

## gateProtect Command Center® V2

### Managed Security Service für MSSP (Managed Security Service Provider) und Unternehmen mit global vernetzten IT-Systemen

Das gateProtect Command Center® V2 ist das ideale Werkzeug für Anbieter von Managed Security Services sowie Unternehmen, die eine Vielzahl von Firewalls zentral verwalten wollen. Das Command Center ermöglicht die zentrale Verwaltung, Konfiguration und Überwachung von bis zu 500 gateProtect xUTM und VM Appliances. Dies ermöglicht den MSS-Providern einen sicheren und kosteneffizienten Einsatz von Managed Security Services und den Unternehmen ihre Total Cost of Ownership (TCO) deutlich zu reduzieren.

Den MSS-Providern und den IT-Abteilungen der Unternehmen steht mit dem gateProtect Command Center eine Vielzahl von Features zur Verfügung, die das globale Management von IT-Security-Systemen ermöglichen. Dazu gehören das aktive Management der angebotenen Firewall-Systeme, das komplette Monitoring, d.h. dem Überwachen aller betriebs- und sicherheitsrelevanten Parameter. Desweiteren die zentrale Backup Steuerung und Speicherung, die Lizenzverwaltung, die VPN Zertifikatsverwaltung und -einrichtung sowie vieles mehr.

Dank des prozessorientierten Frontends mit der von gateProtect patentierten eGUI® Technologie (ergonomic Graphic User Interface) bleibt auch bei einer Vielzahl von IT-Systemen stets die volle Übersicht erhalten, wodurch die effektive Effizienz und Sicherheit nachweislich um ein Vielfaches gesteigert wird.

#### Rollouts schnell und effizient managen

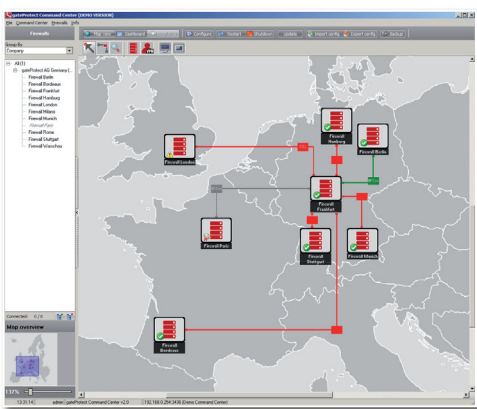
Größere Rollouts von IT-Netzen sind für Administratoren eine besondere Herausforderung. Das gateProtect Command Center® bietet hier eine enorme und professionelle Erleichterung. Zuvor erstellte Standardkonfigurationen (bis in jede Detailtiefe) können sofort und zentral verteilt und installiert werden.

So kann innerhalb kürzester Zeit ein firmenweiter Standard für alle Firewalls erstellt und eingespielt werden. Natürlich können die so auf den einzelnen Firewalls erstellten Konfiguration individuell angepasst werden. Dies minimiert den Aufwand deutlich und beschleunigt den Rollout erheblich.

#### 1. Zentrale Verwaltung und Konfiguration

Der zentrale Konfigurationsdesktop zeigt die Gesamtübersicht der angebotenen Firewall-Systeme und ermöglicht gleichzeitig die aktive Verwaltung und Konfiguration der angebotenen Systeme:

- Zentrale Konfiguration der Firewall-Systeme
- Zentrale Konfiguration der VPN Verbindungen
- Gruppierung nach Unternehmen, Land, Stadt usw.



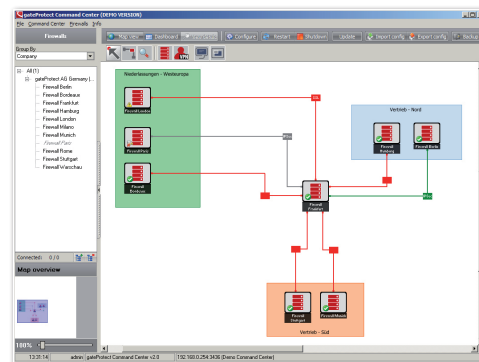
#### Fazit:

Auf diese Weise lässt sich der Zusammenhang zwischen den Firewalls sofort, strukturiert und übersichtlich darstellen. Die Analyse und Pflege des gesamten Netzwerks wird dadurch deutlich vereinfacht.

#### 2. VPN-Verbindungen

Der zentrale Konfigurationsdesktop des Command Center V2 unterstützt die Einrichtung und Verwaltung von VPN-Verbindungen.

- Darstellung aller VPN-Verbindungen
- Komplette Zertifikatsverwaltung
- Erstellen von VPN-Verbindungen
- VPN Wizard
- Unterstützung von IPSec und VPN-SSL

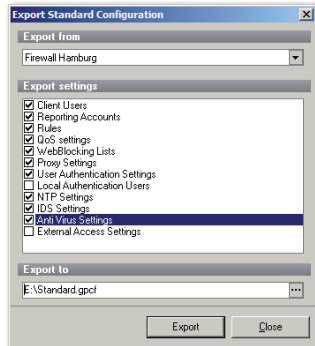


#### Fazit:

Der Administrator hat stets die aktuelle Übersicht der bestehenden VPN-Verbindungen und kann bei Bedarf sofort eingreifen, beispielsweise um eine Verbindung temporär zu trennen oder ggf. neu zu starten.

## 3. Sicherungsdateien (Automatisches Backup)

Das Command Center V2 bietet die Möglichkeit, eine Vielzahl von Profilen zu definieren mit Intervallen, wann Backups gestartet werden sollen, sowie wo diese gespeichert werden sollen (z.B. FTP Server).



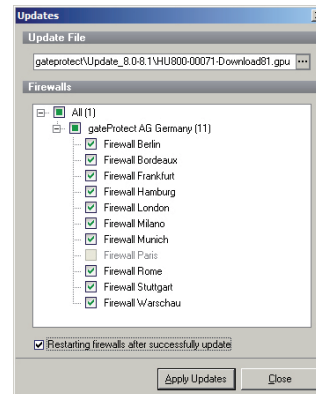
- Erstellen von unterschiedlichen Profilen (Zeit, Benennung usw.)
- Automatische Erzeugung von Backups
- Freie Definition, wann welche Backups wo gespeichert werden sollen (z.B. FTP Server, etc.)

### Fazit:

Das Backup beinhaltet alle Einstellungen und ermöglicht somit bei einem Totalausfall einer Firewall ein Ersatzsystem innerhalb von Minuten wieder in Betrieb zu nehmen.

## 4. Zentrales Einspielen von Updates

Das Command Center erleichtert es, alle gateProtect xUTM und VM Appliances auf aktuellem Stand zu halten. Die von gateProtect gelieferten Updates, Patches und Hotfixes können vom Command Center zentral und automatisch eingelesen und auf ausgewählte Firewalls verteilt werden.

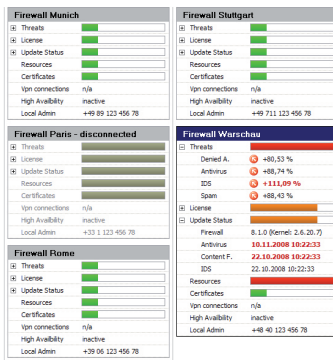


- Hinweis bei neuen Updates\*
- Verteilen von Updates auf alle oder ausgewählte Firewalls
- Update-Status
- Bei Bedarf Auslösen eines Reboots

\*ab Firewall Version 8.5

## 5. Zentrales Berichtssystem / Monitoring

Das zentrale Berichtssystem zeigt alle wichtigen und sicherheitsrelevanten Vorkommnisse, diese werden zudem deutlich gekennzeichnet. Im Folgenden die wichtigsten Monitoringdaten:



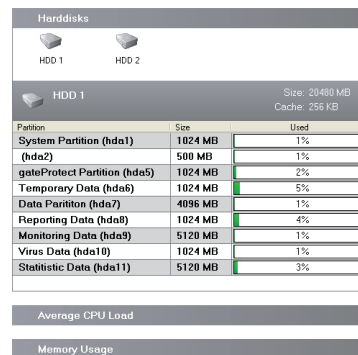
- Firewall Bericht
- IDS- Berichte
- Abgewiesene Zugriffe
- Zugriffsverletzungen
- Gefundene Viren
- Spam-Vorkommen

### Fazit:

Das Berichts- und Monitoringsystem macht rechtzeitig auf drohende Risiken aufmerksam und ermöglicht damit dem Administrator rechtzeitig einzugreifen. Diese Übersicht ist eine notwendige Voraussetzung, um Probleme rechtzeitig zu erkennen und zu analysieren. Für ein nachhaltiges Risikomanagement ist diese Funktion daher unabdingbar und im täglichen Gebrauch von besonderer Bedeutung.

## Hardware Auslastung

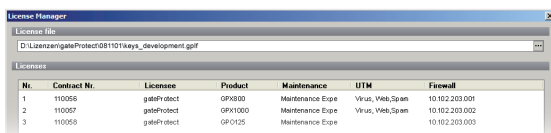
Die Übersicht der Hardware Auslastung zeigt die Betriebszustände der jeweiligen Firewalls zentral und übersichtlich an. Im Folgenden die überwachten Betriebszustände:



- Ressourcen
- Festplattenauslastung
- RAID-Status
- CPU-Auslastung
- Speicherauslastung
- SWAP-Auslastung

## 6. Zentrale Lizenzierung über globale Lizenzdateien

Die Lizenzierung der gateProtect xUTM Appliances erfolgt über globale Lizenzdateien. Lizenzen für einen gesamten Rollout werden gesammelt aus einer Lizenzdatei in das Command Center eingelesen, verwaltet und auf die verschiedenen Firewalls individuell verteilt.



- Eine globale Lizenzdatei für bis zu 500 Firewall-Systeme
- Zentrale Verwaltung aller Lizenzen
- Status der Laufzeitverträge
- Warnung bei falscher Lizenzverteilung

## Hardware-Voraussetzungen

### CPU

INTEL® Dual Core (3.0 GHz)

### Memory

4096 MB

### Hard disk

160 GB HDD (24/7)

Die Einhaltung dieser Hardware-Voraussetzungen ist für den einwandfreien Betrieb des Command Centers unabdingbar.