

## LEISTUNGSBESCHREIBUNG

# Erneuerung eines Perimeter-Firewall-Systems

## Auftraggeber

Das Helmholtz-Zentrum Hereon ist eine außeruniversitäre Forschungseinrichtung der Helmholtz-Gemeinschaft und betreibt internationale Spitzenforschung in den Bereichen Hochleistungswerkstoffe, innovative Verfahren, nachhaltige Technologien sowie Biomaterialien für medizinische Anwendungen.

## Gegenstand der Ausschreibung

Gegenstand dieser Ausschreibung ist die Beschaffung, Lieferung, Installation, Migration sowie Inbetriebnahme eines hochverfügbaren Firewall-Clusters zur Nutzung als Perimeter-Firewall im Rechenzentrum des Auftraggebers (AG).

Zusätzlich umfasst die Leistung:

- Migrationsplanung und -durchführung
- Dokumentation
- Schulung
- Service- und Supportleistungen

## Zielsetzung und Rahmenbedingungen

Ziel ist die Erneuerung der bestehenden Firewall-Infrastruktur zur Sicherstellung von:

- hoher Verfügbarkeit
- ausreichender Leistungsfähigkeit
- nachhaltiger Zukunftsfähigkeit

Die Firewall muss:

- interne Netze sicher von WAN und DMZ trennen
- Datenverkehr analysieren (Layer 7)
- Bedrohungen aktiv erkennen und abwehren

## Herstellerfestlegung

Im Rahmen der bestehenden IT-Sicherheitsarchitektur wird eine Firewall-Lösung des Herstellers Palo Alto Networks oder eine gleichwertige, vollständig kompatible Lösung beschafft.

Begründung:

Die bestehende Firewall-Infrastruktur basiert auf Systemen dieses Herstellers und umfasst eine über mehrere Jahre gewachsene, produktiv genutzte Konfiguration. Diese beinhaltet insbesondere:

- umfangreiche Regelwerke
- mehrere tausend Netzwerkobjekte
- komplexe VPN-Konfigurationen
- sicherheitskritische Policies
- Schnittstellen zu SIEM, SOC, Monitoring, externen dynamischen Listen und Identity-Systemen

Eine Migration auf ein inkompatibles System würde:

- eine vollständige manuelle Neuimplementierung erfordern
- nicht verlustfrei oder automatisiert möglich sein
- erhebliche Risiken für den Produktivbetrieb mit sich bringen
- zu erheblichen technischen Inkompatibilitäten führen.

Zusätzlich wären:

- umfangreiche Anpassungen von Betriebsprozessen
- erhebliche Schulungsaufwände

erforderlich.

Zur Gewährleistung eines stabilen und sicheren Betriebs sowie zur Vermeidung unverhältnismäßiger Mehrkosten und Risiken ist daher ausschließlich eine Lösung des Herstellers Palo Alto Networks oder eine gleichwertige Lösung, sofern vollständige Kompatibilität auf Konfigurationsdatei-Ebene nachgewiesen wird, zulässig.

Der wirtschaftliche Aufwand eines inkompatiblen Systems wäre unverhältnismäßig im Verhältnis zum Beschaffungsgegenstand.

Die Festlegung erfolgt aus zwingenden technischen und wirtschaftlichen Gründen.

## Ist-Situation

### Bestandssystem

- 2 × Palo Alto PA-3260
- Betrieb: Active/Passive HA

### Wesentliche Dienste

- Webserver
- Remote VPN
- Clientless VPN
- Site-to-Site VPN
- Internetzugang
- Datenimport von Messrechnern

### Konfiguration

- ca. 2.100 Network Objects
- ca. 150 Group Objects
- ca. 60 NAT Objects
- ca. 450 Policies
- ca. 30 Remote-VPN-Policies
- ca. 10 Clientless applications

### Lizenzen

- Advanced URL Filtering
- GlobalProtect Gateway
- Threat Prevention
- Premium Partner

## Soll-Konzept

- Ersatz der bestehenden Firewall durch aktuelles System
- Betrieb als hochverfügbares HA-Cluster (Active/Passive)
- Migration der bestehenden Konfiguration möglichst unverändert
- Zielsystemklasse: Die Lösung soll sich an den im folgenden beschriebenen technischen Anforderungen orientieren. Die Leistungsklasse eines Palo Alto Networks PA-3420 Geräts entspräche diesen Anforderungen.

## Technische Anforderungen (MUSS)

- Hardware-Appliance
- 19"-Rackmountfähig
- vollständiges Montagematerial
- redundante Komponenten:
  - $\geq 2$  Netzteile (hot-swappable)
  - $\geq 2$  Lüfter (hot-swappable)
- Front-to-Back-Airflow
  
- HA-Betrieb Active/Passive

## Schnittstellen (MUSS)

Pro Node:

- 10 × 10G SFP+ LR
- 4 × 10G SFP+ SR
- 1 x Management-Interface
- 1 x Management Console RJ45
- 2 x HA-Interfaces

Es sind nur herstellereigene Komponenten zulässig.

## VPN-Durchsatz (MUSS)

2 GB/s

1000 Sessions/s

## RAM (MUSS)

32 GB

## CPU (MUSS)

10 GB/s Threat prevention throughput

## Funktionale Anforderungen (MUSS)

- Stateful Inspection
- Layer-7-Analyse
- IPS / Threat Prevention
- URL Filtering
- VPN:
  - Remote Access
  - Site-to-Site

- Clientless
- Zentrales Management
- Hochverfügbarkeit

## Dienstleistungen

### Installation, Migration und Inbetriebnahme

#### *Leistungen*

- Einbau der Hardware
- Netzwerkintegration
- Lizenzaktivierung
- vollständige Migration der Konfiguration

#### *zusätzliche Anforderungen*

- Migrationskonzept
- Minimierung von Ausfallzeiten
- Durchführung in Wartungsfenstern

#### *Besonderheiten*

- Parallelbetrieb erforderlich
- Fallback muss möglich sein

#### *Wartungsfenster*

- regulär: der dem ersten Montag im Jahr folgende Mittwoch
- 06:00 – 09:00 Uhr

Alle Nebenkosten sind im Preis enthalten.

## Dokumentation (MUSS)

### Bereitstellung

Bereitstellung spätestens 10 Werktage vor Abnahme.

### Inhalte

- Systemdokumentation
- vollständige Konfiguration
- Inventarliste (inkl. Seriennummern)
- Patch-/Verkabelungsplan

- Lizenzübersicht
- Supportinformationen

## Format

- Open Document Format (ODF)

## Schulung

### Rahmenbedingungen

- Dauer: 1 bis 2 Tage
- vor Ort beim AG
- Sprache: Deutsch oder Englisch

### Inhalte

- Administration über GUI und CLI
- Operativer Betrieb
- Unterschiede Alt-/Neusystem
- Best Practices in Bezug auf die o.g. wesentlichen Dienste.

## Service und Support

### Laufzeit

- 4 Jahre
- Verlängerungsoption auf weitere 2 Jahre, optional bis EOL (End of Life)

## Leistungen

### Hardware

- Austausch defekter Komponenten
- Datenträger verbleiben beim AG

### Software

- Updates / Patches / Upgrades
- Lizenzpflege

## Servicezeiten

- 24/7 Störannahme
- deutschsprachig zu Bürozeiten

## SLAs

### Prioritäten

| Priorität | Beschreibung    |
|-----------|-----------------|
| P1        | Komplettausfall |
| P2        | Teilstörung     |

### Reaktionszeiten

| Leistung          | P1        | P2               | Support |
|-------------------|-----------|------------------|---------|
| Reaktion          | 1h (24/7) | 4h               | 4h      |
| Wiederherstellung | 4h        | nächster Werktag | -       |

## Ort der Leistungserbringung

Helmholtz-Zentrum Hereon  
Rechenzentren

## Zeitplan

Fertigstellung und produktiver Betrieb:  
spätestens Ende Q1/2027

# Bewertung der Angebote

## Bewertungsmethodik

### Kosten 50%

- Firewall-System 15%
- Erstinstallation, Migration und Inbetriebnahme 10%
- Dokumentation 5%
- Produktschulung 5%
- Service und Support 10%
- Stundensätze 5%

### Qualitative Kriterien 30%

- Nachvollziehbarkeit und Qualität der technischen Begründung der angebotenen Hardware  
Leistungsfähigkeit und Skalierbarkeit der Lösung  
Zukunftssicherheit (z. B. Supportdauer, Erweiterbarkeit um QoS oder Decryption) 10%
- Migrationskonzept:  
Vollständigkeit und Plausibilität, Minimierung von Ausfallzeiten und Risiken, Vorgehen für Rollback-/Fallback-Szenarien 7%
- Support-Rahmenbedingungen:  
Qualität der Support-Rahmenbedingungen (SLA)  
Garantierte Reaktionszeiten; Verfügbarkeit des Supports; Qualifikation und Standort des Supports  
(z. B. deutschsprachig) 5%
- Leistungsbeschreibung und Angebot:  
Vollständigkeit und Verständlichkeit der Angebotsunterlagen  
Detaillierungsgrad der Leistungsbeschreibung; Nachvollziehbarkeit der Kalkulation 5%
- Angebotene Schulung 3%

### Bietergespräche 20%

- Kompetenz und Verständnis der Hereon-Anforderung
- Nachvollziehbarkeit des Migrationskonzepts
- Qualität der Risikobetrachtung
- Fachliche Tiefe der Antworten
- Klarheit und Praxisbezug der Präsentation



## Preis

Die Bieter haben ihre Preise für die Leistung im Angebot vollständig auszuweisen. Das preisniedrigste Angebot erhält 10 Punkte. Für die preislich nachfolgenden Angebote wird die Punktzahl wie folgt bestimmt:

$$\text{Punktzahl Bieter} = \text{Niedrigstpreis} \times 10 / \text{Preis Bieter}$$

Die Helmholtz-Zentrum Hereon ist berechtigt, Angebote auszuschließen, deren Einzelpreise spekulativ abgegeben wurden. Ein spekulativer Preis liegt vor, wenn der Bieter bei einer bestimmten Leistung nicht die von ihm für diese Leistung tatsächlich verlangte Vergütung, sondern einen geringeren Preis ausweist, weil er bestimmte Kostenfaktoren, die nach seiner eigenen Kalkulation bei jener Leistung tatsächlich anfallen, auf die für andere Leistungen geforderte Vergütung umgelegt hat. Vergleichsmaßstab sind die eigenen Schätzungen der Helmholtz-Zentrum Hereon und die Vergleichspositionen anderer Bieter.

## Qualitative Kriterien

Bei der Wertung übt die Helmholtz-Zentrum Hereon ihren Beurteilungsspielraum aus und nimmt eine Bewertung entsprechend der Bietererklärung vor. Die Punktvergabe erfolgt entsprechend den aufgezeigten Unterkriterien.

Dabei gilt Folgendes:

- 0 Punkte: Ungenügende Darstellung/Leistungserwartung (ungenügend; der Bieter präsentiert eine Lösung, die die geforderten Anforderungen in allen Belangen ungenügend bzw. unzureichend erfüllt)
- 2 Punkte: Mangelbehaftete Darstellung/Leistungserwartung (mangelhaft; der Bieter präsentiert eine Lösung, die die geforderten Anforderungen mit gewichtigen Defiziten und Schwächen in allen Belangen erfüllt)
- 4 Punkte: Mittelmäßige Darstellung/Leistungserwartung (ausreichend; der Bieter präsentiert eine Lösung, die die geforderten Anforderungen mit weitreichenden bzw. gewichtigen Defiziten und Schwächen erfüllt)
- 6 Punkte: Gute Darstellung/Leistungserwartung (befriedigend; der Bieter präsentiert eine Lösung, die die geforderten Anforderungen mit mehreren bzw. nicht lediglich geringfügigen Defiziten und Schwächen erfüllt)
- 8 Punkte: Sehr gute Darstellung/Leistungserwartung (gut; der Bieter präsentiert eine Lösung, die die geforderten Anforderungen mit geringfügigen Defiziten bzw. vereinzelten Schwächen erfüllt)

- 10 Punkte: Hervorragende Darstellung/Leistungserwartung (sehr gut; der Bieter präsentiert eine Lösung, die die geforderten Anforderungen vollumfänglich und uneingeschränkt erfüllt)

## Bietergespräche

Bei der Wertung der Kriterien Bietergespräche übt das Hereon seinen Beurteilungsspielraum aus und nimmt eine Bewertung entsprechend folgenden Schwerpunkten vor:

Ablauf Bietergespräche (max. 60 Minuten):

- Vorstellung Hereon
- Vorstellung des Unternehmens
- Vorstellung des Ansprechpartners
- Vorstellung der angebotenen Lösung
- Vorstellung des Ablaufs der Migration
- Vorstellung der Support-Rahmenbedingungen
- Fragerunde
- Abschluss

Die Punkte werden wie folgt bewertet:

- Kompetenz und Verständnis der Hereon-Anforderung
- Nachvollziehbarkeit des Migrationskonzepts
- Qualität der Risikobetrachtung
- Fachliche Tiefe der Antworten
- Klarheit und Praxisbezug der Präsentation

Die Punktvergabe erfolgt entsprechend den aufgezeigten Unterkriterien. Dabei gilt Folgendes:

- 0 Punkte: Ungenügende Darstellung/Leistungserwartung (ungenügend; der Bieter präsentiert eine Lösung, die die geforderten Anforderungen in allen Belangen ungenügend bzw. unzureichend erfüllt)

- 2 Punkte: Mangelbehaftete Darstellung/Leistungserwartung (mangelhaft; der Bieter präsentiert eine Lösung, die die geforderten Anforderungen mit gewichtigen Defiziten und Schwächen in allen Belangen erfüllt)
- 4 Punkte: Mittelmäßige Darstellung/Leistungserwartung (ausreichend; der Bieter präsentiert eine Lösung, die die geforderten Anforderungen mit weitreichenden bzw. gewichtigen Defiziten und Schwächen erfüllt)
- 6 Punkte: Gute Darstellung/Leistungserwartung (befriedigend; der Bieter präsentiert eine Lösung, die die geforderten Anforderungen mit mehreren bzw. nicht lediglich geringfügigen Defiziten und Schwächen erfüllt)
- 8 Punkte: Sehr gute Darstellung/Leistungserwartung (gut; der Bieter präsentiert eine Lösung, die die geforderten Anforderungen mit geringfügigen Defiziten bzw. vereinzelt Schwächen erfüllt)
- 10 Punkte: Hervorragende Darstellung/Leistungserwartung (sehr gut; der Bieter präsentiert eine Lösung, die die geforderten Anforderungen vollumfänglich und uneingeschränkt erfüllt)

Das Hereon wird das Bietergespräch in seiner Gesamtheit bewerten.