auftraggebers

Der Auftraggeber erbringt die nachfolgenden Mitwirkungsleistungen (Obliegenheiten). Diese sind bei der Angebotskalkulation zu berücksichtigen und begründen keine gesonderte Vergütung.

- Bereitstellung der Rack-Flächen einschließlich Stromversorgung und Klimatisierung
- Bereitstellung der Netzwerkverkabelung bis zum Aufstellort
- Bereitstellung der erforderlichen IP-Adressen, VLAN-Konfigurationen und DNS-Einträge
- Bereitstellung von Zugängen zu den anzubindenden Umsystemen sowie Benennung der jeweils zuständigen Ansprechpartner
- Bereitstellung der Dokumentation der Bestandsumgebung sowie Exporte der Bestandskonfiguration
- Gewährung des physischen Zutritts zu den Rechenzentrumsflächen nach Voranmeldung im Rahmen der geltenden Sicherheitsvorgaben
- Benennung eines verantwortlichen Ansprechpartners auf Seiten des Auftraggebers
- Fristgerechte Prüfung und Freigabe der vorgelegten Konzepte innerhalb 10 Werktagen
- Teilnahme an Statustermen und Mitwirkung bei Tests und Abnahmen

Für Tätigkeiten des Auftragnehmers in den Räumlichkeiten des Auftraggebers gelten die Sicherheits- und Zutrittsregelungen des Auftraggebers. Eingesetztes Personal ist vorab namentlich zu benennen.

10 Dokumentation

Der Auftragnehmer übergibt spätestens zum Zeitpunkt der Gesamtabnahme eine vollständige Dokumentation in deutscher Sprache in bearbeitbarer elektronischer Form. Die Dokumentation umfasst mindestens:

- Systemdokumentation der gesamten Zielarchitektur einschließlich Netzwerk- und Zonenplänen
- Konfigurationsdokumentation aller Systeme einschließlich der Virtual-System-Aufteilung
- Portbelegungs- und Verkabelungsplan
- Dokumentation der eingerichteten Schnittstellen und Integrationen
- Dokumentation des Berechtigungs- und Rollenkonzepts
- Betriebshandbuch mit Beschreibung der regelmäßigen Betriebsaufgaben
- Verfahrensdokumentation für Backup, Wiederherstellung und Failover
- Migrationsprotokoll mit Nachweis der durchgeführten Prüffälle
- Übersicht aller Seriennummern, Lizenzen und Supportverträge einschließlich Laufzeiten und Registrierungsnachweisen

Der Auftraggeber erhält das Recht, die Dokumentation für interne Zwecke uneingeschränkt zu vervielfältigen und zu bearbeiten.

11 Leistungen nach Abnahme

11.1 Wartung und Support

Der Auftragnehmer erbringt über die gesamte Vertragslaufzeit Wartungs- und Supportleistungen. Diese umfassen sowohl die Vermittlung und Koordination des Herstellersupports als auch eigene Supportleistungen des Auftragnehmers als erste Anlaufstelle für den Auftraggeber (Single Point of Contact).

Der Leistungsumfang umfasst mindestens:

- Entgegennahme und Qualifizierung von Störungsmeldungen über E-Mail oder Ticketsystem
- Störungsanalyse und Störungsbehebung einschließlich Eskalation an den Hersteller
- Koordination des Hardwareaustauschs im Rahmen der Herstellersupportvereinbarung
- Bereitstellung und Unterstützung bei der Einspielung von Software- und Sicherheitsupdates
- Proaktive Information über sicherheitsrelevante Herstellerhinweise und End-of-Life-Ankündigungen
- Unterstützung bei Konfigurationsänderungen im Rahmen des vereinbarten Leistungsumfangs

Es gelten die nachfolgenden Reaktionszeiten. Die Reaktionszeit bezeichnet den Zeitraum zwischen dem Eingang der Störungsmeldung und der qualifizierten Rückmeldung des Auftragnehmers.

Stufe	Reaktionszeit	Servicezeit
Severity 1 (Betriebsverhindernder Mangel)	1 Stunde	24x7
Severity 2 (Betriebsbehindernder Mangel)	2 Stunden	Montag - Freitag von 08.00 - 17.00 Uhr
Severity 3 (Leichter Mangel)	4 Stunden	Montag - Freitag von 08.00 - 17.00 Uhr
Severity 4 (Allgemeine Anfragen, Konfigurationsunterstützung)	8 Stunden	Montag - Freitag von 08.00 - 17.00 Uhr

11.2 Weiterentwicklung und Optimierung

Der Auftraggeber behält sich vor, über die Vertragslaufzeit weitere Dienstleistungen des Auftragnehmers abzurufen. Hierzu zählen insbesondere Unterstützung bei Konfigurationsanpassungen, Optimierung der Regelwerke, Durchführung von Versionswechseln sowie beratende Leistungen zur Weiterentwicklung der Sicherheitsarchitektur.

Der Auftragnehmer hat hierfür im Preisblatt Tagessätze je Qualifikationsstufe verbindlich anzugeben. Die Abrufe erfolgen auf Basis vorheriger schriftlicher Beauftragung mit vorheriger Aufwandsschätzung.

12 Rückbau der Altsysteme

Nach erfolgreicher Migration und Abschluss des Parallelbetriebs sind die abzulösenden Systeme außer Betrieb zu nehmen. Der Leistungsumfang umfasst:

- Kontrollierte Außerbetriebnahme der Altsysteme nach Freigabe durch den Auftraggeber
- Nachweisliche Löschung sämtlicher Konfigurations- und Protokolldaten auf den Altsystemen
- Physischer Ausbau der Altsysteme aus den Racks

Stand: 09.09.2026 | Dieses Dokument ist Bestandteil der Vergabeunterlagen.