



GeNUCard 2

Mobile Security Device

Technische Informationen



Inhaltsverzeichnis

1 GeNUCard: Mobile Security Device	1
1.1 Problemstellung.....	1
1.2 Lösungsansätze.....	1
1.3 Anforderungen an ein Sicherheitspaket für externe Clients.....	1
2 Die Lösung: Die GeNUCard	2
2.1 Autarkes, umfassendes Mobile Security Device.....	2
2.2 Einfache Bedienung.....	3
2.2.1 Kompatibilität.....	3
2.2.2 Windows Tray App.....	3
2.2.3 Anwenderinformation.....	3
2.3 Authentisierung.....	3
2.3.1 Smartcard.....	3
2.3.2 Keyserver.....	4
2.4 Stateful Packet Filter für Firewall-Funktionen.....	4
2.5 Sichere VPN-Datenkommunikation.....	5
2.5.1 Standard IPsec-Betriebsart (Layer 3).....	5
2.5.2 VPN über SSH-Port Forwarding (Layer 4).....	5
2.6 Bandbreiten-Management.....	6
2.7 Komfortable Administration.....	6
2.8 Investitionssicherheit durch IPv6-Integration.....	7
3 Zulassung	7
4 Hardware	7
4.1 Gehäuse.....	7
4.2 Schnittstellen.....	8
5 Einsatzszenarien	8
5.1 Sichere Internetverbindung mit der GeNUCard.....	8
5.2 Remote-Zugriff auf Unternehmensdaten via VPN.....	8
6 Support	9
6.1 Einführung.....	9
6.2 Laufender Betrieb – Software Support.....	10
6.3 Support von Vertriebspartnern.....	10
7 Glossar	11



1 GeNUCard: Mobile Security Device

Diese Informationsbroschüre richtet sich an IT-Sicherheitsverantwortliche, die für die externe bzw. mobile IT-Infrastruktur und deren Absicherung zuständig sind.

Sie bietet Ihnen einen kompakten Überblick, wie Sie mit Hilfe des Mobile Security Device Mitarbeitern außerhalb des Unternehmens Zugriff auf Firmendaten im LAN gewähren können, ohne dass die IT-Sicherheit im gesamten Unternehmensnetzwerk gefährdet wird.

1.1 Problemstellung

In einer globalisierten Arbeitswelt steigt der Anteil reisender Mitarbeiter, die von unterwegs per Laptop auf Geschäftsdaten zugreifen. Die Verbindungen werden flexibel über alle heute möglichen Wege aufgebaut: Ethernet, WLAN, Mobilfunk oder aus abgelegenen Regionen sogar via Satellitenstrecken.

Ein weiterer Aspekt ist die zunehmende Zahl von Home Office-Arbeitsplätzen. Glaubt man Prognosen, so werden zukünftig immer mehr Büros regelmäßig leer stehen und unsere Zusammenarbeit zunehmend per E-Mail, Groupware und Online-Konferenzen stattfinden.

Der technische Fortschritt ermöglicht diese mobile und dezentralisierte Arbeitsweise. Doch diese Entwicklung schafft auch Probleme: Immer öfter liegen Netzwerkzugänge außerhalb des Firmennetzes, und das unsichere Internet dient als Kommunikationsmedium für E-Mail und Datenbankzugriffe sowie Workflow- und Synchronisationsprozesse.

Damit reicht es nicht mehr aus, das interne LAN mit einer Firewall abzuschotten. Auch die externen Clients und deren Zugriffe auf die interne IT-Infrastruktur müssen sicher abgeschirmt werden. Denn ohne effektive Schutzmaßnahmen drohen finanzielle Schäden, der Verlust von Kundenvertrauen sowie Strafen wegen Vernachlässigung gesetzlicher Bestimmungen.

1.2 Lösungsansätze

In vielen Fällen begegnen Organisationen diesem Problem mit Security-Komplettpaketen. Diese werden auf einem Client installiert und filtern den ein- und ausgehenden Datenverkehr. Doch diese Lösungen bieten keine zuverlässige Sicherheit: Einerseits lassen sich die Regeln der Anwendung umgehen, andererseits ist das Security-Komplettpaket auf einem kompromittierten Betriebssystem nicht mehr in der Lage, einwandfrei zu funktionieren. Weitere Aspekte eines „Rundum-Schutzes“, wie z. B. eine sichere Datenkommunikation, bleiben bei diesen Lösungen häufig außen vor.

1.3 Anforderungen an ein Sicherheitspaket für externe Clients

Eine Sicherheitslösung für Clients, mit denen von außen auf das Netzwerk einer Organisation zugegriffen werden kann, sollte folgende Anforderungen erfüllen:



- Die Sicherheitslösung ist kein integraler Bestandteil des zu schützenden Rechners. Sie besitzt ein eigenes, gehärtetes Betriebssystem und ihre Funktionalität wird bei Störungen des Rechners nicht beeinträchtigt.
- Die Sicherheitslösung ist sofort startklar und einfach zu bedienen.
- Anwender können sich eindeutig authentisieren.
- Eine Firewall beschränkt die Kommunikation auf zulässige Verbindungen.
- VPN gewährleistet einen verschlüsselten Datenaustausch über öffentliche Netze.
- Intelligentes Bandbreitenmanagement ermöglicht priorisierte Anwendungen.
- Die IT-Sicherheitsrichtlinie des Unternehmens kann fortlaufend gegenüber allen externen Clients zentral administriert und durchgesetzt werden.
- Als zukunftssichere Investition unterstützt die Sicherheitslösung den Standard IPv6.

2 Die Lösung: Die GeNUCard

Anhand dieses Anforderungskatalogs hat GeNUA die GeNUCard entwickelt. Sie erfüllt alle aufgeführten Anforderungen und bietet darüber hinaus weitere Vorteile.

2.1 Autarkes, umfassendes Mobile Security Device

Die GeNUCard bietet Ihnen eine physikalische Trennung von Mobile Security Device und Computer: Die Sicherheitsanwendungen sind nicht auf dem Client installiert, den sie schützen sollen, sondern auf einem autarken Device. Die GeNUCard bleibt selbst dann voll wirksam, wenn der zu schützende Rechner durch unvorsichtigen Umgang bereits kompromittiert sein sollte. So ist Ihnen die starke Sicherheitsleistung für Ihre IT genau zum entscheidenden Zeitpunkt garantiert – im Ernstfall.



GeNUCard – Mobile Security Device für Laptops



Ein wichtiges Merkmal der GeNUCard ist zudem, dass alle Sicherheitsanwendungen wie Paketfilter, Verschlüsselungsfunktionen und Authentisierungsmethoden aufeinander abgestimmt sind. Konflikte, die der Einsatz von Sicherheits-Software verschiedener Hersteller verursachen kann, werden vermieden.

Ein weiterer Pluspunkt: Die GeNUCard ist ein eigenständiger Rechner mit eigenen Interfaces. Durch das Konzept eines autarken Systems mit eigenem Prozessor und Speicher werden keine Ressourcen des geschützten Clients beansprucht, während Sicherheits-Software erhebliche Leistungseinschränkungen verursachen kann.

2.2 Einfache Bedienung

Sobald die GeNUCard via USB an einen Rechner angeschlossen ist, schützt sie diesen vor Gefahren aus dem Internet. LED-Anzeigen informieren den Anwender über Systemzustand und Verbindungsstatus.

2.2.1 Kompatibilität

Die GeNUCard unterstützt die Betriebssysteme Windows XP (ab SP3), Windows Vista, Windows 7 und Linux (ab Kernel 2.6).

2.2.2 Windows Tray App

Um die Verwendung von GeNUCard unter Windows zu erleichtern, ist eine native Windows-Applikation erhältlich. Diese ist im sog. Tray (Benachrichtigungsfeld neben der Uhr) zu finden und bietet folgende Funktionen/Anzeigen:

- System: Uptime, Software-Version, Hardware-Version
- Internet: Status, Verbinden und Trennen von Internet-Profilen
- VPN: Status, Verbinden und Trennen von VPN-Profilen
- Host: Benutzer, Software-Version, Screensaver/Sleep-Status

2.2.3 Anwenderinformation

Auf der Central Management Station GeNUCenter (siehe Kapitel 2.7) lassen sich Meldungen hinterlegen, die dem Anwender der GeNUCard angezeigt werden. Dabei erfolgt die Anzeige sowohl im Web-GUI als auch mittels Tray App unter Windows. So kann z. B. über geplante Wartungen informiert werden.

2.3 Authentisierung

2.3.1 Smartcard

Zur Authentisierung werden Identität und Zugriffsberechtigung überprüft: Anwender stecken die GeNUCard mit Smartcard an den Rechner und geben eine PIN (Personal Identification Number) ein. Nur wenn beide Sicherheitsmerkmale erfüllt sind, kann eine Verbindung ins Firmennetz aufgebaut werden.



2.3.2 Keyserver

Ab einer Stückzahl von etwa 1.000 Einheiten der GeNUCard und je nach Nutzerverhalten empfehlen wir den Einsatz eines zentralen Keyserver zusätzlich zur zentralen Firewall & VPN-Appliance GeNUScreen anstatt von Smartcards, um Wartezeiten der Anwender zu vermeiden. Der Keyserver übernimmt die Funktionalität der Smartcards, ist in großen Setups jedoch um Größenordnungen schneller. Damit können VPN-Infrastrukturen mit einer vierstelligen Anzahl von Außenstellen äußerst performant realisiert werden.

2.4 Stateful Packet Filter für Firewall-Funktionen

Die integrierte Firewall der GeNUCard ist als Stateful Packet Filter ausgelegt. Im Gegensatz zu zustandslosen Paketfiltern kann diese Lösung Pakete als Teil einer aktiven Session wahrnehmen.

Kommunizieren zwei Rechner über einen *zustandslosen Paketfilter*, müssen die Filterregeln den Datenaustausch generell in beide Richtungen zulassen – für die Anfrage von Rechner A und das entsprechende Antwortpaket von Rechner B. In diesem Fall erlauben die Filterregeln B auch dann eine Sendung an A, wenn A überhaupt keine Anfrage gestellt hat. Damit birgt das Regelwerk ein erhebliches Sicherheitsrisiko.

Der *Stateful Packet Filter* der GeNUCard merkt sich anhand bestimmter Merkmale, die schwer vorzutäuschen sind, den Verlauf der Kommunikation. Stellt Rechner A eine Anfrage an Rechner B, so darf B lediglich auf diese Anfrage antworten. Diese Lösung lässt somit keine Sicherheitslücke zu.

Die Paketfilter-Firewall der GeNUCard bietet folgende Features:

Stateful Tracking

Die individuellen Verbindungen werden anhand verschiedener Kriterien kontrolliert, wie

- Anzahl der Verbindungen pro Source IP-Adresse
- Anzahl der Verbindungen pro Zeitintervall
- Anzahl von Source IP-Adressen, die Verbindungen aufbauen

Filtern anhand von TCP-Flags

TCP-Pakete können anhand ihrer jeweiligen Statusindikatoren überprüft und gefiltert werden.

DOS-Schutz

Bei Denial of Service-Attacken werden von einer IP-Adresse unvollständige TCP-Verbindungen aufgebaut. Die GeNUCard wehrt derartige Angriffe ab, indem sie Pakete erst weiterreicht, nachdem eine vollständige TCP-Verbindung etabliert wurde.



2.5 Sichere VPN-Datenkommunikation

Zur sicheren Datenübertragung über das Internet können mit der GeNUCard performante VPN-Verbindungen aufgebaut werden. Es kommen ausschließlich starke Verschlüsselungsalgorithmen und große Schlüssellängen zum Einsatz.

Es gibt folgende Möglichkeiten, VPN-Netze aufzubauen:

- VPN-Tunnel mit IPsec im Tunnel- und Transport-Mode (Layer 3)
- VPN-Tunnel für TCP-Verbindungen über SSH (Layer 4)

Dabei stehen verschiedene kryptografische Alternativen zur Auswahl:

- Asymmetrische Verschlüsselungsalgorithmen: Diffie-Hellman
- Symmetrische Verschlüsselungsalgorithmen: AES, 3DES
- Prüfsummenverfahren (Hashcodes) zur Authentizitätsprüfung von Datenpaketen, Nachrichten und VPN-Verbindungen: SHA2, SHA1, MD5
- Default: AES-192, SHA 2-256

2.5.1 Standard IPsec-Betriebsart (Layer 3)

Die GeNUCard kann als Layer 3-basiertes IPsec-Gateway eingesetzt werden. Bei IPsec wird pro Host bzw. Netz, das verschlüsselt kommuniziert, eine Security Association (SA) ausgehandelt. Dabei gilt: Je mehr SAs, desto höher die Beanspruchung der VPN-Ressourcen. Kommt es zu einer Überlastung, spricht man von einer SA-Krise.

Da ein Client mit GeNUCard nur ein Netzwerk darstellt, ist die Gefahr einer Überlastung geringer als im Rahmen gewöhnlicher Netzkopplungen. Sollen jedoch viele Netzwerke auf der Gegenseite mit der GeNUCard und zusätzlich mehrere GeNUCards untereinander verbunden werden, wird eine SA-Krise wahrscheinlicher.

Um einem resultierenden Ressourcen-Engpass am VPN-Gateway vorzubeugen, kann der Network Mode verwendet werden: Dabei wird eine IPsec-Verbindung hergestellt, die durch IP-in-IP-Tunnel (Gateway-to-Gateway) im Transport Mode betrieben wird.

Die Kommunikationspartner der GeNUCard werden im Network Mode nicht mehr einzeln angesprochen, sondern hinter dem Ziel-Gateway zu Gruppen zusammengefasst. Dadurch sinkt die Anzahl der auszuhandelnden SAs erheblich zugunsten einer besseren Performance und Skalierbarkeit.

2.5.2 VPN über SSH-Port Forwarding (Layer 4)

SSH (Secure Shell) bietet die Möglichkeit, TCP-Verbindungen authentisiert und verschlüsselt zu tunneln.

Authentisierung und Verschlüsselung erfolgen dabei mit kryptografisch starken Algorithmen, die der Qualität von IPsec in keiner Weise nachstehen. Das SSH-Protokoll lässt sich jedoch deutlich flexibler als IPsec einsetzen, z. B. für Verbindungen über Firewalls und NAT-Router hinweg.

Zum einen erhöht eine derartige personenbezogene Komponente die Hürde eines missbräuchlichen Zugriffs und zum anderen lässt SSH die Weiterleitung von TCP-Verbin-



dungen nur durch ausdrücklich freigeschaltete Tunnel zu. Da keine „geroutete“ Verbindung besteht, weist diese Betriebsart gegenüber IPsec ein zusätzliches Sicherheitsmerkmal auf.

2.6 Bandbreiten-Management

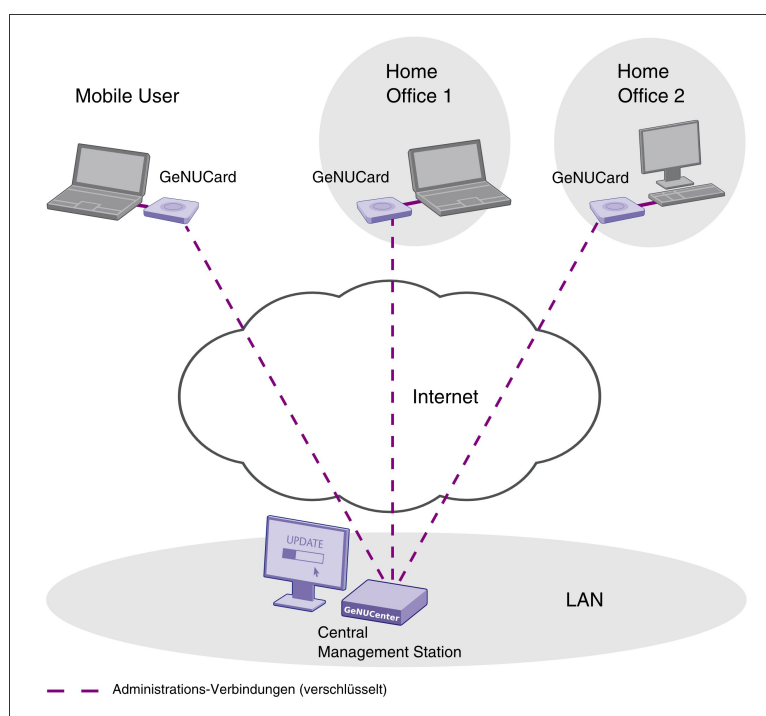
Die Firewall der GeNUCard kann auch mit Sprache umgehen und das verbreitete VoIP-Protokoll SIP absichern. Ihr ausgefeiltes Bandbreiten-Management mit Alternative Queuing (ALTQ) sorgt dabei für eine zuverlässige Performance: Basierend auf den Kriterien Source- und Destination-Adresse sowie Port und Protokoll werden Pakete unterschiedlichen Warteschlangen zugeordnet. So können Sie z. B. für VoIP die erforderliche Bandbreite reservieren. Auch andere wichtige Protokolle können auf Wunsch beim Datentransfer bevorzugt werden.

2.7 Komfortable Administration

Die GeNUCard bietet verschiedene Möglichkeiten der Administration:

Der Benutzer hat die Möglichkeit, elementare Einstellungen der GeNUCard, wie z. B. die Konfiguration einer Bluetooth-Verbindung zu einem Mobiltelefon, selbstständig am jeweiligen Rechner über ein lokales GUI vorzunehmen.

Die Konfiguration, Administration und Überwachung mehrerer Devices erfolgt komfortabel mit der Central Management Station GeNUCenter. Änderungen, Updates und Patches können über praktische Gruppierungs-Funktionen gleichzeitig auf beliebig viele Devices übertragen werden.



Zentrales Management mit GeNUCenter



Mit GeNUCenter ist auch die konsequente Durchsetzung von Sicherheitsrichtlinien bezüglich Firewall und VPN-Einwahl bei allen Clients möglich, die sich im externen Einsatz befinden. In wachsenden Installationen können die zusätzlichen Devices ganz einfach in die Central Management Station integriert und mit bewährten Konfigurationen ausgestattet werden.

2.8 Investitionssicherheit durch IPv6-Integration

Das rapide Wachstum des Internets führt zusammen mit den Beschränkungen von IPv4 zu Engpässen, die durch IPv6 beseitigt werden sollen. Mit der Erweiterung der Adresskapazitäten wurde auch die Chance genutzt, das Internet Protocol an moderne Erfordernisse anzupassen.

Die Umstellung des Internets auf IPv6 läuft bereits und wird sich in den kommenden Jahren beschleunigen. Inzwischen gibt es bereits Bereiche, die nur mittels IPv6 erreichbar sind, andere Teile, die über beide Protokolle angebunden sind, und große Teile, die ausschließlich auf IPv4 basieren.

Dies hat Konsequenzen für Ihre IT-Infrastruktur: So müssen z. B. für IPv6 die Filterregeln für Firewalls neu erstellt werden. Eine Firewall, die nicht für den Umgang mit IPv6 ausgelegt ist, wird in der Regel IPv6-Datenverkehr nicht bemerken und durchlassen.

Mit Blick auf diese Entwicklung bieten wir mit der GeNUCard eine Lösung, die sicher mit IPv4 und IPv6 umgehen kann – Sie tätigen eine Investition in ein Produkt, das sowohl heutigen als auch zukünftigen Standards entspricht.

3 Zulassung

Die GeNUCard 1.1 ist für den verschlüsselten Datenversand via IPsec-VPN vom BSI für den Geheimhaltungsgrad VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) zugelassen, ebenso für NATO Restricted, UE Restreint und OCCAR Restricted.

Auch die GeNUCard 2.0 wird das Zulassungsverfahren beim BSI durchlaufen. Für weitere Informationen zum Thema Zulassung nehmen Sie bitte Kontakt mit uns auf. Wir beraten Sie umfassend.

4 Hardware

4.1 Gehäuse

Die GeNUCard zeichnet sich durch ein attraktives, robustes Gehäusedesign aus. Dabei gewährleistet der Anschluss via USB die Kompatibilität zu praktisch allen Rechnern.



4.2 Schnittstellen

Die GeNUCard ist mit den folgenden Schnittstellen ausgestattet:

- Ethernet
- WLAN
- UMTS (inkl. SIM-Karten-Slot)
- USB (für Datenübertragung und Stromversorgung)
- Smartcard Reader

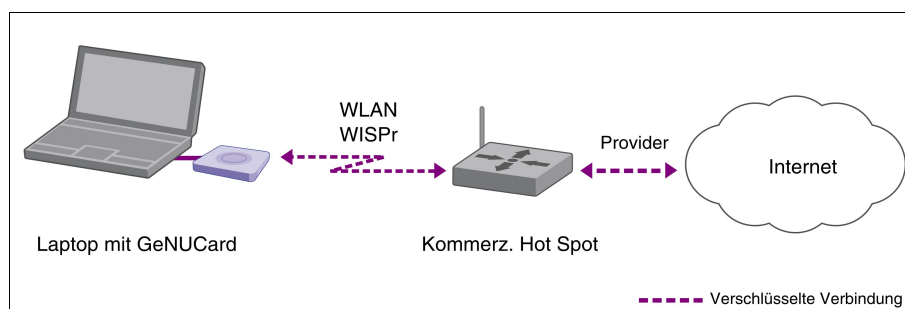
Damit bietet sie in jeder denkbaren Konstellation flexible Kommunikations- und Anschlussmöglichkeiten.

5 Einsatzszenarien

5.1 Sichere Internetverbindung mit der GeNUCard

Das Beispiel zeigt den Aufbau einer verschlüsselten Verbindung zum Internet mit der GeNUCard an einem kommerziellen Hot Spot.

Der Anwender authentisiert sich und konfiguriert über das lokale GUI eine WLAN-Verbindung zu einem kommerziellen Hot Spot. Beim Provider authentifiziert er sich über das WISPr-Protokoll. Dieser stellt daraufhin eine Verbindung zum Internet her. Die integrierte Firewall der GeNUCard schützt dabei den Laptop vor unerlaubten Zugriffen von außen.

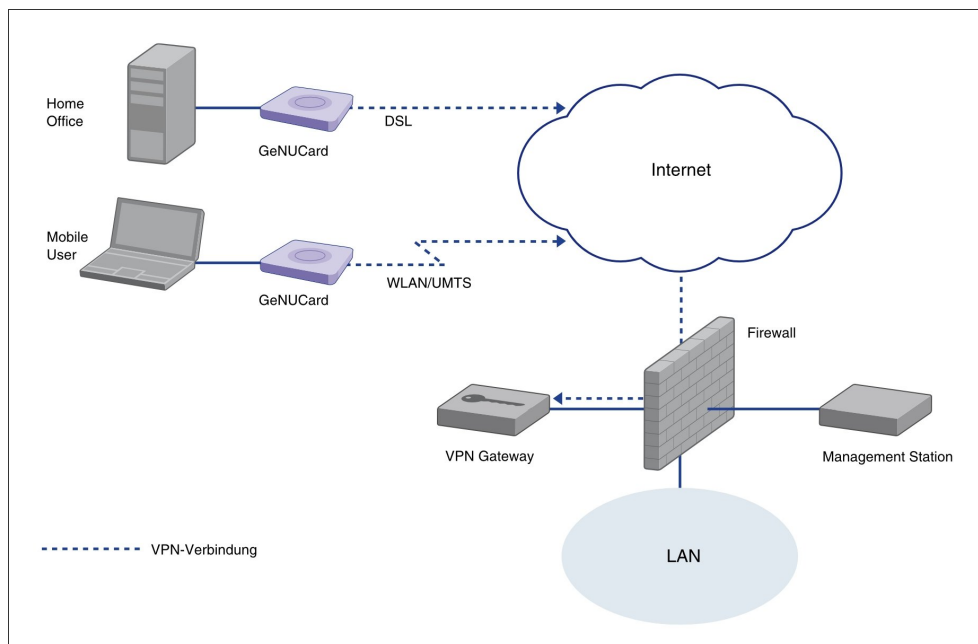


Sichere Internetverbindung mit der GeNUCard

5.2 Remote-Zugriff auf Unternehmensdaten via VPN

Im Folgenden greifen Mitarbeiter, die sich außerhalb des Firmennetzes befinden, über öffentlich zugängliche Übertragungsnetze auf Daten zu, die sich innerhalb des geschützten Firmennetzes (LAN) befinden.

Dazu werden sowohl die Home Office-Rechner als auch die Laptops mobiler User mit GeNUCards ausgestattet. Zur Authentifizierung erhalten die Mitarbeiter eine Smartcard und eine PIN. Als Übertragungsverfahren kommen DSL, UMTS und WLAN zum Einsatz.



Verschlüsselter LAN-Zugang mit externen Endgeräten

Durch die GeNUCard werden verschlüsselte Verbindungen – Virtual Private Networks (VPN) – aufgebaut, mit denen der öffentliche Bereich sicher überbrückt wird. Auf diese Weise können Daten komfortabel und zuverlässig abgeschirmt via Internet ausgetauscht werden.

Die GeNUCard ist kompatibel zu weiteren IT-Sicherheitslösungen von GeNUA:

- Firewall GeNUScreen
- VPN-Appliance GeNUCrypt

Sie lässt sich zusammen mit diesen Produkten in spezifische Anwendungen einbinden.

6 Support

6.1 Einführung

Installations- und Konfiguration-Service: GeNUA und spezialisierte Vertriebspartner unterstützen Sie auf Wunsch bei der Installation, Konfiguration und Inbetriebnahme der Sicherheitslösung GeNUCard und der Management Station GeNUCenter. Dabei werden die Administratoren ausführlich in die Benutzung und Pflege des Systems eingewiesen.

Anfangs-Support: Die GeNUCard ist so dokumentiert, dass die Inbetriebnahme und der laufende Betrieb keinerlei Schwierigkeiten bereiten sollten. Wenn Sie dennoch Fragen haben oder auf Schwierigkeiten stoßen, steht Ihnen unsere Hotline kostenlos 14 Tage lang zur Verfügung.



6.2 Laufender Betrieb – Software Support

Update Service: Die GeNUCard wird ständig weiterentwickelt. Regelmäßig erscheinen neue Versionen, in denen aktuelle Entwicklungen aufgegriffen werden und der Funktionsumfang sinnvoll ergänzt wird. Je nach Bedarf erscheinen zusätzlich Zwischenversionen.

Unser Update-Service sichert Ihnen die automatische Lieferung der neuesten Versionen und Zugriff auf unsere komplette Patch-Datenbank.

Hotline: Zusätzlich zu unserem Update Service bieten wir deutsch- und englischsprachigen Support via Telefon und E-Mail. Sie können unsere Hotline für alle Fragen zu Ihrer Lösung mit der GeNUCard nutzen. Der telefonische Hotline Support steht Ihnen auf Wunsch 24 Stunden an allen Tagen zur Verfügung.

Security System Management: Diese Leistung umfasst die ständige Überwachung und Wartung unserer Lösungen, die bei Kunden für IT-Sicherheit sorgen, über stark verschlüsselte Internet-Verbindungen.

6.3 Support von Vertriebspartnern

Support-Leistungen von Vertriebspartnern: Viele autorisierte Vertriebspartner von GeNUA bieten zum Teil erweiterte Support-Optionen an, z. B. Vor-Ort-Austauschservice von Hardware innerhalb garantierter Maximalzeiten.

GC-WP-0312-11-D

So erreichen Sie uns:

GeNUA mbH, Domagkstraße 7, 85551 Kirchheim bei München
tel +49 89 991950-0, fax +49 89 991950-999, info@genua.de, www.genua.de



7 Glossar

IPsec	Internet Protocol Security – Sicherheitsprotokoll, das bei der Kommunikation über IP-Netze Vertraulichkeit, Authentizität und Integrität gewährleisten soll. Es kann zum Aufbau von virtuellen privaten Netzwerken (VPN) verwendet werden.
PFL	Paketfilter: Firewall, die auf der Basis von IP-Adressen und Portnummern Filterregeln umsetzt. Ist die Verbindung nach den Regeln zulässig, lässt der PFL die Daten der Verbindung wie ein Router passieren. Angriffe auf IP-Ebene kann ein PFL daher nur abwehren, wenn zusätzliche Schutzmechanismen greifen. So genannte „Stateful Inspection“ gewährt zusätzlichen Schutz. Ein klassischer PFL hat keinen Zugriff auf Anwendungsdaten und kann daher keine Angriffe auf Anwendungsebene (z. B. Viren) erkennen.
SSH	Secure Shell – Netzwerkprotokoll, mit dem sicher eine verschlüsselte Netzwerkverbindung zu einem entfernten Computer hergestellt werden kann.
TCP	Transmission Control Protocol – Netzprotokoll für eine zuverlässige Übertragung, die verbindungs- und stromorientiert ist
Smartcard	Hardware-Komponente, die Teil eines Systems zur Identifizierung und Authentisierung von Benutzern ist.
Transport Mode	Im Transport Mode kommunizieren zwei Hosts direkt via Internet miteinander. Dabei gewährleistet IPsec die Authentizität und Integrität der Daten. Per Verschlüsselung lässt sich zudem verhindern, dass Unbefugte die transportierten Inhalte mitlesen. Da die Kommunikation über ein frei zugängliches Netz stattfindet, lassen sich jedoch Ursprung und Ziel des Datenstroms nicht verschleiern.
Tunnel Mode	Der Tunnel Mode kommt zum Einsatz, wenn zumindest einer der beteiligten Rechner nicht direkt angesprochen, sondern als Security Gateway genutzt wird. In diesem Fall bleibt der Kommunikationspartner hinter dem Gateway anonym. Tauschen gar zwei Netze über ihre Security Gateways Daten aus, dann lässt sich von außen gar nicht mehr bestimmen, welche Rechner miteinander kommunizieren. Es lassen sich Authentisierung, Integritätskontrolle und Verschlüsselung einsetzen.



VPN

Virtual Private Network – Technik zur Verbindung externer Rechner mit einem lokalen Netzwerk, bei der das Internet als Transportmedium dient. Die Daten werden dabei verschlüsselt.