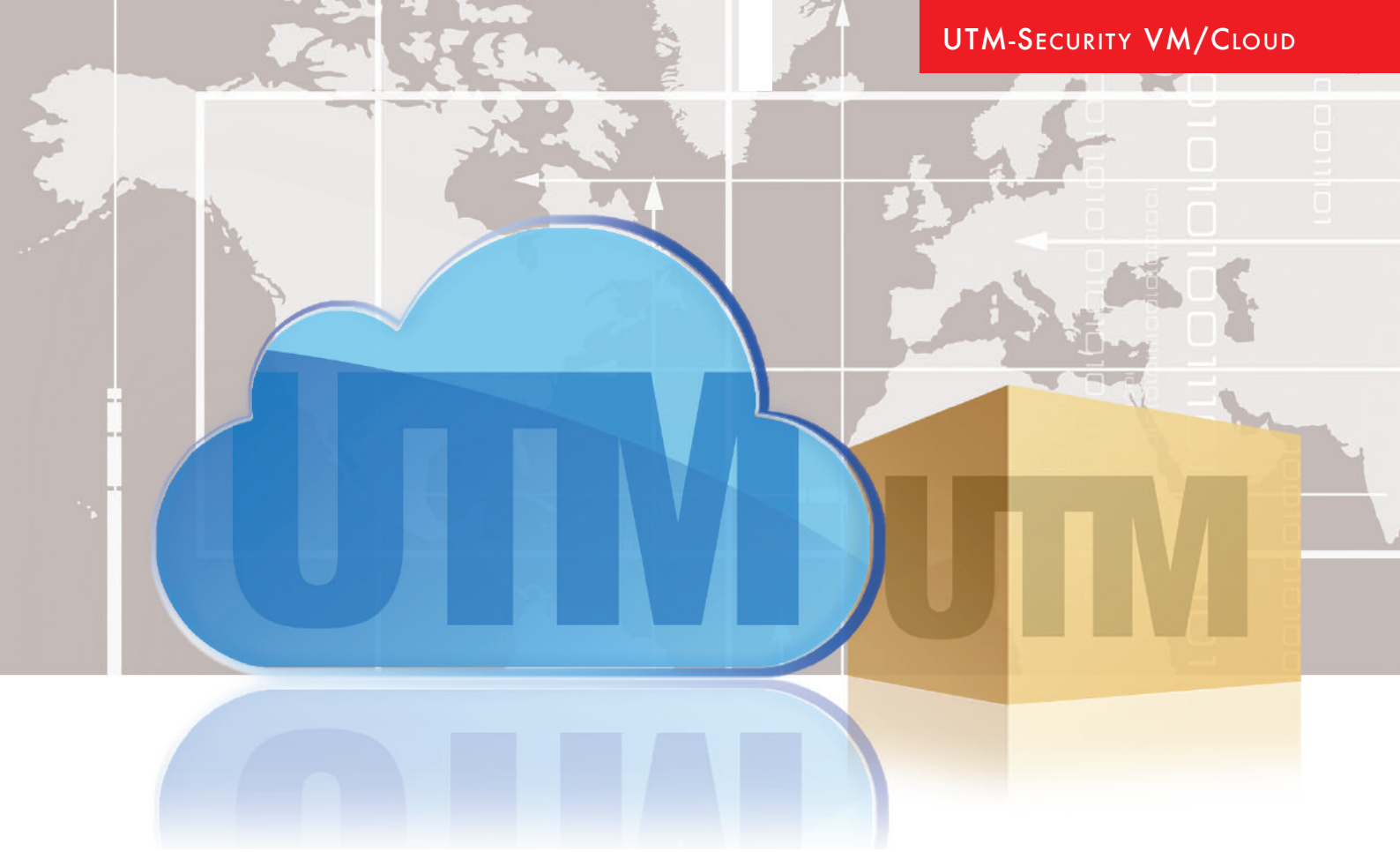


Next Generation UTM-Firewalls: Virtuelle UTM-Gateways/Cloud-UTMs

Die Securepoint virtuellen UTM-Gateways sind auf VMware, Citrix XEN Server, Hyper-V, Oracle VirtualBox oder auf dedizierter Hardware lauffähige IT-Security-Systeme zum Schutz von Unternehmensnetzwerken, Rechenzentren und Clouds. Securepoint UTM-Gateways sind komplette All-in-inclusive-Sicherheitslösungen und beinhalten alle IT-Sicherheitsanwendungen (Firewall, VPN-Gateway, doppelter Virus-/Malware-Scanner, Spamfilter, Content-/Webfilter, IDS etc.)

Sichere, verschlüsselte Anbindung an die Cloud
Sie überlegen Ihre IT-Infrastruktur in eine Cloud zu verlegen? Hierzu bietet Securepoint die virtuellen UTM-Gateways, die mit einem physikalischen Gateway verbunden werden und Ihnen so eine sichere, verschlüsselte Anbindung an eine Cloud und die Verlagerung Ihrer IT-Security in die Cloud so erst möglich macht.

Virtuelle Gateways als kostengünstige HA- oder Spare-Lösung
Securepoint virtuelle UTM-Gateways können ebenfalls als sehr kostengünstige Hochverfügbarskeitslösung oder Spare in Zusammenarbeit mit einer anderen Securepoint UTM oder direkt zur Absicherung von Unternehmensnetzen genutzt werden.

Von 1 bis 2.500 Anwender im Netzwerk
Eine beliebige Skalierung ist selbstverständlich möglich. Die UTM-Gateways ermöglichen für einen bis zu 2.500 PC-Anwender/Server den professionellen und sicheren Internet-Zugang.

SecurITy made in Germany

SECUREPOINT SECURITY SOLUTIONS

Securepoint virtuelle UTM-Gateways für die Sicherheit von Clouds

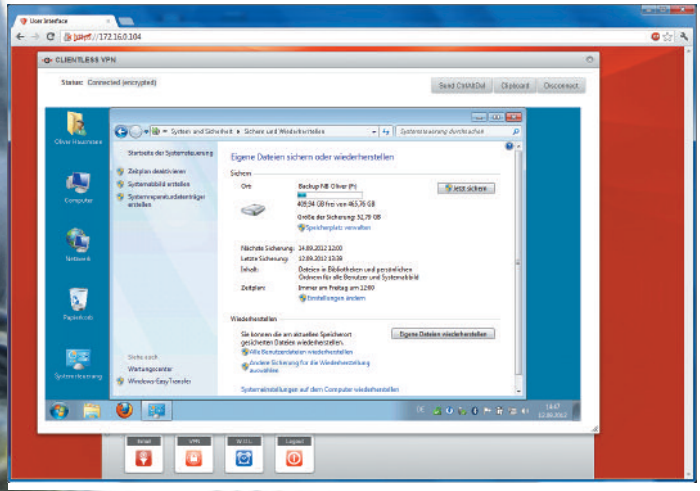
Komplette all-inclusive UTM-Gateways

Die virtuellen Securepoint UTM-Gateways beinhalten alle IT-Sicherheitsanwendungen (wie Firewall, VPN-Gateways, doppelter (!) Virus-/Malware-Scanner, Spamfilter, Webfilter, IDS, Authentisierung etc.). Die virtuellen UTM-Gateways sind speziell zum Schutz von modernen Netzwerken mit bis zu 2.500 PC-Anwendern/Servern und zur Vernetzung vorgesehen.

Securepoint WebGUI: UTM-Bedienung und -Monitoring

IT-Security für mobile Geräte und ClientlessVPN

Immer häufiger werden in Unternehmen mobile Privatgeräte zur Nutzung erlaubt. BYOD stellt aber auch ein Sicherheitsrisiko dar, da damit Firmendaten auf nicht- oder nur teilweise kontrollierbaren, fremden Geräten wie Smartphones oder Tablets verarbeitet werden. Die Securepoint-UTM-Gateways ermöglichen einen kontrollierten und sicheren BYOD-Betrieb, da Datenströme zwischen den Systemen gefiltert werden, bzw. nur ein abgekapselter Zugriff möglich ist. Über die ClientlessVPN-Funktion der Gateways kann von Smartphones/Tablets verschlüsselt auf interne Systeme im Firmennetzwerk zugegriffen werden.



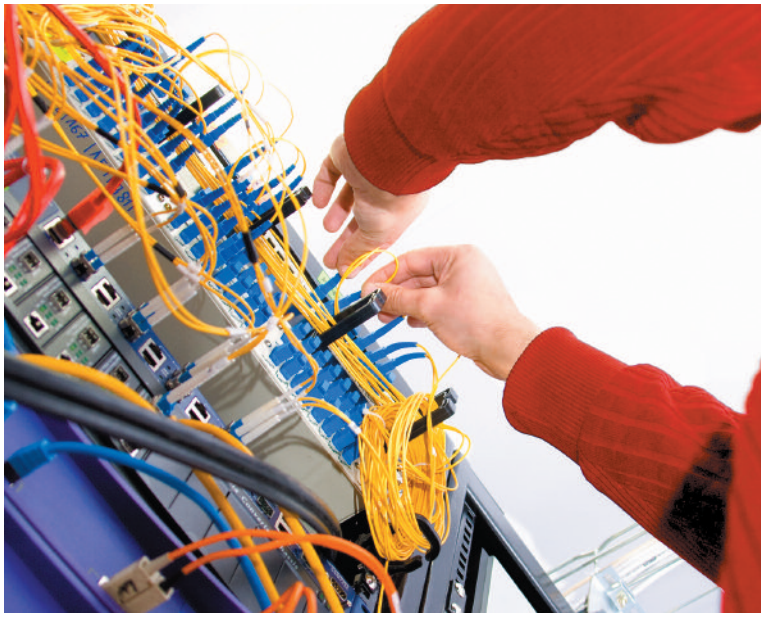
Securepoint WebGUI: UTM-Bedienung und -Monitoring

Arbeiten mit der Cloud: Virtuelles UTM-Gateway und physikalisches UTM-Gateway

Das physikalische UTM-Gateway von Securepoint ist der primäre Schutz für den Internetzugang und das Unternehmensnetzwerk. Es wird vor Ort beim Kunden installiert, stellt die sichere VPN-Verbindung zu einer beliebigen Cloud/Rechenzentren her. Das virtuelle Gateway läuft in der Cloud und dient dem Schutz der Cloud, d. h. deren Infrastruktur, Netzwerk und Diensten.

Securepoint virtuelles UTM-Gateway:

Typ:	virtual UTM Gateway
Geeignet für:	von 1 bis zu 2.500 User
Kurzübersicht Features:	– Stateful Inspection Firewall (DPI) – zwei Virus-/Malware-Scanner on Board: CommtouchAV und ClamAV – Spam-Filter: CommtouchAS – Content-/Web-Filter; URL-Filter – VPN-Server: – IPSec und L2TP/PPTP – SSL/OpenVPN – ClientlessVPN (HTML-VPN) – Intrusion Detection System – Authentisierungs-Funktionen – VPN-Standortkoppelung mit beliebig vielen VPN-Kanälen – VPN-Clients inklusive (kostenlos) für SSL/OpenVPN und ClientlessVPN – kompletter Router (IPv4 und IPv6)
IPv6-Ready:	√
LAN-Ports MBit/s:	beliebig
VPN-Clients inklusive:	√; OpenVPN, ClientlessVPN
Multi-Manag./Monitoring:	Securepoint Operation Center (SOC)
Hardware:	abhängig von der virtuellen Umgebung
Subscription:	zwischen 1 bis 5 Jahre buchbar



Professionelle und sichere Standortvernetzung

Die VPN-fähigen UTM-Gateways erlauben die sichere Vernetzung beliebig vieler Standorte und die Bereitstellung von VPN-Einwahlzugängen. Der kostenlose beiliegende Securepoint VPN-Client ermöglicht mobilen Berufstätigen einen verschlüsselten VPN-Zugang. Integrierte VPN-Server für IPSec, OpenVPN/SSL-VPN, L2TP, ClientlessVPN sowie Quality of Service-Funktionen mit dynamischen Bandbreitenmanagement und die bis zu 10 Gigabit-LAN-Ports sorgen dafür, dass der Datenverkehr im Netzwerk sicher verschlüsselt, richtig priorisiert und performant weitergeleitet wird.

IT-Security-Zentrale:
Securepoint Operation Center (SOC)

Mit dem Securepoint Operation Center (SOC) können alle VPN-/UTM-Systeme in der Cloud verwaltet und gemonitort werden, damit auch sehr weitverzweigte Netzwerke sicher bleiben. Eine übersichtliche Darstellung aller Systeme steht Ihnen zur Verfügung. Zahlreiche Sortier- und Filter-Funktionen helfen dem Administrator, den Überblick auch über sehr große UTM- und VPN-Infrastrukturen zu behalten.

Securepoint Operation Center (SOC)

Bedien-Funktionen

Administrator-Bedienung:
- Sprachen: English, Deutsch
- Rollenbasierte Administration;audit-fähig
- Vier-Augen-Prinzip, Anonymisierung von Log-Daten/Reports
- Verschlüsselung von Konfigurationen, Log-Daten/Reports
- Realtime-Monitoring-Funktionen
- Objektorientierte Konfiguration
- Konfigurationsmanagement bis zu 5.000 UTM-/VPN-Systemen
- Konfigurationssicherungsmanagement in Securepoint Cloud
- Passwort-/Zugangsdaten-Management
- Konfigurations-Management (mehrere Konfigurationen auf einem System)
- Firmware-Management (Update von Firmware-Versionen)
- Backup-Management (Backups von Konfigurationen)
- Konfiguration über:
  - CLI (Command Line Interface): Scriptbasiertes Management für automatisierte Rollouts
  - Web-Bedienoberfläche: Single-System-Management
  - Securepoint Operation Center (SOC): Multi-System-Management
- SSH-Zugriff auf CLI
- Individuell gestaltbares Dashboard

Enduser-Bedienung:
- Sprachen: English, Deutsch
- ClientlessVPN (VPN über Browser für RDP, VNC ohne zusätzliche Plugins)
- Download von automatisch vorkonfigurierten SSL-VPN-Clients (OpenVPN)
- Zugriff auf Spamfilter-Interface des eigenen E-Mail-Accounts
- Wake-on-LAN

Monitoring, Logging- und Report-Funktionen

Monitoring, Logging und Reporting:
- **Vier-Augen-Prinzip**
- **Verschlüsselung von**:
  - Konfigurationen
  - Log-Daten und Reports
- **Anonymisierung Log-Daten/Reports**
- WLAN-Monitoring
- UMTS-Monitoring
- Internet-Connection-Monitoring
- System-/Dienst-Status
- Hardware-Status
- Netzwerk-Status
- Dienste-/Prozess-Status
- Traffic-Status
- VPN-Status
- User-Authentisierung-Status
- Live-Logging
- Syslog-Protokoll-Unterstützung und integrierter Syslog-Server (siehe SOC)
- Logging zu versch. Syslog-Servers

SNMP:
- SNMPv1
- SNMPv2c
- SNMP-traps
- Überwachung:
  - CPU, RAM, HDD/SSD/RAID, Ethernet
  - Internet-Connections
  - VPN-Tunnel
  - Usern
  - Statistiken, Updates und Lizenzen
  - DHCP
  - HA**

Statistiken und Reports (SOC):
- Export Statistik als PDF und CSV
- Antivirus-/Antispam-Statistiken
- Alerts: Ausgelöste Alarme
- Malware: Namen, Art, Anzahl
- Top Websites: Traffic auf Webseiten
- Top Surfer: Alle User, die Traffic verurs.
- Traffics eines Users
- Surfer+Websites: Websites nach Usern
- Content-/Webfilter blockierte Kategorien
- Blocked Websites: blockierte Webseiten
- Interface-Auslastung/-Traffic
- SMTP-Angriffe
- IDS Angriffe-Übersicht
- IDS IP Angreiferer und Angriffsarten
- Top abgelehnte Pakete
- Top angenommene Pakete
- Top zurückgewiesene Pakete
- Top zurückgew. E-Mails
- Top angenom. E-Mails
- Top angenom./zurückgewies. E-Mails
- Top angenommene Mailserver
- Top zurückgewiesene Mailserver
- Top Server in Greylisting whitelisted
- Top Server in Greylisting rejected

Netzwerk-Funktionen

IPv6-ready:
- Konfiguration zu externen Tunnel-brokern (z. B. HE.net)
- IPv6-DHCP und Router Advertisment
- DHCP-Relay, auch durch VPN-Tunnel
- Regeln für DHCP werden automatisch für die jeweiligen Interfaces angelegt

LAN / WAN:
- Ethernet 10/100/1.000/10.000 Mbit/s
- Twisted-Pair und Fibre-Optics
- MTU veränderbar (Ethernet/DSL)
- PPPoE
- Kabelmodem, xDSL
- Load-Balancing
- Bandbreitenmanagement
- Zeitkontrollierte Internet-Connections
- Manuelles und automatisches DNS-Assignment
- DynDNS-Unterstützung (kostenfrei über http://www.spdns.de)

Routing:
- Source Routing
- Destination Routing
- Multipath Routing auf im Mischbetrieb (bis zu 15 Leitungen),
- NAT (Static-/Hide-NAT), virtuelle IP-Adressen
- PAT (Port Address Translation)
- BGP4
- VLAN

DHCP:
- DHCP-Relay
- DHCP-Client
- DHCP-Server (Dynamische/feste IP)

DMZ:
- Port-forwarding
- Port Address Translation (PAT)
- Dedicated DMZ-Links

VLAN:
- Max. 4094 VLANs per Interface
- 802.1q Ethernet Header Tagging
- Kombinierbar mit Bridging**

Bridge-Mode:
- OSI-Layer 2 Firewall-Funktionen
- Spanning Tree (Bridge-ID, Port-Cost)
- Unlimitierte Bridges
- Unlimitierte Interfaces pro Bridge

Traffic Shaping/Quality of Service (QoS):
- QoS/Traffic Shaping (auch für VPN)
- Up-/Download-Stream-Traffic einstellbar
- Alle Dienste separat konfigurierbar
- Minimale, maximale und garantierte Bandbreiten individuell konfigurierbar
- QoS mit TOS-Flag-Unterstützung
- Unterstützung von Multiple-Internet-Connections

Hoch-Verfügbarkeit:
- Active-Passive HA**
- Synchronisation von Single-/Multiple-Verbindungen
- Manual Switch Roles

Name Server:
- Forwarder
- Relay-Zonen
- Master-Zonen (Domain und Reverse)

UTM-Security-Funktionen

Firewall Deep Packet Inspec. (DPI):
- Stateful Inspection
- Connection Tracking TCP/UDP/ICMP
- SPI und Proxy kombinierbar
- OSI-Layer 7-Filter
- Zeitkontrollierte Firewall-Regeln, Content-/Web-Filter, Internet-Connection
- Gruppenbasierte Firewall Regeln, Content-/Web-Filter, Internet-Connection
- Unterstützte Protokolle: TCP, UDP, ICMP, GRE, ESP, AH
- Implied Rules Konfiguration:
  - Standarddienste wie Bootp, Netbios Broadcast... können per On-Click aus dem Logging entfernt werden
  - Standarddienste wie VPN können per On-Click der Zugriff gewährt werden, ohne dafür eine Regel zu schreiben
- Static-NAT, Hide-NAT und deren Ausnahmen konfigurierbar im Paketfilter
- Automatische Update-Funktionen

VPN:
- VPN– und Zertifikat-Assistent

ClientLessVPN:
- Client-to-Site (VPN Home-Arbeitsplätze)
- VPN über Browser für RDP/VNC ohne zusätzliche Plugins (moderne Browser)
- Authentisierung: Active Directory, Radius, lokale User-Datenbank
- SSL-Verschlüsselung

IPSec:
- Site-to-Site (VPN Zweigstellen)
- Client-to-Site (VPN Home-Arbeitsplätze)
- Authentisierung: Active Directory, lokale User-Datenbank
- Verschlüsselung: 3DES, AES 128/256Bit, Twofish, Hash-Algo., MD5-HMAC/SHA1
- Windows 7/8-Ready mit IKEv1, IKEv2
- Preshared Keys (PSK)
- X.509-Zertifikate
- Tunnel-Mode
- DPD (Dead Peer Detection)
- NAT-T
- Daten-Kompression
- PFS (Perfect Forward Secrecy)
- Export für One-Click-Connection
- XAUTH, L2TP

SSL:
- Site-to-Site (VPN Zweigstellen)
- Client-to-Site (VPN Home-Arbeitsplätze)
- Authentisierung: Active Directory, lokale User-Datenbank
- SSL-Verschlüsselung (OpenVPN)
- Verschlüsselung: 3DES, AES (128, 192, 256) CAST5, Blowfish
- Routing-Mode-VPN
- X.509-Zertifikate
- TCP/UDP Port wechselbar
- Daten-Kompression
- Spezifische WINS– und DNS-Server
- Export für One-Click-Connection

L2TP:
- Site-to-Site (VPN Zweigstellen)
- Client-to-Site (VPN Home-Arbeitsplätze)
- Authentisierung: Active Directory, Radius, lokale User-Datenbank
- Windows-L2TP-Unterstützung

PPTP:
- Site-to-Site (VPN für Zweigstellen)
- Authentisierung: Active Directory, Radius, lokale User-Datenbank
- Windows-PPTP-Unterstützung

X.509 Zertifikat-Server:
- Zertifikatsperrliste (CRL)
- Online Certificate Status Protocol (OCSP)
- Templates
- Multi-CA-Unterstützung
- Multi-Host-Zertifikat-Unterstützung

VPN-Clienten (kostenlos):

OpenVPN-Client (OpenVPN):
- Zentral konfigurierbar über Administrationsoberfläche
- Inklusive Konfiguration downloadbar über User-Webinterface
- Installierbar ohne Adminrechte auf Windows-Geräten
- Bedienung: On-Click-VPN-Connection

ClientlessVPN:
- Zentral konfigurierbar über Administrationsoberfläche
- Aufrufbar über User-Interface
- Bedienung: On-Click-VPN-Connection

Antivirus (AV):
- Zwei Virenscanner standardmäßig:
  - Commtouch AV
  - ClamAV
- Virenscanner kaskadierbar SMTP, POP3
- Scann-Protokolle: HTTP, HTTPS, FTP over HTTP, POP3, SMTP
- Scann von verschlüsselten Daten (SSL-Interception/-Bump)
- Scann von komprimierten Daten, Archiven (zip etc.) und Anhängen
- Manuelle und automatische Updates

Antispam (AS):
- Protokolle SMTP, POP3
- Authentisierung: Active Directory, LDAP, lokale User-Datenbank
- Zero-Day-Schutz
- RBL-Listen (SMTP)
- Black-/White-Listen
- Grey-Listing (SMTP)
- Regular Expressions
- SMTP-Gateway:
  - Greeting Pause, Schutz vor „Recipient Flooding", Rate Control
  - Greylisting mit Whitelisten von E-Mail Adressen und Domains
  - E-Mail-Adressen-Validierung direkt über SMTP-Protokoll
- Kombinierbar mit Contentfilter (Sperrung Kategorien wie Pornographie etc.)

Proxys:
- HTTP, HTTPS, FTP over HTTP, POP3, SMTP, SIP/RTP, VNC
- Transparenter Mode (HTTP, POP3)
- Authentisierung: Active Directory, lokale User-Datenbank
- Integrierter URL-/Content-/Web-Filter (siehe Content-/Web-Filter)
- Integrierter Antivirus-System (siehe AV)
- Integrierter Spam-Filter (siehe AS)
- Gruppen-/zeitkontrollierte Regeln

Reverse Proxy:
- Reverse Proxy für HTTP, HTTPS
- Loadbalacing auf interne Server
- Bandbreitenmanagement
- diverse Filtermöglichkeiten

Content-/Web-Filter:
- Content-Filter mit 46 Kategorien
- Kategorie-basiertes Website-Blocken
- Authentisierung: Active Directory, lokale User-Datenbank
- Scan-Technology mit online-Datenbank
- URL-Filter mit Im-/Export URL-Listen
- Black-/White-Listen
- File-Extension/MIME-Types Filter
- Werbe-Blocking (entfernt ca. 50% der Werbeanzeigen von Webseiten)

IDS/IPS:
- Schutz vor DoS-/dDoS-Angriffen
- Portscan Protection
- Invalid Network Packet Protection
- Automatisierte Warnung (E-Mail etc.)

User Authentisierung:
- Vollständige Active Directory-Integration
- Authentisierung gegen Active Directory für alle VPN Protokolle, Filter und Proxies der UTM
- Zusätzlich Radius-Authentisierung für VPN Protokolle PPTP/L2TP

Backup:
- Lokal am Arbeitsplatz, lokal auf UTM/VPN-System, in SOC-Datenbank und Securepoint Cloud
- Automatische und zeitbasierte Backups
- Backups verschlüsselbar
- Backups auf laufen. System möglich

** ab Version 11.3

SecurITy made in Germany

Securepoint GmbH, Salzstraße 1, 21335 Lüneburg
Tel.: 0 41 31 / 24 01-0, Fax: 0 41 31 / 24 01-50
Email: info@securepoint.de
Internet: www.securepoint.de

SECUREPOINT SECURITY SOLUTIONS