

•• SECUREPOINT





UTM OPERATOR «NextGen UTM-Firewall»

Daniel Meyer
Meyer IT-Service

Folgende Inhalte wurden erfolgreich vermittelt:

- Grundlagen Erstinstallation und Bedienung einer Securepoint NextGen UTM-Firewall
- Grundlagen Netzwerktechnik
- Grundlagen Protokollsuite TCP/IP
- Adressierung, Routing und Zusammenhänge im Netzwerk

 Geschult, geprüft und zertifiziert.	Zertifikat-ID: 7XQP37Ca4u 
https://akademie.securepoint.de	

07.04.2025



Datum und Unterschrift

Dieses Zertifikat ist ein (1) Jahr gültig



•O• SECUREPOINT

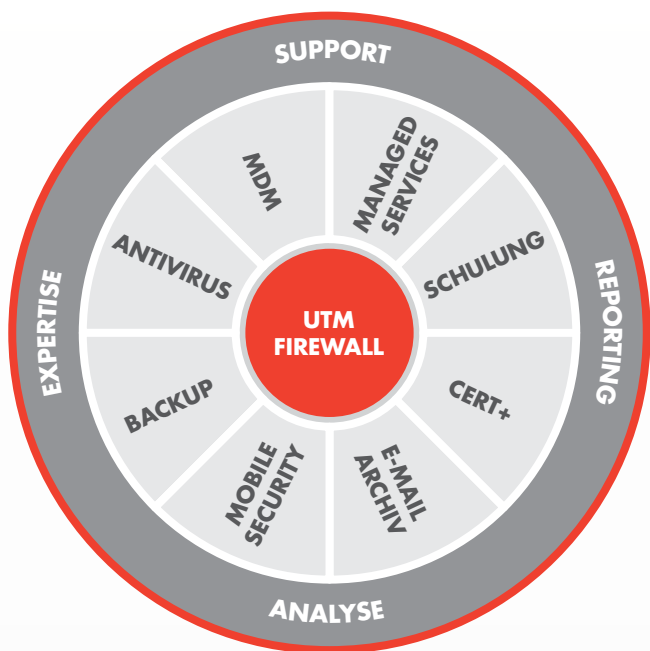
SECUREPOINT UTM-FIREWALLS



PASSGENAUE IT-SECURITY FÜR UNTERNEHMEN JEDER GRÖSSE

Securepoint UTM-Firewalls sichern Netzwerke von Ein-Personen-Unternehmen und mittelständischen Firmen, von Behörden oder Healthcare-Einrichtungen.





SECUREPOINT UNIFIED SECURITY

Unified Security bedeutet Netzwerksicherheit auf allen Ebenen. Wie beim Auto, wo Nackenstütze, Gurt und Knautschzone gemeinsam auf höchstmögliche Sicherheit hinwirken, verbinden sich individuell wirksame IT-Schutzmaßnahmen zu einer starken Sicherheits-Infrastruktur.

IT-Sicherheit ganzheitlich betrachten mit Unified Security von Securepoint.

Netzwerksicherheit, die Spaß macht

Sichern Sie LAN- und WLAN-Netzwerke mit einer NextGen UTM-Firewall von Securepoint.

Einfach

- Zentrale Verwaltung aus der Cloud
- Wizard-gestützte Inbetriebnahme
- Kostenloser Support aus Deutschland
- Intuitive Anwenderoberflächen
- Umfangreiche Schulungsangebote
- Individuell anpassbare Lizenzmodelle

Zuverlässiger Ransomware-Schutz

Die UTM-Firewall wird durch Securepoints Cyber Defence Cloud automatisch und in Echtzeit mit Sicherheitsupdates versorgt.

Vielfach geschützt

Der Einsatz einer Firewall schützt Sie vor Haftungsansprüchen und ermöglicht Ihnen die sichere Nutzung internetbasierter Anwendungen.

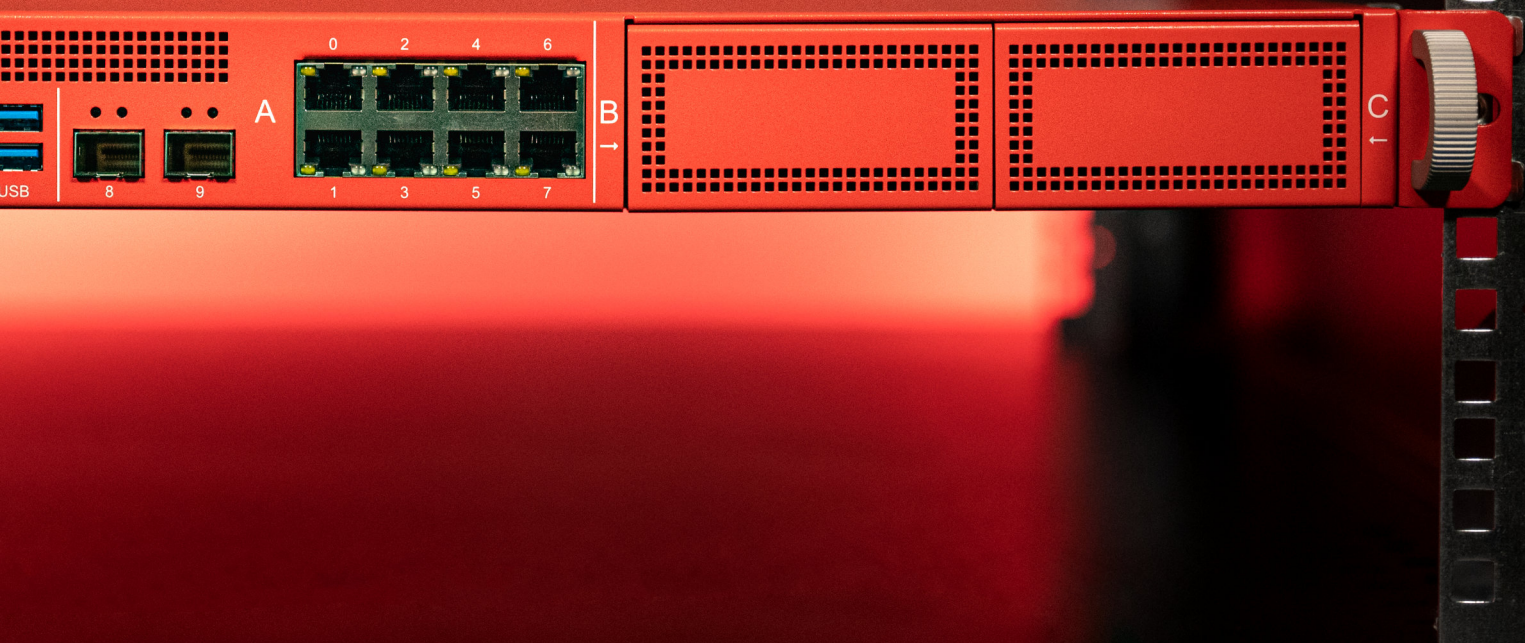
Nur vertrauenswürdige Daten für Ihr Netzwerk

Verschlüsselung und Identifikation sorgen für sichere Verbindungen nach Innen und Außen.

Exzellente Performance

Die hochleistungsfähige, zukunftssichere Hardware und unsere in Deutschland entwickelte





Schnell

- Extrem schlanke 64-Bit Architektur
- Hochleistungsfähige Hardware
- Sicherheitsupdates in Echtzeit
- Automatisches Bandbreitenmanagement
- Glasfaseranschlüsse (optional)
- Vorabaustausch im Bedarfsfall

Sicher

- Zuverlässiger Schutz vor Ransomware
- VPN für sichere Verbindungen
- Keine versteckten Hintertüren
- Eigene Softwareentwicklung in Deutschland
- Cloud-Dienste in Deutschland gehostet
- Datenanalysen durch Securepoint-Experten

Sicherheitssoftware wurden für ihre Leistung mehrfach ausgezeichnet.

Lizensierung

Eine Lizenz, einmal abgeschlossen, sorgt für umfassenden Schutz: Ihre Infinity Licence. Dank der automatischen Lizenz-Verlängerung bleibt das Schutzniveau selbsttätig bis zum eindeutig gewünschten Ende erhalten. Lizenznehmende können sich über das Online-Portal automatisch per E-Mail über aktuelle Vertragslaufzeiten informieren lassen und Lizenzen bei Bedarf direkt anpassen.

Passend zu Ihren Bedürfnissen stehen Ihnen verschiedene Hardware-Modelle zum Kauf, zur Miete, virtuell und als Managed Service zur Verfügung. Vom kleinen Black Dwarf bis hin zur großen RC1000R werden die Menschen in großen und kleinen Netzwerken zuverlässig vor Viren, Trojanern und Spam geschützt.



Schutz für Netzwerke, Nutzergruppen oder individuelle Geräte

Sicherheit wächst, wenn Angriffsfläche verringert wird. Dieser Gedanke prägt Securepoints „Unified Security“-Konzept, bei dem einander ergänzende Maßnahmen von Secure DNS bis Antivirus Schicht um Schicht für mehr Sicherheit im Netzwerk sorgen. Das Herzstück sicherer Netzwerke ist immer eine UTM-Firewall (UTM = Unified Threat Management).

Sicher online surfen und arbeiten

Der Contentfilter ermöglicht es Ihnen, einzelne Webseiten oder Kategorien von Inhalten für bestimmte Zeiten und bestimmte Nutzer zu sperren. So kann beispielsweise der Jugendschutz sichergestellt werden oder die Social-Media-Nutzung auf bestimmte Zeiten beschränkt werden.

Sicher dank Threat-Intelligent-Filter

Hier werden für Sie gefährliche IP-Adressen geblockt und wichtige Datenpakete priorisiert. In der Praxis bedeutet das, dass ins Netzwerk gelangte Malware handlungsunfähig wird, während für Videokonferenzen genügend Bandbreite zur Verfügung steht.

Cloud-gestützter Echtzeit-Schutz

Die Cyber Defence Cloud ermöglicht die Aktualisierung und Absicherung sämtlicher angeschlossener Firewalls in Echtzeit. Mittels Machine Learning, Schwarmintelligenz, und dem Know-how unseres Analyseteams verarbeitet die CDC über 300.000 Ereignisse pro Sekunde - für echte Zero Hour Protection.

Schutz vor Ransomware und Viren

Die ausgezeichnete E-Mail-Security hält Ihre Postfächer sauber: Vier unabhängige, leistungsfähige Scan-Engines prüfen permanent die eingehenden Daten auf ihr Bedrohungspotenzial und lassen gefährliche Nachrichten gar nicht erst zu Ihnen vordringen.

Zugang zu öffentlichen WLANs und internen Netzen kontrollieren

Aktuelle Zugriffs- und Identifikationsverfahren vereinfachen die Rollenzuweisung in Ihrem WLAN. Einmal-Passwörter, die integrierte Anmeldemaske (Captive Portal) sowie zuverlässige Verschlüsselung machen den Zugang für Sie und Ihre Gäste einfach und dank des Zero-Trust-Konzeptes zugleich sicher.

Inklusive DynDNS und SSL-Zertifikaten

Der Securepoint DynDNS-Dienst stellt sicher, dass Ihre Firewall auch bei wechselnder IP-Adresse erreichbar ist. Die eingebaute Möglichkeit, LetsEncrypt-Zertifikate zu erstellen, erhöht das Schutzniveau dieser Verbindungen.

Für den Fall der Fälle: Backup

Alle Konfigurationen der UTM-Firewall werden automatisch verschlüsselt und gesichert als Backup in der Cyber Defence Cloud hinterlegt.

Überreicht durch Ihren Securepoint-Partner

