LANDRATSAMT
ERZGEBIRGSKREIS

Offenes Verfahren:
Ausschreibung einer Multifunktions Security Gateway Lösung für Schulen in Trägerschaft des Erzgebirgskreises

Vergabe-Nr.: 60101/2/6/25/151 **Stand: 08.07.2025**

Leistungsverzeichnis mit Vorbemerkungen

Für die Schulen in Trägerschaft des Erzgebirgskreises soll ein Multifunktions Security Gateway (UTM / Unified Threat Management Lösung) zwischen dem Internet und verschiedenen internen Netzen platziert werden. Das Security Gateway hat den Datenverkehr zwischen den einzelnen angeschlossenen physikalischen und/oder virtuellen Netzwerken (VLANs) zu kontrollieren und das Eindringen von Angreifern und/oder schadhaften Dateninhalten zu verhindern.
Im Folgenden sind die Anforderungen an die Sicherheitslösung beschrieben.
Der Anbieter hat sicherzustellen, dass sämtliche als „MUSS“ Kriterien dargestellte Funktionalitäten erfüllt sind.
Die als „KANN“ spezifizierten Funktionen sind nicht zwingend erforderlich, aber erwünscht; je mehr der KANN-Funktionalitäten erfüllt sind, desto höher wird die angebotene Lösung beim Ranking des Auftraggebers gewertet.
Der Einfluss des Vorhandenseins einer einzelnen KANN-Funktionalität auf die Gesamtwertung ist jeweils aus der Spalte „Wichtigkeit“ ersichtlich, in der mit einem Punktewert von 10 oder 20 die Relevanz angegeben wird.
Die Wichtung der Angebote wird zu 40 Prozent auf den Preis und 60 Prozent auf die erreichten Punkte ausgelegt.

Der Anbieter hat in der Spalte „Erfüllt“ zu vermerken, ob die angegebene Funktionalität durch das von ihm angebotene Produkt erfüllt ist nach folgendem Schema:

„**X**“ bedeutet: ohne Einschränkung erfüllt bedeutet in der Wertung die volle Punktzahl
„**–**“ bedeutet: nicht erfüllt/nicht vorhanden bedeutet in der Wertung keine Punkte
„**O**“ bedeutet: mit Einschränkungen erfüllt bedeutet in der Wertung die halbe Punktzahl

Das Feld für Bemerkungen ist für weitere Erläuterungen hinterlegt bei einer Erfüllung mit Einschränkungen.

Hinweis:
Performance-Prüfmethodik: gemessener Durchsatz unter idealen Testbedingungen unter Verwendung der Branchenstandard-Performance-Test-Tools Keysight-Ixia Breaking Point
Firewall: gemessen mit HTTP-Datenverkehr und 512 KB Antwortgröße
IPS: gemessen mit IPS mit HTTP-Datenverkehr mit Standard-IPS-Regelsatz und 512 KB Objektgröße
TLS Inspection: Performance gemessen mit IPS mit HTTPS Sessions und verschiedenen Cipher Suites

Allgemeine Anforderungen an die Firewall die mit Nachweisen zu bestätigen sind

- DSGVO- konforme Bereitstellung der Dienste in Zusammenhang mit der Firewall innerhalb der EU
- keine automatisierte Datenübertragung in Drittländer außerhalb der EU
- Lieferung innerhalb von 14 Tagen frei Haus
- Support 24 Stunden x 7 Tage die Woche in Englisch oder Deutsch
- EAL4+ Zertifizierung
- Einschlägige Kunden-Referenzen im öffentlichen Sektor
- Vorabaustausch im Schadensfall innerhalb der 5-jährigen Garantiezeit
- Nach End-of-Sales (EOS) mindestens noch 5 Jahre Support und aktuell kein EOS erklärt oder angekündigt
- Als Hilfestellung sollten die Hersteller Ablaufpläne (z. B. mithilfe von Datenflussdiagrammen) anbieten, die die konkrete Abarbeitung der Regelsätze erläutert. Dadurch sollte auch ersichtlich werden, welche Kriterien zu welchen Aktionen führen.
- Die Überprüfung von Netzwerkverkehr in der Cloud des Herstellers sollte optional sein. Ist die Funktion vorhanden, muss diese deaktivierbar sowie konfigurierbar sein. Es sollte konfigurierbar sein, ob und in welcher Form Dateien in der Cloud übertragen werden dürfen (z. B. nur Hashwerte einer Datei oder die komplette Datei).
- Am Paketfilter MÜSSEN Schutzmechanismen aktiviert sein, um IPv4- sowie IPv6 Fragmentierungsangriffe abzuwehren (NET.3.2.A10)
- Die Uhrzeit der Firewall SOLLTE mit einem Network-Time-Protocol (NTP)-Server synchronisiert werden. Die Firewall SOLLTE keine externe Zeitsynchronisation zulassen. (Nur Relevant, wenn eine Zeitsynchronisation in diesem Fall überhaupt relevant ist)

Die allgemeinen Anforderungen verstehen sich als Grundvoraussetzungen für die Einbeziehung der abgegebenen Angebote in die Angebotsauswertung.

Anforderungen an die anzubietende Security Gateway Lösung

Basis Firewall Verwaltung

Angeforderte Funktionalität	Wichtigkeit (MUSS oder 0-20 Punkte)	Erfüllt? Angabe mit X /O/–	Bemerkung
Benutzeroberfläche über Webbrowser, Bedienung ohne zusätzliche Plugins oder Java möglich	**MUSS**		
Benutzeroberfläche in deutscher Sprache	**MUSS**		
Erweiterte Fehlerbehebungswerkzeuge in der GUI (z.B. Paketerfassung, Verbindungsliste, URL Kategorie Suche, Systemdiagramme, Support Zugriff)	**20 Punkte**		
Kommandozeilenschnittstelle (CLI) über GUI zugänglich	**10 Punkte**		
Kontextsensitive Suche über die vollständige Menüstruktur	**10 Punkte**		
Rollenbasierte Verwaltung	**20 Punkte**		
Automatisierte Firmware-Update-Benachrichtigung mit einfachem automatisiertem Update-Prozess und Rollback-Funktionen	**MUSS**		
Automatisches Rollback bei fehlerhaften Firmware Update	**MUSS**		
Kritische Hotfixes automatisch einspielbar	**MUSS**		
Wiederverwendbare Systemobjektdefinitionen für Netzwerke, Dienste, Hosts, Zeiträume, Benutzer und Gruppen, Clients und Server	**20 Punkte**		
Selbstbedienungs-Benutzerportal (Self-Service)	**10 Punkte**		
Self-Service in deutscher Sprache	**10 Punkte**		
Nachverfolgung von Konfigurationsänderungen	**MUSS**		
Flexible Gerätezugangskontrolle für Dienste nach Zonen	**10 Punkte**		
E-Mail- oder SNMP-Trap-Benachrichtigungsoptionen	**10 Punkte**		
E-Mailbenachrichtigungsoptionen über ein cloudbasiertes Management System	**10 Punkte**		
SNMP (v1,v2c,v3) und Netflow Unterstützung	**10 Punkte**		
Sicherungs- und Wiederherstellungs-konfigurationen: lokal, per FTP, E-Mail oder Cloudbasiert; On-Demand, täglich, wöchentlich oder monatlich	**20 Punkte**		
Automatische Erstellung verschlüsselter Konfigurationsbackups	**MUSS**		

Angeforderte Funktionalität	Wichtigkeit (MUSS oder 0-20 Punkte)	Erfüllt? Angabe mit X /O/–	Bemerkung
API für die Integration von Drittanbietern	**10 Punkte**		
Integrierte Anleitungen im Dashboard	**10 Punkte**		
Fernzugriffsoption für Hersteller-Support über GUI	**10 Punkte**		
Fernzugriffsoption für Hersteller-Support über SSH	**10 Punkte**		
Secure Syslog Unterstützung	**20 Punkte**		
Airgap Support (Ermöglicht das Update von Firewalls, die in Umgebungen eingesetzt werden, die physisch vom Internet isoliert sind)	**10 Punkte**		
Generieren und automatisches Erneuern von Let's Encrypt Zertifikaten	**MUSS**		
Nutzung von Let´s Encrypt Zertifikaten in allen technisch unterstützen Modulen	**MUSS**		
Hochverfügbarkeit			
Stateful HA failover untersützt Aktiv/Passiv und Aktiv/Aktiv	**20 Punkte**		
Unterstützt virtuelle MAC Adressen oder physikalische MAC Adressen	**10 Punkte**		
Benötigt keine zusätzliche Lizenz für Aktiv/Passiv	**20 Punkte**		
Unterstützung von Zero Downtime bei Firmware Upgrade	**20 Punkte**		
Automatischer Konfigurationsabgleich zwischen den HA Firewall Geräten	**20 Punkte**		
Stateful HA failover: Nahtloser Übergang für routenbasierte, richtlinienbasierte, Fernzugriffs-VPNs und dynamische Routen ohne Verlust der Tunnelkonnektivität bei Hochverfügbarkeits-Failover.	**20 Punkte**		

Basis Firewall Funktionen

Angeforderte Funktionalität	Wichtigkeit (MUSS oder 0-20 Punkte)	Erfüllt? Angabe mit X /O/–	Bemerkung
Firewall, Netzwerk & Routing			
Einheitliches Richtlinienmodell zur Verwaltung von Richtlinien auf einen Blick	**MUSS**		
Policy-Test-Simulator-Tool, um Firewall-Regel und Web Test zu ermöglichen Policy-Simulation und Testen nach Benutzer, IP und Tageszeit	**20 Punkte**		
Stateful Deep Packet Inspection Firewall	**MUSS**		
FastPath Paket-Optimierung	**10 Punkte**		
Benutzer-, Gruppen-, Zeit- oder Netzwerkbasierte Richtlinien	**MUSS**		
Zugriffszeitrichtlinien pro Benutzer/Gruppe	**MUSS**		
Durchsetzung von Richtlinien über Zonen, Netzwerken oder nach Servicetypen	**MUSS**		
Zonenisolierung und zonenbasierte Richtlinienunterstützung	**20 Punkte**		
Automatische Gruppierung von Regeln für große Regelsätze	**10 Punkte**		
Standardzonen für LAN, WAN, DMZ, VPN und WLAN	**10 Punkte**		
Benutzerdefinierte Zonen für LAN oder DMZ	**20 Punkte**		
Anpassbare Standard IP-Maskierungsrichtlinie für NAT	**MUSS**		
Wizard für die NAT Konfiguration	**10 Punkte**		
Flood Protection für DoS & DDoS	**MUSS**		
Ländersperrung durch geo-IP	**MUSS**		
Routing: statisch, Multicast (PIM-SM) und dynamisch (BGP, OSPF, RIP, OSPFv3)	**20 Punkte**		
Statische Blackhole Route	**20 Punkte**		
Unterstützung für Equal-Cost Multi-Path (ECMP)	**10 Punkte**		
Upstream-Proxy-Unterstützung	**MUSS**		
Protokollunabhängiges Multicast-Routing mit IGMP-Snooping	**10 Punkte**		
Bridging mit STP-Unterstützung und ARP-Broadcast Weiterleitung	**20 Punkte**		
WAN-Link-Balancing: mehrere Internetverbindungen, Auto-Link-Zustandsprüfung, automatischer Failover, automatischer und gewichteter Abgleich und granulare Mehrwege-Regel	**MUSS**		

Angeforderte Funktionalität	Wichtigkeit (MUSS oder 0-20 Punkte)	Erfüllt? Angabe mit X /O/–	Bemerkung
Mobiles WAN-Unterstützung (USB, LTE, UMTS)	**20 Punkte**		
802.3ad Schnittstellen Link Aggregation	**20 Punkte**		
Vollständige Konfiguration von DNS, DHCP und NTP	**MUSS**		
Dynamisches DNS	**20 Punkte**		
Jumbo Frame Unterstützung	**10 Punkte**		
IPv6-Unterstützung mit Tunneling-Unterstützung einschließlich 6in4, 6to4, 4in6, IPv6 Rapid Deployment (6.) über IPSec, IPv6 DHCP prefix delegation	**20 Punkte**		
Wildcard-Unterstützung für Domain-Namen-Host-Objekte	**MUSS**		
VLAN DHCP Unterstützung und Tagging	**20 Punkte**		
Unterstützung mehrerer Bridges	**20 Punkte**		
VLAN Mitglieder in Bridge	**20 Punkte**		
Layer 2 Bridge mit erlaubten VLAN‘(s)	**20 Punkte**		
Möglichkeit Interface zu aktivieren und deaktivieren ohne Konfigurationsverlust	**MUSS**		
Traffic Shaping & Quoten			
Netzwerk- oder benutzerbasiertes Traffic Shaping (QoS)	**MUSS**		
Festlegen von benutzerbezogenen Traffickontingenten beim Upload/Download oder Gesamttraffic und zyklischen oder nicht-zyklischen Verkehr.	**MUSS**		
VoIP-Optimierung in Echtzeit	**20 Punkte**		
Authentifizierung			
Transparente Client-Authentifizierung	**20 Punkte**		
Authentifizierung über: Active Directory, EntraID, eDirectory, RADIUS, LDAP oder TACACS+	**MUSS**		
Webadmin Zugriff rollenbasiert mit Active Diretory, EntraID, lokale Authentifizierung	**MUSS**		
Terminal Server Authentifizierung via Client oder Kerberos	**MUSS**		
Kerberos Authentifizierung	**MUSS**		
NTLM Unterstützung	**MUSS**		
Server-Authentifizierungsagenten für Active Directory SSO	**20 Punkte**		
Client-Authentifizierungs-Agenten für Windows, Mac OS X, Linux 32/64	**20 Punkte**		

Angeforderte Funktionalität	Wichtigkeit (MUSS oder 0-20 Punkte)	Erfüllt? Angabe mit X /O/–	Bemerkung
Authentifizierungszertifikate für iOS und Android	**10 Punkte**		
Single sign-on: Active directory	**MUSS**		
Authentifizierungsdienste für IPSec, L2TP, PPTP, SSL	**20 Punkte**		
Captive Portal	**MUSS**		
Single Sign On mit Radius-Accounting-Anfragen	**20 Punkte**		
Single Sign On mit Chromebook	**20 Punkte**		
Benutzer Self-Service Portal			
Möglichkeit Authentication Client herunterzuladen	**10 Punkte**		
Download SSL & IPsec Remote Access Client (Windows) und Konfigurationsdateien	**20 Punkte**		
Download IPsec Remote Access Client (MacOS) und Konfigurationsdateien	**20 Punkte**		
Download SSL & IPsec Remote Access Konfigurationsdateien für andere Betriebssysteme (iOS/Android/Linux)	**20 Punkte**		
Hotspot-Zugriffsinformationen	**20 Punkte**		
Benutzername und Passwort ändern	**20 Punkte**		
Persönliche Internetnutzung anzeigen	**20 Punkte**		
Site-to-Site-VPN			
Routenbasiertes IPsec Site-to-Site VPN	**20 Punkte**		
Richtlinienbasiertes IPsec Site-to-Site VPN	**20 Punkte**		
Native Unterstützung von Site-to-Site VPN zu Amazon VPC	**10 Punkte**		
SSL-VPN basiertes Site-to-Site VPN	**20 Punkte**		
Vordefinierte IPsec Profile mit Verschlüsselungsalgorithmen	**10 Punkte**		
IKEv1 & IKEv2 Unterstützung	**20 Punkte**		
Verschlüsselung: AES(128/192/256), AES128GCM16, AES192GCM, AES256GCM16, AES128GMAC, AES192GMAC, AES256GMAC, 3DES (112/168), Blowfish	**20 Punkte**		
Authentifizierung: MD5, SHA2-256/384/512, SHA1	**20 Punkte**		
DH-Gruppen(Schlüsselgruppe): DH1,2,5,14,15,16,17,18,25,26,19,20,21,27-30,31	**20 Punkte**		
Dead Peer Detection (DPD)	**10 Punkte**		
NAT-Traversal-Unterstützung	**20 Punkte**		

Angeforderte Funktionalität	Wichtigkeit (MUSS oder 0-20 Punkte)	Erfüllt? Angabe mit X /O/–	Bemerkung
Hardwarebeschleunigung für IPsec VPN	**20 Punkte**		
DHCP Relay Funktionalität für routen- und richtlinienbasiertes IPSec VPN.	**20 Punkte**		
Fernzugriff-VPN			
Separates, gehärtetes VPN Portal für Zugriffe aus dem Internet	**MUSS**		
Integrierter IPsec & SSL VPN Client	**MUSS**		
Optionaler Multifaktor Zwang für Benutzer in SSL- und IPsec VPN	**MUSS**		
Optionaler Zustandsinformation des Clients auswerten	**10 Punkte**		
Optional Benutzern erlauben, Benutzername und Kennwort zu speichern	**10 Punkte**		
Unterstützung für IPsec, SSL-VPN, L2TP, PPTP Clientlose SSL-VPN.	**20 Punkte**		
AD-Anmeldungsskript nach Verbindungsaufnahme laufen lassen	**20 Punkte**		
Intelligentes Split-Tunneling für optimales Routing in SSL-VPN und IPsec	**20 Punkte**		
NAT-Traversal-Unterstützung	**20 Punkte**		
Client-Monitor zur grafischen Übersicht über den Verbindungsstatus	**10 Punkte**		
Profilbasierter SSL-VPN Zugriff	**20 Punkte**		
Verschlüsslung SSL-VPN: AES-256-GCM, AES-192-GCM, AES-128-GCM, AES-256-CBC, AES-192-CBC, AES-128-CBC, DES-EDE3-CBC, BF-CBC	**20 Punkte**		
Verschlüsslung IPsec VPN: AES(128/192/256), , AES128GCM16, AES192GCM, AES256GCM16, AES128GMAC, AES192GMAC, AES256GMAC, 3DES (112/168)	**20 Punkte**		
Mehrsprachig: Deutsch, Englisch und Französisch	**10 Punkte**		
Verschlüsseltes HTML5-Self-Service-Portal mit Unterstützung für RDP, SSH, Telnet und VNC	**20 Punkte**		

SD-WAN

Angeforderte Funktionalität	**Wichtigkeit (MUSS oder 0-20 Punkte)**	**Erfüllt? Angabe mit X /O/–**	**Bemerkung**
SD-WAN Routen anhand von Verkehrskennzeichner Quelle Netzwerke, Ziel Netzwerk & Dienst	**20 Punkte**		
SD-WAN Routen anhand von Verkehrskennzeichner Anwendungen	**20 Punkte**		
SD-WAN Routen anhand von Verkehrskennzeichner Benutzer oder Gruppen	**20 Punkte**		
Linkauswahl anhand von Primären und Reserve Gateway	**20 Punkte**		
Linkauswahl anhand von SD-WAN Profilen	**20 Punkte**		
SD-WAN Profile mit Dienstleistungsvereinbarungen (SLA) für Paketverlust, Jitter und Latenz	**20 Punkte**		
Herstellervordefinierte SLA-Strategien	**10 Punkte**		
Benutzerspezifische SLA-Strategien	**10 Punkte**		
Schnittstelle Zustandsüberprüfung mit TCP oder Ping	**20 Punkte**		
ThirdParty Integration Cloudfare, Akamai, Azure	**10 Punkte**		

Network Protection Funktionen

Angeforderte Funktionalität	Wichtigkeit (MUSS oder 0-20 Punkte)	Erfüllt? Angabe mit X /O/–	Bemerkung
Intrusion Prevention Systems (IPS)			
Leistungsstarke IPS Deep Packet Inspection Engine der nächsten Generation mit selektiven IPS-Mustern für maximale Leistung und Schutz.	**MUSS**		
Bereitstellung unterschiedlicher IPS Regelwerke zur parallelen Anwendung auf Basis zu schützender Systeme und/oder Benutzer	**MUSS**		
Erweiterter Bedrohungsschutz und synchronisierte Sicherheit			
Advanced Threat Protection (Erkennen und Blockieren von Netzwerkverkehr, der versucht, über mehrschichtige DNS-, AFC- und Firewall-Verbindungen mit Befehls- und Steuerungsservern in Kontakt zu treten) mit Machine Learning	**MUSS**		
Deep Packet Inspection	**MUSS**		
SSL Inspection TLS 1.2	**MUSS**		
SSL Inspection TLS 1.3	**MUSS**		
Möglichkeit unerwünschte Cipher zu blockieren.	**10 Punkte**		
Möglichkeit Minimum SSL/TLS Version zu definieren	**20 Punkte**		
Synchronisierung der Benutzer-ID zwischen Endpoint und Firewall. Voraussetzungen bitte nennen.	**20 Punkte**		
Unmittelbarer Einblick in den Zustand der Endgeräte mit der Möglichkeit, automatisch auf Sicherheitsvorfälle zu reagieren, indem infizierte Systeme isoliert werden. Voraussetzungen bitte nennen.	**20 Punkte**		
Übersicht von Benutzern mit hohem Risiko, unbekannte Anwendungen, erweiterte Bedrohungen und verdächtige Nutzlasten. Voraussetzungen bitte nennen.	**20 Punkte**		
Automatisches Identifizieren, Klassifizieren und Steuern aller unbekannten Anwendungen im Netzwerk. Voraussetzungen bitte nennen.	**20 Punkte**		
Einholen von Applikationsinformationen vom Endpoint für den Datenverkehr, der nicht mit einer Signatur der Applikationskontrolle übereinstimmt. Voraussetzungen bitte nennen.	**20 Punkte**		

Angeforderte Funktionalität	Wichtigkeit (MUSS oder 0-20 Punkte)	Erfüllt? Angabe mit X /O/–	Bemerkung
Umfassende forensische Analysemöglichkeiten nach Benutzer, Bedrohungen, Anwendungen, Internetnutzung und andere Aktivitäten im Netzwerk.	**20 Punkte**		
Begrenzt den Zugriff auf Netzwerkressourcen oder isoliert kompromittierte Systeme, bis sie bereinigt sind. Voraussetzungen bitte nennen.	**20 Punkte**		
Gemeinsame Nutzung von Telemetrie und Zustandsdaten zwischen Endpoint und Firewall um eine koordinierte Maßnahme durchzuführen. Voraussetzungen bitte nennen.	**20 Punkte**		
Möglichkeit der Layer2 Isolierung von verwalteten Endpoints Voraussetzungen bitte nennen.	**20 Punkte**		
Integration in Security Operation Center			
Optionaler, automatisierter Telemetriedaten Upload	**10 Punkte**		
Herstellereigene Analysten zur Bekämpfung von Bedrohungen verfügbar	**10 Punkte**		
Automatische Integration der Firewall in ein Hersteller Security Operation Center	**10 Punkte**		
Analyst kann automatisiert im Bedrohungsfall URL, DNS und IP Adressen blockieren und monitoren	**10 Punkte**		
Analyst kann automatisiert Layer2 Isolierung von verwalteten Endpoints durchführen	**10 Punkte**		
Analyst kann kundenspezifische Blocklisten verwalten	**10 Punkte**		
Möglichkeit Bedrohungs-Feeds aus externen Quellen hinzufügen, um Bedrohungen zu erkennen	**10 Punkte**		
Möglichkeit Bedrohungs-Feeds aus externen Quellen hinzufügen, um Bedrohungen zu blockieren	**10 Punkte**		
Unterstützung von DNS, IP und URL Listen aus externen Quellen	**10 Punkte**		
Automatische Reaktion auf Erkennungen	**10 Punkte**		

Web Protection Funktionen

Angeforderte Funktionalität	Wichtigkeit (MUSS oder 0-20 Punkte)	Erfüllt? Angabe mit X /O/–	Bemerkung
Web-Schutz und -Kontrolle			
Vollständig transparenter Proxy für Anti-Malware und Web-Filterung	**MUSS**		
URL-Filter-Datenbank mit Millionen von Websites in 92 Kategorien, die von einer Datenbank bereitgestellt werden.	**MUSS**		
Surfquota-Zeitrichtlinien pro Benutzer/Gruppe	**MUSS**		
Zugriffszeitrichtlinien pro Benutzer/Gruppe	**MUSS**		
Malware-Scanning: Blockierung aller Formen von Viren, Web-Malware, Trojanern und Spyware auf HTTP/S, FTP und webbasierten E-Mails.	**MUSS**		
Erweiterter Web-Malware-Schutz mit JavaScript-Emulation	**10 Punkte**		
Live-Schutz mit Echtzeit Abfragen der neuesten Bedrohungsinformationen	**20 Punkte**		
Scannen in Echtzeit oder im Stapelbetrieb	**10 Punkte**		
Schutz vor Pharming	**10 Punkte**		
HTTP- und HTTPS-Scans pro Benutzer oder Netzwerkrichtlinie mit anpassbaren Regeln und Ausnahmen	**20 Punkte**		
Erkennung und Durchsetzung von SSL-Protokoll-Tunneln	**20 Punkte**		
Überwachung und Durchsetzung von Web-Schlüsselwörtern	**10 Punkte**		
Zertifikatsvalidierung	**20 Punkte**		
Leistungsstarkes Caching von Webinhalten	**10 Punkte**		
Dateityp-Filterung nach Mime-Type, Erweiterung und aktiven Inhaltstypen (z.B. Active-X, Applets, Cookies, etc.)	**20 Punkte**		
Umsetzung von YouTube für Schulen	**MUSS**		
Umsetzung von SafeSearch	**MUSS**		
Regelbasierte Steuerung von SafeSearch and YouTube	**MUSS**		
Anwendungschutz und Kontrolle			
Verbesserte Anwendungskontrolle mit Signaturen und Layer-7-Mustern für Tausende von Anwendungen	**20 Punkte**		

Angeforderte Funktionalität	Wichtigkeit (MUSS oder 0-20 Punkte)	Erfüllt? Angabe mit X /O/–	Bemerkung
Anwendungssteuerung nach Kategorie, Eigenschaften (z.B. Bandbreiten- und Produktivitätsverbrauch), Technologie (z.B. P2P) und Risikostufe	**20 Punkte**		
Application Risk Meter liefert einen Gesamtrisikofaktor, der auf dem Risikoniveau der Anwendungen im Netzwerk basiert.	**20 Punkte**		
Identifizieren, klassifizieren und kontrollieren von bisher unbekannten Anwendungen, die im Netzwerk aktiv sind. Voraussetzungen bitte nennen.	**20 Punkte**		
Durchsetzung von Richtlinien zur Anwendungskontrolle pro Benutzer oder Netzwerkregel	**MUSS**		
Bereitstellung unterschiedlicher Applikationskontrolle Regelwerke zur parallelen Anwendung auf Basis zu schützender Systeme und/oder Benutzer	**MUSS**		
Web & App Traffic Shaping			
Individuelle Traffic Shaping (QoS)-Optionen nach Webkategorie oder Anwendung, um Upload/Download oder Total Traffic Priority und Bitrate individuell oder gemeinsam zu begrenzen oder zu garantieren.	**20 Punkte**		

Funktionen Sandboxing

Angeforderte Funktionalität	**Wichtigkeit (MUSS oder 0-20 Punkte)**	**Erfüllt? Angabe mit X /O/–**	**Bemerkung**
Überprüft ausführbare Dateien und Dokumente mit ausführbaren Inhalten	**MUSS**		
Dynamische Malware-Verhaltensanalyse mit Merkmalanalyse, Merkmalkombinationsanalyse und Strukturanalyse	**MUSS**		
Reputationsanalyse	**20 Punkte**		
Sandbox-Detonation mit Screenshots, Prozesse, Datei- und Netzwerkaktivitäten	**20 Punkte**		
Dateianalyse mit Signatur und Zertifikat, Dateiabschnitte, Quellen und Importe	**20 Punkte**		
Überprüft ausführbare Inhalte in Archiven (ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet)	**MUSS**		
Detaillierte Reports zu Schaddateien und Möglichkeit zur Dashboard-Dateifreigabe	**10 Punkte**		
Detaillierte, ereignisorientierte Reports	**10 Punkte**		

Zentrale Verwaltung

Angeforderte Funktionalität	**Wichtigkeit (MUSS oder 0-20 Punkte)**	**Erfüllt? Angabe mit X /O/–**	**Bemerkung**
Möglichkeit zentrales Management cloudbasiert	**MUSS**		
Möglichkeit zentrales Alertmanagment cloudbasiert	**MUSS**		
Möglichkeit zentrales Backupmanagement cloudbasiert	**MUSS**		

Protokollierung und Reporting

Angeforderte Funktionalität	**Wichtigkeit (MUSS oder 0-20 Punkte)**	**Erfüllt? Angabe mit X /O/–**	**Bemerkung**
Vordefinierte Reports mit benutzerdefinierten Berichtsoptionen (HINWEIS: Die Verfügbarkeit von individuellen Protokollen, Berichten und Widgets hängt von aktivierten Software-Abonnements ab):	**10 Punkte**		
Dashboards (Traffic, Sicherheit,User Threat Quotient und Bedrohungs-Feeds aus externen Quellen)	**10 Punkte**		
Anwendungsbericht (Anwendungsrisiko, Blockierte Anwendungen, Webanwendungen, Suchmaschinen, Webserver, FTP),	**20 Punkte**		
Netzwerk- und Bedrohungsbericht (IPS, ATP, Wireless, Security Heartbeat),	**20 Punkte**		
VPN-Berichte	**10 Punkte**		
Konformitätsberichte (HIPAA, GLBA, SOX, FISMA, PCI-DSS, NERC CIP v3 und CIPA)	**10 Punkte**		
Aktuelle Aktivitätsüberwachung: Systemzustand, Live-Benutzer, IPsec-Verbindungen, Remote-Benutzer, Live-Verbindungen, Wireless-Clients, Quarantäne- und DoS-Angriffe	**20 Punkte**		
Anonymisierung von Berichten	**20 Punkte**		
Berichtsplanung an mehrere Empfänger pro Berichtsgruppe mit flexiblen Optionen	**10 Punkte**		
Standard- und granulare Protokollierungsoptionen	**10 Punkte**		
Berichte als HTML, PDF, Excel (XLS) exportieren	**10 Punkte**		
Security-Audit-Bericht	**20 Punkte**		
Web-Schlüsselwort Content Report	**10 Punkte**		
Detailliertes Threat Intelligence Reporting	**10 Punkte**		
Unterstützung cloudbasiertes Reporting	**10 Punkte**		
Vollständiger Log-Viewer mit individueller Anpassung der Aufbewahrung nach Kategorie	**10 Punkte**		

Leistungsklasse 1 (Schulen bis max. 150 Clients [Lehrer + Schüler])

Hardware Anforderungen und Performance

Angeforderte Funktionalität	**Wichtigkeit (MUSS oder 0-20 Punkte)**	**Erfüllt? Angabe mit X /O/–**	**Bemerkung**
Auslegung im 19“ Rack Format	**10 Punkte**		
Ethernet Ports : mind. 8x 1GbE	**MUSS**		
Davon SFP Glasfaserports: mind. 1x 1GbE	**20 Punkte**		
redundante Stromversorgung möglich	**20 Punkte**		
Produktzertifizierungen (Safety, EMC) : CB, CE, FCC Class A, CTick, IC, VCCI, RCM, UL, CCC	**MUSS**		
Firewall Durchsatz: mind. 18.000 Mbit/s	**MUSS**		
IPS Durchsatz: mind. 4.000 Mbit/s	**MUSS**		
SSL/TLS Inspection Durchsatz: mind. 1.000 Mbit/s	**MUSS**		
Gleichzeitige Verbindungen: mind. 5.000.000	**MUSS**		
Neue Verbindungen / Sek: mind. 70.000	**MUSS**		
Maximum lizenzierte Benutzer: mind. 250	**MUSS**		

Angebotene Lösung

Hersteller der Hardware:	
Modellbezeichnung:	
Hersteller der Software:	
Bezeichnung der Software:	
HW oder SW Erweiterungen:	

Initiale Anschaffungskosten Hardware:		EUR
Initiale Anschaffungskosten Software		EUR
Kosten für 60 Monate Wartung der Hardware		EUR
Kosten für 60 Monate Wartung der Software:		EUR
Sonstige Kosten (Angabe unter Benennung)		EUR

Leistungsklasse 2 (Schulen bis max. 400 Clients [Lehrer + Schüler])

Hardware Anforderungen und Performance

Angeforderte Funktionalität	**Wichtigkeit (MUSS oder 0-20 Punkte)**	**Erfüllt? Angabe mit X /O/–**	**Bemerkung**
Auslegung im 19“ Rack Format	**MUSS**		
Ethernet Ports : mind. 8x 1GbE	**MUSS**		
Davon SFP Glasfaserports: mind. 1x 1GbE	**MUSS**		
Erweiterbar auf 10GbE (mind. 2x 10GbE SFP+)	**20 Punkte**		
Display : Multi-Function LCD module	**20 Punkte**		
redundante Stromversorgung möglich	**MUSS**		
Produktzertifizierungen (Safety, EMC) : CB, CE, FCC Class A, CTick, IC, VCCI, RCM, UL, CCC	**MUSS**		
Firewall Durchsatz: mind. 25.000 Mbit/s	**MUSS**		
IPS Durchsatz: mind. 5.000 Mbit/s	**MUSS**		
SSL/TLS Inspection Durchsatz: mind. 1.000 Mbit/s	**MUSS**		
Gleichzeitige Verbindungen: mind. 5.000.000	**MUSS**		
Neue Verbindungen / Sek: mind. 100.000	**MUSS**		
Maximum lizenzierte Benutzer: mind. 400	**MUSS**		

Angebotene Lösung:

Hersteller der Hardware:	
Modellbezeichnung:	
Hersteller der Software:	
Bezeichnung der Software:	
HW oder SW Erweiterungen:	

Initiale Anschaffungskosten Hardware:		EUR
Initiale Anschaffungskosten Software		EUR
Kosten für 60 Monate Wartung der Hardware		EUR
Kosten für 60 Monate Wartung der Software:		EUR
Sonstige Kosten (Angabe unter Benennung)		EUR

Leistungsklasse 3 (Schulen bis max. 650 Clients [Lehrer + Schüler])

Hardware Anforderungen und Performance

Angeforderte Funktionalität	**Wichtigkeit (MUSS oder 0-20 Punkte)**	**Erfüllt? Angabe mit X /O/–**	**Bemerkung**
Auslegung im 19“ Rack Format	**MUSS**		
Ethernet Ports : mind. 8x 1GbE	**MUSS**		
Davon SFP Glasfaserports: mind. 1x 1GbE	**MUSS**		
Erweiterbar auf 10GbE (mind. 2x 10GbE SFP+)	**MUSS**		
Display : Multi-Function LCD module	**20 Punkte**		
redundante Stromversorgung möglich	**MUSS**		
Produktzertifizierungen (Safety, EMC) : CB, CE, FCC Class A, CTick, IC, VCCI, RCM, UL, CCC	**MUSS**		
Firewall Durchsatz: mind. 35.000 Mbit/s	**MUSS**		
IPS Durchsatz: mind. 6.500 Mbit/s	**MUSS**		
SSL/TLS Inspection Durchsatz: mind. 1.000 Mbit/s	**MUSS**		
Gleichzeitige Verbindungen: mind. 6.000.000	**MUSS**		
Neue Verbindungen / Sek: mind. 120.000	**MUSS**		
Maximum lizenzierte Benutzer: mind. 1000	**MUSS**		

Angebotene Lösung:

Hersteller der Hardware:	
Modellbezeichnung:	
Hersteller der Software:	
Bezeichnung der Software:	
HW oder SW Erweiterungen:	

Initiale Anschaffungskosten Hardware:		EUR
Initiale Anschaffungskosten Software		EUR
Kosten für 60 Monate Wartung der Hardware		EUR
Kosten für 60 Monate Wartung der Software:		EUR
Sonstige Kosten (Angabe unter Benennung)		EUR

Leistungsklasse 4 (Schulen bis max. 1500 Clients [Lehrer + Schüler])

Hardware Anforderungen und Performance

Angeforderte Funktionalität	**Wichtigkeit (MUSS oder 0-20 Punkte)**	**Erfüllt? Angabe mit X /O/–**	**Bemerkung**
Auslegung im 19“ Rack Format	**MUSS**		
1GbE Ethernet Ports : mind. 10x 1GbE	**MUSS**		
Davon SFP Glasfaserports: mind. 2x 1GbE	**MUSS**		
10GbE Port: mind. 2x 10GbE SFP+	**MUSS**		
Erweiterbar um mind. 2x 10GbE SFP+ Ports	**MUSS**		
Display : Multi-Function LCD module	**MUSS**		
redundante Stromversorgung möglich	**MUSS**		
Produktzertifizierungen (Safety, EMC) : CB, CE, FCC Class A, CTick, IC, VCCI, RCM, UL, CCC	**MUSS**		
Firewall Durchsatz: mind. 45.000 Mbit/s	**MUSS**		
IPS Durchsatz: mind. 10.000 Mbit/s	**MUSS**		
SSL/TLS Inspection Durchsatz: mind. 2.000 Mbit/s	**MUSS**		
Gleichzeitige Verbindungen: mind. 12.000.000	**MUSS**		
Neue Verbindungen / Sek: mind. 180.000	**MUSS**		
Maximum lizenzierte Benutzer: mind. 2500	**MUSS**		

Angebotene Lösung:

Hersteller der Hardware:	
Modellbezeichnung:	
Hersteller der Software:	
Bezeichnung der Software:	
HW oder SW Erweiterungen:	

Initiale Anschaffungskosten Hardware:		EUR
Initiale Anschaffungskosten Software		EUR
Kosten für 60 Monate Wartung der Hardware		EUR
Kosten für 60 Monate Wartung der Software:		EUR
Sonstige Kosten (Angabe unter Benennung)		EUR

Bezeichnung	Menge	Einzelpreis netto in EUR	Gesamtpreis netto in EUR
Leistungsklasse 1 **(Schulen bis max. 150 Clients [Lehrer + Schüler])**	**12 Stück**		
Leistungsklasse 2 **(Schulen bis max. 400 Clients [Lehrer + Schüler])**	**5 Stück**		
Leistungsklasse 3 **(Schulen bis max. 650 Clients [Lehrer + Schüler])**	**8 Stück**		
Leistungsklasse 4 **(Schulen bis max. 1500 Clients [Lehrer + Schüler])**	**6 Stück**		
		Zwischensumme netto:	
		Schulrabatt _____ %	
		Nettosumme:	
		Mehrwertsteuer 19%:	
		Gesamtsumme:	