
Virtuelle Private Netze

mit IPSec

Zusammenfassung

Durch die Bereitstellung moderner Kommunikationsstrukturen werden Organisation und Durchführung von Geschäftsabläufen in Unternehmen verändert. Eine zentrale Rolle kommt dabei der standortübergreifenden Vernetzung zugute, die immer häufiger auf den Vorteilen des globalen Internets aufsetzt. Virtuelle Private Netze (VPNs) stellen einen Lösungsansatz dar, mit dem sich die aus den lokalen Netzwerken bekannten Zugriffsstrukturen über ein unsicheres Medium realisieren lassen. Die Einbeziehung des Internets in die interne Kommunikation eines Unternehmens deckt jedoch spezielle Sicherheitsaspekte - wie z. B. Schutz der Privatsphäre, Datenintegrität oder Authentifizierung - von Systemen und Benutzern nur unzureichend ab. Erst Erweiterungen wie IPSec ermöglichen die sichere Kommunikation zwischen Standorten auf Basis eines unsicheren Netzes.

Inhaltsverzeichnis

1	Grundbausteine der Unternehmenssicherheit	3
1.1	Neue Kommunikationsformen.....	4
1.2	Virtuelle Private Netze	5
2	Sicherheitsanforderungen.....	5
2.1	Verlust der Privatsphäre	5
2.2	Veränderung der Datenintegrität.....	6
2.3	Einspeisung verfälschter Datenströme	7
2.4	Einstellung des Dienstes.....	8
3	Virtuelle Private Netze mit IPSec	8
4	Die Bintec VPN Access Serie	11

1 Grundbausteine der Unternehmenssicherheit

Zu den Grundpfeilern einer jeden Unternehmensstrategie gehört im Zeitalter des modernen Informationsaustausches auch eine entsprechende Richtlinie für die Unternehmenssicherheit. Hier gilt es, die notwendigen Regelwerke für die verschiedensten Zugriffsmöglichkeiten mit den Sicherheitsanforderungen zu verknüpfen. Kommunikationspfade heutiger Netze erstrecken sich über unterschiedliche Applikationen im Anwendungsumfeld des Intranets, Extranets und Internets. Es mag zwar in den Ohren eines IT Sicherheitsverantwortlichen nicht gerade Begeisterungstürme auslösen, aber es gibt keinen Prozess, der eine 100 %-ige Sicherheit für Kommunikationsnetze gewährleistet. Den gegebenen Anforderungen und Bedingungen des Unternehmens folgend gilt es, bei der Definition der Sicherheitsrichtlinie das optimale Maß zwischen dem akzeptablen Sicherheitsgrad und den zu erwartenden Kosten zu ermitteln.

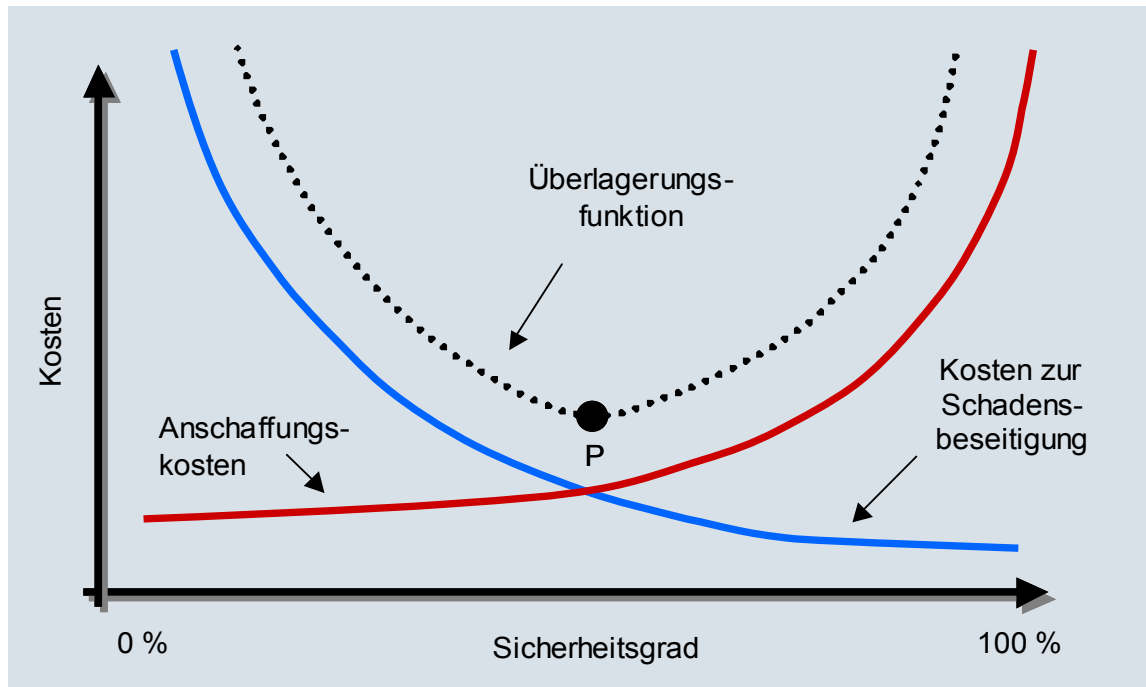


Abbildung 1: Kosten zur Bestimmung des Sicherheitsgrades

Abbildung 1 stellt die beiden maßgebenden Funktionen zur Bestimmung des Sicherheitsgrades gegenüber. Eine annähernd 100%-ige Sicherheit ist mit einer stark ansteigenden Kostenfunktion verbunden. Einen entgegengesetzten Verlauf zeigt die Funktion der zu erwartenden Aufwände zur Beseitigung bzw. Wiederherstellung im Falle eines erfolgreichen Angriffs auf die Unternehmensdaten. Ein möglicher, optimierter Ansatz besteht in der Überlagerung beider Kurven und liefert den Punkt P. Die exakte Lage dieses Punktes auf der Sicherheitsskala wird direkt durch die beiden Kostenfunktionen bestimmt. Es ist jedoch zu beachten, dass dieser Punkt den Anforderungen der internen Sicherheitsrichtlinie nicht immer in ausreichendem Maße entspricht. In diesem Falle ist ein Mehrwert an Sicherheit nur mit zusätzlichen Kosten zu erzielen.

Die zunehmende Einbeziehung moderner Kommunikationsformen in die alltäglichen Unternehmensabläufe wirft auch die Frage nach neuen bzw. veränderten Sicherheitsanforderungen auf. Der Zugriff auf interne Informationen von fast jedem beliebigen Ort der Erde aus wird zum wettbewerbsbestimmenden Faktor. Die Kommunikation ist deutlich über die Grenzen des lokalen Netzes hinausgewandert und nun Teil einer standortübergreifenden Infrastruktur. Ein entscheidender Baustein bildet hier zunehmend die weltweite Vernetzung über das Internet, über die sich z.B. effiziente Remote Access Lösungen realisieren lassen. Aus sicherheitstechnischen Gründen rücken Aspekte wie Privatsphäre, Integrität der Daten oder Authentifizierung von Benutzern und Endgeräten immer stärker in den Vordergrund.

1.1 Neue Kommunikationsformen

- *Intranet*: Ein Intranet bietet die Möglichkeit, mehrere Unternehmensstandorte sicher miteinander zu verbinden. Mit entsprechenden Sicherheitsmaßnahmen können dynamische Strukturen aufgebaut werden, die teure Standleitungen ersetzen.
- *Extranet*: Die gesicherte Kommunikation eines Intranet muss natürlich nicht nur auf das eigene Unternehmen beschränkt bleiben: Die konsequente

Erweiterung ist beispielsweise ein Geschäftsmodell für die Interaktion mit Partnern und Zulieferern.

- *Remote Access*: Remote Access Lösungen bieten einen eleganten Ansatz zur Ablösung bestehender Modem-Pools und zur Reduzierung der Einwahlkosten. Nach der initialen Einwahl in den lokalen Zugangspunkt des Service Providers werden die Daten über das Internet zum Unternehmensnetz übermittelt.

1.2 Virtuelle Private Netze

Ein zentraler Grundbaustein der neuen Kommunikationsformen ist das Internet. Das Internet bietet zwar sehr viele Freiräume, um kostengünstige und standortübergreifende Lösungen zu realisieren - es bietet aber von Natur aus keine inhärenten Mechanismen bezüglich Sicherheit, Dienstklassen oder Verfügbarkeit. Unter all diesen Anforderungen hat der sichere Datenaustausch in der Regel die höchste Priorität. Der Grundgedanke eines VPN ist es, den standortübergreifenden Ansatz mit der erforderlichen Sicherheit zu verbinden. Die Virtualität wird durch die Verwendung des Internets, die Privatsphäre durch Verschlüsselung realisiert. Die Absicherung der Daten kann dabei auf verschiedenen Ebenen erfolgen.

2 Sicherheitsanforderungen

Die Zunahme der unternehmensweiten Kommunikation unter Einbeziehung des Internets stellt erweiterte Ansprüche an die Sicherheitskonzept des Unternehmens. Ein häufig gewählter Ansatz zur Definition dieser Richtlinien besteht in der Betrachtung möglicher Sicherheitsrisiken, um daraus entsprechende Maßnahmen ableiten zu können.

2.1 Verlust der Privatsphäre

Bei der Verwendung eines ungesicherten Mediums zur Übertragung von Informationen stehen diese Daten prinzipiell jedem offen, der Zugang zu diesem

Medium besitzt oder sich diesen beschafft. Die unverschlüsselte Übertragung der Daten stellt dabei ein besonders starkes Risiko dar - sie ermöglicht passive Angriffe. Ein derartiger Angriff, der auf das Ausspähen von Datenströmen abzielt, ist ohne großes Know-how zu realisieren: es existieren zahlreiche Tools und Programme, die genau auf diese Angriffsart zugeschnitten und zudem häufig frei erhältlich sind. Abwehren lassen sich passive Angriffe durch Verschlüsselung, wobei die Effektivität im besonderen Maße von der Vertraulichkeit der Schlüssel und deren Stärke - also deren Länge - abhängt.

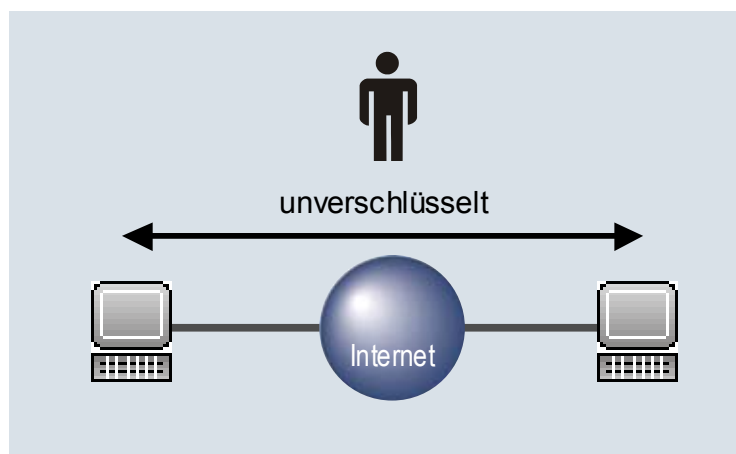
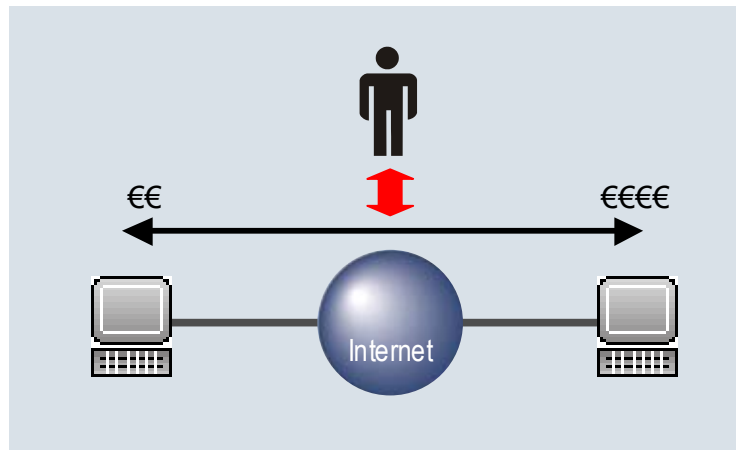


Abbildung 2: Ausspähen unverschlüsselter Daten

2.2 Veränderung der Datenintegrität

Der Verlust der Privatsphäre ist besonders kritisch, wenn es sich um vertrauliche Daten handelt. Aber selbst für weniger sensible Informationen ist es notwendig, die Integrität - also die Unversehrtheit dieser Daten - sicherzustellen. Dies gilt natürlich in besonderem Maße für die Übertragung über eine gesicherte Verbindung. Man stelle sich nur einmal vor, dass die Anmeldung an einem Bankterminal gesichert erfolgt, die eigentliche Übermittlung der hochsensiblen Daten jedoch von einem Angreifer leicht verändert werden kann.



2.3 Einspeisung verfälschter Datenströme

Eine offensichtliche Form des Angriffs besteht im Abfangen von Informationen. Sind die Daten erst einmal abgefangen, besteht prinzipiell die Möglichkeit, diese jederzeit wieder in das Netzwerk einzuleiten. Hierbei handelt es sich um einen klassischen Angriff auf die Datenintegrität. Sofern dem Angreifer genügend Informationen vorliegen, kann dieser allerdings noch eine weitere Form des Angriffs starten. Die Vortäuschung einer vertrauenswürdigen Identität kann dazu genutzt werden, um vertrauliche Informationen auf „legalem“ Wege zu erhalten. In vielen Fällen wird die Schwere solcher Angriffe falsch eingeschätzt, da der eigentliche Angriff erst zu einem späteren Zeitpunkt erfolgt. Sicherheitsmaßnahmen, die sich rein auf die Korrektheit der Datenintegrität konzentrieren, greifen ins Leere. Für die erfolgreiche Abwehr dieser Angriffsmuster sind spezielle Verfahren zur Authentifizierung erforderlich.

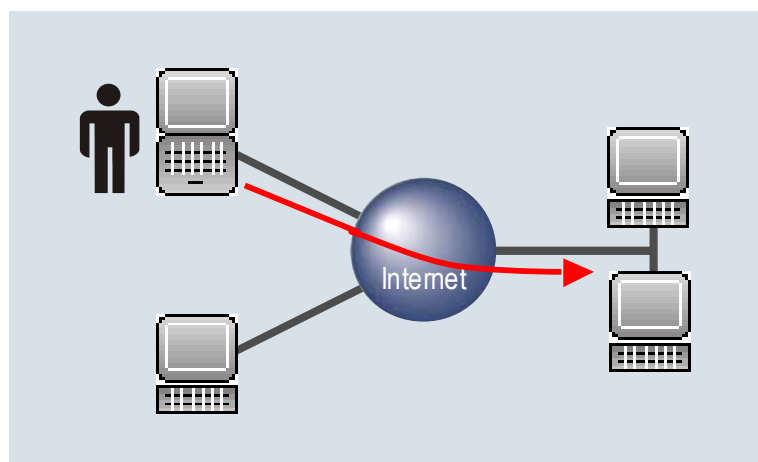


Abbildung 4: Verwendung einer anderen Identität

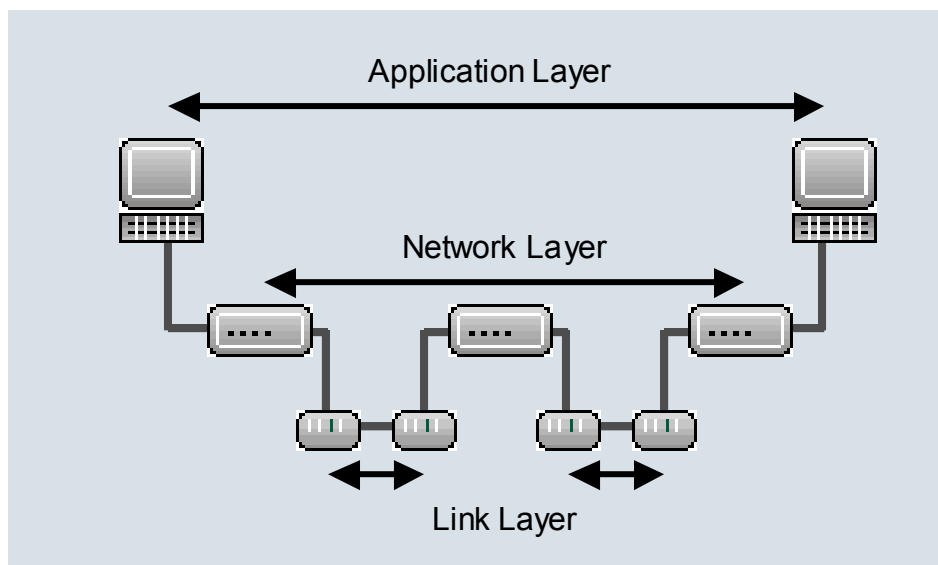
2.4 Einstellung des Dienstes

Die bisher betrachteten Angriffsmöglichkeiten befassen sich ausschließlich mit dem Abfangen und der Veränderung von Daten. Es geht also darum, vertrauliche Informationen zu bekommen oder veränderte Daten einzuschleusen. Prinzipiell werden die Daten auf Systemen erzeugt, verwaltet und weiterverarbeitet. Die obigen Angriffe zielen somit allesamt auf den eigentlichen Informationsinhalt dieser Systeme ab. Es existiert aber eine weitere Angriffsform, die sich rein auf die Systeme selbst konzentriert und allgemein als „Denial-of-Service Attacke“ bezeichnet wird: Die Systeme werden so lange mit unsinnigen Aufgaben überhäuft, bis diese aufgrund ihrer erreichten Leistungs- und Kapazitätsgrenzen ihren Dienst vollkommen einstellen. Je nach Relevanz für die Unternehmensprozesse kann der temporäre Ausfall einzelner Systeme erheblichen Schaden anrichten.

3 Virtuelle Private Netze mit IPSec

Die in Abschnitt 2 angesprochenen Angriffe können durch Mechanismen zur Sicherstellung der Vertraulichkeit, der Integrität und der Authentifizierung erfolgreich abgewehrt werden. Mit IPSec steht eine standardisierte Protokoll-Suite zur Verfügung, die diese Verfahren für das IP-Protokoll bereit stellt und auf Netzwerkebene realisiert. Die einzelnen Funktionalitäten werden von der Internet Engineering Task Force (IETF) in mehreren Standards beschrieben. Eine detaillierte technische Beschreibung zur Funktionsweise von IPSec ist in dem Bintec White Paper „*Verschlüsselte Datenübertragung über öffentliche Netze*“ beschrieben. Da IPSec den sicheren Austausch von Informationen über ein unsicheres Medium wie z.B. das Internet ermöglicht, ist es eine weit verbreitete Lösung zur Realisierung von VPNs.

Die Implementierung der Verfahren für einen gesicherten Datenaustausch kann prinzipiell auf verschiedenen Ebenen erfolgen. IPSec ist, wie bereits erwähnt, auf der Netzwerkebene anzusiedeln. Abbildung 5 zeigt die Einordnung von IPSec zu anderen Ebenen des OSI-Modells, auf denen ebenfalls Mechanismen zur Absicherung von Datenströmen bereitgestellt werden können. Hierzu zählt die Secure Socket Layer (SSL) Verschlüsselung auf Applikationsebene oder die Verschlüsselung jedes einzelnen Links auf physikalischer Ebene.



Da es sich bei SSL um eine Verschlüsselung auf Applikationsebene handelt (z.B. für Web Browser), lassen sich sehr gezielt Daten schützen, die von der jeweiligen Applikation verwendet werden. Allerdings bietet dieses Verfahren keinen Schutz für Daten, die von anderen Anwendungen erzeugt wurden, sofern diese Informationen nicht ebenfalls durch entsprechende Mechanismen abgesichert werden. Die Verschlüsselung auf der physikalischen Ebene bietet zwar einen sehr hohen Schutz, setzt aber an jedem Ende eines Links entsprechende Geräte voraus. Dies macht dieses Verfahren sehr unflexibel in der Handhabung und ist zudem nur sehr schwer mit dem Internet vereinbar, da hier in der Regel kein Zugriff auf die einzelnen Links besteht. Zudem sollte sichergestellt werden, dass die Entpackung der Daten in einer gesicherten Umgebung erfolgt.

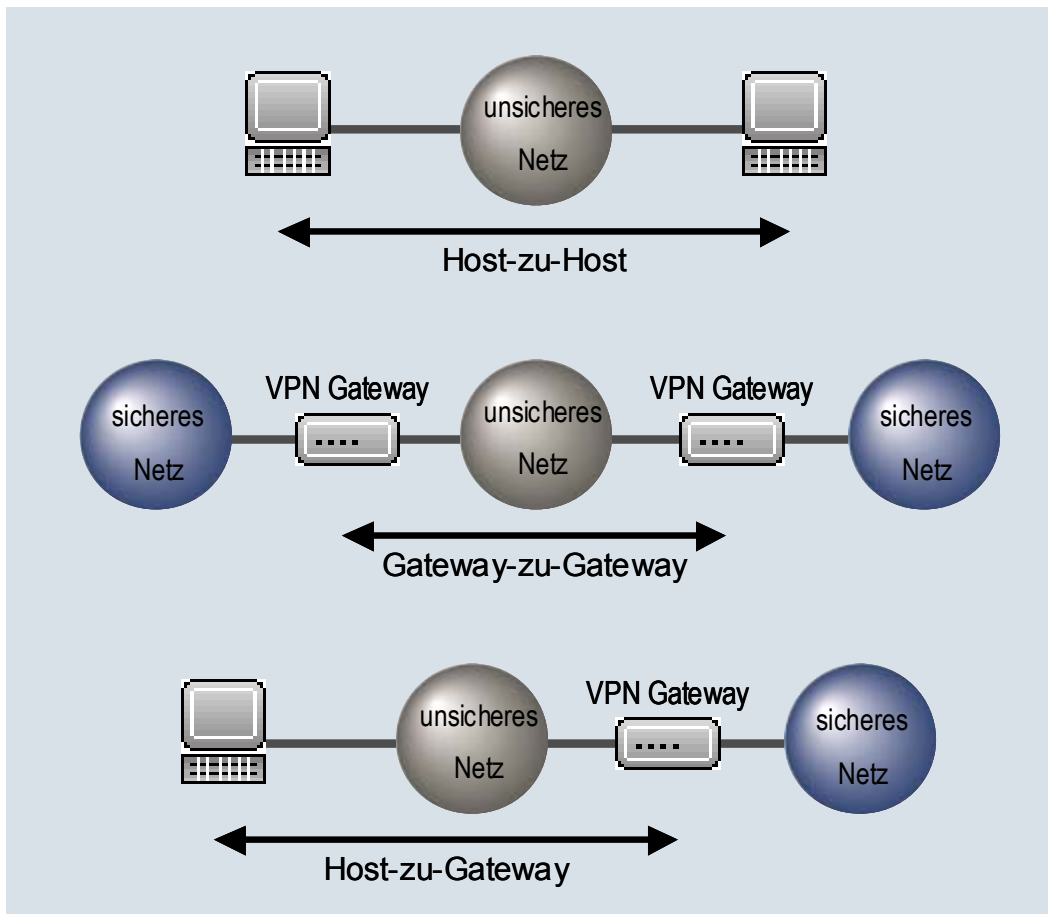


Abbildung 6: Aufbau möglicher VPN Tunnel

Die auf der Netzwerkebene angesiedelte Funktionalität von IPSec hingegen bietet eine Ende-zu-Ende Sicherheit, die ohne Änderungen in die Architektur des Netzwerkes integriert werden kann. Die verschlüsselten Pakete werden wie herkömmliche IP-Pakete behandelt und lassen sich somit problemlos von IP-Routern verarbeiten. Nur an den Kommunikationsendpunkten müssen die Informationen über die Verschlüsselung bereitgestellt werden. Ein sicherer Kommunikationskanal lässt sich dabei entweder zwischen zwei Host-Systemen, zwei VPN-Gateways oder zwischen einem Host-System und einem Gateway aufbauen (vgl. Abbildung 6).

4 Die Bintec VPN Access Serie

Die Bintec Router der X-Generation bieten allesamt die Möglichkeit, eine gesicherte Verbindung über IPSec zu realisieren. Zur Bereitstellung dieser Funktionalität ist eine entsprechende IPSec-Lizenz erforderlich. Mit Einführung der neuen VPN Access Produktreihe bietet Bintec eine neue Gerätegeneration von VPN Gateways, die alle bisherigen Vorteile der Bintec Geräte in sich vereinen und speziell für den hochverfügbaren Einsatz im VPN Umfeld optimiert wurden. Die Verschlüsselungsfunktion mittels IPSec ist in diesen Geräten bereits standardmäßig integriert und unterstützt z.B. den aktuellen Verschlüsselungsstandard AES (Advanced Encryption Standard). Die neue Produktreihe umfasst fünf verschiedene Modelle, die unterschiedliche VPN-Tunnelanzahlen unterstützen. Mit Ausnahme des kleinsten Gerätes der Serie besitzen alle Modelle zwei WAN-Ports, einen ISDN und einen LAN-Port sowie eine Konsole für AUX-Verbindungen.



Zu den erweiterten Leistungsmerkmalen dieser neuen VPN-Gateways zählen weiterhin

- Load Balancing zwischen den WAN-Schnittstellen
- Starke Verschlüsselung mit Schlüssellängen bis zu 256 Bit
- Bereitstellung von QoS-Funktionalitäten zur Priorisierung des Datenverkehrs
- Unterstützung von Zertifikaten und Preshared Keys mit bis zu 255 Zeichen Länge
- Integration in Content Filtering Systeme zur Klassifizierung des Internetverkehrs
- Umfangreiche Backup Möglichkeiten z.B. über ISDN oder Analog- bzw. GSM-Modems
- Hohe Verfügbarkeit durch Geräteredundanz mittels BRRP (Bintec Router Redundancy Protocol)
- Unterstützung von VPNs mit dynamischen IP-Adressen
- Einsatz von Kompressionsverfahren zur Erhöhung der Leistungsfähigkeit