

Sirrix. TrustedVPN.

- **Turaya™ Security Kernel**, providing Trusted Computing support with
 - Trusted Boot
 - TPM Security-Anchor
 - Remote Attestation
 - Sealed Storage
- **Foolproof Configuration and Operation Management**

Sirrix. TrustedVPN.

- Kompromisslose Sicherheit
- Einfache Verwaltung

Technische Spezifikation

System

- | | |
|------------|---|
| Dienste | <ul style="list-style-type: none"> ■ IKE-Server, IPsec-Server, IP-Filter, DHCP-Client/Server, NTP-Client, PoE-Support ■ VLAN-Support, QoS Prioritätssteuerung nach Netz/Port-Profilen ■ Policy-based Access und Routing nach Netz/Port-Profilen ■ optional: redundante VPN-Gateways und Unterstützung von Backupwegen (z.B. UMTS) |
| Management | <ul style="list-style-type: none"> ■ Appliances zentral über Management-Server gemäß globaler Trust Relationship Definitionen, gesichert durch TPM-basierte gegenseitige Authentifikation und Attestation ■ webbasierter Administratorzugriff auf Management-Server über eigenen Ethernet-Port ■ integrierter Provisioning-Service mit Firmware-Rollout gemäß frei wählbarer Gruppen ■ umfassendes Monitoring sowie revisionsfestes Reporting |

IPsec Protokolle

- Encapsulating Security Payload (ESP), Authentication Header (AH)
- Tunnel- oder Transportmodus
- NAT-Traversal (NAT-T)
- Dead Peer Detection (DPD)
- Standorte ohne statische öffentliche IP Adresse einbindbar

VPN Modi

- Site-to-Site VPN zur direkten Verbindung zwischen zwei Standorten
- VPN Software-Client-Support (Windows 7, Windows Vista, Windows XP (alle 32/64 Bit), Linux und Mac) für mobile Mitarbeiter z.B. am Hotspot
- Interne IP-Adresse für Road Warrior im Source-NAT-Verfahren zuweisbar
- Interoperabilitätsmodus zur Anbindung fremder VPN-Systeme

Sicherheitsverfahren

- | | |
|---------------------------|--|
| Internet Key Exchange | <ul style="list-style-type: none"> ■ Main und Aggressive Modus ■ Diffie-Hellman (2048 – 8192 Bit) ■ Perfect Forward Secrecy (PFS) |
| Authentisierungsverfahren | <ul style="list-style-type: none"> ■ TPM-/HSM-basiert, über X.509 Zertifikate (RSA 2048 – 8192 Bit) ■ externe oder integrierte Zertifizierungsstelle (CA) ■ optional: SmartCard Tokens für mobile Mitarbeiter |

Verschlüsselung

- | | |
|------------------------|--|
| Symmetrische Verfahren | ■ AES-128, AES-256, Blowfish, CAST, 3DES |
| Hash-Funktionen | ■ SHA-2 256, SHA-2 512, Md5, SHA-1 |

Performance

- | | Sirrix.TrustedVPN S | Sirrix.TrustedVPN L |
|---------------------------|---------------------|---------------------|
| Durchsatz in MBit/s | ■ 80 | ■ 500 |
| Empfohlene Anzahl Clients | ■ 100 | ■ 1000 |

System

- | | | |
|----------------|---|--|
| CPU | <ul style="list-style-type: none"> ■ 1,8 Ghz VIA C7 ■ Hardware-Accelerated Hash und Encryption mit PadLock™ ACE | <ul style="list-style-type: none"> ■ 3,0 GHz Intel Core2Duo ■ Software-Accelerated CCM Modus (integrierte authentication / encryption) |
| RAM | ■ 1 GB RAM | ■ 2 GB RAM |
| Festspeicher | ■ 2 GB Solid State Disk | ■ 2 x 250GB Raid-1 Festplatte |
| Schnittstellen | ■ 1 x 100 Mbit und 1 x Gbit LAN | ■ 4 x 1 GBit LAN |
| Abmessungen | ■ 300 x 217 x 74mm | ■ 19" 2HE Rack Server |

Weltweite Vernetzung Ihrer Standorte und Mitarbeiter.

Die Vernetzung von Arbeitsplätzen ist aus dem Unternehmensalltag nicht wegzudenken. VPN-Technologie (Virtual Private Network) ermöglicht den sicheren Datenaustausch sowie VoIP-basierte Telefonie zwischen entfernten Standorten über das öffentliche Internet. Damit können die Vorteile der offenen IP-Technologie mit der hohen Sicherheit der früher üblichen privaten Mietleitungen kombiniert werden.

Sicherheit zentrale Anforderung.

Die Nutzung des Internets als Rückgrat für die unternehmensinterne Kommunikation bedeutet einerseits eine deutlich verbesserte Wirtschaftlichkeit durch eine effiziente Verwendung bereits vorhandener Infrastruktur aber andererseits auch ein deutlich erhöhtes Risiko in Bezug auf die Authentizität der Kommunikationsteilnehmer sowie die Vertraulichkeit und die Integrität der zu übertragenden Daten. Daher ist kompromisslose Sicherheit ein wesentliches Kriterium für VPN-Lösungen.

Anforderungen an Administrierbarkeit oft unterschätzt.

Die Nutzung offener Standards führt zu erheblichen Vorteilen für den Anwender, da sie für Interoperabilität sorgt und so einen Wettbewerb zwischen den verschiedenen Anbietern ermöglicht.

Unter dem Oberbegriff VPN verbirgt sich eine Vielzahl von Varianten,

Parametern und Protokollen, die äußerste Sorgfalt bei der Konfiguration der beteiligten Komponenten erfordern. Die Inbetriebnahme eines VPN (insbesondere bei vielen Standorten) endet nicht selten in einem Hürdenlauf von Inkompatibilitäten.

Darüber hinaus bergen fehlerkonfigurierte VPNs erhebliche Sicherheitsrisiken, die nicht unmittelbar auffallen. Die hohen technischen Kompetenzanforderungen an den Administrator kombiniert mit den typischen Benutzerschnittstellen herkömmlicher VPN-Produkte, die logische Konfigurationsfehler ungeprüft zulassen, stellen also ein enormes eigenständiges Sicherheitsrisiko dar.

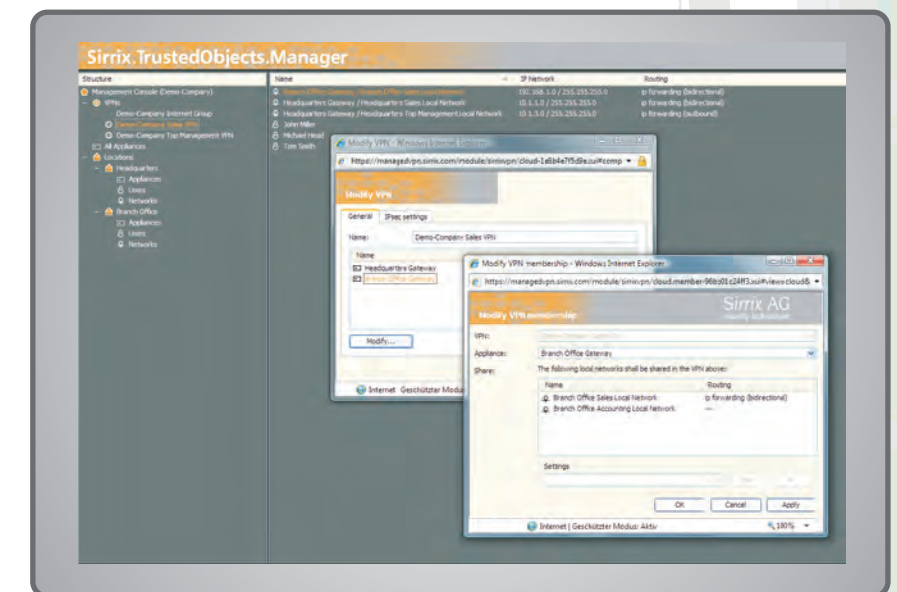
Die Anforderungen an die Administrierbarkeit eines VPN-Produktes müssen daher als eine entscheidende Sicherheitskomponente beim Design von Unternehmensnetzen verstanden werden.

Die Alleinstellungsmerkmale.

Die Sirrix.TrustedVPN-Lösung wurde auf der Basis zweier grundlegender Designziele entwickelt:

- kompromisslose Sicherheit und
- einfache Verwaltung.

Sirrix.TrustedVPN integriert moderne Security-Standards in jeweils hoher Instanzierung als Defaultstrategie und stellt dazu eine optimale Hardwarebasis bereit.



Für die Erweiterung eines logischen VPN reicht es aus, ein neues VPN-Gateway sowie das gewünschte Subnetz auszuwählen. Fertig.

Sirrix.TrustedVPN.

Das Bedienungskonzept konzentriert sich ganz auf die systemweiten logischen Vertrauensbeziehungen zwischen Netzen und Nutzern anstatt wie bei herkömmlichen Produkten die einzelnen beteiligten Geräte individuell administrieren zu müssen.

Damit können auch „normale“ Netzwerkadministratoren ohne besondere Security- oder VPN-Ausbildung hochsichere virtuelle Netze sehr schnell einrichten und pflegen. Gleichzeitig ermöglicht dieses Konzept ein einfaches und aussagekräftiges Audit in Bezug auf die Funktionstüchtigkeit und Sicherheit erwünschter Kommunikationsbeziehungen sowie auf den Ausschluss unerwünschter Verbindungen.

Die Architektur.

Die Lösung besteht aus zwei wesentlichen Komponenten:

- der **Sirrix.TrustedObjects Manager** ist der zentrale Server für Management und Konfiguration.
- die **Sirrix.TrustedVPN Appliance** wird in mehreren Ausprägungen dezentral als VPN-Gateway an den einzelnen Standorten eingesetzt.

Beide Komponenten werden als unmittelbar einsatzbereite gehärtete Appliances bereitgestellt.

Trusted Infrastructure.

Die durchgängige Integration von Prinzipien vertrauenswürdiger Kommunikation und Nutzung standardisierter Schnittstellen, wie Sie beispielsweise von der Trusted Computing Group (TCG) spezifiziert werden, ermöglicht eine völlig neue Stufe der Gesamtsystemsicherheit.

Dabei kommt in den VPN Appliances mit dem Trusted Platform Module (TPM) ein Hardware-Chip zum Einsatz, der als Sicherheitsanker dient, und bis hinauf in die Anwendungen vollständig in die Gesamtarchitektur eingebunden ist.

Die Sirrix.TrustedVPN Lösung basiert auf einem Trust Relationship Konzept. Die Hauptaufgabe des Administrators besteht in der Definition von logischen VPNs in der Form von einfachen White Lists von Netzen, Servern und individuellen mobilen Clients. Der Sirrix.TrustedObjects Manager sorgt dann vollautomatisch für die Einrichtung aller entsprechenden sicheren Tunnel zwischen den beteiligten Endpunkten.

Im Sirrix.TrustedObjects Manager kommt ein speziell versiegeltes und FIPS140-2 Level3/4 zertifiziertes Hardware-Sicherheitsmodul (HSM) als Certification Authority zum Einsatz.

Konkret dient das TPM in den Appliances dazu,

- die **privaten Schlüssel der einzelnen Appliances sicher zu speichern und zu verarbeiten. Die Schlüssel verlassen nie den Sicherheitschip und ermöglichen dadurch eine zuverlässige, manipulationsfreie Identifizierung der einzelnen Appliances durch das integrierte PKI-Verfahren.**
- ein **vertrauenswürdigen Booten durch eine Hardware-basierte Überprüfung aller wesentlichen zu ladenden Module zu garantieren.**
- die **Firmware und die dauerhaft gespeicherten Konfigurationsdaten nachhaltig zu verschlüsseln.**

Das Ergebnis ist ein Gesamtsystem, das sich ständig überwacht und Manipulationen - ob lokal oder aus der Ferne - zuverlässig unterbindet.

Erst dieser außergewöhnliche Selbstschutz ermöglicht nun eine tatsächlich vertrauenswürdige Realisierung der eigentlichen Funktionen der Lösung.

Der Sirrix.TrustedObjects Manager.

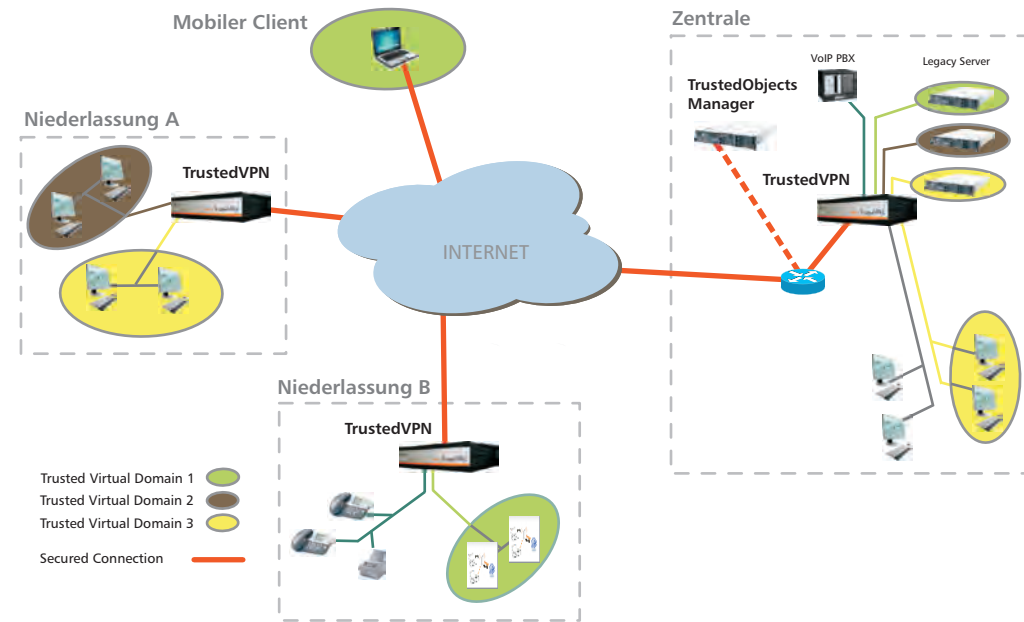
Die zentrale Management-Station wird über ein internes Web-Interface gesteuert, so dass die berechtigten Administratoren physikalisch getrennt mit einem Webbrowser auf die Verwaltungsfunktionen zugreifen können. Die gemanagten VPN-Gateways selbst sind „zustandslos“ und speichern lediglich die eigene IP-Adresse und die des zugehörigen Management-Servers. Diese Daten lassen sich komfortabel mit Hilfe

eines vom Management-Server generierbaren Datensatzes, beispielsweise per USB-Medium direkt ins Gerät übertragen.

Der Sirrix.TrustedObjects Manager übernimmt die gesamte restliche Verwaltung für Inbetriebnahme und Betrieb der einzelnen Gateways. Das Anschließen der VPN-Appliances erfordert also keine besonderen technischen Kompetenzen an den dezentralen Standorten.

Sobald die VPN Appliance an das Netz angeschlossen ist, meldet sie sich bei dem Sirrix.TrustedObjects Manager an.

Nach gegenseitiger Authentifizierung überzeugt sich die Management-Station mittels „Remote Attestation“ von der Korrektheit der eingesetzten Software. Anschließend identifiziert der Sirrix.TrustedObjects Manager



die Appliance anhand ihrer eindeutigen, durch den Sicherheitschip bereitgestellten Identifikationsschlüssel und lädt entsprechend den Vorgaben des Administrators die Konfigurationsdaten.

Die Kernaufgabe des Administrators besteht nun darin, logische VPNs einzurichten, die jeweils aus einer bestimmten Auswahl von Netzen bzw. Subnetzen an den einzelnen Standorten bestehen. Das Hinzufügen eines solchen Netzes zu einem logischen VPN führt zu einem Konfigurationsupdate aller beteiligten Systeme mit dem Ergebnis eines voll vermaschten virtuellen über das Internet getunnelten Netzes zwischen den beteiligten Teilnetzen.

Alle so erreichbaren Rechner können nun sicher sein,

- dass der über öffentliche Netze geführte Datenverkehr vertraulich und integer bleibt und
- dass ausschließlich Verkehrsbeziehungen zwischen zugelassenen Rechnern an definierten Standorten hergestellt werden können.

Die Sirrix.TrustedVPN-Lösung beinhaltet ein eigenständiges, integriertes PKI-System. Ohne weiteres Zutun wird beim Anlegen eines logischen VPNs eine zugehörige Zertifizierungsinstanz auf dem TrustedObjects Manager generiert. Die beteiligte Appliance wird dazu aufgefordert, ein Schlüsselpaar lokal zu erzeugen, das von dieser Instanz

zertifiziert wird und anschließend in der VPN Appliance zur Verfügung steht.

Hohe Sicherheit durch IPsec in stärkster Ausprägung.

Die Kommunikation über das Internet zwischen den einzelnen Sirrix.TrustedVPN Appliances wird über die standardisierten IPsec-Protokolle abgewickelt.

Die Sirrix.TrustedVPN Gateways sind mit sicheren Parametern vollständig für die Kommunikation untereinander vorkonfiguriert. Dies verhindert Inkompatibilitäten, vermeidet unsichere oder fehlerhafte Einstellungen durch Administratoren ohne ausreichende Security-Kompetenz und realisiert eine äußerst strenge Sicherheit. Diese beruht:

- in der Internet Key Exchange Phase auf dem Diffie-Hellman Schlüsselaustauschverfahren bei 4096 Bit und Perfect Forward Secrecy.
- bei der Authentisierung der Kommunikationspartner auf automatisch generierten und ausschließlich innerhalb des sicheren Hardwarechips verarbeiteten X.509 Schlüssel und Zertifikaten.
- in der Übertragungsphase auf ESP-Paketen im Tunnel-Mode sowie AES-256 Verschlüsselung der Daten und SHA256-Hash-Funktionen für ihre Integrität und Authentizität.



Die Sirrix.TrustedVPN Lösung wird als gehärtete Appliance in zwei Varianten an den einzelnen Standorten eingesetzt. Sie wird vollständig über einen Managementserver zentral administriert.