



UNIVERSITÄT ZU LÜBECK
IT-SERVICE-CENTER

Erweiterung und Erneuerung der IPS-/NG-Firewall-Lösung für die Universität zu Lübeck 2027

Leistungsbeschreibung

Version: 1.0
Datum: 30.06.2026
Verantwortlich: Helge Illig
Betriebsleiter

Universität zu Lübeck
IT-Service-Center
Ratzeburger Allee 160
23562 Lübeck

Tel.: +49 451 3101 2000
Fax: +49 451 3101 2004
E-Mail : helge.illig@uni-luebeck.de

Inhaltsverzeichnis

Ziel des Projekts	4
Ausgangslage.....	5
Einsatzzweck.....	5
Leistungsbeschreibung	6
Anforderungen	6
Hardware.....	7
Durchsatzraten.....	7
Funktionalitäten	8
Cluster.....	8
Netzwerk-Protokolle und -Standards	8
Routing	9
DHCP-Funktionen	9
Bandbreitenmanagement (QoS)	9
Virtuelle Firewall.....	9
Adressobjekte.....	9
Abwehr von Netzwerkangriffen	9
IPS	9
Störungsfreie Sitzungsverwaltung.....	10
Next-Generation-Firewall-Funktionen	10
VPN/IPSEC.....	10
Weitere Funktionalitäten	11
Managementsystem	11
Firewall-Regeln	11
Logging und Reporting	12
Datenpaketanalyse	12
Monitoring.....	13
Dienstleistungen.....	13
Aufbau, Installation und Migration	13
Schulung	13
Migration.....	13

Service und Support.....	14
Servicevertrag.....	14
Hersteller-Support und Updates	14
Lizenzen	15
Hardwareprobleme und Austauschgerät	15
Leistungsbestandteile der Ausschreibung.....	16
Ansprechpartner	17
Verträge.....	17
Anhang	19
Anbindungsskizze/Topologie 2026 Ausgangslage	19
Geplante Anbindung 2027 mit RZ-Anbindung.....	20

Ziel des Projekts

Das erste Firewall-Cluster des Herstellers Forcepoint wurde 2013 an der Universität zu Lübeck in Betrieb genommen. Die Supportverträge inklusive 2018 beschafften Hardware laufen im Dezember 2026 aus und können aufgrund der nicht mehr unter Support stehenden Hardware verlängert werden. Die Anforderungen steigen dazu jährlich mit der Bedeutung der IT-Sicherheit bei zugleich steigenden Leistungsanforderungen. Der Schutz und die Absicherung der universitären Rechenzentren erfordern eine Anbindung des Firewall-Clusters auch in diesem Netzsegment in vollem Umfang.

Aufgrund der Betriebserfahrung der letzten 14 Jahre, der Störungsfreiheit sowie der guten Administrierbarkeit des Systems, soll ein neues Firewall-Cluster des gleichen Herstellers beschafft und in Betrieb genommen werden. Dieses soll um eine redundante 100-Gigabit-Anbindung an die Rechenzentrums-Infrastruktur erweitert werden und den Netzwerk-Durchsatz von 400Gbit/s erfüllen. Ein Wechsel des Herstellers inklusive Systempartners bedeutet einen erheblichen Administrationsmehraufwand und eine Überarbeitung/Neukonfiguration des Firewall-Sicherheitskonzeptes sowie die Schulung der Firewall-Administratoren. Hierbei ist von einer mehrmonatigen Einarbeitungszeit und kostenintensiven Schulung während des laufenden IT-Betriebes auszugehen. Dabei darf zu keinem Zeitpunkt die IT-Sicherheit der Universität gefährdet werden. Eine Übergangslösung mit dem jetzigen Hersteller und der Aufbau eines parallel betriebenen neuen Clusters wäre ab 2027 notwendig. Diese Mehrkosten und der damit verbundene Aufwand sind bei der Entscheidung berücksichtigt. Des Weiteren ist für 2027 eine Trennung der Netzbereiche über Firewall-Systeme geplant und den Internetzugang sowie interne Netze durch eine weitere Firewall abzusichern und von kritischen internen Bereichen zu trennen wie es u.a. das BSI empfiehlt. Die Lösung von Forcepoint bietet ein einheitliches unabhängiges Managementsystem mit dem SMC an und ist als einziger Hersteller in der Lage, unterschiedliche Hardwaremodelle in ihr Cluster im laufenden Betrieb zu integrieren und betreiben, so dass es zu keinen Ausfallszeiten während des Betriebs bei der Umstellung kommt. Die Firewalls an den Außenstellen werden ebenfalls über das SMC verwaltet und überwacht. Diese sind noch bis 2029 beim Hersteller unter Support und Wartung. Lediglich die Verwaltung über das SMC muss neu lizenziert werden.

Es ist eine Leistungsabschätzung bis 2035 notwendig, da wir von einer realistischen Betriebszeit von 8-10 Jahren ausgehen. Eine entsprechende Skalierbarkeit muss für das neue System gewährleistet sein. Schwerpunkte bei der Produktwahl bleiben weiterhin das Intrusion Prevention System, die gut zu bedienende Administrationsoberfläche mit den Analyse-Fähigkeiten, der ausgezeichnete Support, die Etablierung im Markt mit einer großen Community im Hochschulumfeld sowie die Möglichkeiten der gezielten Fehlersuche im Datenverkehr (Troubleshooting). Zugleich hat erneut eine Marktanalyse stattgefunden. Dabei haben sich im Vergleich zu 2023 und 2018 kaum Veränderungen bei der Herstellerwahl in dem Segment ergeben. Andere Anbieter im Enterprise-Segment mit Referenzen im Hochschulumfeld sind Fortinet, Checkpoint und Palo Alto. Die Kriterien, die für die Marktanalyse relevant waren, sind den Ausschreibungsunterlagen zur internen Verwendung beigelegt. Alle Kriterien erfüllt der Hersteller Forcepoint sowie der zertifizierte Support-Partner.

Ausgangslage

Das alte Firewall-Cluster der Firma Forcepoint N6205 läuft seit 2018 fehlerfrei und war den Anforderungen stets gewachsen.

Forcepoint zentralisiert seine IT-Security-Produkte um das Firewall-Verwaltungstool SMC und investiert in die Weiterentwicklung u.a. in Finnland. Von technischer Seite gibt es bei dem Produkt NGFW-6205 keine Beanstandungen. Die „concurrent sessions“ liegen bei 90.000 Verbindungen pro Knoten in Spitzenzeiten. Diese Auslastung wird sich durch die Anbindung an das Rechenzentrum und die zeitliche Entwicklung deutlich erhöhen. Die Software SMC (Security Management Center) ist für den Betrieb und das Monitoring notwendig und kann nicht durch andere Lösungen ersetzt werden. Es arbeitet unabhängig vom Betrieb der Firewall-Appliances. Die aktuelle Anbindung an das Universitätsdatennetz und an das DFN ist im Anhang skizziert.

Einsatzzweck

Die IPS-/Firewall-Lösung dient zur Absicherung vielschichtiger Sicherheitsanforderungen, die sich aus dem Betrieb und der Nutzung der IT-Infrastruktur an der Universität ergeben. Dabei werden interne Teilbereiche über das Firewall-System abgesichert. Aktuell ist von folgenden Teilbereichen auszugehen, die entsprechend ihres Bedarfs abzusichern sind. Diese sind u.a.:

- Verwaltungsnetze
- Institutsnetze
- Studentennetze
- WLAN-Netze
- Technische Netze
- Rechenzentrums-Infrastruktur
- Webserver-Netze
- Konferenznetze (WLAN und Firmen)
- Gastnetze (Gästehaus, Wohnheim)
- Netze kooperierender Einrichtungen

Neben der klassischen Firewall-Funktionalität im Perimeter ist der Einsatz eines technologisch aktuellen IPS-Systems von zentraler Bedeutung, um im heterogenen Datenverkehr (unterschiedlichste Nutzergruppen und Geräte) Gefahren zu erkennen und Netzwerkverkehr bis Layer 7 zu identifizieren. Das Modell reiner portbasierter Filter wird als veraltet angesehen. Es ist ungeeignet, um sicheres Freischalten von Serverdiensten zu gewährleisten oder Angriffe zu erkennen und abzuwehren. Hier dienen die Technologien einer Next-Generation-Firewall zur Erkennung von Applikationen in Datennetzströmen zur Erweiterung des Sicherheitsumfangs und Anpassung an die aktuelle Bedrohungslage (Angriffswahrscheinlichkeiten und Schwachstellen). Die IPS-Funktionalität und die anwenderfreundliche Administrierbarkeit stehen im Nutzungsvordergrund. Ein Export der Daten an eine zentrale SIEM-Lösung ist möglich und bereits in Tests.

Im Serverbereich und in den Rechenzentren muss die aktuelle Firewall auch Angriffe über verschlüsselte Verbindungen erkennen können und in der Lage sein, entsprechende SSL-Zertifikate von internen Servern zu verwalten, um den Datenstrom zu analysieren. Ebenso sollen

Datenverkehrsströme durch getunnelte Verbindungen erkennbar sein, um einem Missbrauch entgegenzuwirken bzw. direkte Angriffe zu erkennen. Um mehr Sichtbarkeit im wachsenden Datenverkehr bei zugleich hoher Übertragungsgeschwindigkeit (100Gbit/s und mehr) zu erreichen, ist eine dedizierte Anbindung an die Rechenzentren notwendig. Dafür ist die Anforderung an eine einzelne Appliance ein Netzwerk-Durchsatz von mindestens 400Gbit/s.

Neben der Erkennung von Gefahren durch aktuellste IPS-Signaturen muss die Firewall-Lösung auch Botnetze und deren Datenverkehr zu Kontrollservern erkennen sowie Zero-Day-Angriffe abwehren. Aktuelle Reputations- und URL-Filter können diese Funktion unterstützen, müssen aber im Kosten-Nutzen-Verhältnis realisierbar bleiben.

Leistungsbeschreibung

Anforderungen

Die Absicherung der IT-Infrastruktur im Perimeter und interner Netzbereiche soll zukünftig weiterhin durch die bestehende IPS-/Firewall-Lösung von Forcepoint gewährleistet sein. Hierbei ist von einer Nutzungsdauer von mindestens fünf Jahren mit steigenden Anforderungen (steigende Durchsatzraten und entsprechendem Aufwand der Analyseverfahren) auszugehen. Die zukünftige direkte Anbindung der Rechenzentren mit den hohen Anforderungen (Verfügbarkeit und Leistung) ist Ziel der Erweiterung der Sicherheitsinfrastruktur. Eine Verlängerungsoption der Laufzeit und Supportverträge soll möglich sein, so dass eine Betriebszeit von 8-10 Jahren realistisch ist. Daher darf das Modell des Herstellers nicht älter als 2 Jahre auf dem Markt sein. Berücksichtigt man Studierende, Mitarbeiter und externe Nutzer sowie Anfragen an zentrale Server (z.B. Webserver), so sind z.Zt. ca. 10.000 Clientverbindungen (Endgeräten/Nutzeranfragen) aktiv. Es werden aktuell bis zu 100.000 von der Firewall gleichzeitig zu verwaltenden Sitzungen pro Firewall-Knoten erreicht. Unsere interne Netzanbindungen werden in den nächsten Jahren ebenfalls modernisiert und von 10Gbit auf 25/50Gbit umgestellt. Die Rechenzentren erhalten eine 100Gbit-Anbindung und arbeiten intern bereits mit dieser Geschwindigkeit. Angesichts der Anforderungen und Entwicklung wird folgende Hardware für die Ausschreibung vorgegeben, die seit Juni 2025 auf dem Markt erschienen ist und die 100-Gbit-Tauglichkeit bei 400 Gbit/s Netzwerkdurchsatz erfüllt:

Bezeichnung	Anzahl	Produktnummer
Forcepoint NGFW 3505	2	N3505

Im Rahmen der Vorbereitung der Ausschreibung wurden vergleichbare Modelle anderer Hersteller betrachtet und die Merkmale herausgearbeitet. Alleinstellungsmerkmale der Forcepoint-Lösung sind der Cluster-Betrieb im Aktiv-Aktiv-Modus mit bis zu 16 Knoten, wodurch ein Austausch der Hardware oder die Erweiterung im laufenden Betrieb ermöglicht wird und in der Vergangenheit problemlos im Betrieb funktioniert hat. Dabei können die Modelle unterschiedlicher Bauart sein, was maximale Flexibilität ermöglicht und kein anderer Hersteller derzeit kann. Dadurch verringert sich der Zeitaufwand beim Austausch und Integration neuer Hardware auf wenige Minuten nach der Verkabelung oder ein Clusterknoten wird direkt im laufenden Betrieb ersetzt. Weitere Merkmale sind

die Erkennung von Verschleierungsangriffen im Datenverkehr (Evasions) sowie die in unabhängigen Tests (NSSLABs, Cyberratings) nachgewiesene hohe Erkennungsrate des IPS-Systems. Im Gegensatz zu den ASIC-basierten Spezial-Appliances von Checkpoint und Fortinet ist das System von Forcepoint ausschließlich softwarebasiert und damit gerade bei einer langen Laufzeit sehr anpassungsfähig durch den Hersteller (Funktionserweiterungen, Fehlerbehebungen).

Die Installation und Wartung soll als Dienstleistung durch ein Systemhaus zusammen mit dem IT-Service-Center der Universität zu Lübeck erfolgen.

Das Projekt beinhaltet die Integration der neuen Firewall-Appliance-Hardware in das bestehende Cluster gemeinsam mit dem IT-Service-Center der Universität zu Lübeck und die Migration der bestehenden Konfiguration im laufenden Betrieb. Die alten Hardware-Geräte werden im Anschluss aus dem Cluster entfernt.

Die Universität zu Lübeck wird dem Dienstleister die dazu erforderlichen Netzwerkinformationen und Ressourcen zur Verfügung stellen. Dieses beinhaltet auch die virtuellen Umgebungen für das Management.

Alle Abläufe für die Installation müssen mit der Universität zu Lübeck abgestimmt und dokumentiert werden.

Hardware

Das Firewall-Cluster soll aus herstellereigener Hardware (Appliances) bestehen, für die Hardware-Support des Herstellers verfügbar ist. Die Hardware muss fabrikneu und originalverpackt geliefert werden, und das Modell nicht älter als 2 Jahre auf dem Markt sein (im Verkauf seit 2025). Folgende weitere Anforderungen muss das Einzelgerät erfüllen:

- Einbau in 19-Zoll-Datennetzschränke, Lieferung passender Einbauschienen, verkürzte Einbautiefe 600mm (Vertikalschienenabstand 550mm) in Gebäude 64
- Bauhöhe: Maximal 2U (Rack-Höheneinheiten)
- Redundante Netzteile (Betrieb auf zwei unterschiedlichen Stromphasen)
- Herstellersupport: Mindestens 5 Jahre mit Option der Verlängerung (aktuelle Hardware)
- Notwendige Clusteranschlüsse für Zwei- bzw. Mehrgerätebetrieb, Lieferung notwendiger Clusterverbindungskabel

Ein baugleiches Ersatzgerät (N3505-Spare) wird mit dem Kaufvertrag erworben und steht für den Support-Fall sofort vor Ort zur Verfügung. Dadurch minimiert sich das Ausfallrisiko bzw. der Ausfall der Redundanz während einer notwendigen Ersatzlieferung entfällt.

Durchsatzraten

Folgende Durchsatzraten sind von einem Firewall-Knoten aufgrund der neuen Anforderungen für die Rechenzentrumsanbindung mindestens zu leisten:

IPv4/IPv6 (no inspection) ¹	400 Gbps
IPv4/IPv6 (with inspection) ¹	40 Gbps
IPS IPv4/IPv6 (Sicherheitsfunktionen aktiv)	30 Gbps

Funktionalitäten

Die Funktionalitäten entsprechenden u.a. den Kriterien von 2013 und 2018, die sich im Betrieb bis zum heutigen Tag bewährt haben.

Cluster

Das ausfallsichere Cluster hat folgende Kriterien zu erfüllen:

- Automatischer Failover im Fehlerfall
- Konfigurierbare Fehlerfallerkennung und Benachrichtigung
- Manueller Failover ohne Leistungsausfall für Wartungsaufgaben
- Zwei Netzteile pro Gerät (Stromredundanz)
- Active/Active-Betrieb (Performance-Verbesserung)
- Die Performance des Active/Active-Clusters muss mindestens 150% eines Single-Nodes erreichen
- Für den Austausch- und Wartungsfall muss ein weiterer (dritter) Firewall-Knoten zum aktiven Cluster hinzufügbare sein ohne dass es zu einem Betriebsausfall oder Störung kommt

Netzwerk-Protokolle und -Standards

Folgende Netzwerk-Protokolle und Standards muss das Firewall-System auf allen Schnittstellen mindestens beherrschen:

Protokoll/Standard	Anmerkung
IPv4	notwendig
IPv6	notwendig
802.3ad	notwendig
802.1q	notwendig

Die Performance der IPv6-Funktionalitäten muss analog zur IPv4-Performance sein und darf nicht signifikant (mehr als 10%) abweichen. Die Firewalls werden über LACP (802.3ad) an die Cisco-Geräte des Backbones, Rechenzentrums und DFN angebunden. Eine korrekte Verbindungsaushandlung und Ausfallerkennung muss gewährleistet sein.

Folgende Netzwerk-Protokolle und Standards soll das Firewall-System im aktiven Modus auf allen Schnittstellen beherrschen:

Multicast

Multicast IPv4	u.a. PIM, IGMP
----------------	----------------

¹ UDP 1518 byte packet size

Multicast IPv6	PIMv6, MLD
----------------	------------

Routing

Statisches Routing	
Dynamisches Routing	RIPv2, OSPFv2/3, BGPv4

DHCP-Funktionen

Für einzelne Netzbereiche (VLANs) müssen DHCP-Forwarder (IPv4) die Anbindung zentraler DHCP-Server zur Verfügung stellen können, um Clients dynamisch mit Adressen zu versorgen.

Bandbreitenmanagement (QoS)

Eine Lastverteilung und ein Bandbreitenmanagement für einzelne Interfaces bzw. VLANs müssen möglich sein.

Virtuelle Firewall

In der Firewall-Konfiguration müssen durch virtuelle Firewallinstanzen (getrenntes Routing, virtuelle Firewallfunktionen) die Komplexität der notwendigen Zugriffsregeln und deren Verwaltung reduziert werden können.

Adressobjekte

Folgende Adressobjekt-Formate müssen in Zugriffsregeln verfügbar sein:

- IPv4-Adresse, IPv6-Adresse
- IPv4-Range, IPv6-Range
- IPv4-Netz, IPv6-Netz
- Adressgruppe
- Domainnamen

Abwehr von Netzwerkangriffen

Folgende Standardnetzangriffe müssen u.a. über Schutzfunktionen abwehrbar sein:

- Spoofing
- Portscans
- Flooding (TCP/UDP)
- DoS/DDoS
- Anomalien im TCP-Handshake (SYN-Flooding, gleichzeitige Flags SYN/FIN, FIN ohne ACK)
- Blockieren unbekannter Protokolle (einstellbar)
- IPv6-Schutzmechanismen (Next-Header-Analyse, Anomalien)

IPS

Die IPS-Funktionalität ist zentraler Bestandteil der Lösung. Das Management muss zur Administration umfangreiche Hilfsmittel zur Verfügung stellen:

- Aktualisierung (manuell und automatisch) der Signaturen

- Definition eigener Signaturen
- Definition von Ausnahmen
- Blockieren oder Kontrollieren von Angreifern
- Tägliche Loganalyse-Funktion
- Dokumentation (z.B. Online-Referenz) zu Signaturen und erkannten Schwachstellen (CVE-Referenz, etc.)
- Flexibler Einsatz für jeweiliges Anwendungsumfeld (z.B. Absicherung von Webservern)

Störungsfreie Sitzungsverwaltung

Zur Erfüllung der Sicherheitsaufgaben ist eine Paketanalyse und Sitzungsverwaltung mit niedrigen Latenzen notwendig. Diese Sitzungsverwaltung (Sessions) für Verbindungen muss einen störungsfreien Betrieb insbesondere für folgende Funktionen garantieren:

- VPN-Verbindungen
- SSH-Verbindungen
- SIP/H.323
- Datenbankverbindungen (auch bei fehlendem „Keep-Alive“)

Eine granulare Steuerung der Time-Outs für bestimmte Dienste (TCP, UDP, etc.) muss möglich sein, um Verbindungsabbrüche wichtiger Dienste zu vermeiden.

Next-Generation-Firewall-Funktionen

Folgende Anforderungen für weitere Sicherheitsfunktionen müssen erfüllt sein:

- Applikationserkennung und Statistiken
- Applikationskontrolle
- Anomalie-Erkennung (z.B. ungewöhnlicher Datenverkehr über bestimmte Protokolle bzw. im IP-Stack)
- Verzeichnisdienstanbindung (LDAP/Microsoft Active Directory)
- Zertifikatsverwaltung und Speicher
- SSL-Decryption
- URL-Filtermöglichkeiten (Definition eigener Filter, Reputationsdatenbank optional)
- Botnet-Datenverkehr-Erkennung
- Zero-Day-Angriffserkennung bzw. andere besondere Angriffsformen
- Erkennung und Abwehr von Advanced Evasion-Angriffen (Tarnmethoden im IP-Stack)

Alle physikalischen und virtuellen Interfaces müssen für den gleichen Schutzzumfang konfigurierbar sein, um sowohl internen Datenverkehr zu analysieren, als auch im Perimeter entsprechend Schutz zu bieten.

VPN/IPSEC

Die Firewall muss in der Lage sein, Außenstellen/Drittgeräte über VPN/IPSEC statisch anzubinden. Dabei muss u.a. das IKEv2-Protokoll (RFC 5996) unterstützt werden.

Weitere Funktionalitäten

- Die Packet Inspection darf sich nicht nur auf das erste Paket eines IP-Datenstroms beziehen.
- Es muss ein zusätzliches Firewall-System des Herstellers zur Performance-Erhöhung in das Active/Active-Cluster integrierbar sein. Hierbei muss der Produkt-Typ des zusätzlichen Gerätes von den bereits in Betrieb befindlichen Cluster-Systemen abweichen können.
- Jumbo Frames müssen unterstützt werden.
- Browser-Hinweise für Nutzer (z.B. beim Blockieren einer Verbindung) müssen möglich sein.

Managementsystem

Die Anbindung des Managementsystems muss über ein dediziertes Netz erfolgen. Der Managementserver kann wahlweise virtuell (auf Basis von Nutanix, VMware) sein und läuft in einer Linux-Umgebung als Betriebssystem.

Die Management-Software muss folgende Kriterien erfüllen:

- Managementsoftware autark (unabhängig vom Firewall-System)
- Ohne Ausfall der Firewallfunktionalität wartungsfähig
- Vorbereitung und Sicherung von Konfigurationen
- Backup der Konfigurationsstände
- Konsistente Wiederherstellung von Konfigurationsständen
- Revisionsfähig (Verwaltung von Konfigurationsständen)
- Auditfähig (personalisierte Accounts mit Zugriffs- und Änderungsprotokollierung)
- Mehrbenutzerfähig (minimal 5 administrative Nutzer)
- Zentrale Logging-Funktionen (Systemzustand-Logs, Datenverkehr-Logs, IPS-Daten, NG-Daten)
- Reporting (Erstellung von vor- und selbstdefinierten Sicherheitsberichten)

Firewall-Regeln

Die Zugriffs- und Steuerungsregeln müssen übersichtlich im Management konfiguriert und sichtbar sein. Dabei sind Lösungen über Gruppierungen und Hierarchien möglich. In den Regeln ist einzustellen, welche weiteren Schutzfunktionen (IPS, SSL-Decryption usw.) durchlaufen werden sollen, so dass eine feingranulare Steuerung des Paketflusses möglich ist.

Folgende weitere Kriterien muss das Managementsystem erfüllen:

- Verbindungsstatistiken: Nutzungshäufigkeit einzelner Regeln
- Vorbereitung von Zugriffsregeln und Konfigurationen ohne Aktivierung im Firewallsystem (Provisioning)
- Aktivierung eines Regelsatzes / Netzwerkkonfiguration nach dem Provisioning
- Aufbau von Regelgruppen bzw. Ordnungsstrukturen (Hierarchien)
- Äquivalente Unterstützung von IPv4/IPv6 (Dualstackbetrieb), optimal in einem Regelsatz
- Übersicht über angelegte Adressobjekte

- Definition freier Adressobjekte (mindestens 10.000 Stück)
- Einfache Auswahl und Suche von Objekten (Adressobjekte, Serviceobjekte)
- Direkte Eingabe/Erstellung von Objekten in der Regelkonstruktion
- Freie Definition von Serviceobjekten (IP-Dienste) und deren Verwaltung
- Darstellung von Versionsständen als Differenzübersicht (Änderungsprotokoll)
- Sprungfunktionen in der Anwendung vom Logging zur entsprechenden Policy und umgekehrt
- Einblick in die aktuelle Session-Tabelle für die Echtzeit-Fehleranalyse

Logging und Reporting

Das Firewall-Managementsystem muss Logging- und Reporting-Funktionen mit umfangreichen Filterfunktionen zur Verfügung stellen, um eine tägliche Sicherheitsanalyse durchzuführen zu können. Der Logserver läuft dediziert und getrennt vom Management in einer virtuellen Umgebung mit einem virtualisierten Linux.

Es müssen Filterfunktionen u.a. für folgende Logging-Objekte zu Verfügung stehen:

- Netzobjekte nach Quelle oder Ziel für u.a. IP-Adresse, IP-Netz, Adressgruppe
- IP-Dienste, IP-Protokolle, Applikationen
- Aktion der Regeln (drop/discard, deny/reject, accept/allow)
- Einzelregel (ID)
- Zeitraum
- IPS-Ereignis
- TCP-Verbindungszustände

Sollte eine der Funktionalitäten zum Ausschreibungszeitpunkt nicht zur Verfügung stehen, wird ein entsprechendes „Feature Request“ eingereicht, der in angemessener Zeit zu erfüllen ist.

Es müssen zusätzlich regelmäßig automatische Reports erstellt werden können. Die Informationen müssen außerhalb des Firewall-Clusters in einem abgesicherten Bereich vorliegen. Logs und Reports müssen granular und nach Vorgaben des deutschen Datenschutzrechts konfigurierbar sein (Anonymisierung von Berichten).

Das Logvolumen muss überprüfbar sein und die Protokollfunktion Möglichkeiten zur Wartung bieten, damit Protokolle zeitlich bereinigt (gelöscht) bzw. das Logvolumen geprüft werden kann.

Logfunktionen für Drittgeräte (andere Hersteller) müssen vorhanden sein.

Datenpaketanalyse

Der Export von Datenpaketen zur Problem- und Detailanalyse muss möglich sein. Hierfür ist ein fehlerfreies Aufzeichnen des Datenverkehrs notwendig, so dass eine Echtzeitanalyse möglich ist.

Das Firewall-System muss Netflow v9 für IPv4 und IPv6 unterstützen.

Alle Leistungskriterien sind in der Anforderungstabelle aufgelistet und die Stärken der Forcepoint-Lösung hervorgehoben.

Monitoring

Ein Funktions- und Netzwerk-Monitoring wird durch diese standardisierten Protokolle ermöglicht:

- SNMPv2/SNMPv3
- Syslog

Die erforderlichen MIB-Dateien des Herstellers sind dem Auftraggeber zur Verfügung zu stellen. Als Monitoring-System wird von der Universität unter anderem die Software LibreNMS, Cisco Splunk und Cisco XDR eingesetzt. Das Monitoring bezieht sich zum einen auf das Firewall-System und zum anderen auf das Management, um Probleme frühzeitig zu erkennen. Der operative Status der aktiven Komponenten sowie des Managementsystems muss dargestellt und überprüfbar sein. Dieser umfasst u.a. Speicher- und Lastprobleme sowie den Zustand der Hardwarekomponenten (u.a. Lüfter, Prozessoren, Festplatten, Netzteile, Temperaturen).

Dienstleistungen

Aufbau, Installation und Migration

Installation und Konfiguration erfolgen nach Vorgaben des Auftraggebers zur Anbindung des Firewall-Clusters an die bestehende Infrastruktur. Eine Planungsbesprechung vor dem Migrationstermin klärt offene Fragen und stellt dem Dienstleister alle Informationen und Dokumentationen des bestehenden Systems sowie die Anbindung zur Verfügung. Log-Servers und das Managementsystem sind getrennt. Danach kann mit der Migration begonnen werden. Eine Aufwandsabschätzung hat ergeben, dass die Migration inklusive Nachbetrachtung innerhalb von 2 Arbeitstagen erfolgt.

Der Auftragnehmer erstellt zum Projektabschluss eine ausführliche Dokumentation für sich und die Universität.

Schulung

Eine Schulung durch das Systemhaus ist Bestandteil der Ausschreibung. Dieses umfasst die Einweisung und die Konfiguration der neuen Hardware sowie neuer Funktionalitäten und konzeptioneller Änderungen. Dieses kann Bestandteil der Nachbetrachtung nach der Migration sein. Der geschätzte Aufwand umfasst einen Dienstleistungstag.

Migration

Die Migration und Inbetriebnahme der NGFW 3505 bis zur Deaktivierung der alten Hardware wird vom Systempartner gemeinsam mit dem IT-Service-Center durchgeführt. Der Ein- und Ausbau der Hardware erfolgt durch die Universität. Die für den Betrieb notwendigen Lizenzen werden vom Systemhaus geliefert und installiert. Für den Forcepoint-Appliance-Austausch wird ein Dienstleistungstag veranschlagt. Die Ablösung der alten Hardware (NGFW 6205) muss bis zum 31.12.2026 erfolgen. Übergangslösungen sind möglich, aber zu vermeiden und gehen zu Lasten des Auftragnehmers (Arbeitsaufwand). Die Migration muss unter Nutzung des Forcepoint Multi-Link-Clusterings im laufenden Betrieb erfolgen.

Service und Support

Servicevertrag

In Störungsfällen und bei Fragen ist eine Unterstützung durch Mitarbeiter des Auftragnehmers (Systemhaus) erforderlich.

Das Systemhaus ist zugleich direkter Ansprechpartner zum Hersteller. Das Systemhaus muss über eine ausreichende technische Qualifikation (Herstellerstatus, Anzahl an herstellertestifizierten Systemtechnikern) verfügen. Das Systemhaus muss den Partner-Status Forcepoint Titanium erfüllen. Der Auftragnehmer muss 4 ähnliche Referenzprojekte im Hochschulfeld in den letzten 2 Jahren angeben mit Namen der Hochschule, Volumen und Ansprechpartner.

Folgende Dienstleistungen muss der abzuschließende Servicevertrag erfüllen:

- 24x7 Systemhaus-Support für angebotenes Firewall-Cluster
- 24x7 Verfügbarkeitsmonitoring (Systemüberwachung mit Fehlerfrüherkennung)
- Call-Abwicklung beim Hersteller
- Vertragslaufzeit 5 Jahre
- Jährliche Review vor Ort
- Beratung/Empfehlung und Unterstützung bei Updates

Die detaillierten Vertragsvereinbarungen regelt ein Servicevertrag, der Bestandteil dieser Ausschreibung ist. Es wird ein EVB-IT-Vertrag abgeschlossen.

Hersteller-Support und Updates

Es müssen Hardware- und Software-Support sowie Updates für das Firewallsystem wie auch für die Managementsoftware und die Sicherheitssignaturen verfügbar sein. Zentrale Systemupdates werden in Rücksprache mit Hersteller und Systemhaus durchgeführt oder beauftragt.

- 5 Jahre Hersteller (Enterprise-Support)
- 5 Jahre Hersteller Subscriptions für IPS/Threat Prevention, Updates, SMC
- 5 Jahre Hardware-Support inkl. Forcepoint-Module und -Transceiver.

Ein Anschlussvertrag soll nach Ablauf der Vertragsdauer möglich sein.

Jährliche Case-Reviews finden im Rahmen des Education-Roundtable mit dem Hersteller oder über den Systempartner statt. Der Hersteller-Enterprise-Support umfasst folgende Leistungen:

- 24/7-Service mit zertifizierten technischen Ansprechpartnern
- Deutschsprachiger Technical-Account-Manager
- Zugriff auf das Support-Portal (Erstellung und Verwaltung von Support-Cases)
- Direkter persönlicher Kontakt beim Hersteller zur Eskalation (dedicated escalation contact)
- Zugriff auf Feature-Request-Portal: direkten Einfluss auf die Produktentwicklung
- Customer Success Manager
- Produktaktualisierungen, Support- und Download-Portal
- Produktdokumentation
- Reaktionszeiten für erstellte Support-Cases nach Schweregrad 1-4
 - o Severity 1: 30 Minuten

- Severity 2: 2 Stunden
- Severity 3: 4 Stunden (Werktag)
- Severity 4: 1 Werktag

Über die Hochschul-Community werden neue Anforderungen besprochen und über ein Support-Portal des Dienstleisters dokumentiert. Diese werden zweimal im Jahr beim Hersteller mit der Entwicklungsabteilung bewertet und besprochen. So können fehlende technische Anforderungen aus der Praxis laufend neu implementiert werden und die Kunden haben direkten Einfluss auf die Produktverbesserung und Entwicklung.

Lizenzen

Die Lizenzen sind als sogenannte dynamische Lizenzen zu liefern, um bei einem Hardwareaustausch oder Managementserverwechsel die Ausfallzeit zu verringern und nicht in die Gefahr von Lizenzaktivierungsproblemen zu laufen.

Hardwareprobleme und Austauschgerät

Die Clusterlösung verringert die Wahrscheinlichkeit eines Totalausfalls erheblich. Bei einem Hardwareproblem muss jedoch zwingend eine zeitnahe Lösung zur Verfügung stehen. Ein baugleiches Austauschgerät ist beim Auftraggeber vorzuhalten.

Leistungsbestandteile der Ausschreibung

1. Hardware
2. Software
3. Subscriptions (5 Jahre)
4. Hersteller-Support (5 Jahre)
5. Migrationsleistung und Schulung mit einem Systempartner
6. Service-Vertrag mit zertifiziertem Forcepoint-Partner (5 Jahre)

Pos.	Leistung/Artikel	Anzahl	Beschreibung	Preis
1	Hardware			
1.1	Appliance Forcepoint N3505	2	Appliance inkl. IPS/NGWF-Lizenzen für 60 Monate	
1.2	Firewall-Netzwerk-Module		Siehe Einzelaufstellung	
1.3	Transceiver		Siehe Einzelaufstellung	
1.4	Spare-Parts Ersatzteile			
1.4.1	N3505-Spare-Unit	1	Ersatzgerät vor Ort	
1.4.2	1-Port 100G-Modul	1	Spare-Part	
1.4.3	SFP28-LR	1	zertifiziertes Ersatzmodul	
1.4.4	SFP28-SR	1	zertifiziertes Ersatzmodul	
1.4.5	SFP100-LR	1	zertifiziertes Ersatzmodul	
1.4.6	SFP100-SR	1	zertifiziertes Ersatzmodul	
2	Software			
2.1	SMC-Lizenzen für Cluster und 4 Außenstellen	60 Monate	Managementserverlizenz inklusive Logserver. Logserver wird getrennt vom Managementserver betrieben.	
3	Lizenz Subscriptions			
	IPS/NGFW-Lizenzen	60 Monate	In Pos 1.1 bereits enthalten	
4	Hersteller-Support			
4.1	Forcepoint NGFW-Essential-Support	60 Monate	Support auf Hard- und Software, automatisches kostenfreies Upgrade auf Enterprise-Support für Hochschulkunden, Support für Netzwerkmodule mit enthalten	
4.2	Forcepoint SMC-Essential-Support	60 Monate	Software-Support für Management- und Log-Software, automatisches kostenfreies Upgrade auf Enterprise-Support für Hochschulkunden	
5	Dienstleistung Migration durch Systemhaus	2 Tage	Migration der neuen Hardware in Cluster, Tests und Schulung	
6	Service-Vertrag	60 Monate	Service-Vertrag des Systemdienstleisters, jährliche Zahlweise gemäß Vertrag	

Die erforderliche Hardware für den Austausch der bestehenden Firewall und die Anbindung an das Rechenzentrum erfordert folgende Hardwarekomponenten:

Pos	Typ	Anzahl	Hersteller-Bezeichnung	Anmerkung
Netzwerk-Module				
1.2.1	1-Port 100G-Modul	4	MOD100F1	100Gbit-Anbindung RZ
1.2.2	2-Port SFP28-Modul	4	MOD25F2	Verteilung auf 2 CPUs, Redundanz
1.2.3	4-Port SFP+ Modul (10G)	2	MOD10F4	HA-Links
Optische Transceiver				
1.3.1	Transceiver 25G LR (SFP28)	6	SFP25LR	Anbindung DFN/Backbone
1.3.2	Transceiver 25G SR (SFP28)	2	SFP25SR	Anbindung DFN/Backbone
1.3.3	Transceiver 100G LR (QSFP)	3	SFP100-LR	Anbindung RZ
1.3.4	Transceiver 100G SR (QSFP)	1	SFP100-SR	(MPO-Verbindung), Anbindung RZ
1.3.5	SFP+ Single Mode Transceiver LX	4	SFP10LR	Cluster-Link (HA und Backup)

Ansprechpartner

Die folgenden Personen werden als Ansprechpartner an der Universität zu Lübeck benannt.

Rolle	Name	Telefon	E-Mail
Projektinitiator	Helge Illig	+49 451 3101 2000	helge.illig@uni-luebeck.de
Projektleiter	Martin Bruhns	+49 451 3101 2011	martin.bruhns@uni-luebeck.de
Administrator	Thomas Kranz	+49 451 3101 2013	thomas.kranz@uni-luebeck.de
Administrator	Stefan Schmalzer	+49 451 3101 2014	stefan.schmalzer@uni-luebeck.de

Verträge

Es werden ein EVB-IT Systemvertrag und ein EVB-IT Instandhaltungsvertrag in der jeweils aktuellen Fassung abgeschlossen. Zu dem Instandhaltungsvertrag wird ein genauer spezifizierter Servicevertrag mit einem von Forcepoint zertifizierten Systempartner abgeschlossen und ist den Ausschreibungsunterlagen beigelegt. Dieses Leistungsverzeichnis wird Vertragsbestandteil.

Für den gesamten Wartungszeitraum (und die darauffolgende Zeit) ist ein Datenschutzvertrag zwischen dem Hersteller und der Universität zu Lübeck und auch dem Auftragnehmer und der Universität zu Lübeck abzuschließen, in dem der Hersteller bzw. der Auftragnehmer die Einhaltung der Bundes- und Landesdatenschutzgesetze der Bundesrepublik Deutschland und Schleswig-Holstein garantiert, sowie eventuelle besondere Datenschutzregelungen der Universität zu Lübeck. Dieser Datenschutzvertrag muss den Schutz aller potenziell durch das System laufenden Daten beinhalten, dazu gehören u.a. Verbindungsdaten, Verbindungsinhalte und personenbezogene Daten. Das

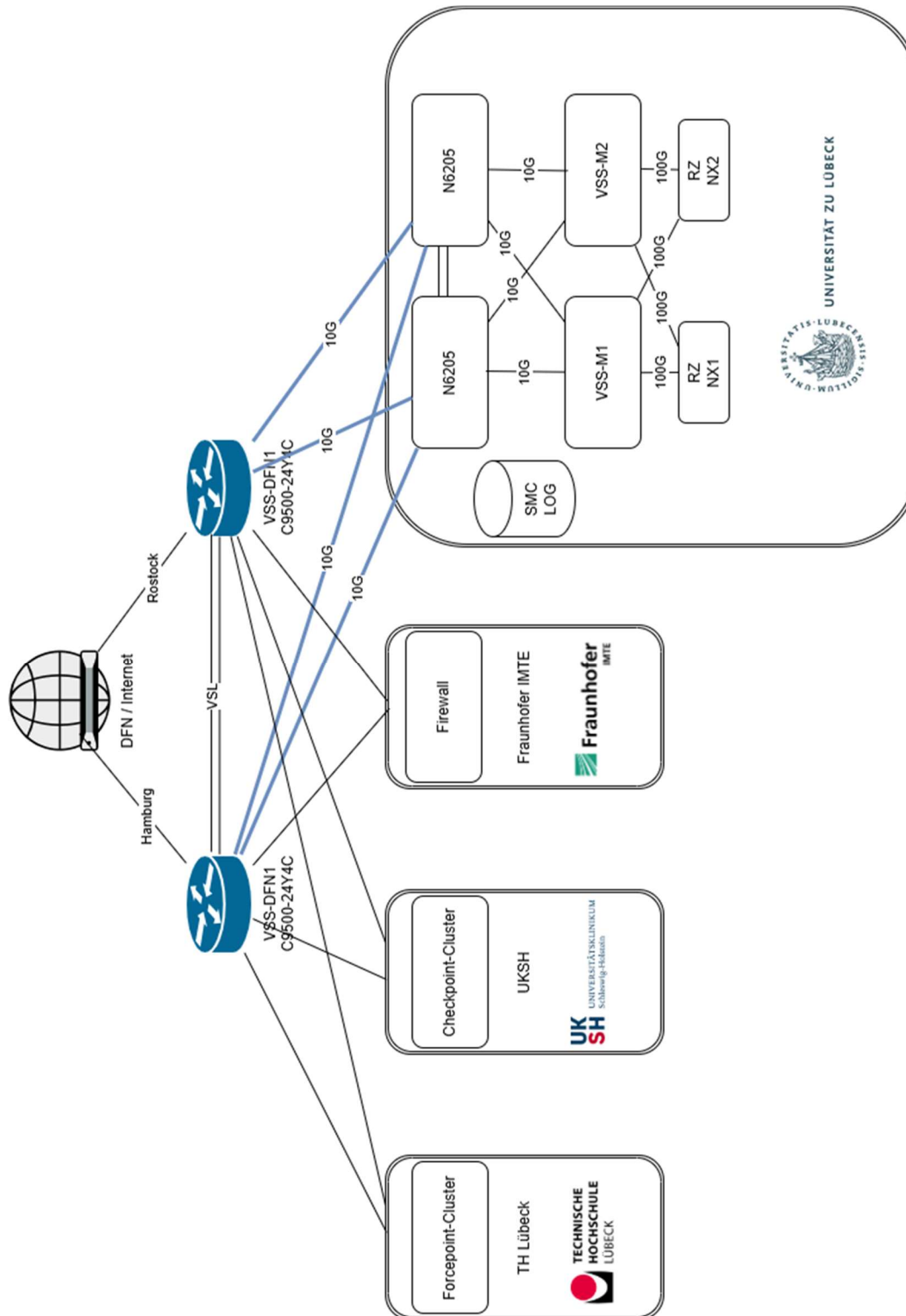
Datenschutzabkommen hat den Zweck, dass bei der Wahrnehmung von Support-Aufgaben oder bei Installationsarbeiten o.ä. der Schutz der Daten nach DSGVO garantiert ist ("Auftragsverarbeitung").

Ort, Datum _____

Unterschrift _____

Anhang

Anbindungsskizze/Topologie 2026 Ausgangslage



Geplante Anbindung 2027 mit RZ-Anbindung

