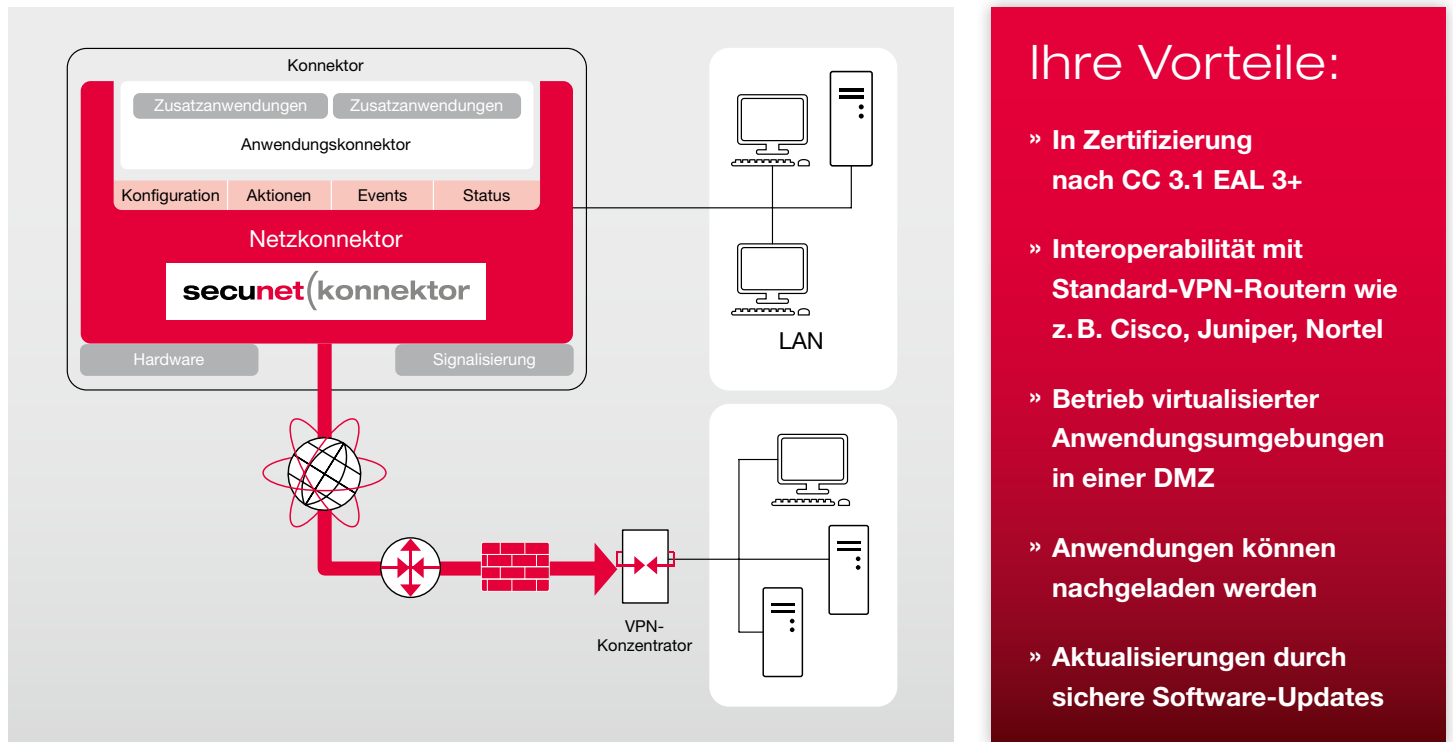


Software VPN-Appliance der besonderen Art



Der konnektor von secunet ist der Vertrauensanker zur sicheren Kommunikation mit zentralen Infrastrukturen. Neben dem effektiven Schutz der Daten bei der Übertragung sowie der angeschlossenen lokalen Netze bietet die Software VPN-Appliance eine sichere Ausführungsplattform für Anwendungen. Hierbei ermöglicht der Einsatz von Virtualisierungstechnologien den unabhängigen Betrieb mehrerer Anwendungen. Der secunet konnektor verwendet die Sicherheitsfunktionen der Hochsicherheitslösung SINA, die secunet gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik entwickelt hat. SINA ist seit mehr als 10 Jahren in vielen Behörden und Unternehmen erfolgreich im Einsatz.

Als zentraler Vertrauensanker garantiert der secunet konnektor den sicheren Betrieb von Anwendungen – dies unterscheidet ihn von herkömmlichen VPN-Appliances. Die bewährten Sicherheitsmechanismen schützen hierbei die angeschlossenen lokalen Netze genauso wie die Anwendungen vor Bedrohungen von außen. Der Betrieb der Anwendungen in virtualisierten Umgebungen garantiert eine strikte Trennung voneinander, diese Architektur sorgt für ein maximales Sicherheitsniveau. Mit dem sicheren Software-Update-Mechanismus ist das Nachladen von Anwendungen und Aktualisieren von Softwarekomponenten jederzeit möglich. Die Sicherheitseigenschaften können lokal wie zentral gesteuert und bei Bedarf remote vom jeweiligen Diensteanbieter aktualisiert werden. Die vom Konnektor unterstützten Standard-VPN-Schnittstellen stellen die Interoperabilität mit etablierten VPN-Routern sicher. Der secunet konnektor kann bedarfsgerecht auf unterschiedlichen Hardware-Plattformen betrieben werden.

In den **Telematikinfrastrukturen** des Gesundheitswesens schützt der secunet konnektor beispielsweise die hochsensiblen Daten der Ärzte und Versicherten. Die Appliance ist aber auch für weitere Anwendungsszenarien eine hervorragende Lösung:

- Als **De-Mail Konnektor** ermöglicht er die einfache Integration zum Versand und Empfang von **De-Mails** in der vorhandenen E-Mail-Infrastruktur
- Als vertrauenswürdige Plattform dient er zum Schutz und zur sicheren Ausführung von Anwendungen in ungeschützten Umgebungen (**Automotive**)

Daten und Fakten

VPN	
Typ	L2TP over IPSec
Standards	RFC 1334 (PAP), RFC 1994 (CHAP), RFC 2406 (ESP), RFC 2407 (The Internet IP Security Domain of Interpretation for ISAKMP), RFC 2408 (ISAKMP), RFC 2409 (IKE), RFC 2451 (ESP CBC-Mode), RFC 2661 (L2TP/PPP over IPSec), RFC 3602 (AES-CBC), RFC 3706 (Dead Peer Detection), RFC3947 (NAT-Traversal in the IKE), RFC3948 (UDP Encapsulation of IPSec ESP Packets)
Authentisierung	Smartcard-basiert, RSA 1024/2048 Hashfunktionen: SHA1 bis SHA2-Familie
Verschlüsselung	AES-256 (symmetrisch) HMAC SHA1
Schlüsselaustausch	Diffie Hellman Gruppe 5 (Modulus 1536)
Zertifikate	X.509v3, BridgeCA, Trusted-Component-List (TCL), CRL
Interoperabilität	Cisco, Juniper, Nortel, OpenSwan, FreeSwan, StrongSwan
Unterstützung für Accounting	L2TP/PPP over IPSec mit PAP, CHAP, MS-CHAP, EAP
IPSec-Mode	Transportmode, Tunnelmode (optional)
Anzahl der Tunnel	> 50 parallele Tunnel
Durchsatz	> 20 MBit (Voraussetzung 1 GHz CPU, 512 MB RAM)
Netzwerk	
Protokolle	IPv4, NAT, PPPoE
NAT	NAT-Traversal für IPSec
Separierung	Trennung der Netze in LAN, WAN, DMZ
Firewall	Stateful Inspection Firewall mit getrennten Regeln für LAN, WAN, DMZ
Routing	Policy-basiertes Routing
Dienste LAN	DHCP Client, DHCP Server, DNS Client, DNS Server, NTP Server (Draft-IETF-NTPv4)
Genutzte Infrastruktur	DHCP Client, DNS Client, NTP Client
WAN-Verbindung	Router, DSL-Modem, direkter Netzanschluss
Paketgröße	Adaption über Management (MTU und MSS) möglich
Hochverfügbarkeit	CARP, bis zu 4 Geräte im Cluster

Zulassung	
Gematik	On- und Offline, ProOnlineVSDD
Common Criteria	CC 3.1 EAL 3+ (in Bearbeitung, ZertID liegt vor)
Schnittstellen	
Netzwerk	Ethernet IEEE 802.3
Management	SOAP Schnittstelle (Zugriff via http/https)
Management	
Konfiguration	XML-basierte Konfiguration mit automatischer Validierung, separates Konfigurationsset als Default, permanenter Konfigurations- und Protokollspeicher
Status	Systemstatus und Protokollierung via Managementschnittstelle
Events	Events über die Managementschnittstellen via CERP
Nutzung	Lokales Management (Web-Management) Fernwartung (SOAP-Schnittstelle via http/https)
Hardwareanforderungen	
Prozessor	X86-kompatibler Prozessor (>= 800 MHz)
Hauptspeicher	Mindestens 512 Mbyte
Datenspeicher	Mindestens 1 Gbyte (HDD, CF, SDD)
Netzwerk	2 x Ethernet IEEE 802.3 (3 x für erweiterte Anwendungen)
Kartenleser	Integrierter Kartenleser
USB	Mindestens 2 externe USB-Anschlüsse (inklusive USB Bootoption)
RTC	Echtzeituhr mit einem Fehllauf von +/- 20ppm
ACPI	ACPI Zustände S0 (Working) und S5 (Soft off)
BIOS	Standard BIOS oder coreboot (vormals LinuxBios) mit sicheren BIOS Bootprozess
Treiber	Linux Treiber (Kernel 2.6.2x) für alle Komponenten
Betrieb	
Installation	Automatische Installation
Software-Update/Recovery	Manuelles oder automatisches Software-Update aller Komponenten einschließlich Konfigurationsupdate, Fall- und Rollback auf vorherigen Software- und Konfigurationsstand im Fehlerfall
Backup/Recovery	Sicherung und Wiederherstellung der Konfiguration über Managementschnittstelle möglich

Der secunet konnektor kann für unterschiedlichste Hardwareplattformen realisiert werden:



Weitere Informationen:
www.secunet.com/konnektor

secunet

secunet Security Networks AG
Kronprinzenstraße 30
45128 Essen

Tel.: +49-201-54 54-0
Fax: +49-201-54 54-1000
E-Mail: info@secunet.com
www.secunet.com