

>> Nuvaja VP2000

High Security Gateways - Made in Germany

In der globalisierten Welt ist Kommunikation das Rückgrat moderner Unternehmen – und damit zugleich ihr empfindlichster Nerv! Servicemannschaft, mobile Mitarbeiter, Geschäftspartner, Kunden und externe Spezialisten sind es bereits gewohnt, von jedem Ort und zu jeder Zeit auf Datenbestände und Ressourcen im Unternehmensnetz zugreifen zu können. Damit werden sehr hohe Anforderungen an die Sicherheit der Datenverbindung und die Verfügbarkeit der zentralen Kommunikationskomponenten gestellt.

Nuvaja Secure Gateways dienen als Zentralkomponenten der hochsicheren Unternehmenskommunikation, die neben dem Schutz der Daten auch das Bandbreitenmanagement übernehmen. Das Angebot von High Availability Services ist unverzichtbar, um ein Höchstmaß an Verfügbarkeit und Ausfallsicherheit der zentralen Systeme zu garantieren.

Als Hersteller der Nuvaja Secure Gateways orientieren wir uns an den Maßnahmenempfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) für den Aufbau eines mehrstufigen Sicherheitskonzepts.

Darüber hinaus sind wir als aktives Mitglied der Bundesinitiative „IT-Security – Made in Germany“ (ITSMIG) ausschließlich den Schutzinteressen unserer Kunden verpflichtet: Nuvaja Secure Gateways enthalten keine versteckten „Hintertüren“.

Das **Nuvaja Secure Gateway VP2000** lässt sich idealerweise als zentrale Kommunikationsschnittstelle in der unternehmensweiten Sicherheitsarchitektur einsetzen.

Über zwei Mainboards mit separater Stromversorgung in einem Gerät wird eine voll redundante Auslegung der Hardware erreicht, die den Cold-StandBy-Betrieb ermöglicht. Per optional erhältlichem Softwareupdate lässt sich *Failsafe-* und *Load Balancing-Mode* realisieren. Der Failsafe Server kommt dann zum Einsatz, wenn die dauerhafte Verfügbarkeit des Enterprise Servers (Backup-System) sichergestellt werden soll. Für die Tunnelverwaltung über mehrere Server hinweg ist der Load Balancing Mode erforderlich, damit sorgt er einerseits für eine gleichmäßige Auslastung und andererseits für die automatische Ausgliederung eines VPN-Systems im Service- oder Störfall.

Per Option statten Sie die Nuvaja VP2000 als multimandantenfähige, zentral managbare RAS/VPN-Plattform aus – mit allen Vorteilen einer komfortablen zentralen Administration, einfachen Massenrollout-Verfahren, der Abdeckung differenzierter Risikoprofile, der flexiblen Anpassung an geänderte Unternehmensanforderungen.



Abbildung ähnlich

Produktvorteile Nuvaja VP2000

- Zentralkomponente mit bis zu 50 mbps Verschlüsselungsleistung*
- Redundante Hardware
- Cold-Standby, Parallelbetrieb oder als High Availability Solution (Option)
- Unterstützt *Load Balancing-* und *Failsafe-Mode* (Option)
- NCP Secure Enterprise SSL-VPN Server (Option)
- *EasyConfig-Mode*: Einfache Konfiguration via Enterprise Management oder USB-Stick (Option)
- Weboberfläche zur einfachen Basis-konfiguration
- Zentrales Management (Option)
- Strong Authentication

* bei IPSec over TCP/IP, 256bit AES-Verschlüsselung

Entwickeln, Realisieren, Perfektionieren
>> unter diesem Fokus werden spezifische Hardware-Komponenten, Betriebssystem und hochsichere VPN-Software zur ganzheitlichen Lösung Nuvaja Secure Gateway zusammengeführt.

SecurITy
made
in
Germany

VP2000

Securing Remote Access  **nuvaja**
Secure Gateway

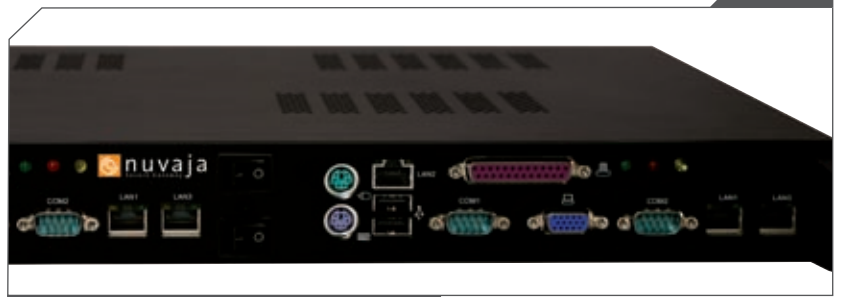


Abbildung ähnlich

Technische Daten

System

CPU	VIA C7 Processor 1.0 GHz
System Indicators	Power / CF / LAN LEDs

Anschlüsse

LAN Port	3x LAN (RJ45)
USB Port	2x USB 2.0
COM Port	RS232

Stromversorgung

Interne Stromversorgung	60W
Power Input	2x DC 12V, 60W/5A

Betriebsumgebung und Gehäuse

Operating Temperature	0 ~ 40 °C (32 ~ 104°F)
Storage Temperature	-20 ~ 75 °C (-4 ~ 167°F)
Relative Humidity	5 - 90% @ 40 °C (104°F), relative humidity, non-condensing
Dimensions	B440 x T310 x H45 mm
Box Dimension	B550 x T420 x H150 mm
Net Weight	6.4 kg

Zertifikat

- CE

Leistungsmerkmale

- Verschlüsselung* bis zu 50 mbps
- Zentral managebar (optional)
- NCP Secure Enterprise SSL-VPN Server (optional)
- Easy configuration & rollout via USB memory stick
- Redundante Hardware
- Cold-Standby, Parallelbetrieb oder als HA-Lösung (optional)

Betriebssystem

- Gehärtetes Linux System auf CF-Karte

Software

- NCP Secure Enterprise Gateway
- Nuvaja WebConfig Interface
- Stateful Inspection Firewall
- PKI Gateway

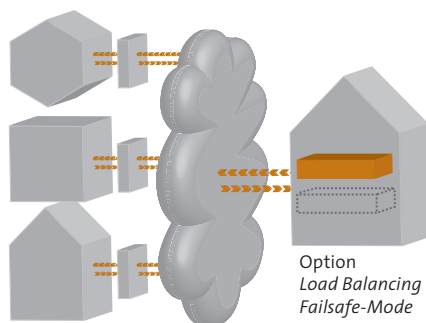
Verschlüsselung

- IPSec (RFC 2401-2409, XAUTH, IKE Config, NAT-T)
- IPSec over L2TP (pre-shared key, certificates, central configuration of IPSec proposals)
- L2Sec (SSL handshake, TLS/EAP, RFC 2716, SSLCP with or without certificate)

Technische Änderungen vorbehalten.

Einsatzempfehlung VP2000

Decentral Gateway Internet Central Gateway



Ihr Ansprechpartner

Securing Remote Access  **nuvaja**
Secure Gateway