Virtuelle/Cloud UTM-Gateways

NextGen UTM-Firewalls

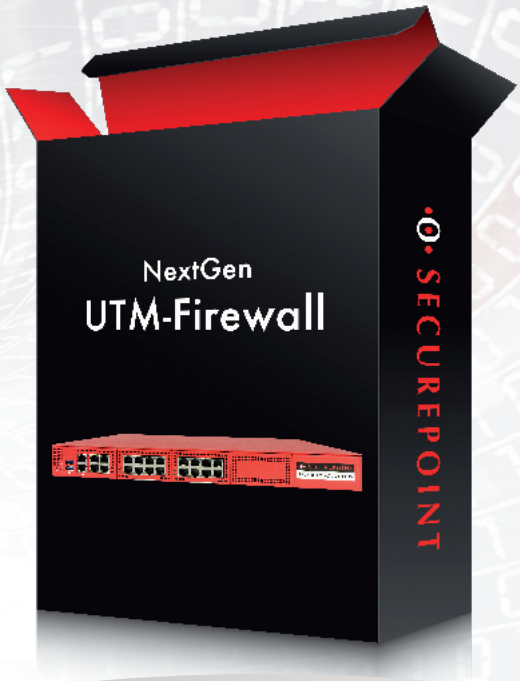
SECUREPOINT SECURITY SOLUTIONS

BPJM Modul 2018

FSM

Info: www.bundespruefstelle.de

Allianz für Cyber-Sicherheit



IT Security bis 2.500 Benutzer

Antivirus Pro

Die optimale Ergänzung für mehr IT-Sicherheit!

Sicheres Netzwerk.

EU DS-GVO ready

SecurITy made in Germany

Virtuelle UTM-Gateways

Securepoint UTM-Gateways können in den virtuellen Umgebungen VMware®, Microsoft Hyper-V® sowie Oracle VirtualBox betrieben und problemlos skaliert werden.

Cloud Security

Virtuelle Securepoint UTM-Gateways in der Cloud schützen Daten und Dienste. So wird die Verlagerung der IT-Infrastruktur in eine Cloud-Umgebung sicher.

Schutz vor Angriffen

Mit Deep Packet Inspection (DPI) und weiteren effizienten Angriffserkennungen schützt die NextGen UTM-Firewall z. B. vor Industrie-spionage und Angriffen aus dem Internet.

Sichere Kommunikation

Schutz vor Viren, Phishing, Spy- und Malware durch die Überwachung und Bereinigung von Kommunikationskanälen (E-Mail), auch bei ver-schlüsselten Verbindungen (POP3S/IMAPS).

Virtuelle UTM-Gateways/Cloud-UTMs

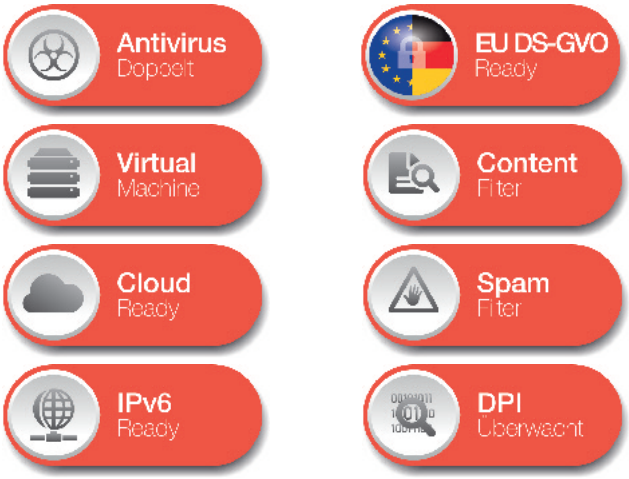
Virtuelle UTM-Gateways
Die virtuellen Securepoint UTM-Gateways sind auf VMware®, Microsoft Hyper-V® sowie Oracle VirtualBox lauffähig. Dedizierte Hardware lässt sich ebenfalls nutzen, um die IT-Security-Lösung zum Schutz von Unternehmensnetzwerken, Rechenzentren und Cloud-Systemen zu betreiben.

Virtuelle UTM-Gateways lassen sich vielfältig einsetzen. Z. B. als kostengünstige Hochverfügbarskeitslösung oder als Spare-System zusammen mit anderen Securepoint UTM-Gateways. Durch die hervorragende Skalierbarkeit sind die virtuellen Systeme perfekt für das Enterprise-Segment geeignet.

Sichere Cloud mit Securepoint UTM-Gateways
Soll die IT-Infrastruktur ganz oder teilweise in die Cloud ausgelagert werden, bieten sich die virtuellen Securepoint UTM-Gateways geradezu an. Ein virtuelles Gateway innerhalb der Cloud, schützt die Daten und Dienste, die an dieser Stelle genutzt werden sollen.

Weitere Securepoint UTM-Gateways (physikalisch oder virtuell) an z. B. verteilten Standorten, schützen die dort vorhandenen Netzwerke und können zusätzlich für eine verschlüsselte Verbindungen in die Cloud sorgen.

Dieser Aufbau macht eine sichere Verlagerung der IT-Infrastuktur in die Cloud erst möglich.



Die Features im Überblick:

- EU DS-GVO ready: Garantiert ohne Backdoors
- Deep Packet Inspection Firewall (DPI)
- Zero-Hour-Protection
- Zwei Viren-/Malwarescanner
- High-End Spam-Filter
- Echtzeit Content-Filter für Web und E-Mail
- Breite VPN-Konnektivität (IPSEC, XAUTH, SSL-VPN)
- Keine Lizenzkosten für VPN-Client und Verbindungen
- Clientless VPN: Browserbasiertes VPN ohne Plug-in (RDP, VNC)
- Komplette Routerfunktionalität
- Vollständige IPv6-Unterstützung
- Umfassende Behandlung von Spam im Benutzerinterface und über Spam-Reports

UTM-Security bis 2.500 Benutzer

Professionelle und sichere Standortvernetzung
Die VPN-fähigen UTM-Gateways erlauben die sichere Vernetzung beliebig vieler Standorte und die Bereitstellung von VPN-Einwahlzugängen für den sicheren Zugriff auf das Netzwerk. Der kostenlos beiliegende Securepoint SSL-VPN-Client ermöglicht mobilen Mitarbeitern einen verschlüsselten VPN-Zugang. Die umfassenden VPN-Konnektivitäten über IPSEC, XAUTH, SSL-VPN sowie Clientless VPN sorgen dafür, dass der Datenverkehr im Internet verschlüsselt wird.
Durch die permanente Weiterentwicklung und regelmäßige Updates schützen die Securepoint NextGen UTM-Firewalls Unternehmensdaten – heute und morgen – zuverlässig vor Gefahren aus dem Internet.

Komplette all-inclusive UTM-Gateways
Leistungsfähige IT-Sicherheitsanwendungen (Firewall, VPN-Gateway, zwei Virus-/Malware-Scanner, High-End Spam-Filter, Echtzeit Content-Filter für Web und E-Mail, Zero-Hour-Protection, IDS, Authentisierung etc.) sorgen für einen durch gängig sicheren Netzwerkbetrieb. Die virtuellen UTM- Gateways schützen moderne Netzwerke mit bis zu 2.500 PC-Systemen/Servern.

Die virtuellen UTM-Gateways kommen als Komplettlösung. Alle UTM-Funktionen sind verfügbar und müssen nicht zusätzlich lizenziert werden.

Sicheres Netzwerk.

- Automatisches Bandbreitenmanagement (QoS)
- Verschlüsselungsprotokolle und Algorithmen können für einzelne Applikationen angepasst werden
- Integrierter Einmalpasswort-Server (OTP) für hochsichere Mehrfaktor-Authentifizierung
- Mail-Connector für sichere Anbindung von POP3(S)/IMAP(S) Konten an E-Mail-Server (SMTP)
- Transparente Filterung von HTTP, HTTPS (HTTPS-Interception), POP3 (Transparent Proxy)
- Angriffserkennung und -abwehr
- Ausfallsicherheit bei Nutzung mehrere Internetzugänge (Fallback)
- Lastverteilung über mehrere Internetzugänge (Loadbalancing/Multipath Routing)

Geeignet für:	bis zu 2.500 Benutzer
Virtuelle Umgebungen:	VMware®, Microsoft Hyper-V® und Oracle VirtualBox
LAN-Ports MBit/s:	bis zu 16 LAN-Ports, mit VLAN erweiterbar
Hardware:	abhängig von der virtuellen Umgebung
Subscription:	1 bis 5 Jahre

Securepoint UTM Funktionsumfang

Bedien-Funktionen

Administrator-Bedienung:
- Sprachen: Englisch, Deutsch
- Audit-fähig
- Verschlüsselung von Konfigurationen, Log-Daten/Reports
- Realtime-Monitoring-Funktionen
- Konfigurations-Management (mehrere Konfigurationen auf einem System)
- Tripple-Firmware-System (optimale Sicherheit bei Upgrades)
- Backup-Management (manuell, automatisch mittels SOC oder Cloud)
- Konfiguration über:
  - Web-Bedienoberfläche: Single-System-Management
  - Securepoint Operation Center (SOC): Multi-System-Management
  - CLI (Command Line Interface): Consolen basierte Verwaltung – Scripting und Remoteverwaltung möglich
  - SSH-Zugriff auf CLI
- Oberfläche passt sich Browserauflösung an (Responsive)
- Individuell gestaltbares Dashboard

Enduser-Bedienung:
- Sprachen: Englisch, Deutsch
- Umfassendes Spam-Management inkl. Sekretärinnen-Funktion
- Clientless VPN (VPN über Browser für RDP, VNC ohne zusätzliche Plug-ins)
- Download von automatisch vorkonfigurierten SSL-VPN-Clients (OpenVPN)
- 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
- 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
- SNMPv3
- Überwachung:
  - CPU, RAM, HDD/SSD/RAID, Ethernet
  - Internet-Connections

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 verursachen
- Traffics eines Users
- Surfer+Websites: Websites nach Usern
- Content-/Web-Filter blockierte Kategorien
- Blocked Websites: blockierte Webseiten
- Interface-Auslastung/-Traffic
- SMTP-Angriffe
- IDS Angriffe-Übersicht
- IDS IP Angreifer 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

LTE/UMTS (Black Dwarf, RC100, RC200):
- Internetverbindung über LTE/UMTS
- LTE/UMTS-Nutzung als Fallback

WLAN Access Point (Black Dwarf, RC100, RC200):
- Virtuelle WLANs (z. B. Gäste-Netze)
- Authentisierung: Active Directory, Pre-Shared Key (PSK)
- WLAN-Monitoring
- WPA2-Verschlüsselung
- Automatische Kanalsuche

LAN/WAN:
- xDSL (PPPoE), Kabelmodem
- Load-Balancing
- Bandbreitenmanagement
- Zeitkontrollierte Internet-Connections
- DynDNS-Unterstützung (kostenfrei über https://www.spdyn.de)

IPv6:
- Konfiguration zu externen Tunnelbrokern (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

Routing:
- Source Routing
- Destination Routing
- Multipath Routing auch im Mischbetrieb (bis zu 15 Leitungen)
- NAT (Static-/Hide-NAT), virtuelle IP-Adressen
- BGP4/OSPF/RIP

DHCP (IPv4/IPv6):
- 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:
- Spanning Tree (Bridge-ID, Port-Cost)
- Unlimitierte Bridges
- Unlimitierte Interfaces pro Bridge

Bandbreitenmanagement:
- Automatische QoS-Einstellungen priorisieren nötige Protokolle um geringere Latenzen zu gewährleisten

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
- Unterstützung von Multiple-Internet-Connections

Hoch-Verfügbarkeit:
- Active-Passive HA
- Synchronisation von Single-/Multiple-Verbindungen

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

UTM-Security-Funktionen

Firewall Deep Packet Inspection (DPI):
- Deep Packet Inspection
- Connection Tracking TCP/UDP/ICMP
- SPI und Proxy kombinierbar
- OSI-Layer 7-Filter
- Zeitkontrollierte 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

VPN:
- VPN- und Zertifikat-Assistent

IPSec:
- Site-to-Site (Netzwerkkopplung)
- Client-to-Site (Anbindung Einzelgeräte)
- Authentisierung: Active Directory, lokale User-Datenbank
- Verschlüsselung: 3DES, AES 128/256Bit, Twofish
- Hash-Algo., MD5-HMAC/SHA1, SHA2
- Windows 7/8/10-Ready mit IKEv1, IKEv2
- Preshared Keys (PSK)
- X.509-Zertifikate
- Tunnel-Mode
- DPD (Dead Peer Detection)
- NAT-T
- Daten-Kompression
- PFS (Perfect Forward Secrecy)
- XAUTH

SSL:
- Site-to-Site (Netzwerkkopplung)
- Client-to-Site (Anbindung Einzelgeräte)
- 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
- Export für One-Click-Connection

X.509 Zertifikat-Server:
- Zertifikatsperrliste (CRL)
- Multi-CA-Unterstützung
- Multi-Host-Zertifikat-Unterstützung

VPN-Client:

Securepoint SSL VPN-Client (OpenVPN):
- Zentral konfigurierbar über Administrationsoberfläche
- Inklusive Konfiguration downloadbar über User-Webinterface
- Anwendung ohne Adminrechte unter Windows
- Bedienung: On-Click-VPN-Connection

ClientLessVPN:
- Client-to-Site (Anbindung Einzelgeräte)
- VPN über Browser für RDP/VNC ohne zusätzliche Plug-ins
- Zentral konfigurierbar über Admnioberfläche
- Authentisierung: Active Directory, lokale User-Datenbank
- SSL-Verschlüsselung
- Aufrufbar über User-Interface
- Bedienung: On-Click-VPN-Connection

Antivirus (AV):
- Zwei Virenscanner standardmäßig:
  - Cyren AV & ClamAV
- Virenscanner kaskadierbar SMTP, POP3
- Scann-Protokolle: HTTP, HTTPS, FTP over HTTP, POP3, POP3S, SMTP, SMTPS
- Scann von verschlüsselten Daten (SSL-Interception/-Bump)
- Scann von komprimierten Daten, Archiven (zip etc.) und Anhängen
- Manuelle und automatische Updates

Antispam (AS):
- Protokolle SMTP, SMTPS, POP3, POP3S
- Authentisierung: Active Directory, LDAP, lokale User-Datenbank
- Zero-Day-Schutz
- 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 Content-Filter (Sperrung von Kategorien wie Danger, Hacking, Pornographie etc.)

Proxys:
- HTTP, HTTPS, FTP over HTTP, POP3, SMTP
- SNI Unterstützung
- Transparenter Mode (HTTP, HTTPS, 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
- DNS-Rebinding Schutz
- Portscan Protection
- Invalid Network Packet Protection

User Authentisierung:
- Vollständige Active Directory-Integration
- Authentisierung gegen Active Directory für alle VPN-Protokolle, Filter und Proxies der UTM

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

Einmalpasswort (OTP):
- Integrierter Einmalpasswort-Server für hoch-sichere Zwei- und Drei-Faktor-Authentifizierung

Mail-Connector:
- Integriert zum Abrufen von E-Mails über POP3(S)/IMAP(S) und Weiterleiten per SMTP
- Steigert Spamerkennung und Virenschutz

Captive Portal:
- Automatische Umleitung von Benutzern bei Seitenaufruf (http)
- Angabe von Nutzungsbedingungen
- Dynamische Regeln (Portfilter) für angemeldete Benutzer
- Optionale Benutzeranmeldung mit Benutzername und Passwort

Virtualisierung:
- Unterstützung von Hyper-V® und VMware® (ab Version 4.1)

Änderungen und Irrtümer vorbehalten

SECUREPOINT SECURITY SOLUTIONS

Securepoint GmbH
Bleckeder Landstraße 28
21337 Lüneburg
Deutschland

Tel.: 0 41 31 / 24 01-0
Fax: 0 41 31 / 24 01-50
E-Mail: info@securepoint.de
Web: www.securepoint.de

EU DS-GVO ready

SecurITy made in Germany

Systemhaus/Partner: