NextGen UTM-Firewalls

Protect your network infrastructure

SECUREPOINT SECURITY SOLUTIONS

BPJM Modul 2018

Bundesprüfstelle für jugendgefährdende Medien

FSM

Info: www.bundespruefstelle.de

Allianz für Cyber-Sicherheit

Secure network.

IT security for up to 2.500 users

UTM Firewall

EU DS-GVO ready

SecurITy made in Germany

Security when surfing

Access restrictions are enforced via the content filter with Zero-Hour-Protection. The two virus scanners provide security when surfing on the Internet.

Protection from attacks

With Deep Packet Inspection (DPI) and other efficient attack detection tools, the NextGen UTM-Firewall protects against e.g. industrial espionage and attacks from the internet.

Secure connectivity

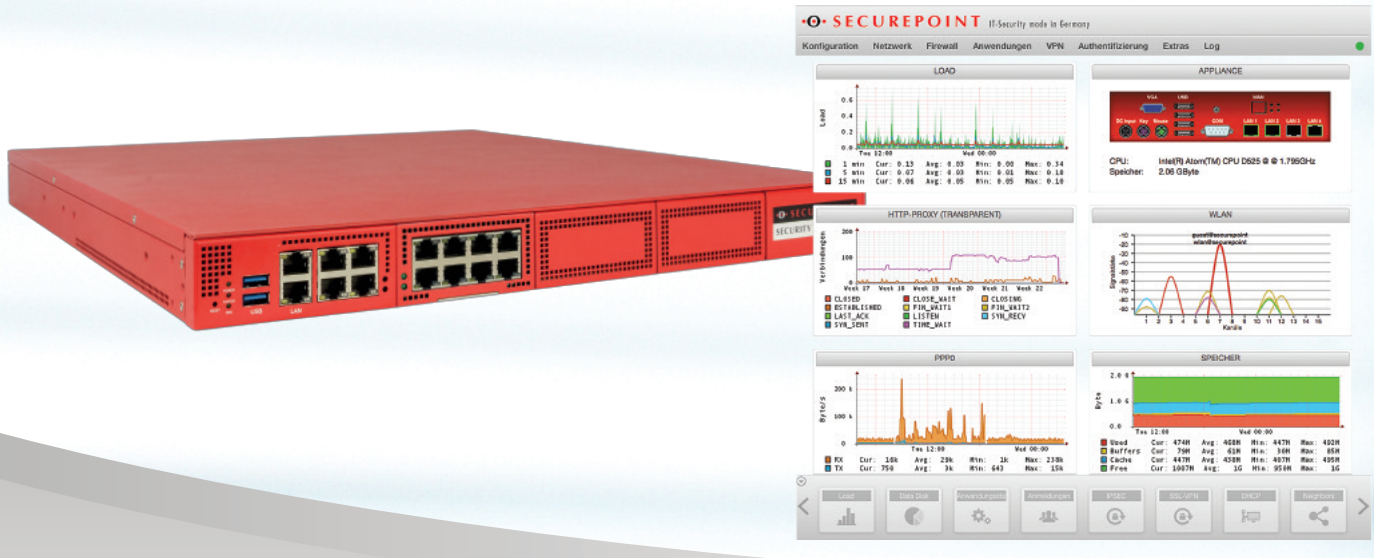
The ability to link any number of locations, provide VPN dial-up accesses and connect to mobile workplaces via different VPN protocols.

Secure communication

Protection against viruses, phishing, spyware and malware via monitoring and adjustment of communication channels (email), also in the case of encrypted connections (POP3S/IMAPS).

IT-Security made in Germany

NextGen UTM-Firewalls



Complete all-inclusive NextGen UTM-Firewalls

NextGen UTM-Firewalls provide companies with secure Internet access. They are a perfect fit for the structure and protection of modern company networks. Secure network operation across the board is ensured, thanks to efficient IT security applications (firewall, VPN-Gateway, two virus/malware scanners, high-end spam filters, real-time content filters for web and email traffic, zero-hour-protection, IDS, authentication, etc.). An UTM system at a central point protects the complete network.

The NextGen UTM-Firewalls are delivered as a complete package. Additional licences are not required for individual UTM functions.

Professional and secure location networking

The VPN ready UTM-Gateways allow any number of locations to be linked securely and VPN dial-up is provided for secure access to the network. The free accompanying Securepoint SSL-VPN client provides mobile employees with encrypted VPN access. The extensive VPN connectivity via IPSEC, XAUTH, SSL-VPN, L2TP, PPTP and clientless VPN, ensures encryption for data sent over the Internet.
The Securepoint NextGen UTM-Firewalls protect company data reliably - today and tomorrow - against threats from the Internet thanks to constant development and updates.

Features overview:

- Deep Packet Inspection Firewall (DPI)
- Zero-Hour-Protection
- Two virus/malware scanners
- High-end spam filter
- Real-time content filter for web and email traffic
- Extensive VPN connectivity (IPSEC, XAUTH, SSL-VPN, L2TP, PPTP)
- No licence costs for VPN connections
- Clientless VPN: Browser-based VPN client (HTML5, RDP, VNC, no plug-in required)
- Complete router functionality
- Complete IPv6 support
- Extensive handling of spam in the user interface and via spam reports

UTM security for up to 2.500 users

Black Dwarf (Up to 10 users)

RC300/400/1000 (Up to 150/250/1.000 users)

RC100/200 (Up to 25/50 users)

Virtual UTM-Gateway/Cloud (Up to 2.500 users)

- Automatic bandwidth management (QoS)
- Encryption protocols and algorithms can be customized for individual applications
- Integrated one-time password server (OTP) for high security multi-factor authentication
- Mail connector for secure connection of POP3(S)/ IMAP(S) accounts to your email server (SMTP)
- Transparent filtering of HTTP, HTTPS (HTTPS interception), POP3 (transparent proxy)
- Attack detection and defence
- Reliability when using multiple Internet connections (fallback)
- Load distribution across multiple Internet connections (load balancing/multipath routing)

Securepoint UTM functions

Operating functions

Administrator operation:
- Languages: English, German
- Audit-ready
- Encryption of configurations, log data/reports
- Real-time monitoring functions
- Object-oriented configuration
- Configuration backup management in Securepoint Cloud
- Password/access data management
- Configuration management (multiple configurations in one system)
- Firmware management (updating firmware versions)
- Backup management (configuration backups)
- Configuration via:
  - CLI (Command Line Interface): Script-based management for automated roll-outs
  - Web user interface: Single-System-Management
  - Securepoint Operation Center (SOC): Multi-System-Management
- SSH access to CLI
- Customisable dashboard

End user operation:
- Languages: English, German
- Clientless VPN (VPN via browser for RDP, VNC without additional plug-ins)
- Download of automatically preconfigured SSL-VPN clients (OpenVPN)
- Wake-on-LAN

Monitoring, logging and report functions

Monitoring, logging and reporting:
- Two-man rule
- Encryption of configurations, log data and reports
- Anonymization of log data/reports
- System/service status
- Hardware status
- Network status
- Service/process status
- Traffic status
- VPN status
- User authentication status
- Live logging
- Syslog protocol support and integrated syslog server (see SOC)
- Logging for various syslog servers

SNMP:
- SNMPv1
- SNMPv2c
- SNMP-traps
- Monitoring:
  - CPU, RAM, HDD/SSD/RAID, Ethernet
  - Internet connections

Statistics and reports (SOC):
- Export statistics as PDF and CSV
- Antivirus/antispam statistics
- Alerts: Triggered alarms
- Malware: Name, type, number
- Top websites: The websites with the most traffic
- Top surfers: The users that have the most traffic
- Per user traffic
- Surfers+websites: Websites by users
- Categories blocked by content/web filter
- Blocked websites
- Interface utilisation/traffic
- SMTP attacks
- Overview of IDS attacks
- IDS IP address of attackers and types of attack
- Top dropped packets
- Top accepted packets
- Top rejected packets
- Top rejected emails
- Top accepted emails
- Top accepted/rejected emails
- Top accepted mail servers
- Top rejected mail servers
- Top server in greylisting whitelisted
- Top server in greylisting rejected

Network functions

IPv6-ready:
- Configuration for external tunnel brokers (e.g. HE.net)
- IPv6-DHCP and router advertisement
- DHCP-relay, also via VPN tunnel
- Rules for DHCP are automatically created for the respective interfaces

LAN/WAN:
- xDSL (PPPoE), cable modem
- Load balancing
- Bandwidth management
- Time-controlled Internet connections
- DynDNS support (free of charge via http://www.spdns.de)

Routing:
- Source routing
- Destination routing
- Multipath routing in mixed operation also (up to 15 lines)
- NAT (static/hide NAT), virtual IP addresses
- BGP4

DHCP (IPv4/IPv6):
- DHCP relay
- DHCP client
- DHCP server (dynamic/fixed IP)

DMZ:
- Port forwarding
- Port address translation (PAT)
- Dedicated DMZ links

VLAN:
- Max. 4094 VLANs per interface
- 802.1q Ethernet header tagging
- Can be combined with bridging

Bridge mode:
- OSI layer 2 firewall functions
- Spanning tree (bridge ID, port cost)
- Unlimited bridges
- Unlimited interfaces per bridge

Traffic shaping/ Quality of service (QoS):
- QoS/traffic shaping (also for VPN)
- Adjustable upload/download traffic streams
- All services can be configured separately
- Minimum, maximum and guaranteed bandwidths can be configured individually
- Multiple Internet connections supported

High availability:
- Active-passive HA
- Synchronisation of single/multiple connections

Name server:
- Forwarder
- Relay zones
- Master zones (domain and reverse)

Bandwidth management:
- Prioritise automatic QoS settings required protocols to guarantee lower latencies

UTM security functions

Firewall deep packet inspection (DPI):
- Deep packet inspection
- Connection tracking TCP/UDP/ICMP
- SPI and proxy can be combined
- OSI layer 7 filter
- Time-controlled firewall rules, content/web filters, Internet connection
- Group-based firewall rules, content/web filters, Internet connection
- Supported protocols: TCP, UDP, ICMP, GRE, ESP, AH

Implied rules configuration:
- Standard services such as Bootp, Netbios Broadcast... can be removed from logging via One-Click
- Standard services such as VPN can be granted access via One-Click without a rule having to be written
- Static-NAT, hide-NAT and their exceptions can be configured in the packet filter

VPN:
- VPN and certificate assistant

ClientLessVPN:
- Client-to-site (VPN home offices)
- VPN via browser for RDP/VNC without additional plug-ins (modern browsers)
- Authentication: Active directory, local user database
- SSL encryption

IPSec:
- Site-to-site (VPN branches)
- Client-to-site (VPN home offices)
- Authentication: Active directory, local user database
- Encryption: 3DES, AES 128/ 256Bit, Twofish
- Hash Algorithms: MD5-HMAC/SHA1, SHA2
- Windows 7/8-ready with IKEv1, IKEv2
- Pre-shared keys (PSK)
- X.509 certificates
- Tunnel mode
- DPD (dead peer detection)
- NAT-T
- Data compression
- PFS (perfect forward secrecy)
- XAUTH, L2TP

SSL:
- Site-to-site (VPN branches)
- Client-to-site (VPN home offices)
- Authentication: Active directory, local user database
- SSL encryption (OpenVPN)
- Encryption: 3DES, AES (128, 192, 256) CAST5, Blowfish
- Routing mode VPN
- X.509 certificates
- TCP/UDP port can be changed
- Data compression
- Export for One-Click connection

L2TP:
- Client-to-site (VPN home offices)
- Authentication: Active directory, radius, local user database
- Windows L2TP support

PPTP (not recommended):
- Client-to-site (VPN home offices)
- Authentication: Active directory, radius, local user database
- Windows PPTP support

X.509 certificate server:
- Certificate revocation list (CRL)
- Multi-CA support
- Multi-host certificate support

VPN clients (free):

OpenVPN client (OpenVPN):
- Can be configured centrally via the administration interface
- An included configuration that can be downloaded via user web interface
- Can be run without administrator rights on Windows
- Operation: One-Click VPN connection

ClientlessVPN:
- Can be configured centrally via the administration interface
- Usable via the user interface
- Operation: One-Click VPN connection

Antivirus (AV):
- Two virus scanners as standard:
  - Commtouch AV & ClamAV
- Virus scanner cascadable SMTP, POP3
- Scan protocols: HTTP, HTTPS, FTP over HTTP, POP3, SMTP
- Encrypted data scanned (SSL interception/bump)
- Compromised data, archives (zip etc.) and attachments scanned
- Manual and automatic updates

Antispam (AS):
- Protocols: SMTP, POP3
- Authentication: Active directory, LDAP, local user database
- Zero-Day-Protection
- RBL lists (SMTP)
- Black/whitelists
- Greylisting (SMTP)
- Regular expressions
- SMTP gateway:
  - Greeting pause, protection against "recipient flooding", rate control
  - Greylisting with whitelists of email addresses and domains
  - Email address validation directly via SMTP protocol
- Can be combined with the content filter (blocking categories such as pornography etc.)

Proxies:
- HTTP, HTTPS, FTP over HTTP, POP3, SMTP, SIP/RTP, VNC
- Transparent mode (HTTP, POP3)
- Authentication: Active directory, local user database
- Integrated URL/content/web filter (see content/web filter)
- Integrated antivirus system (see AV)
- Integrated spam filter (see AS)
- Group/time-controlled rules

Reverse proxy:
- Reverse proxy for HTTP, HTTPS
- Load balancing on internal server
- Bandwidth management
- Different filter options

Content/web filter:
- Content filter with 46 categories
- Category-based website blocking
- Authentication: Active directory, local user database
- Scan technology with online database
- URL filter with import/export URL lists
- Black/whitelists
- File extension/MIME type filter
- Advertisement blocking (approx. 50% of adverts removed from websites)

IDS/IPS:
- Protection against DoS/DDoS attacks
- Port scan protection
- Invalid network packet protection
- Automated warning (email etc.)

User authentication:
- Complete active directory integration
- Authentication against active directory for all VPN protocols, filters and proxies of the UTM
- Radius authentication for the VPN protocols PPTP/L2TP

Backup:
- Locally in the workplace, locally in the UTM/VPN system, in the SOC database, and in the Securepoint Cloud
- Automatic and time-based backups
- Backups can be encrypted
- Backups of the running system are possible

One-time password (OTP):
- Integrated one-time password server for high security two and three factor authentication

Mail connector:
- Integrated for retrieving emails via POP3(S)/IMAP(S) and forwarding via SMTP
- Increases spam detection and virus protection

Errors and omissions excepted.

SECUREPOINT SECURITY SOLUTIONS

Securepoint GmbH
Bleckeder Landstraße 28
D-21337 Lüneburg
Germany

Phone: +49 41 31 / 24 01-0
Fax: +49 41 31 / 24 01-50
Email: info@securepoint.de
Web: www.securepoint.de

EU DS-GVO ready

SecurITy made in Germany

System house/partner:

IT-Security made in Germany