

Muster-Leistungsbeschreibung

Firewall und Jugendschutzfilter für Schulen

Zweck

Dieses **Muster** dient dazu, Schulträgern bei der Beschaffung einer Firewall für pädagogisch genutzte schulische IT-Netzwerke zu unterstützen. Das vorliegende Muster enthält zentrale Anforderungen an die Firewall und den Jugendschutzfilter für Schulen. Diese und weitere Muster-Leistungsbeschreibungen in diesem Modul verstehen sich als Ergänzung und Vertiefung gegenüber den Empfehlungen des Bitkom in der Handreichung *Hardware produktneutral ausschreiben für den Schulbereich - Leitfaden für den öffentlichen IT-Einkauf*¹ (Stand: Juli 2023).

Anwendungsempfehlung

Die in dieser Muster-Leistungsbeschreibung aufgeführten Empfehlungen für Anforderungen müssen in der Vorbereitungsphase zur Beschaffung mit dem Zielbild des Schulträgers für die konkreten Leistungsanforderungen angepasst werden. Die Firewall kann Bestandteil von WLAN-Routern sein oder als externe Hardwarekomponente angeschafft werden. Die in diesem Dokument enthaltenen Empfehlungen sind für beide Varianten relevant. Zur Unterstützung und Orientierung für die Arbeit mit den Muster-Leistungsbeschreibungen empfehlen wir zudem die *Anleitung zur Nutzung der Muster-Leistungsbeschreibungen*.²

Die vorliegende Muster-Leistungsbeschreibung stellt ein beispielhaftes Musterdokument dar. Die darin enthaltenen Inhalte und Empfehlungen müssen stets vor einer Ausschreibung für den konkreten Anwendungsfall der betreffenden Organisation geprüft und angepasst werden. Die PD übernimmt keine Gewähr für die Richtigkeit der Angaben.

¹ Bitkom e.V. (2023): Hardware produktneutral ausschreiben für den Schulbereich. Leitfaden für den öffentlichen IT-Einkauf.
URL: <https://www.itk-beschaffung.de/Leitfaden/Schule>

² Schul-IT-Navigator (Website): „Anleitung zur Nutzung der Muster-Leistungsbeschreibungen“ (Modul „Ausstattung und Beschaffung“)



Schon gewusst?

Mehr Fachwissen zum Thema Schul-IT finden Sie auf unserer Webseite:

 www.schul-it-navigator.de

Haben Sie Feedback zu den Umsetzungshilfen für uns? Fehlt Ihnen noch etwas?

Ihre Rückmeldungen sind für uns wichtig, da die Umsetzungshilfen kontinuierlich überarbeitet werden. Wir freuen uns auf Ihre Rückmeldung.

 feedback@schul-it-navigator.de

Inhaltsverzeichnis

Zweck	1
Anwendungsempfehlung	1
Beschreibung Beschaffungsgegenstand	3
Muster-Leistungsbeschreibung Next-Generation-Firewall	4
Grundlagen	4
Schnittstellen	5
Sicherheit	5
Quality of Service & Support	6
Glossar	7
Autorinnen und Autoren	9

Beschreibung Beschaffungsgegenstand

Die Firewall ist ein IT-System, welches den Schutz von Netzwerken oder Endgeräten vor unbefugtem Zugriff, Datenverlust und Angriffen zum Ziel hat. Dazu analysiert sie den Datenverkehr und filtert ihn gemäß vordefinierter Regeln. Bei einer Firewall handelt es sich um eine Software, die entweder direkt auf der zu schützenden Hardware oder auf einer dedizierten Hardware installiert werden kann. Häufig befinden sich Firewalls an der Schnittstelle zwischen dem internen und dem externen Netzwerk und kontrollieren dort den ein- und ausgehenden Datenverkehr.

Firewalls besitzen in der Regel eine Reihe an Funktionen, wobei die Anzahl und der Umfang dieser individuell von den Bedürfnissen der Nutzenden abhängig ist. In der Schul-IT spielt Sicherheit eine große Rolle und bedarf somit eine umfangreiche Funktionalität der Firewall. Zum einen handelt es sich bei den personenbezogenen Daten der Lernenden um besonders sensible und schützenswerte Daten. Zum anderen bedarf es im Schulumfeld vor allem auch eines sogenannten Content-Filters um den Jugenschutz zu gewährleisten. Dieser ist darauf ausgelegt, den Zugang zu bestimmten Arten von Inhalten im Internet zu beschränken. Er überprüft hierfür Online-Ressourcen wie Websites, E-Mails oder Instant-Messages auf bestimmte Schlüsselwörter, URLs oder Kategorien, die darauf hinweisen, dass der Inhalt explizit, gewalttätig, illegal oder anderweitig unangemessen ist.

Router, die auf die Nutzung in Schulen und Unternehmen ausgelegt sind („Enterprise“ Geräte), haben in der Regel eine solche Firewall integriert. Sofern der ausgewählte Router die benötigten Firewall-Funktionalitäten bietet, ist keine separate Firewall notwendig.

Muster-Leistungsbeschreibung Next-Generation-Firewall

Grundlagen

Mindestanforderungen	
Konfiguration / Management	<ul style="list-style-type: none"> Soll via Konsole, Weboberfläche (HTTPS) oder SSH oder Telnet möglich sein Protokollierung aller Anmeldungen und Aktivitäten (bei unbeaufsichtigter Nutzung), inkl. Belegung via Netztrittsseite
Firewall	<ul style="list-style-type: none"> Stateful Packet Inspection Firewall für richtungsunabhängige Paketfilterung inkl. Statusüberwachung der Pakete Integrierter Webfiltermechanismus zur einfachen Gefahrenabwehr Bei großen Netzwerken empfiehlt sich eine Firewall mit Sandboxing Die Firewall muss über eine SSL-Inspection oder Deep Packet Inspection verfügen
Routing Durchsatz	<ul style="list-style-type: none"> Mind. 2x so hoch wie die anliegende Internetverbindung Wenn Router zur Netztrennung verwendet wird, dann mind. 1 Gbit/s
VPN	<ul style="list-style-type: none"> VPN Verbindungen via IPSec, und PPTP müssen konfigurierbar sein, mindestens fünf parallele Verbindungen müssen möglich sein (optional) Unterstützung für SSL-VPN
DNS/DHCP	<ul style="list-style-type: none"> Muss im Gateway für jedes konfigurierte Netz einzeln konfigurierbar sein
Montage	<ul style="list-style-type: none"> 19"-Gerät zum Einbau in einen Rack bzw. Tischgerät
Hochverfügbarkeit und Ausfallsicherheit	<ul style="list-style-type: none"> Die Firewall unterstützt Hochverfügbarkeitsfunktionen wie Active/Standby-Konfigurationen und Failover-Mechanismen, um sicherzustellen, dass Ihr Netzwerk jederzeit geschützt ist. Im Falle eines Hardwareausfalls oder einer Störung übernimmt eine Backup-Firewall nahtlos den Betrieb, um Unterbrechungen zu vermeiden.
Auswahlkriterien	
DNS/DHCP	<ul style="list-style-type: none"> Weitere Zusatzfunktionen wie DNS-Relay, DNS-Proxy und Dynamisches DNS sind wünschenswert
Benutzerfreundliche Verwaltung	<ul style="list-style-type: none"> Die Firewall bietet einen browserbasierten Zugriff, über den die Firewall-Konfiguration, Sicherheitsrichtlinien und Benutzerkonten verwaltet werden können. Es können Logs und Berichte über Netzwerkaktivitäten angezeigt werden, um potenzielle Bedrohungen zu identifizieren und zu überprüfen.

Schnittstellen

Mindestanforderungen	
LAN-Schnittstellen	<ul style="list-style-type: none"> Mind. 2x Gbit Ethernet Ports
WAN-Schnittstellen	<ul style="list-style-type: none"> Schnittstellen sollten als internes Modem mit PPPoE konfigurierbar sein
VLANs	<ul style="list-style-type: none"> Müssen sich auf allen Schnittstellen konfigurieren lassen VLAN nach IEEE 802.1Q, Routing zwischen VLAN's

Auswahlkriterien	
	<ul style="list-style-type: none"> Ggf. mind. 1x 10 Gbit Ethernet Port Zusätzliche Gbit Ethernet Ports mit der Möglichkeit der Netzwerktrennung, je nach Leistungsfähigkeit der Firewall Mind. 2x WAN-Port zum Anschluss eines redundanten Internetzugangs (optional) internes ADSL/ADSL2+ / VDSL/VDSL2 Modem

Sicherheit

Mindestanforderungen	
Intrusion Prevention System (IPS)	<ul style="list-style-type: none"> Schutz vor Viren, Spyware und Würmern, HTML-, Javascript-, PDF-Virenschutz usw., Überwachung gepackter Dateien. Es kann Angriffe wie Denial-of-Service (DoS)-Angriffe, Port-Scans oder bekannte Angriffsmuster erkennen und entsprechende Maßnahmen ergreifen, um sie zu blockieren.
Content Filtering	<ul style="list-style-type: none"> Zugriff auf bestimmte Websites oder Webinhalte sollte gesteuert werden können. Es können Richtlinien festgelegt werden, um den Zugriff auf soziale Medien, Glücksspiel- oder nicht schulrelevante Websites zu blockieren oder einzuschränken. Die URL-Filterung wird anhand einer dem deutschen Jugendmedienschutz entsprechenden tagesaktuellen Liste umgesetzt; die Filterung ist auf Nutzer, Gruppen oder MAC- bzw. IP-Adressen anwendbar.
Daten-Filterung	<ul style="list-style-type: none"> Überwachung von nicht autorisiertem Datenverkehr (personalisierte Daten, Zahlungsdaten etc.).
Application Control	<ul style="list-style-type: none"> Es wird eine umfangreiche Anwendungskontrolle geboten, mit der Zugriff auf bestimmte Anwendungen und Dienste im Netzwerk gesteuert werden kann. Es können Regeln festgelegt werden, um den Datenverkehr von Peer-to-Peer-Netzwerken, Instant Messaging-Diensten oder anderen nicht genehmigten Anwendungen zu blockieren oder einzuschränken.
User-Kontrolle	<ul style="list-style-type: none"> Zur Nutzerverwaltung bietet sich eine Schnittstelle zu einem zentralen Verzeichnisdienst (z. B. LDAP/Active Directory) an
Jugendschutzfilter	<ul style="list-style-type: none"> Jugendschutzfilterung muss unabhängig vom eingesetzten Endgerät und der Softwareversion / ohne Installationsaufforderung gewährleistet sein – dafür Nutzervereinbarungen mit Lernenden/ Eltern, Lehrkräften und Angestellten

Auswahlkriterien	
	<ul style="list-style-type: none"> Bandbreitenregulierung Unterstützung und Bündelung mehrerer Internetanschlüsse



Hinweis zum Jugendschutzfilter

Innerhalb des Schulnetzes kann ein Jugendschutzfilter durch verschiedene Methoden implementiert werden. Wenn Geräte des Schulträgers auch außerhalb des Schulnetzwerks genutzt werden sollen, muss in den Geräteeinstellungen der Jugendschutzfilter z. B. über DNS realisiert werden.

Auf Konformität der Hardware mit dem europäischen Datenschutz ist zu achten. Ist der Hersteller z. B. zum Einbau von Backdoors verpflichtet?

Quality of Service & Support

Mindestanforderungen

- Gewährleistung mind. 60 Monate
- Gerät muss für die Dauer der Nutzung Herstellersupport (Softwarepflege) erhalten
- Hersteller verfügt über deutschsprachigen Service

Auswahlkriterien

- Ein Updateabonnement der Signaturen kann notwendig sein

Glossar

ADSL/ADSL2+	ADSL (Asymmetric Digital Subscriber Line) ist eine Breitband-Internet-Verbindungstechnologie, die über herkömmliche Telefonleitungen hohe Datenübertragungsraten ermöglicht, wobei die Download-Geschwindigkeit höher ist als die Upload-Geschwindigkeit. ADSL2+ ist eine Weiterentwicklung von ADSL und bietet verbesserte Übertragungsgeschwindigkeiten und Stabilität, indem es höhere Frequenzbereiche nutzt, um noch schnellere Internetverbindungen für Heimnutzer und kleine Unternehmen bereitzustellen.
Content Filtering	Content-Filtering bezieht sich auf den Prozess der automatischen Überwachung und Steuerung von digitalen Inhalten, um unerwünschte oder schädliche Elemente zu identifizieren und zu blockieren, basierend auf vordefinierten Kriterien wie Schlüsselwörtern, Kategorien oder Regeln, um eine sicherere und zielgerichtete Online-Erfahrung zu gewährleisten. Dies wird oft in Netzwerken, sozialen Medien und Webanwendungen eingesetzt, um den Zugriff auf fragwürdige oder ungeeignete Inhalte einzuschränken.
DNS (DNS-Relay, DNS-Proxy und Dynamisches DNS)	Das Domain Name System (DNS) ist ein Internet-Dienst, der menschenfreundliche Domainnamen in numerische IP-Adressen umwandelt, um die Kommunikation zwischen Geräten im Internet zu ermöglichen. Es fungiert als eine Art "Telefonbuch" des Internets, das die Zuordnung von leicht merkbaren Namen zu den tatsächlichen Adressen der Server erleichtert. Ein DNS-Relay leitet DNS-Anfragen von lokalen Geräten an externe DNS-Server weiter, um die Auflösung von Domainnamen zu ermöglichen, ohne dass jede Anfrage direkt an öffentliche DNS-Server gesendet werden muss. Ein DNS-Proxy fungiert als Vermittler zwischen lokalen Geräten und externen DNS-Servern, um Anfragen zu puffern, zu filtern oder zu beschleunigen, was die Effizienz und Sicherheit der DNS-Kommunikation verbessert. Dynamisches DNS ermöglicht die automatische Aktualisierung von DNS-Einträgen für sich ändernde IP-Adressen von Geräten, die keine statischen IP-Adressen haben, und erleichtert so den Zugriff auf diese Geräte über konstante Domainnamen.
Denial of Service (DoS)-Angriffe	Eine Denial of Service (DoS) Attacke ist eine bösartige Handlung, bei der ein Angreifer versucht, eine Online-Dienstleistung oder Website durch Überlastung mit einem hohen Volumen an Anfragen lahmzulegen, sodass legitime Nutzende keinen Zugriff mehr haben. Ziel ist es, die Ressourcen des Zielsystems zu erschöpfen und einen Zusammenbruch der Dienstleistung zu verursachen.
Failover-Mechanismen	Failover-Mechanismen sind Maßnahmen, die in Computersystemen oder Netzwerken implementiert werden, um automatisch den Betrieb auf ein Backup-System umzuschalten, falls das primäre System ausfällt. Dies gewährleistet eine kontinuierliche Verfügbarkeit und reduziert Ausfallzeiten.
IEEE 802.1Q	IEEE 802.1Q ist ein Standard für das Tagging von Ethernet-Frames in Netzwerken, der VLAN (Virtual Local Area Network) Implementierungen ermöglicht. Dabei werden zusätzliche Informationen in den Ethernet-Frames hinzugefügt, um den Datenverkehr logisch zu segmentieren und in separate virtuelle Netzwerke aufzuteilen.
Intrusion Prevention System (IPS)	Ein Intrusion Prevention System ist eine Sicherheitslösung für Netzwerke, die darauf abzielt, unbefugte Zugriffsversuche, Angriffe und schädliche Aktivitäten zu erkennen und zu blockieren, bevor sie das Netzwerk erreichen. Es überwacht den Datenverkehr in Echtzeit, analysiert ihn auf verdächtige Muster und ergreift proaktiv Maßnahmen, um potenzielle Bedrohungen zu verhindern.
Paketfilterung	Paketfilterung bezieht sich auf die Praxis, den Datenverkehr in einem Computernetzwerk anhand vordefinierter Regeln zu überprüfen und zu steuern, um zu entscheiden, welche Datenpakete zugelassen oder blockiert werden sollen. Dabei werden Paketattribute wie Quell- und Zieladressen, Ports und Protokolle analysiert, um die Sicherheit und Effizienz der Netzwerkkommunikation zu gewährleisten.
Port-Scans	Port-Scans sind Netzwerktechniken, bei denen Software automatisch verschiedene Netzwerkports auf einem Zielcomputer untersucht, um festzustellen, welche Dienste oder Anwendungen auf diesen Ports lauschen. Dies ermöglicht es Angreifenden, potenzielle Schwachstellen zu identifizieren und Sicherheitslücken auszunutzen.

PPPoE	PPP over Ethernet (PPPoE) ist ein Netzwerkprotokoll, das Point to Point Protocol (PPP) zur Einrichtung einer Verbindung zwischen den Nutzenden und einem Internetdiensteanbieter über eine Ethernet-Verbindung verwendet. Es ermöglicht die Authentifizierung und den Datenverkehr zwischen dem Benutzermodem/Router und dem ISP-Server über Ethernetbasierte Netzwerke.
Sandboxing	Sandboxing bezieht sich auf eine Sicherheitspraxis, bei der eine Anwendung oder ein Prozess in einer isolierten Umgebung ausgeführt wird, um potenzielle Schäden oder Sicherheitsverletzungen auf das umgebende System oder andere Anwendungen zu begrenzen. Diese Methode zielt darauf ab, unerwünschte Interaktionen zu verhindern und die Auswirkungen potenziell schädlicher Aktivitäten einzudämmen.
SSL-Inspection (Deep Packet Inspection)	SSL-Inspection, auch bekannt als Deep Packet Inspection, bezieht sich auf die Praxis, verschlüsselten Netzwerkverkehr zu überwachen, indem die Transportverschlüsselung von Datenpaketen entschlüsselt wird, um den Inhalt für Sicherheits- oder Analyse Zwecke zu überprüfen. Dies wird oft von Netzwerk-Sicherheitsgeräten verwendet, um Bedrohungen zu identifizieren, kann jedoch auch Bedenken hinsichtlich der Privatsphäre und Sicherheit aufwerfen.
VLAN	Ein VLAN (Virtual Local Area Network) ist ein logisches Netzwerk, das innerhalb eines physischen Netzwerks erstellt wird, um Geräte zu gruppieren und den Datenverkehr zu isolieren. Es ermöglicht die Segmentierung und Verwaltung des Netzwerkverkehrs, als ob es sich um separate physische Netzwerke handelt würde.
VPN	Ein VPN (Virtual Private Network) ist eine Technologie, die eine sichere und verschlüsselte Verbindung über ein öffentliches Netzwerk herstellt, um die Online-Privatsphäre zu wahren und die Datenübertragung zwischen Ihrem Gerät und dem Zielsever abzusichern. Es ermöglicht Benutzern, ihre IP-Adresse zu verschleiern und ihre Online-Aktivitäten vor neugierigen Blicken zu schützen.
VDSL/VDSL2	VDSL (Very High Bitrate Digital Subscriber Line) bzw. VDSL2 ist eine fortschrittliche Breitband-Telekommunikationstechnologie, die Hochgeschwindigkeits-Internetzugänge über herkömmliche Kupfer-Telefonleitungen ermöglicht, indem sie höhere Frequenzen nutzt als herkömmliche ADSL-Verbindungen, was zu deutlich schnelleren Datenübertragungsraten führt.
WAN	Ein WAN (Wide Area Network) ist ein Netzwerk, das sich über große geografische Entfernungen erstreckt und verschiedene lokale Netzwerke miteinander verbindet, um die Kommunikation und den Datenaustausch zwischen entfernten Standorten zu ermöglichen. Es nutzt typischerweise öffentliche oder private Kommunikationsinfrastrukturen wie Internetleitungen, Satellitenverbindungen oder dedizierte Leitungen.

Autorinnen und Autoren

Jennifer Droese (PD – Berater der öffentlichen Hand GmbH)

Dr. Michael Krause (PD – Berater der öffentlichen Hand GmbH)

Mathias Ragnow (PD – Berater der öffentlichen Hand GmbH)

PD – Berater der öffentlichen Hand GmbH Friedrichstr. 149, 10117 Berlin | www.pd-g.de | schuedigital@pd-g.de



Schon gewusst?

Mehr Fachwissen zum Thema Schul-IT
finden Sie auf unserer Webseite:

 www.schul-it-navigator.de

Haben Sie Feedback zu den Umsetzungshilfen für uns? Fehlt Ihnen noch etwas?

Ihre Rückmeldungen sind für uns wichtig, da die Umsetzungshilfen kontinuierlich überarbeitet werden. Wir freuen uns auf Ihre Rückmeldung.

 feedback@schul-it-navigator.de