

Greenbone Security Manager

Sustainable Resilience



Der **Greenbone Security Manager (GSM)** ist eine Produktlinie zweckorientierter Appliances für Schwachstellen-Scanning und -Management. Sie integrieren sich transparent in ein bestehendes Abwehr-Management und wirken präventiv gegen Angriffe. Zudem werden Verstöße gegen Sicherheitsrichtlinien des Unternehmens oder gegen gesetzliche Vorgaben aufgedeckt. Alle Arbeitsschritte lassen sich weitestgehend automatisieren.

Der **GSM 5300** kann Sensoren für bis zu 30 Sicherheitszonen steuern und deckt bis zu 30.000 IPs ab. Das Einsatzfeld ist Großunternehmens-IT.



Vorteile:

- Schlüsselfertige Lösung: Inbetriebnahme innerhalb 10 Minuten
- Leistungsstarkes Appliance-Betriebssystem *Greenbone OS* mit speziell angepasster konsolen-basierter Administration und aufbauend auf einer umfangreichen Sicherheitskonzeption
- Integriert *Greenbone Security Feed* mit über 55.000 Netzwerk Schwachstellen-Tests mit täglicher, automatisierter Aktualisierung
- Integriertes Backup, Restore, Snapshot und Update
- Integrierter Security Assistant als zentrale Web-Schnittstelle
- Keine Begrenzung bezüglich Anzahl der Zielsysteme bzw. IPs (erreichbare Anzahl hängt vom Scan-Muster und Scan-Zielen ab)
- Flatrate-Subscription umfasst das Platinum Support Paket, den *Greenbone Security Feed* und Feature-Updates

Spezifikation



Maße

430mm x 580mm x 88mm

Zertifizierung

- CE
- FCC Class A
- UL

Umgebung

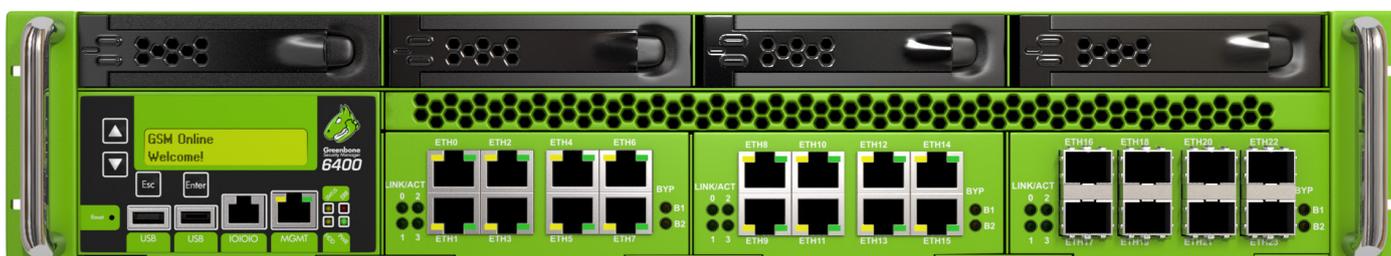
- Betriebstemperatur:
0° bis 45°C (32° bis 113°F)
- Lagertemperatur
-20° bis 80°C (-4° bis 176°F)
- Luftfeuchtigkeit: 10% bis 90%
(nicht kondensierend)

Anschlüsse

- bis 3 Module mit jeweils wahlweise
 - 8 Port GbE
10/100/1000 Base-TX (Kupfer)
 - 8 Port GbE SFP
(Kupfer oder Glasfaser)
 - 2 Port 10 GbE XFP
- 1 Port serielle Konsole RS-232

Konstruktion

- 2HE Chassis, stabiles Stahlgehäuse
- 16x2 Zeichen LCD Anzeige
- Redundant und Hot Swap: HDD, Power Lüfter



Greenbone Security Manager

Sustainable Resilience



Unterstützte Standards

- Netzwerkintegration: SMTP (Email), SNMP, SysLog, LDAP, NTP, DHCP, IPv4/IPv6
- Schwachstellendetektion: CVE, CPE, CVSS, OVAL
- Netzwerkskans: WMI, LDAP, HTTP, SMB, SSH, TCP, UDP, ...
- Richtlinien: IT-Grundschutz, PCI-DSS, ISO 27001



Web-basierte Schnittstelle (HTTPS)

- Management von Scan-Aufgaben mit Notizen und False-Positive-Markierungen
- Unterstützung für Mehrbenutzer-Betrieb
- Clustering und verteiltes Scanning über Master-Slave-Betrieb
- Berichtsdurchsicht mit Filterung, Sortierung, Notizen und Risikoeinstufung
- Plugin-Framework für Berichte: XML, PDF, ...
- Performance-Übersicht der Appliance

Web



Integration (API)

- Greenbone Management Protocol (GMP), verschlüsselt
- Alle Anwenderfunktionen der Web-Schnittstelle in der API verfügbar
- Leichte Integration mit anderen Applikationen via API
- Einfache Automatisierungen via Kommandozeilen-Tools (CLI)

API

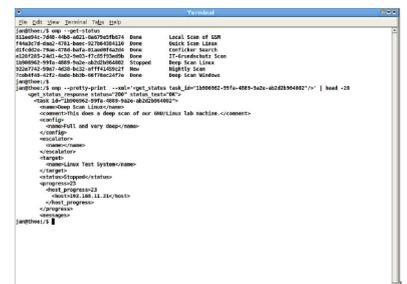


Administration über Konsolen-Schnittstelle

(erfolgt über eine angepasste Shell via SSHv2 oder RS232)

- Konfiguration der Netzwerkintegration
- Backup, Restore, Snapshot, Factory Reset, Update

CLI



Scan-Applikationen (geprüfte und angepasste Versionen)

- Scan Engine und Framework: OpenVAS mit integriertem *Greenbone Security Feed*
- Zusätzliche Scan Tools: Nmap, w3af

Ihr Greenbone Security Solutions Partner:



Greenbone

Sustainable Resilience

Greenbone Networks GmbH
Neumarkt 12
49074 Osnabrück
Deutschland

Telefon: +49-541-760278-0
Fax: +49-541-760278-90
Email: sales@greenbone.net
Web: www.greenbone.net