LEITFADEN SCHULNETZWERK

MIT SECUREPOINT NEXTGEN UTM-FIREWALL

Im Zuge der Digitalisierung sind die Anforderungen an ein performantes und sicheres Netzwerk auch bei nicht-kommerziellen Organisationen stark gestiegen. Aus den Verwaltungsrichtlinien zum „Digitalpakt Schule" geht hervor, dass zu den Grundlagen neben einem flächendeckenden WLAN auch die Trennung der Netzwerke und weitere Schutzmechanismen gehören. An Schulen mit Minderjährigen ist dazu bspw. auch ein zum Jugendschutz geeigneter Content Filter unerlässlich.

Entsprechend können bzw. konnten UTM-Firewalls (UTM = Unified Thread Management), inklusive der Dienste- und Service-Lizenz (Subscription/Garantieerweiterung) bis zu einer Laufzeit von 5 Jahren vollumfänglich mit Fördergeldern abgedeckt werden.

Einige Bundesländer – z. B. Thüringen – geben konkrete Ausstattungsempfehlungen und empfehlen, als zentrale Schutzinstanz eine UTM-Firewall einzusetzen. Diese bietet die Möglichkeit, Netzwerke zu trennen und Zugänge zu sichern, sowie einen Content Filter und weitere Schutzmechanismen.

Auch die steigenden Bedrohungen durch Cyber-Kriminalität, machen eine gute Firewall unerlässlich. So schreibt das BSI in seinem aktuellen Lagebericht*: Cyberkriminelle gingen im Berichtszeitraum zunehmend den Weg des geringsten Widerstands und wählten verstärkt solche Opfer aus, die ihnen leicht angreifbar erschienen. Nicht mehr die Maximierung des potenziellen Lösegelds stand im Vordergrund, sondern das rationale Kosten-Nutzen-Kalkül. So wurden vermehrt kleine und mittlere Unternehmen sowie Behörden der Landes- und Kommunalverwaltungen, wissenschaftliche Einrichtungen sowie Schulen und Hochschulen Opfer von Ransomware-Angriffen. Cyberresilienz ist daher das Gebot der Stunde.

Dieser Leitfaden zeigt, wie Schulen Ihre IT-Sicherheit und Cyberresilienz mit den verschiedenen Funktionen einer UTM-Firewall erhöhen können

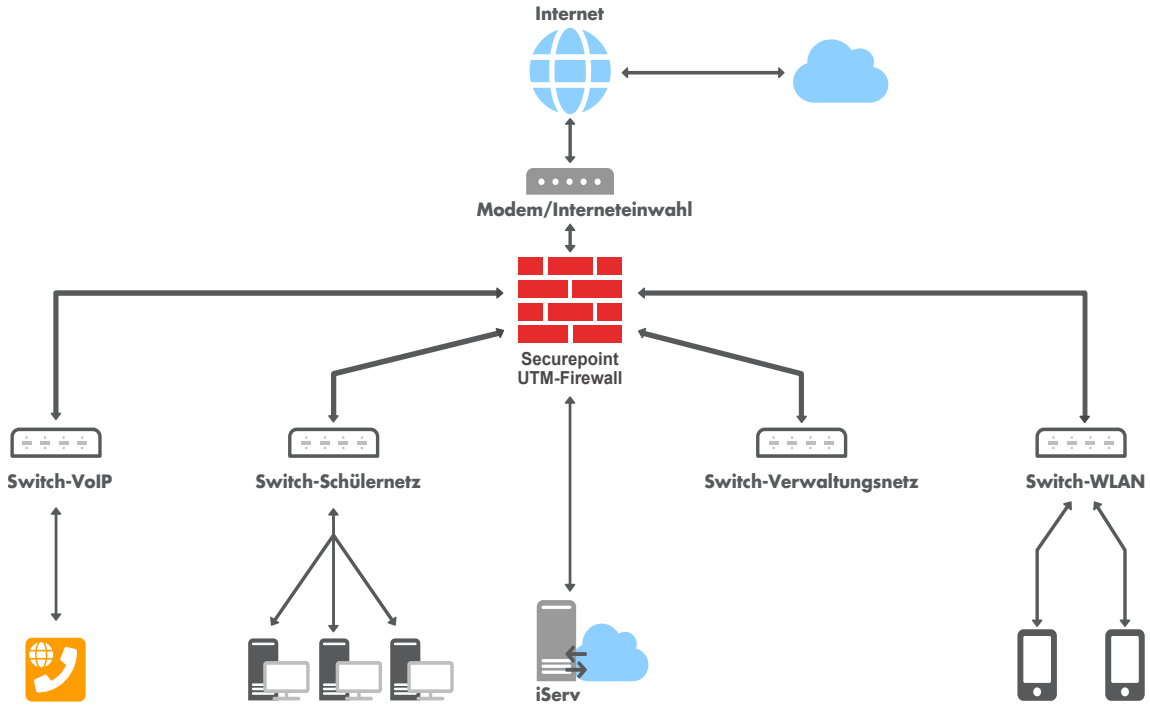
*Bundesamt für Sicherheit in der Informationstechnik (BSI) – Die Lage der IT-Sicherheit in Deutschland 2023 - Teil-A Bedrohungslage /S.11 Absatz „Cyberresilienz

Netzwerksegmentierung

Ziel der Segmentierung bzw. der Trennung verschiedener Teile eines Netzwerkes ist es, das allgemeine Sicherheitslevel anzuheben, Angriffsfläche zu verringern und die Ausbreitung von schadhaften Vorgängen zu verhindern oder deutlich zu verlangsamen.

Dabei wird ein Netzwerk in kleinere, separate Subnetzwerke unterteilt, die voneinander abgeschottet sind und für die jeweils eigene Sicherheitskontrollen und Services bereitgestellt werden können. Vorteile sind u.a.:

- Isolation von extern erreichbaren Systemen
- Möglichkeit, der Priorisierung bestimmte Netzwerksegmente
- Einfachere Diagnosemöglichkeiten im Fehlerfall
- Umsetzung von „Zero Trust" – Geräte und Nutzer, erhalten nur die Zugriffsrechte, die benötigt werden.



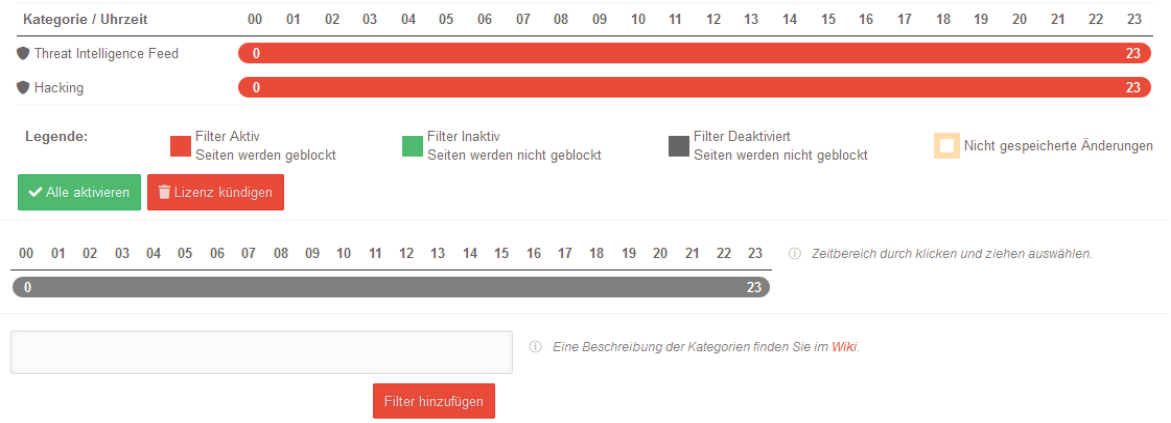
Content-Filter

Content-Filter übernehmen im Schulnetzwerk die Aufgabe unerwünschte Inhalte zu blocken, bevor diese zu den Schülerinnen und Schülern sowie Lehrkräften gelangen können. Diese Gruppe und die von ihnen eingesetzten Geräte können so vor gefährlichen und illegalen Inhalten geschützt werden.

Vorteile des Securepoint Content-Filter:

- Ausgezeichnet und kuratiert von echten Menschen (Redaktionsteam)
- Einfache Administration durch mehr als 40 vorgegebene Kategorien, die ständig vom Redaktionsteam gepflegt werden
- Unterschiedliche Regelsätze sind für einzelne Netze und User-Gruppen möglich
- Die Regelsätze können auch mit zeitlichen Vorgaben versehen werden

Neben dem Zugangsschutz zu ungewünschten Inhalten und Web-Seiten, die Malware verbreiten, können mit dem Content-Filter auch andere unerwünschte Verbindungen ins Internet verhindert werden. So kann beispielsweise unterbunden werden, dass sich Schüler im Schulnetz ein iOS-(oder Android-)Update für ihre Smartphones herunterladen oder dass per VPN versucht wird, den Content Filter und andere Reglementierungen der Firewall zu umgehen.



Webfilter Kategorien

Bezeichnung	Beschreibung
Porno und Erotik	Pornographische oder vorwiegend sexuelle Inhalte
Waffen	Waffenshops, Waffeninfos, Militaria, militärische Inhalte, Sportschützen, Jagd
Abstoßend	Extrem blutig, Anleitung oder Aufruf zu Mord, Selbstmord und Gewalt, Ekelerregend
BPJM Kinder-/Jugendschutz	Inhalt nicht geeignet für Kinder und Jugendliche nach deutscher BPjM
Spiele	Seiten zum Thema Spiele, Spiele zum Download, Online Spiele, Gewinnspiele, Lotto, Glücksspiele
Unseriös Geld verdienen	Geld schnell verdienen, reich werden, Beteiligungen, Kettenbriefe
Hacking	Ratgeber zum Thema Hacking, Warez, Malware bauen, Systeme überlisten, Abofallen
Danger	→ Threat Intelligence Feed
Threat Intelligence Feed	Aktuell als schädlich eingestufte URLs (Phishing, Malware, Botnetze, Crimeware usw.)
Proxy	Anonymisierungsproxies und Listen dieser Rechner
Soziale Netzwerke	Soziale Netzwerke
Dating	Dating, Kennenlernen, Partnerschaftssuche, Freunde finden
Auktionen	Internet Auktionen, Kleinanzeigen, Annoncenmarkt
Kurz-URL-Dienst	URL Kürzungs Dienste
Werbe Dienste	Werbe Dienste
Tracking strict	Sperrt welche private Informationen durch das Beobachten von Aktivitäten auf Webseiten sammeln

GeoIP-Funktion

Mit der GeoIP werden Internetadressen von Organisationen und Institutionen einem bestimmten Land zugewiesen. Die Securepoint Firewall stellt dazu eine Datenbank bereit, die ständig aktualisiert wird. Dadurch können systemweit oder auf Basis einer Portfilterregel, IP-Netzwerke von bestimmten Ländern blockiert oder

Unterstützung Google SafeSearch

Neben dem Content Filter mit den verschiedenen Kategorien bietet der Webfilter (Proxy) der Firewall weitere vorgegebene Regelsätze an. Von Schulen sehr oft gewünscht ist die „Safe Search Funktion“ von Google. Mit dem hinterlegten Regelsatz können Sie das für die Google-Suche geschaffene Filtersystem nutzen. Mit der Option "strict" werden sexuell eindeutige Videos und Bilder sowie Ergebnisse, die mit eindeutigen Inhalten verlinkt sein könnten, aus den Google-Suchergebnisseiten gefiltert. Bei der moderaten Filterung werden sexuell eindeutige Videos und Bilder aus den Google-Suchergebnisseiten ausgeschlossen; Ergebnisse, die mit eindeutigen Inhalten verlinkt sein könnten, werden jedoch nicht gefiltert.

IDS/IPS

Die kontinuierliche Erkennung und Protokollierung sowie das Stoppen und Melden von potenziell gefährlichen Vorfällen an den Sicherheitsadministrator, werden vom Intrusion Detection System (IDS) sowie dem Intrusion Prevention System (IPS) übernommen.

- Schutz vor DoS-/DDoS-Angriffen
- DNS-Rebinding Schutz
- Portscan Protection
- Invalid Network Packet Protection
- IP-Sperrungen bei wiederholter fehlerhafter Anmeldung an Diensten der UTM-Firewall (FailToBan)
- Threat Intelligence Filter (cloudbasierter Filter zur Sperrung / Protokollierung von potenziell gefährlichen Verbindungen)

Quality of Service (QoS)

Als QoS wird die Güte eines Kommunikationsdienstes bezeichnet, also in welchem Maße ein jeweiliger Dienst den Anforderungen der Nutzer entspricht. Zu diesen Anforderungen zählen u.a.:

- Schneller und zuverlässiger Aufbau von Verbindungen
- Stabilität bestehender Verbindungen
- Hohe Übertragungsqualität
- Fehlerfreie und störungsfreie Übertragung
- Kurze Wartezeiten während der Kommunikation

Um eine hohe QoS zu gewährleisten, lassen sich folgende Vorkehrungen treffen:

- Limitierung des Traffics zu Stoßzeiten
- Priorisierung des Traffics anhand der ToS (Type of Service) Information in IP-Paketen

Multicast-Übertragungen / IGMP- Proxy

Das Internet Group Management Protocol (IGMP) ermöglicht die Multicasting-Funktion. Ein Multicast könnte bspw. ein Videostream sein, der an mehrere Clients im Netzwerk gleichzeitig verteilt werden soll. Mit dem IGMP-Proxy ermöglicht die Firewall die Verteilung von Multicast-Streams über mehrere Netzwerksegmente hinweg.

mDNS-Repeater

Der Multicast-DNS-Repeater hilft mDNS-Anfragen zwischen verschiedenen Subnetzen/VLANs weiterzuleiten. Multicast-fähige Geräte, können hiermit über Netzwerksegmente auffindbar gemacht werden. Bspw. könnte ein Schüler damit eine auszudruckende Datei von seinem Smartphone an einen Drucker im Sekretariat senden.

Multi-WAN

Es können mehrere Internetanschlüsse per Multipathrouting zu einem Internetanschluss zusammengefasst werden. Die Firewall übernimmt hierbei die Lastverteilung anhand aktiver Verbindungen. Per Rule-Routing kann bestimmter Traffic auf ein bestimmtes WAN-Interface geroutet werden.

Fallback

Um Ausfallsicherheit durch eine Fallback- bzw. Rückfalllösung zu gewährleisten und möglichen Internetunterbrechungen vorzubeugen, können WAN-Schnittstellen (z.B. ein LTE-Modem) als Fallback für andere WAN-Schnittstellen konfiguriert werden. Wenn ein Internetzugang ausfällt, übernimmt der nächste seine Funktion.

.

Bond-Konfiguration (LACP)

Die Bond-Konfiguration ermöglicht es mehrere Netzwerkschnittstellen zu einer virtuellen Einheit zusammenzufassen. Es wird dazu das Link Aggregation Control Protocol (LACP) genutzt. So wird ermöglicht, dass das System mehrere Interfaces als eines anspricht. Es gibt zwei Konfigurationsmöglichkeiten des Bondings:

- Ausfallsicherung – fällt das laufende Interface aus, springt eines der gebondeten ein.
- Lastverteilung – Der Datenverkehr/Traffic wird auf alle Schnittstellen verteilt.

Verzeichnisdienste – AD / LDAP / AAD (Entra ID)

Die AD/LDAP-Anbindung ermöglicht es, bestehende Verzeichnisdienste wie das Microsoft Active Directory® oder andere auf dem LDAProtocol basierende Systeme wie iServ für die Authentifizierung, Verwaltung von Gruppen und Speichern von Attributen zu nutzen. Zentral verwaltete Benutzer aus dem Verzeichnis können so einfach für die Authentifizierung oder Nutzung von Diensten auf der UTM verwendet werden. Dies erleichtert die Administration komplexer Schulnetzwerke und vereinheitlicht die Benutzer-Verwaltung.

Securepoint Firewalls unterstützen neben den lokalen Verzeichnisdiensten auch die Anbindung an das Azure AD (Entra ID).

Captive Portal

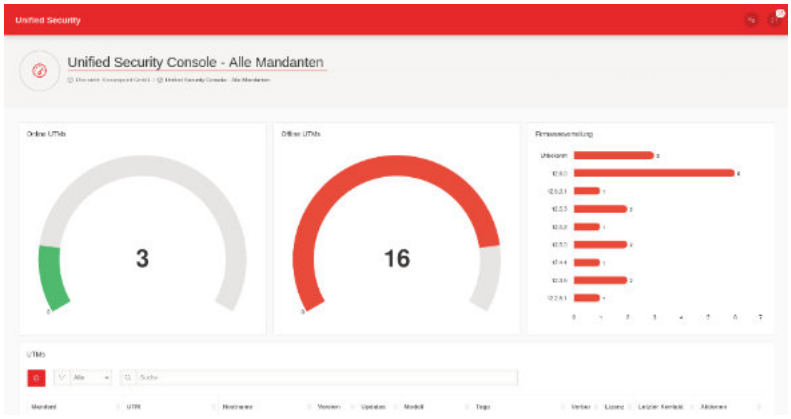
Das Captive Portal leitet einen HTTP-Client in einem Netzwerk auf eine spezielle Webseite (d.h. Landingpage) um, bevor dieser sich normal in das Internet und lokale Netzwerke verbinden kann. So muss die Annahme der Nutzungsbedingung erfolgen und es kann eine zusätzliche Authentifizierung konfiguriert werden. Mit dieser Funktion kann bspw. in kleinen Schulen ein Gast-WLAN-Netz erstellt werden. In größeren Schulen und WLAN-Netzwerken übernimmt diese Funktion üblicherweise ein WLAN-Controller. Sollen verschiedene WLAN-Netze (SSIDs) mit unterschiedlichen Berechtigungen bereitgestellt werden, können diese z. B. per VLAN separiert von der Firewall gemanaged werden.

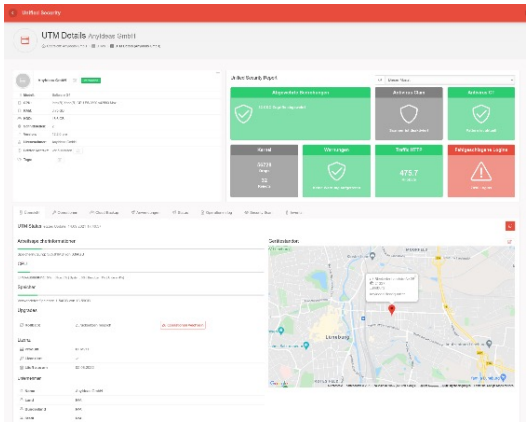
Virtual Private Network (VPN)

Mit VPN wird eine Netzwerkverbindung bezeichnet, die ein privates Netzwerk über ein öffentliches Netzwerk hinweg erweitert und dabei von Unbeteiligten nicht einsehbar ist. So können z.B. Lehrkräfte sicher und über das Internet auf interne Systeme (z.B. iServ-Administration) zugreifen. Securepoint Firewalls ermöglichen Verbindungen zwischen VPN-Gateways (Site-to-Site) und den VPN-Zugriff von Clients auf ein lokales Netzwerk über die Protokolle SSL-VPN, IPSec und Wireguard. Die Anzahl der VPN-Verbindungen ist in der Software nicht limitiert und für die gängigen Betriebssysteme sind kostenlose VPN-Clients verfügbar.

Zentrales Management / Unified Security Console

Die Unified Security Console (USC) ermöglicht den Administratoren das zentrale Monitoring und Management von mehreren Firewalls, unabhängig von deren Standort. In einem übersichtlichen Dashboard wird der Status aller Firewalls dargestellt. Mit der USC können z. B. die Updates für die Firewalls automatisiert und verteilt werden. Bei Bedarf kann sich der Admin zudem einfach per Mausklick auf eine einzelne Firewall aufschalten und so bspw. in die Konfiguration eingreifen. Das kann mit einem beliebigen Endgerät geschehen. Benötigt werden nur eine Internetverbindung und ein Web-Browser. Diese Verbindung ist durch mehrere Authentifizierung-Ebenen und Verschlüsselung gesichert.





Securepoint Single License Modell und EDU-Lizenz

Die Unified Security Console, VPN sowie alle UTM-Funktionen sind ohne Aufpreis bis zur maximalen User-Zahl in einer einzigen Lizenz (UTM-Subscription) enthalten. Für Schulen und Bildungseinrichtungen wird die Lizenzen mit einem EDU-Rabatt angeboten. Damit erhalten Schulen eine Vergünstigung, die sich nach der Größe der Firewall staffelt, von bis zu 50 % gegenüber dem Normalpreis einer Lizenz.

	Kleine Schule "S"	Mittlere Schule "M"	Große Schule "L"
Schultypen	Z. B. Grundschule, Privat-schule, Vorschule (große KiTas)	Z. B. Hauptschule, Realschule, Gymnasium	Z. B. Gesamtschule, Gymnasium, Berufs(fach)schule
Anzahl Schüler/ Schulklassen	Ca. 50-200/2-8	Ca. 200-900/9-36	900+/36+
Anzahl Lehrkräfte	3-20	20-60	60+
Bandbreiten-Bedarf	50 – 250 MBit/s	250 – 1.000 MBit/s	>1.000 MBit/s
Produktempfehlung	RC100/RC200/RC300S	RC350R/RC400R	RC1000R
UTM-Subscription – Infinity Lizenz EDU	**MVL 1/3/5 Jahre**	**MVL 1/3/5 Jahre**	**MVL 1/3/5 Jahre**

SECUREPOINT

Securepoint GmbH • Bleckeder Landstraße 28 • D-21337 Lüneburg • Tel.: 04131 2401-0

www.securepoint.de • info@securepoint.de