



## Next Generation UTM-Firewalls RC300 und RC400 von Securepoint

Die neuen Next Generation UTM-Gateways sind die all-inclusive Security-Lösungen im Markt. Mit dem IPv6-fähigen UTM-Gateways erhalten Unternehmen und Firmen mit verteilten Standorten eine echte Next Generation Unified-Threat-Management-Lösung (UTM) mit Deep-Packet-Inspection Firewall, VPN-Server, zwei professionellen Virensclannern, Spam-/Webfilter und Intrusion Prevention als Komplettlösung ohne zusätzliche Feature-Lizenzierungskosten.

### Unternehmen bis zu 250 Anwender im Netzwerk

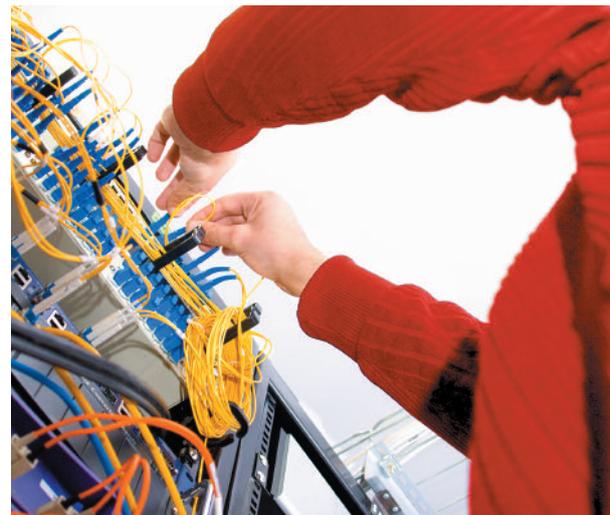
Die UTM-Gateways ermöglichen für bis zu 250 Anwender den professionellen und sicheren Internet-Zugang.

### Schnelle und hochsichere Zweigstellenvernetzung

Die VPN-fähigen UTM-Gateways erlauben die sichere Vernetzung beliebig vieler Standorte und die Bereitstellung von VPN-Zugängen für Mitarbeiter. Securepoint VPN-Clients liegen kostenlos bei.

### High-Lights:

- all-inclusive UTM-Gateways: keine zusätzliche Feature-Lizenzierung
- zukunftssicher mit IPv6
- BYOD-Unterstützung
- zentrale UTM-Verwaltung mit den Securepoint Operation Center
- Vier-Augen-Prinzip und Verschlüsselung von Reports/Logs mit SOC
- Monitoring, Lizenz- und Geräteverwaltung mit SOC
- kostenloser, deutscher Support für Systemhaus-Partner



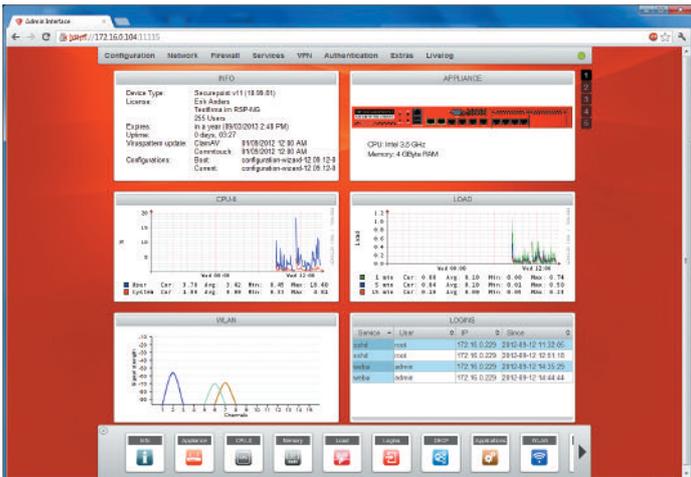
SecurITy  
made  
in  
Germany

SECUREPOINT  
SECURITY SOLUTIONS

## Securepoint UTM-Gateways RC300 und RC400 für Medium & Enterprise Business

### Komplette all-inclusive UTM-Gateways

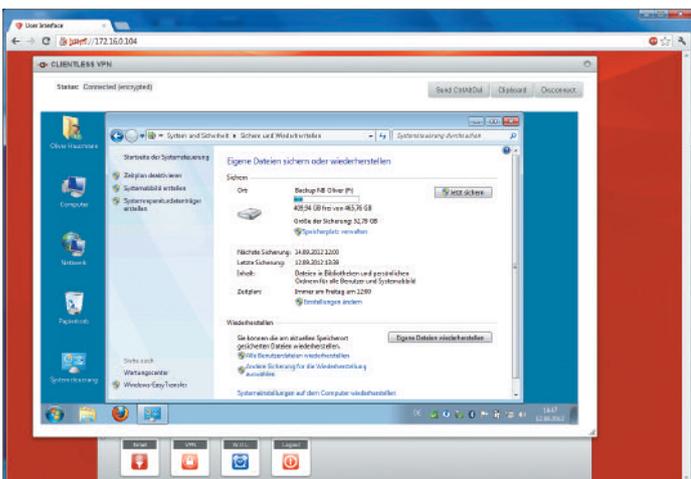
Die stromsparenden Securepoint UTM-Gateways beinhalten alle IT-Sicherheitsanwendungen (wie Firewall, VPN-Gateways, doppelter (!) Virus-/Malware-Scanner, Spamfilter, Webfilter, IDS, Authentisierung etc.). Die UTM-Gateways sind speziell zum Schutz von modernen Netzwerken mit bis zu 250 PC-Arbeitsplätzen/Servern und zur Zweigstellenvernetzung 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

### RC300 UTM-Gateway:



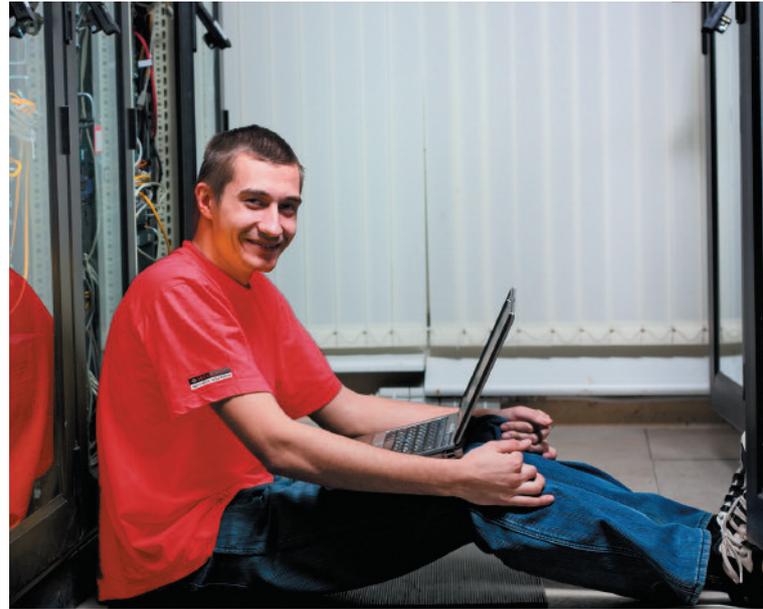
- Typ:** RC300 UTM-Gateway
- Geeignet für:** bis zu 150 User am Standort
- Kurzübersicht Features:** hochintegriertes, energiesparendes UTM-Gateway inklusive:
- Stateful Inspection Firewall (DPI)
  - zwei Virus-/Malware-Scanner on Board: CommtouchAV und ClamAV
  - Spam-Filter: CommtouchAS
  - Content-/Web-Filter; 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
  - bis 1000 gleichzeitige VPN-Verbindungen
  - kompletter Router (IPv4 und IPv6)
- IPv6-Ready:** ✓
- LAN-Ports MBit/s:** 6 x 1 GBit/s
- 2 \* Erweiterungs SLOT vorne:**
- aufrüstbar mit 8 x 10/100/1000 Mbit/s;
  - aufrüstbar mit 2 x 10 Gbit/s
- VGA:** ✓
- USB:** 2
- VPN-Clients inklusive:** ✓; OpenVPN, ClientlessVPN
- Multi-Manag./Monitoring:** Securepoint Operation Center (SOC)
- Hardware:** Intel Pentium G850 2,9 GHz
- Speicher:** 4 GByte RAM
- RAID-Controller:** nein
- SSD-HD:** 1 x 60 GByte SSD; aufrüstbar
- Spare/Hot-Standby:** optional; aufrüstbar
- 19 Zoll-fähig:** ✓; kurzes Rack-Gehäuse, 1 HE inkl. Teleskopschienen
- Subscription:** zwischen 1 bis 5 Jahre buchbar
- Gewährleistung:** 36 Monate Garantie (Bring-in)



**RC400 UTM-Gateway:**



- Typ:** RC400 UTM-Gateway
- Geeignet für:** bis zu 250 User am Standort
- Kurzübersicht Features:** hochintegriertes, energiesparendes UTM-Gateway inklusive:
  - 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
  - bis 1000 gleichzeitige VPN-Verbindungen
  - kompletter Router (IPv4 und IPv6)
- IPv6-Ready:** ✓
- LAN-Ports MBit/s:** 10 x 1 GBit/s
  - 1 \* Erweiterungs SLOT vorne:
    - aufrüstbar mit 4 x 10/100/1000 Mbit/s;
    - aufrüstbar mit 2 x 10 Gbit/s
- VGA:** ✓
- USB:** 2
- VPN-Clients inklusive:** ✓; OpenVPN, ClientlessVPN
- Multi-Manag./Monitoring:** Securepoint Operation Center (SOC)
- Hardware:** Intel XEON E3-1225 3,2 GHz
- Speicher:** 8 GByte RAM
- RAID-Controller:** ✓; Hardware-Raid (RAID1)
- SSD-HD:** 2 x 60 GByte SSD; aufrüstbar
- Spare/Hot-Standby:** optional; aufrüstbar
- 19 Zoll-fähig:** ✓; kurzes Rack-Gehäuse, 1 HE inkl. Teleskopschienen
- Subscription:** zwischen 1 bis 5 Jahre buchbar
- Gewährleistung:** 36 Monate Garantie (Bring-in)

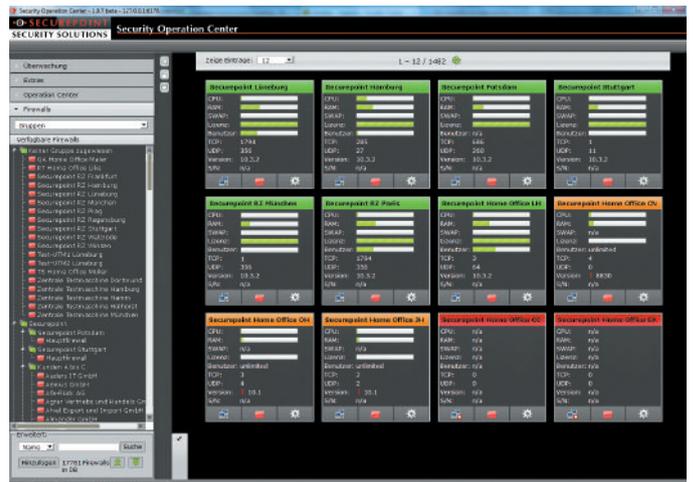


**Professionelle und sichere Standortvernetzung**

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- und UTM-Systeme verwaltet und gemonitort werden, damit auch sehr weitverzweigte Netzwerke sicher gemanagt werden können. 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-Servern

### 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 verur.
- 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 Tunnelbrokern (z. B. HE.net)
- IPv6-DHCP und Router Advertisement
- 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:

- bis zu 1000 gleichzeitige VPN-Verbindungen
- 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

### 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

### X.509 Zertifikat-Server:

- Zertifikatssperlliste (CRL)
- Online Certificate Status Protocol (OCSP)
- Templates
- Multi-CA-Unterstützung
- Multi-Host-Zertifikat-Unterstützung

### Antivirus (AV):

- Zwei Virens Scanner standardmäßig:
  - Commtouch AV
  - ClamAV
- Virens Scanner 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 and 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
  - Loadbalancing 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-Typen 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