Black Dwarf G2 UTM

Die All-In-One Security-Lösung

SECUREPOINT SECURITY SOLUTIONS

BPJM Modul 2015
Bundesprüfstelle für jugendgefährdende Medien
fsm
Info: www.bundespruefstelle.de

Allianz für Cyber-Sicherheit

IT Security bis
10 Benutzer
UTM Firewall

Sicheres Netzwerk.

SecurITy made in Germany

Sicherheit beim Surfen

Durch den starken Content-Filter mit Zero-Hour-Protection werden Zugriffsbeschränkungen durchgesetzt. Die beiden Virus-Scanner sichern das Surfen im Internet ab.

Schutz vor Angriffen

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

Konnektivität

Standortvernetzung über verschiedene VPN-Protokolle sowie die Anbindung mobiler Geräte über WiFi. UMTS ist für Internet und als Fallback-Lösung konfigurierbar.

Sichere Kommunikation

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

IT-Security made in Germany

Next Generation UTM-Firewall

Komplette all-inclusive UTM-Firewalls

Die neuen Next-Generation-UTM-Gateways Black Dwarf stellen Unternehmen einen sicheren Internetzugang zur Verfügung. Sie sind perfekt für den Aufbau und den Schutz moderner Unternehmensnetze geeignet. 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 durchgängig sicheren Netzwerkbetrieb. Ein UTM-System, an einem zentralen Punkt, schützt das komplette Netzwerk.
Die UTM-Firewalls kommen als Komplettlösung. Einzelne Funktionen müssen nicht extra lizensiert werden.

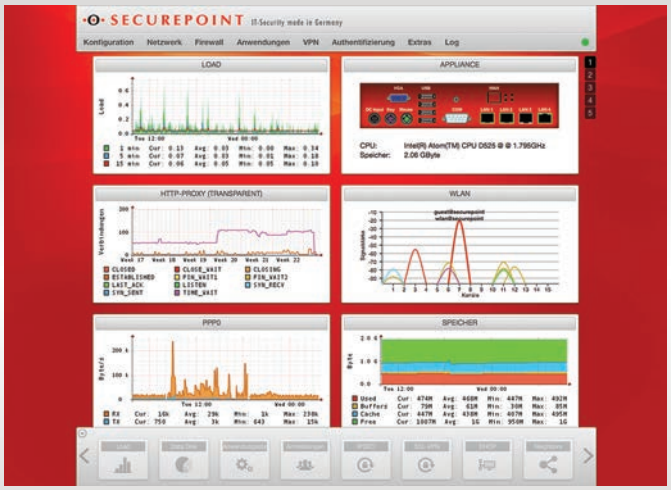
Professionelle und sichere Standortvernetzung

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 umfassende VPN-Konnektivität über IPSEC, XAUTH, SSL-VPN, L2TP, PPTP sowie Clientless VPN sorgt dafür, dass der Datenverkehr im Internet verschlüsselt wird.
Durch die ständige Weiterentwicklung und Updates sichern die Securepoint UTM-Firewalls Unternehmensdaten – heute und morgen – zuverlässig vor Gefahren aus dem Internet.

Die Features im Überblick:

- Deep Packet Inspection Firewall (DPI)
- Zero-Hour-Protection
- Zwei Virus-/Malware-Scanner
- High-End Spam-Filter
- Echtzeit Content-Filter für Web und E-Mail
- Umfassende VPN-Konnektivität (IPSEC, XAUTH, SSL-VPN, L2TP, PPTP)
- Integrierter kostenloser Securepoint SSL-VPN-Client
- Keine Lizenzkosten für VPN-Verbindungen
- Clientless VPN: Browserbasiertes VPN ohne Plug-in (HTML5, RDP, VNC)
- Angriffserkennung und -abwehr
- Anwenderidentifizierung (lokal, Active Directory, LDAP)

UTM-Security bis 10 Benutzer



Securepoint WebGUI: UTM-Bedienung und -Monitoring

WLAN vorinstalliert

Nach dem Einrichten der UTM-Firewall steht das WLAN-Modul 30 Tage kostenfrei zur Verfügung. Nach Ablauf dieser Testphase kann die WiFi-Option mit einem Lizenzkey dauerhaft freigeschaltet werden.

UMTS optional

Ein optionales UMTS-Modul, für eine dauerhafte Internetverbindung oder als Fallback-Lösung, lässt sich jederzeit nachrüsten.

Sicheres Netzwerk.

- Integrierter Einmalpasswort-Server (OTP) für hochsichere Mehrfaktor-Authentifizierung
- Mail-Connector für sichere Anbindung von POP3(S)/ IMAP(S) Konten an Ihren E-Mail-Server (SMTP)
- Transparente Filterung von HTTP, HTTPS (HTTPS-Interception), POP3 (Transparent Proxy)
- Umfassende Behandlung von Spam im Benutzerinterface und über Spam-Reports
- Komplette Routerfunktionalität
- Vollständige IPv6-Unterstützung
- Ausfallsicherheit bei Nutzung mehrere Internetzugänge (Fallback)
- Lastverteilung über mehrere Internetzugänge (Loadbalancing/Multipath Routing)

Geeignet für:	bis zu 10 Benutzer am Standort
LAN-Ports:	3 x 10/100/1.000 MBit/s
WiFi/WLAN:	300 MBit/s (Vorbereitet)
UMTS (optional):	Internet oder Fallback
Monitoring:	Securepoint Operation Center
Leistungsaufnahme:	~19 Watt
Subscription:	1 oder 3 Jahre
Gewährleistung:	36 Monate Garantie (Bring-in)

TERRA Black Dwarf G2 Funktionsumfang

Bedien-Funktionen

Administrator-Bedienung:
- Sprachen: Englisch, Deutsch
- Audit-fähig
- Verschlüsselung von Konfigurationen, Log-Daten/Reports
- Realtime-Monitoring-Funktionen
- Objektorientierte Konfiguration
- 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: Englisch, Deutsch
- 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-Servers

SNMP:
- SNMPv1
- SNMPv2c
- SNMP-traps
- 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

IPv6-ready:
- 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

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

UMTS:
- Internetverbindung über UMTS
- UMTS-Nutzung als Fallback

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

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

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:
- 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
- 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)

UTM-Security-Funktionen

Firewall Deep Packet Inspec. (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
- 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

VPN:
- VPN- und Zertifikat-Assistent

ClientLessVPN:
- Client-to-Site (VPN Home-Arbeitsplätze)
- VPN über Browser für RDP/VNC ohne zusätzliche Plug-ins (moderne Browser)
- Authentisierung: Active Directory, 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, SHA2
- 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)
- 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
- Export für One-Click-Connection

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

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

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

VPN-Clienten (kostenlos):

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

ClientlessVPN:
- Zentral konfigurierbar über Adminioberfläche
- 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 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 Content-Filter (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

Einmalpasswort (OTP):
- Integrierter Einmalpasswort-Server für hochsichere 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

Änderungen und Irrtümer vorbehalten

SECUREPOINT SECURITY SOLUTIONS

Securepoint GmbH
Salzstraße 1
21335 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

SecurITy made in Germany

Systemhaus/Partner:

IT-Security made in Germany