FROST & SULLIVAN

50 Years of Growth, Innovation and Leadership

Next Generation Network Access Technology: Overcoming Business Challenges

Deutsche Version

Ein Frost & Sullivan Whitepaper

für NCP

www.frost.com

INHALTSVERZEICHNIS

1. HINTERGRUND UND ZIEL DES WHITEPAPERS

Es gibt zwei konkurrierende Schlüsseltechnologien für sicheren Remote Access: IPsec und SSL. Seit Jahren diskutiert die Informations- und Telekommunikationsindustrie darüber, welche der beiden Technologien die bessere ist. Dieses Whitepaper gibt Antworten unter folgenden Prämissen:

1. Es gibt keine bessere oder schlechtere Technologie - jede hat ihre auf spezifische Einsatzfälle abgebildeten Vor- und Nachteile;
2. Unternehmen mobilisieren zusehends ihre Geschäftsprozesse auf globaler Ebene. Dies erfordert zwangsweise ein leistungsfähiges zentrales Management um einerseits die Transparenz zu erhöhen und andererseits schnell auf Marktveränderungen reagieren zu können;
3. In einer sich immer stärker öffnenden und vernetzten Welt steht die Sicherheit an erster Stelle. Dabei ist wiederum die Wirtschaftlichkeit der Sicherheitslösung von höchster Priorität.

NCPs Remote Access-Lösung setzt an diesen drei Punkten an. Die integrierte IPsec/SSL Lösung verbindet das Beste beider Welten und hat die praktischen Probleme aus der Kombination dieser beiden Ansätze bereits gelöst. So erhöhen sich beim Ausbau/der Erweiterung einer herkömmlichen Lösung beispielsweise die IT-Ressourcen und die damit verbundenen Personalkosten, da mehr Sicherheitszertifikate verwaltet werden müssen und jede neue Remote Access-Anforderung manuell konfiguriert werden muss. Die Folge ist, dass das Unternehmen weniger schnell auf Marktveränderungen reagieren kann. NCPs Software-Lösung ist darauf ausgelegt, dass Unternehmen auch weiterhin Remote Access Connectivity wirtschaftlich betreiben können.

Viele Unternehmen setzten bereits- IPsec und SSL gleichzeitig ein. Unternehmen die von IPsec auf SSL wechselten, stellten im Nachhinein fest, dass sie von keiner der beiden Technologien die Vorteile so richtig nutzen konnten. NCPs Next Generation Network Access Technology nimmt Unternehmen die Unsicherheit einer Fehlentscheidung, um sich ausschließlich auf ihr Unternehmensziel zu konzentrieren. Dafür sorgt ein flexibles Management, das beide Technologien anbietet und gleichzeitig die Ressourcen reduziert, die für die Administration dieses komplexeren Systems erforderlich sind.

Kapitel 6 erläutert in einer Beispielrechnung die mögliche Kosteneinsparung, die durch NCPs Next Generation Network Access Technology erzielt werden kann. NCPs Lösung rechnet sich insbesondere für Unternehmen mit mehr als 2.000 mobilen Mitarbeitern; hier betragen die Einsparungen der jährlichen Betriebskosten bis zu 41%.

Neben der wichtigen Kostenfrage garantiert NCPs Next Generation Network Access Technology auch die Grundvoraussetzung in Remote Access VPNs: sicherer Netzwerkzugang.

2. BEDARF DER UNTERNEHMEN AN REMOTE CONNECTIVITY

Ein modernes Unternehmen benötigt Remote Connectivity, da die vernetzte Gesellschaft einen integrativen Bestandteil des heutigen Geschäftsumfeldes darstellt. Die Welt ist kleiner geworden - die Menschen sind stärker vernetzt und nutzen eine größere Vielfalt an Technologien und Geräten. Dieser Trend setzt sich rasant fort, je mehr Menschen sich in das globale Kommunikationsnetz einklinken. Entsprechend steigt der Bedarf, Daten möglichst in Echtzeit an jedem Ort der Welt verfügbar zu haben. Basis für den dauerhaften, wirtschaftlichen Erfolg eines Unternehmens sind gezielte Investitionen in die IT- und Kommunikationstechnik. Durch den möglichen exponentiellen Anstieg der Verbindungen zwischen Mitarbeitern, Partnern, Lieferanten und Kunden wird die Netzwerkinfrastruktur der Unternehmen komplexer. Aktuell müssen sich moderne Unternehmen der stetig zunehmenden Vernetzung aller Beteiligten stellen.

Für das Management stellt sich die Frage, ob und wie Einnahmen aufgrund stärkerer Vernetzung die erwarteten Ausgaben durch die Administration der komplexeren Netzwerkinfrastruktur ausgeglichen werden können. Welche organisatorischen und technischen Veränderungen müssen durchgeführt werden, um die komplexen Netzwerke wirtschaftlich und sicher betreiben zu können? Es gilt, eine stetig wachsende Anzahl von Anwendern an das Unternehmensnetzwerk anzubinden, bei gleichzeitig zunehmender Vielfalt der genutzten Geräte, Plattformen und technischen Möglichkeiten. All dies führt zu einer zusätzlichen Belastung der IT-Abteilung und macht es wichtiger, Remote Access wirtschaftlich zu betreiben.

Moderne Unternehmen in einer vernetzten Welt

Moderne Unternehmen benötigen Remote Connectivity auf folgende Art und Weise:

1. **Eine vernetzte Gesellschaft verbindet schneller mehr Menschen miteinander.**

Erfolgreiche Unternehmen nutzen umfassend alle Möglichkeiten, die ihnen die vernetzte Gesellschaft bietet. Je mehr Menschen involviert sind, desto leichter fällt es Unternehmen, ein größeres Publikum anzusprechen - das schließt auch Kunden, Zulieferer, Partner und Mitarbeiter ein. Ende 1999 hatten nur 8 Prozent der Weltbevölkerung einen Mobilfunkvertrag, 5 Prozent nutzten das Internet und 0.1 Prozent einen Breitbandanschluss. Ende 2010 waren mehr als drei Viertel der Weltbevölkerung Mobilfunkkunden, ein Drittel nutzte das Internet und fast 10 Prozent hatten einen Breitbandanschluss. Durch die steigende Anbindung der Menschen brauchen heutige Unternehmen eine Remote Connectivity Lösung, die mehr Verbindungen über mehr Endgeräte, Maschinen und Plattformen zulässt und unterschiedliche Protokolle unterstützt.

Ein modernes Unternehmen nutzt die allgegenwärtige Vernetzung um seine Umsatz- und Gewinnmöglichkeiten zu verbessern. Heute bedeutet Remote VPN Connectivity, dass Unternehmen mehr Verbindungen von mehr Benutzern administrieren müssen, dabei mehr Geräte, Maschinen und Plattformen im Einsatz sind und mehr Kommunikationsprotokolle genutzt werden; zusätzlich steigen die Sicherheitsanforderungen durch Echtzeit- oder annähernd Echtzeit-Datenverbindungen.

2. Die Allgegenwärtigkeit des Internets verändert das User-Verhalten in einer vernetzten Gesellschaft.

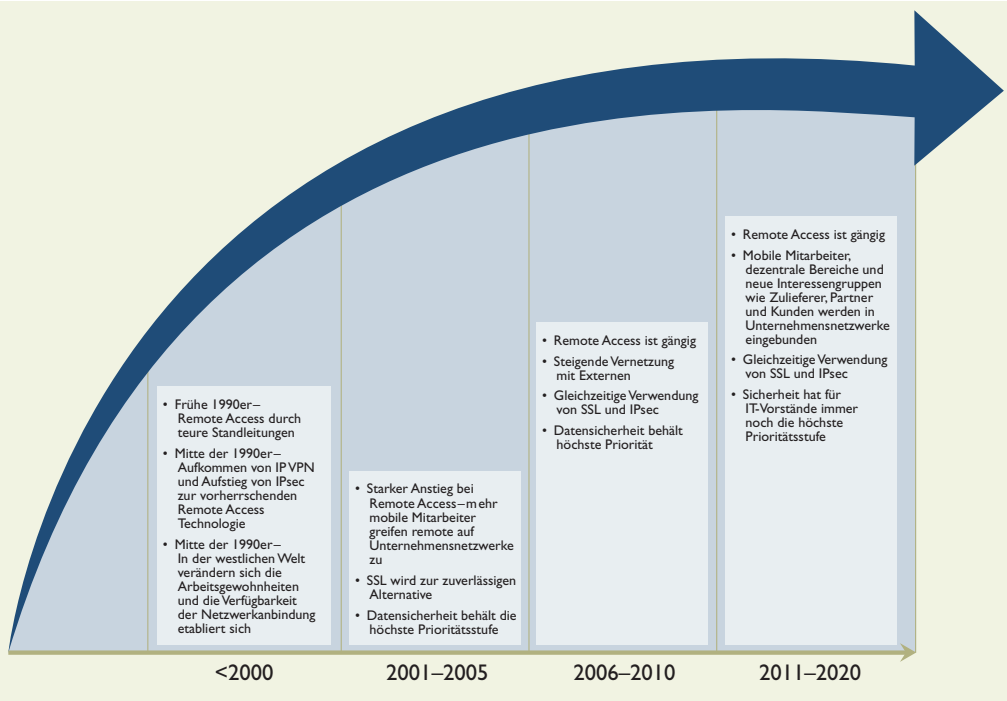
Moderne Unternehmen passen sich stetig an die Veränderungen im Benutzerverhalten an, da die Arbeitsflexibilität mehr Mitarbeitern erlaubt, von mobilen Endgeräten aus ihre tägliche Arbeit zu erledigen und die Allgegenwärtigkeit des Internets die Erreichbarkeit von Dritten erhöht. Unternehmen und Markt interagieren immer häufiger online. Deshalb müssen modern geführte Unternehmen für verschiedenste Nutzerverhalten den Zugriff auf das Firmennetz bereitstellen: einfach, sicher, universell und wirtschaftlich

3. Eine vernetzte Gesellschaft erhöht die Sicherheitsrisiken.

Die Offenheit einer vernetzten Welt erhöht auch die Sicherheitsrisiken, die für sich ganzheitlich und wirtschaftlich gemanagt werden müssen. Je höher die Anzahl der Verbindungen, desto größer die Verwundbarkeit eines Systems. Sobald sich ein Unternehmen der Sicherheitsrisiken bewusst ist, erhöht sich auch der Druck, alles Denkbare zu unternehmen, damit die Daten abgeschottet vor dem Zugriff Dritter, via Internet übertragen werden können. Aufgrund der zunehmenden Komplexität im Web muss das Unternehmen seine Remote Access-Verbindungen stets unter Kontrolle haben, um die Kommunikationswege wirtschaftlich zu schützen.

Die Grafik unten zeigt zusammenfassend wie sich der Bedarf eines modernen Unternehmens an Remote Connectivity im Zeitverlauf entwickelt. Auch die Management-Komplexität der Remote Access Connectivity steigt mit der stärkeren Vernetzung der Geschäftswelt.

Grafik 1: Komplexität der Unternehmens VPN Connectivity steigt



3. REMOTE ACCESS MARKT – ANSÄTZE UND LÖSUNGEN

Die beiden gängigsten Remote Access VPN-Technologien - Internet Protocol Security (IPsec) und Secure Socket Layer (SSL) haben sich am Markt etabliert. IPsec kam in den späten 1990ern auf - als Alternative zu den teuren und unflexiblen Standleitungen die auch für Remote Access verwendet wurden. IPsec setzte sich schnell als zuverlässige und wirtschaftliche Alternative in Unternehmen für den Remote Access von ausgewählten Mitarbeiter und vor allen Dingen sogenannte Site-to-Site-Verbindungen durch. In den frühen 2000ern tauchte SSL als Alternative zu IPsec auf. Unternehmen versuchten mehr externe Mitarbeiter an das Firmennetz anzubinden, die im Gegensatz zum IPsec-Verfahren nur einen eingeschränkten Netzwerkzugriff benötigten.

"Sowohl IPsec als auch SSL kommen zum gleichen Ergebnis: dem Schutz der Datenübertragung im Netzwerk. Allerdings stellt die Umsetzung Unternehmen immer wieder vor praktische Probleme."

Frost & Sullivan

Die Diskussion welche der beiden Tunnelingverfahren die bessere ist, wurde zusehends verwässert. Absolut gesehen gibt es keine bessere Technologie - es gibt nur die geeignetere Lösung, die auf die jeweiligen Merkmale des Unternehmens und seinen spezifischen Bedarf für Remote Access abgestimmt ist. Beide Ansätze haben das gleiche Ziel, aber verwenden andere Methoden, um es zu erreichen. Unabhängig davon predigen sowohl IPsec als auch SSL Anbieter ihren Kunden weiterhin die Vorzüge ihrer priorisierten Lösung. Heute findet man eine Koexistenz beider Technologien in Unternehmensnetzwerken. Frost & Sullivan ist der Meinung, dass das getrennte Management beider Ansätze einige ihrer Vorzüge zunichtemacht, insbesondere im Hinblick auf deren Wirtschaftlichkeit.

IPSec und SSL kommen zum gleichen Ergebnis

Beide Protokolle, IPsec und SSL, sichern die Datenübertragung über öffentliche Netzwerke. Sie erreichen das gleiche Ziel, da sie die Integrität, Vertraulichkeit und Authentizität der Daten sicherstellen. Ein Überblick über beide Ansätze:

Grafik 2: IPsec und SSL – Ein Überblick

	IPSec	SSL
Allgemeine Anwendung	Sicherer Remote Access für die Datenübertragung über das Internet durch vom IETF empfohlene Protokolle	Sicherer Remote Access durch weit verbreitetes Protokoll, das auf den meisten Web-Browsern läuft
Funktionsweise der sicheren Anbindung	Arbeitet auf IP-Schicht, nutzt Verschlüsselungsmechanismen und Authentisierungsprotokolle für Einhaltung der Authentizität, Integrität und Vertraulichkeit der Daten	Arbeitet auf der Anwendungsschicht und verwendet auch Verschlüsselungs- und Authentisierungsprotokolle
Markteinführung	Eingeführt als kostengünstige Alternative zu teuren und unflexiblen Standleitungen für VPNs	Eingeführt als clientlose und anwendungsbezogene Alternative zu herkömmlichen VPN Lösungen
Ursprüngliche Einsatzgebiete	Universeller, sicherer Remote Access für Site-to-Site Kommunikation innerhalb von Unternehmen, für mobile Mitarbeiter und Außendienstmitarbeiter.	Anwendungsbezogene Anbindung mobiler Nutzer, insbesondere externer Interessengruppen wie Geschäftspartner oder Zulieferer.

Quelle: Frost & Sullivan

IPsec - Der dominante Ansatz

Das Protokoll IPsec wurde in den späten 1990ern von der Internet Engineering Task Force (IETF) empfohlen. Durch die Verschlüsselung der Daten im Transport- und im Tunnelmodus wird die Datenübertragung auf der Vermittlungsschicht gesichert und deren Integrität, die Authentizität und die Vertraulichkeit erhalten. Die Daten sind geschützt, da IPsec-fähige Versand- und Empfangsmodule für die Ver- und Entschlüsselung benötigt werden. Für einzelne Datenpakete wird der gleiche Public Key verwendet. Durch ein Protokoll erhält der Empfänger einen Public Key, womit er den Absender durch ein digitales Zertifikat authentisieren kann. IPsec wurde so beliebt, weil es auf offenen Normen basiert, die eine sichere „private" Kommunikation über das „öffentliche" Internet erlauben. Der Einsatz von IPsec ist bei Site-to-Site-Verbindungen und in Remote Access Situationen sinnvoll. Wenn es also gilt, mobilen Mitarbeitern einen hochischeren, transparenten Zugriff auf das Firmennetz zu ermöglichen oder Filialen sicher zu vernetzen.

SSL - Die Alternative

SSL ist die zweite Haupttechnologie für sichere Remote Access Connectivity. Sie nutzt für die Datenübertragung über das Internet das allgemein verfügbare Web-Protokolle HTTPS und erfodert keine weitere Client-Software – Downloads, spezielles Benutzerwissen entfällt.

SSL schützt die Datenübertragung in der Anwendungsschicht und sichert Integrität, Authentizität und Vertraulichkeit der Daten. Der Benutzer erhält nach erfolgreicher Authentisierung nur Zugriff auf die entsprechenden Ressourcen und Anwendungen im Unternehmensnetz. Alle über das Internet übertragenen Daten werden an beiden Endpunkten ver- bzw. entschlüsselt. SSL wurde deshalb als zweite Haupttechnologie für sicheren Remote Access bekannt, weil es zu einer Zeit eingeführt wurde, als sich das Benutzerverhalten spürbar änderte. Das optimale Einsatzszenario für SSL ist eine Umgebung, in der Unternehmen Geschäftspartnern und/oder mobilen Mitarbeitern sicheren Remote Access ermöglichen müssen, wobei nur auf bestimmte Unternehmensanwendungen zugegriffen werden darf.

IPsec und SSL - Die Unterschiede

IPsec und SSL haben die gleiche Zielsetzung, und zwar den sicheren Remote Access auf das Firmennetz. Hierfür nutzen beide unterschiedliche Layer des Netzwerkes. IPsec schützt remote Netzwerke auf der Vermittlungsschicht und wird eingesetzt, um Niederlassungen und mobile Mitarbeiter unter der Zielsetzung eines transparenten Zugriffes in das Firmennetz einzubinden. SSL arbeitet auf der Anwendungsschicht und ermöglicht den Unternehmen ein flexibles Management von Zugriffsrechten. SSL wird überall dort eingesetzt, wo Externe nur auf bestimmte Ressourcen/Applikationen zugreifen dürfen.

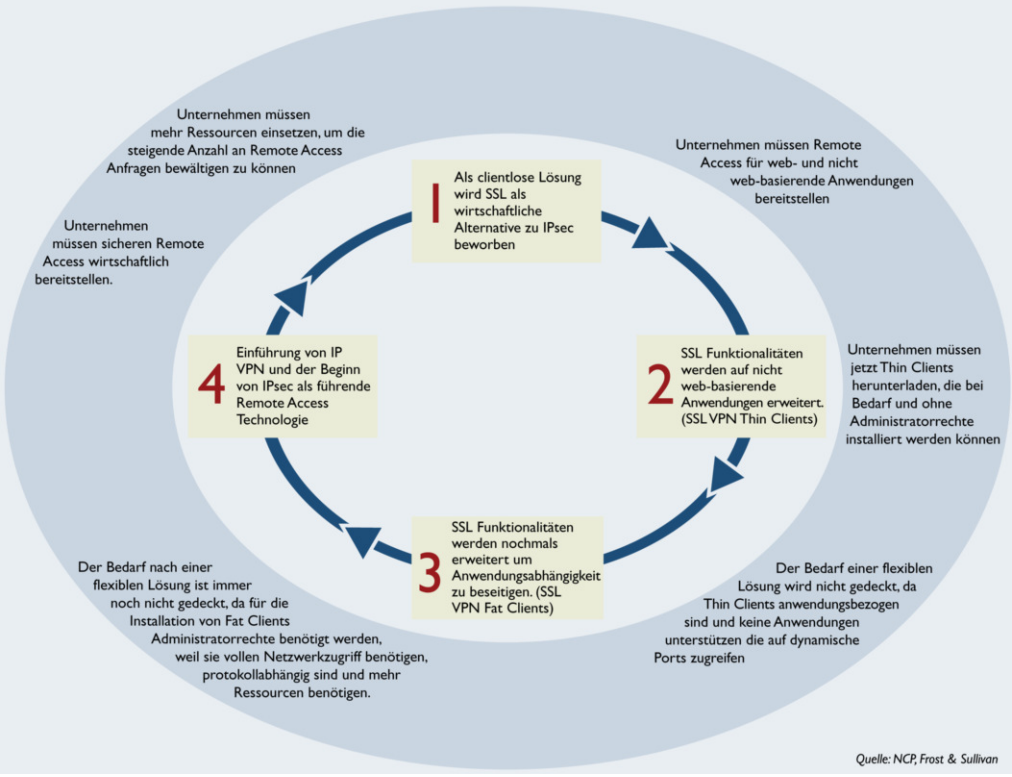
Anders ausgedrückt: IPsec unterscheidet sich auch dadurch von SSL, indem es transparenten Netzwerkzugang ermöglicht. SSL begründet sich auf einen anwendungsbezogenen Ansatz. Der Anspruch des „clientless“ SSL VPN gilt nur für Webanwendungen wie zum Beispiel Outlook Web Access. Wenn Unternehmen weitere Einsatzmöglichkeiten fordern, werden die SSL-Funktionen durch eine Client-Software erweitert. Diese zusätzliche Komplexität wird im nächsten Abschnitt beschrieben.

IPsec und SSL - Gibt es eine Koexistenz?

Eine Möglichkeit von IPsec und SSL zu profitieren, ist beiden Technologien entsprechend ihrer Funktionsweise und der Geschäftserfordernis einzusetzen. Frost & Sullivan stellte fest, dass viele Hersteller eine möglichst vollständige Remote Access Lösung anbieten wollen. So findet man am VPN Markt beispielsweise SSL-Lösungen, die in anderen Technologien integriert sowie auf entsprechend anderen Geräten unterstützt werden, und zu einem einzigen Client Netzwerk zusammengefasst werden können. Darüberhinaus haben SSL-Hersteller die Funktionalität ihrer Lösungen beständig erweitert, um die Implementierungs-probleme der Unternehmen zu beheben.

Diese Erweiterungen der SSL-Lösungen relativieren jedoch die ursprüngliche Behauptung „clientless“ und eine wirtschaftliche Alternative zu IPsec zu sein. Folgende Grafik fasst zusammen wie SSL durch die Funktionserweiterungen IPsec immer ähnlicher wird.

Grafik 3: IPsec & SSL - Der Mittelweg schließt den Kreis zu den praktischen Bedürfnissen von Unternehmen



Wie oben dargestellt löst SSL nicht alle praktischen Kommunikationsbedürfnisse der Unternehmen.

1. SSL wird als „clientless“ Lösung beworben und als einfach einzusetzende und wirtschaftliche Remote Access-Technologie von bestimmten Anbietern auf dem Markt positioniert. Sobald jedoch Implementierungsprobleme auftauchen, stellen die Unternehmen fest, dass sie sehr viel mehr Ressourcen für Remote Access bereitstellen müssen, als ursprünglich für die Realisierung des VPN geplant war. So haben Unternehmen häufig Bedarf an sicherem Remote Access für web- und nicht web-basierte Anwendungen.

2. Um dieses Problem zu beheben, werden SSL VPN Thin Clients benötigt. Die Thin Clients können bei Bedarf ohne Administratorrechte via Internet heruntergeladen werden und ermöglichen Remote Access zu bestimmten Netzwerkanwendungen. Dieser Download von Clients steht im Widerspruch zur ursprünglichen Behauptung und dem Alleinstellungsmerkmal SSL sei „clientless“.

3. Die Kommunikationsanforderungen steigen weiter, wenn Unternehmen zusätzlich Remote Access benötigen, der anwendungs- und portunabhängig ist. Sogenannte SSL VPN Fat Clients sind hier die Lösung. Allerdings werden auch für die Implementierung dieser Fat Clients Administratorrechte benötigt, da der vollständige Netzwerkzugang protokollabhängig ist und mehr Ressourcen benötigt werden.

4. Diese Erweiterungen der SSL-Funktionalitäten entsprechen zwar den zunehmenden Implementierungsbedürfnissen von Unternehmen, sie stellen SSL aber zusehends auf die gleiche Stufe wie IPsec. Flexibilität und Einsparungspotential mit dem SSL Fat Client werden für Unternehmen nun allerdings eingeschränkt, da diese mangels Interoperabilität an einen bestimmten Hersteller gebunden sind.

Kurz gefasst: Unternehmen können von den Vorteilen beider VPN-Welten profitieren, wenn sie IPsec und SSL gleichzeitig einsetzen. Die Herausforderung besteht bei der Implementierung einer Lösung hinsichtlich deren Effektivität. Hier unterscheiden sich die Angebote der verschiedenen Hersteller. Vorteile hat derjenige, dessen Kerngeschäft ausschließlich die Entwicklung von VPN-Komponenten ist.

4. WOMIT LASSEN SICH DIE BEDÜRFNISSE MODERNER UNTERNEHMEN DECKEN?

Moderne Unternehmen nutzen Remote Connectivity als Werkzeug, um ein größeres Publikum von internen und externen Benutzern zu erreichen. Deshalb werden an einen sicheren Remote Access drei Anforderungen gestellt:

1. Sicherung von Integrität, Vertraulichkeit und Authentizität der Daten während der Remote Access Sitzungen;

2. Remote Access über feste und mobile Verbindungen;

3. Wirtschaftlichkeit hinsichtlich des Bedarfes an IT-Ressourcen und einmaligen Investitionsaufwand.

Kurz gefasst: Unternehmen benötigen Lösungen, welche die Kosten minimieren, die Komplexität der IT reduzieren und Einsatzflexibilität garantieren.

"Ein modernes Unternehmen benötigt wirtschaftliche Remote Access Connectivity, die flexibel und im Betrieb wenig komplex ist"

Frost & Sullivan

Moderne Unternehmen benötigen eine wirtschaftliche Lösung

Viele Firmen setzen beide VPN-Technologien parallel ein. In der Praxis zeigt sich allerdings, dass IT-Kosten durch eine Kombination von IPsec und SSL die erwarteten Vorteile übersteigen. Wenn die Hersteller versuchen, beide Remote Access-Verfahren mit den Unternehmenszielen abzustimmen, so entstehen praktische Einsatzprobleme, die zu mehr Aufgaben für die IT-Abteilung führen. Nach Meinung von Frost & Sullivan liegt der Schlüssel zur maximalen Wirtschaftlichkeit einer ganzheitlichen Lösung in deren Implementierung. Eine vergleichende Gesamtkostenrechnung erfolgt in Kapitel 6.

Für die Erhöhung der Kosten in der IT-Abteilung sind drei Hauptgründe verantwortlich:

- **Remote Access Strategie:** Die Kosten werden der IT-Abteilung zugeordnet. Der technische Leiter sorgt dafür, dass die IPsec- und SSL-Strategie zu den internen Prozessen und zur Organisationsstruktur des Unternehmens passen. Er verhandelt mit den Herstellern, um die gewünschten Ergebnisse für die unterschiedlichen Remote Access Einsatzbereiche zu realisieren. Eine große Herausforderung ist dabei, die Sicherheitsrisiken umfassend zu verstehen, um eine technische Entscheidung treffen zu können, ob IPsec, SSL oder beide Ansätze eingesetzt werden können/sollen. Die IT-Abteilung muss beide Remote Access-Technologien testen und dokumentieren. Für die Ausweitung der Lösung um mehr User und/oder Endpunkte ist zusätzlicher Zeitaufwand erforderlich.

- **Remote Access Betrieb:** Die Kostenbelastung durch den Einsatz beider Technologien ist erheblich. Dies gilt insbesondere dann, wenn herkömmliche SSL-Lösungen erweitert werden, um Remote Access-Probleme zu beheben. Nach Meinung von Frost & Sullivan kann das Versprechen, dass SSL eine „clientless"- Lösung sei, in der Praxis nicht umgesetzt werden. Da nicht alle Anwendungen webbasierend sind, muss die IT-Abteilung jede einzelne testen und für den unternehmensweiten Zugriff im richtigen Format bereitstellen. Um dieses Problem zu lösen, haben SSL-Hersteller ihr Angebot dahingehend erweitert, dass Remote User Zugriff auf alle gewünschten unternehmensweiten Ressourcen haben. Diese Anpassungen benötigen wiederum IT-Ressourcen, da Administratorrechte ausgegeben und verwaltet werden müssen.

- **Remote Access Wartung:** Auch die Wartung von IPsec- und SSL-VPNs erhöht die Kostenbelastung. Für beide Technologien muss die IT-Abteilung Ressourcen bereitstellen, um die Dokumentation zu aktualisieren, wenn sich das Einsatzgebiet bezüglich Anwendungen oder Anwender verändert. IT-Ressourcen werden auch dadurch zusätzlich belastet, wenn für eine großen Anzahl Anwender Zugriffsrechte definiert, ausgegeben und verwaltet werden müssen.

Eine Remote Access Connectivity Lösung muss die Komplexität des IT Systems reduzieren

Wie oben beschrieben, schmälert der gleichzeitige Einsatz von IPsec und SSL die Wirtschaftlichkeit einer VPN-Lösung, weil die IT-Abteilung mehr Arbeit damit hat. Zusätzliche Aufgaben und zusätzlicher Zeitaufwand implizieren auch eine gewisse IT-Komplexität. Ein wirtschaftlich geführtes Unternehmen benötigt deshalb eine Lösung, welche die IT-Komplexität reduziert damit alle Prozesse fehlerfrei ablaufen und die Einhaltung transparenter Berichtspflichten gewährleistet.

Die Auswirkungen von IT-Komplexität in den folgenden drei Bereichen:

- **Remote Access Strategie:** Der technische Leiter und die IT-Abteilung stehen vor einer schwierigen Aufgabe, wenn es darum geht, Unternehmensbedürfnisse und marktübliche Lösungen in Überein stimmung zu bringen. Dabei kann es passieren, dass der technische Leiter bei der Optimierung seiner Remote Access-Lösung nur unzureichende Unterstützung vom Hersteller erhält. Die IT-Abteilung erwartet auch, dass manuelle Arbeitsschritte wie die Bereitstellung, das Management und die Kontrolle des Remote Access reduziert oder zumindest vereinfacht werden. Werden IPsec und SSL gleichzeitig eingesetzt, müssen auch mehr Parameter (wie z.B. Endpoint Security-Risiken) bedacht werden. Dies erhöht wiederum die Komplexität für die IT-Abteilung, die für die Minimierung der Endpoint Security-Risiken zusätzlichen Aufwand betreiben muss.

- **Remote Access Betrieb:** Der Vorteil der praktischen Anwendbarkeit von SSL entsprechend der Bedürfnisse des Unternehmens ist in Wirklichkeit minimal. Steigt die Anzahl an SSL-Sitzungen, müssen Unternehmen mehr Sicherheitszertifikate verwalten und haben zudem weniger Transparenz bei der Kontrolle des Remote Access. Das zweite Verkaufsargument von SSL ist, dass es auf dem webbasierten Protokoll HTTP aufbaut. Entsprechend ist die Sicherheit bei SSL am besten in einer Webumgebung gewährleistet. SSL kann wie bereits erwähnt – durch Erweiterungen auch nicht webbasierete Anwendungen unterstützen. Dafür sind zusätzliche IT-Ressourcen erforderlich, die den vermeintlichen Vorteil der Einfachheit von SSL schnell wieder zunichte machen.

- **Remote Access Wartung:** Durch den gleichzeitigen Betrieb von IPsec und SSL erhält die IT-Abteilung ein komplexes Netz mit vielen Aufgaben. Das Risiko, dass sie den Wald vor lauter Bäumen nicht mehr sieht, ist groß. Das birgt ein großes Gefahrenpotential vor allem in Unternehmen, denen bei einem Fehler hohe Geldstrafen oder gar das Aus drohen.

Moderne Unternehmen benötigen Flexibilität bei dem Betrieb des IT-Systems

Herkömmliches IPsec als Insellösung gewährleistet einen sicheren Betrieb - wenn es um zentral verwaltete Geräte in einem abgeschlossenen Netz geht. Man muss aber trotzdem immer proaktiv auf Markttrends reagieren.

Da SSL auf dem webbasierten HTTP aufbaut, können Unternehmen Remote Access Connectivity einfacher verwalten. Dies ist jedoch dann nicht der Fall, wenn beide Protokolle eingesetzt und getrennt gemanagte werden müssen. Nach Meinung von Frost & Sullivan kann sich der Vorteil einer granularen Zugangskontrolle bei SSL nachteilig auswirken und das Sicherheitszertifikatsmanagement erschweren.

Beim gleichzeitigen Betrieb von IPsec und SSL existiert nach Meinung von Frost & Sullivan eine Diskrepanz zwischen den Bedürfnissen des Unternehmens und den auf dem Markt erhältlichen VPN-Lösungen. Diese Diskrepanz lässt sich lt. Frost & Sullivan mit NCPs ganzheitlicher Remote Access VPN-Lösung vermeiden.

"Es gibt eine Lücke bei der Implementierung von IPsec und SSL Lösungen; NCPs Lösung schließt diese Lücke indem es die praktischen Probleme präzise löst und dabei die Unternehmensbedürfnisse im Hinblick auf Kosten, Komplexität und Beweglichkeit der Lösung beibehält"

Frost & Sullivan

5. NCP NEXT GENERATION NETWORK ACCESS TECHNOLOGY - DAS BESTE AUS ZWEI WELTEN

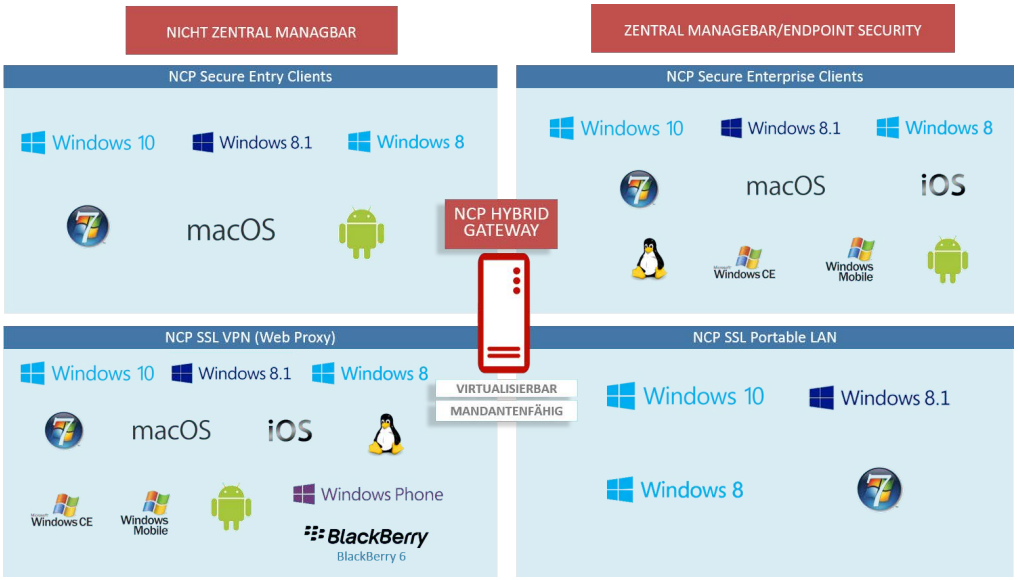
Für Frost & Sullivan ist die VPN-Lösung der NCP gut auf dem Remote Access Markt positioniert. Sie verschafft Unternehmen einzigartige Vorteile und behebt Implementierungsprobleme. Die integrierte IPsec/SSL VPN-Lösung entspricht insbesondere den Anforderungen der Unternehmen hinsichtlich Wirtschaftlichkeit, reduzierter Komplexität und flexiblem Betrieb.

Die NCP Secure Enterprise VPN Lösung besteht aus den folgenden Komponenten:

- **NCP Secure Enterprise Client Suite:** Universeller VPN Client, der es Unternehmen ermöglicht, den Remote Access für alle Benutzer einfach und fehlerfrei zu gestalten.
    - Integrierte dynamische Personal Firewall
    - Integrierter Internet Connector (Dialer)
    - Zentrales Management
    - Path Finder Technology
    - Seamless Roaming
    - Easy-to-Use (One Click)
    - Mobile Broadband

- **NCP Secure Enterprise Management:** Ein System, welches das Remote Access Management auf wenige Klicks reduziert – bei höchster Netzwerktransparenz.
    - Voll automatisierter Remote Access Betrieb
    - Network Access Control
    - Single Point of Administration
    - Change Management

Grafik 4: NCP Secure Enterprise VPN Management und NCP VPN Hybrid Gateway



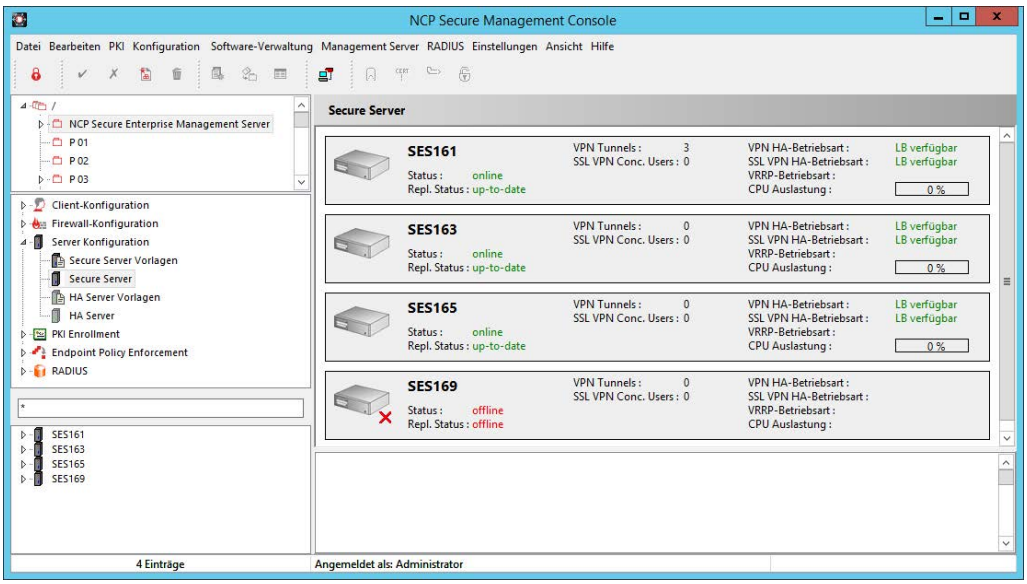
NCP ist wirtschaftlich

NCP ermöglicht ihren Kunden den wirtschaftlichen Betrieb einer Remote Access VPN-Lösung. Die Kosten für Management, Training, Dokumentation, User Helpdesk und Wartung werden nachhaltig reduziert. NCP unterstützt dadurch die Unternehmen bei einer der größten Herausforderung: Kosteneinsparungen.

NCP Secure Enterprise Client Suite ist eine VPN Client-Lösung, die sowohl direkt als auch indirekt die Kosten der IT-Abteilung senkt. Der Anwender arbeitet auf seinem Endgerät mit nur einer intuitiven Softwareoberfläche. Zentrale Konfigurationsvorgaben verhindern Fehlbedienungen und Sicherheitslöcher. Der Vorteil: Die IT-Abteilung muss die Benutzer nicht in jeder neuen Funktionalität oder Verbesserung am Remote Access System schulen und/oder eine Dokumentation erstellen. Indirekte Einsparungen entstehen durch weniger Helpdesk Anfragen, da die geringe Klickzahl Bedienungsfehler reduziert. Kurz gesagt, es reduzieren sich Aufgabenpotential und Serviceaufwand in der zentralen IT-Abteilung und dem User Helpdesk.

NCP Secure Enterprise Management (SEM) ist ein System für die zentrale Steuerung und Überwachung aller kommunikations- und sicherheitstechnischen Funktionen. Das Remote Access Management erfolgt mit nur wenigen Klicks über eine Konsole. Der IT-Administrator nutzt die Konsole u.a. um Lizenzen bereitzustellen, zu konfigurieren und zu verwalten. Dieser „Single Point of Administration“ schafft eine hohe Netzwerktransparenz und ist leicht handhabbar, was wiederum die Supportkosten verringert - ein weiterer Beitrag zur Wirtschaftlichkeit dieser Lösung.

Grafik 5: SEM Konsole



In Kapitel 6 wird dies weiter veranschaulicht.

NCP reduziert die Komplexität des IT-Systems

Alle NCP Produkte wurden unter der Zielsetzung entwickelt, Unternehmen dabei zu helfen, ihre IT-Komplexität zu reduzieren.

NCP Secure Enterprise Client Suite beinhaltet ein universelles Secure Endpoint Produkt, das auf fünf verschiedenen Betriebssystem-Plattformen läuft. Eine Parametersperre verhindert nachträgliche Manipulation - egal ob diese absichtlich oder versehendlich erfolgt. Die Parametersperre ist eine wichtige Funktionalität im Rahmen des ganzheitlichen Security-Managements zur Umsetzung und Aufrechterhaltung eines möglichst hohen Sicherheitsniveaus.

NCPs Secure Enterprise Management setzt auf den „Single Point of Administration“, der teuere IT-Ressourcen von überflüssigen Aufgaben befreit. Die Konsole wurde für die intuitive Nutzung bei voller Transparenz für alle Netzwerkressourcen entwickelt. Unternehmen profitieren von diesem einfachen Ansatz für die Verwaltung und Wartung auch komplexester Remote Access-Umgebungen. Ein Vorteil für das Unternehmen ist die Vereinfachung des Wissenstransfers innerhalb der IT-Abteilung. Der Schulungsbedarf von Administratoren wird verringert. NCPs Secure Enterprise Server fungiert sowohl als IPsec- als auch SSL- Gateway. Die Protokollauswahl pro Benutzer muss nicht mehr vorhergesehen und kann je nach Bedarf geändert werden . Dies ist u.a. von Vorteil bei einem hohen Fluktuationsgrad, ständig verändernden Remote Access-Umgebungen und Anwendergruppen. NCPs softwarebasiertes VPN Gateway erlaubt einem Unternehmen mehr als 100.000 gleichzeitige Verbindungen.

NCP ermöglicht den Unternehmen Flexibilität im IT-Betrieb

Wie oben bereits ausgeführt, erhöht NCPs VPN Lösung die Flexibilität von Unternehmen, indem es kostenintensive IT-Ressourcen von manuellen Aufgaben befreit. Insbesondere erlaubt NCPs Secure VPN Enterprise Management der IT-Abteilung, von zentraler Stelle alle Remote Access Verbindungen zu verwalten und dabei trotzdem Netzwerktransparenz für ein besseres Sicherheitsmanagement bereitzustellen.

Grafik 6: NCP Secure Enterprise Client Suite

NCPs Lösungen beheben die Implementierungsprobleme, vor die sich Unternehmen gestellt sehen. Die leichte Handhabung der Lösung durch die Enterprise Client Suite und das Enterprise Management System reduzieren die IT-bezogene Komplexität der Bereitstellung und Benutzung, des Managements und der Kontrolle des Remote Access. Die Enterprise Client Suite minimiert des Weiteren die Aufgaben im Bezug auf Endpoint Security-Risiken. Zusammengefasst glaubt Frost & Sullivan, dass es nur wenige IT Security-Lösungen gibt, die das Problem der Implementierung so direkt angehen.

6. GESAMTBETRIEBSKOSTENRECHNUNG FÜR NCPS NEXT GENERATION NETWORK ACCESS TECHNOLOGY

Anhand eines Beispielunternehmens mit 2.000 mobilen Benutzern wird die Wirtschaftlichkeit der NCP-Lösung mit der anderer Hersteller verglichen, indem einzelne Kostenstellen untersucht werden. Diese Kostenstellen beinhalten Equipment, das einmalig angeschafft werden muss, Softwarekosten, einmalige Bereitstellungskosten sowie dauerhafte Management- und Wartungskosten.

Das wichtigste vorneweg: Das folgende Gesamtbetriebskostenbeispiel zeigt im Vergleich zu den Ansätzen anderer Hersteller eine 41-prozentige Kostenersparnis mit NCPs Lösung.

Gesamtbetriebskostenbeispiel

Profil eines Beispielunternehmens das NCPs Lösung nutzt. (Die Grundannahmen werden für alle ROI Berechnungen weiter unten verwendet):

- Anzahl der mobilen Mitarbeiter: 2.000
- Kosten einer IT-Ressource: 150 US$ / Stunde

Verglichen mit der Lösung eines anderen Herstellers benötigt man für NCPs Lösung weniger Mannstunden pro User, um Sicherheitszertifikate zu verwalten und zu managen. NCPs Lösung reduziert die Komplexität des Remote Access Managements und damit in dieser Rechnung die pro User benötigte Arbeitszeit.

Die Kostenkalkulation für den ersten Software-Rollout eines anderen Herstellers:

2.000 mobile User * (0,5 Std/User * 150 $/Std) = 150.000 $

Die Kostenkalkulation für den ersten Software-Rollout von NCPs Lösung:

2.000 mobile User * (0,1 Std/User * 150 $/Std) = 30.000 $

"NCPs Lösung bietet im Vergleich zu anderen Remote Access Lösungen eine Kostenersparnis von mindestens 40 Prozent"

Frost & Sullivan

Die Kalkulation der durchschnittlichen, jährlichen Managementkosten der Lösung eines anderen Herstellers:

2.000 mobile User * (0.75 Std/User/Jahr * 150 $/Std) = 675.000 $

Die Kalkulation der durchschnittlichen, jährlichen Managementkosten von NCPs Lösung:

2.000 mobile User * (0.1 Std/User/Jahr * 150 $/Std) = 90.000 $

Die Kalkulation der gesamten zweijährigen Wartungskosten der Lösung eines anderen Herstellers:

20% * Kaufpreis (60.000 $) * 2 Jahre = 24.000 $

Die Kalkulation der gesamten zweijährigen Wartungskosten von NCPs Lösung:

20% * Kaufpreis (300.000 $) * 2 Jahre = 120.000 $

Grafik 7: NCPs Lösung bietet gegenüber anderen Remote Access Lösungen eine Kostenersparnis von 41%

Annahmen:

- Anzahl mobiler Mitarbeiter – 2,000
- IT Stundenlohn – US$150/Std.
- Stundenansatz pro User für:
  - Andere Hersteller:
    Anfangs-Rollout: 0,5 Std./User
    Management: 0,75 Std./User
  - NCP:
    Anfangs-Rollout: 0,1 Std./User
    Management: 0,1 Std./User
- Jährliche Wartungskosten:
  - 20% des Kaufpreises über 2 Jahre
- Hardware & Software:
  - Andere Hersteller: 60,000 US$
  - NCP: 300.000 US$

US$	Andere Hersteller	NCP
Equipment & Software	60,000	300,000
Anfangs-Rollout	150,000	30,000
Jährliche Wartungskosten	24,000	120,000
Jährliche Managementkosten	675,000	90,000
TCO	909,000	540,000
TCO/User	454.50/user	270/user

41% Einsparungen!

Quelle: NCP

7. DIE NCP-LÖSUNG WIRD DEN BEDÜRFNISSEN MODERNER UNTERNEHMEN GERECHT

Nach Meinung von Frost & Sullivan ist die NCP Secure Enterprise Lösung dem Remote Access Bedarf moderner Unternehmen gegenüber sehr gut aufgestellt. NCP fasst die drei Hauptvorteile von Remote Access Connectivity zusammen und, was noch wichtiger ist, löst die Implementierungsprobleme beim gleichzeitigen Einsatz von IPsec und SSL.

Die Wirtschaftlichkeit der NCP-Lösung kommt umso mehr zum Tragen je stärker die Zahl der mobilen Anwendern steigt. Wir glauben, dass ab etwa 2.000 mobilen Usern dieser Vorteil am besten genutzt werden kann. Dieser Effekt macht die NCP-Lösung für große Firmen sehr attraktiv. Für Frost & Sullivan spricht die NCP-Lösung die Bedürfnisse moderner Unternehmen ganzheitlich an und verhilft ihnen zu einem sicheren Standing in einer vernetzten Gesellschaft.

"NCPs Lösung behandelt die praktischen Implementierungs-probleme und behält dabei die Bedürfnisse eines modernen Unternehmens hinsichtlich Kosten, Komplexität und Flexibilität im Blick."

Frost & Sullivan

London
4 Grosvenor Gardens,
London SWIW 0DH
Tel. +44 (0)20 7343 8383
Fax +44 (0)20 7730 3343

Frankfurt
Clemensstraße 9
60487 Frankfurt a.M.
Tel. +49 (0)69 7 70 33-0
Fax +49 (0)69 23 45 66

Silicon Valley
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041
Tel. +1 650 475 4500
Fax +1 650 475 1570

+44 (0)20 7343 8383 • enquiries@frost.com
http://www.frost.com

ÜBER NCP

Die NCP engineering GmbH mit Hauptsitz in Nürnberg vereinfacht den sicheren Zugriff auf zentrale Datennetze via Internet. NCP Produkte und Lösungen erfüllen alle Anforderungen hinsichtlich Benutzerfreundlichkeit, Sicherheit und Wirtschaftlichkeit. Die Kernkompetenzen liegen auf den Gebieten IP-Routing, zentrales Management von remote Systemen sowie Verschlüsselungs-, VPN- und Firewall-Technologien. Das Unternehmen entwickelt Software für die einfache und sichere Anbindung von Endgeräten über öffentliche Netze an die Unternehmenszentrale in den Bereichen Mobile Computing, Teleworking, Filialvernetzung und M2M. Die Technologie der NCP Produkte garantiert die Integration und Kompatibilität mit den Produkten anderer Hersteller. Für die nationale und internationale Vermarktung der Produkte und Lösungen setzt NCP sowohl auf die Zusammenarbeit mit Technologie- und OEM-Partnern als auch auf den Vertrieb über Distributoren und zertifizierte Systemhäuser. Zu den Kunden zählen Unternehmen, Behörden und Organisationen.

ÜBER FROST & SULLIVAN

Frost & Sullivan ist der globale Partner für Unternehmen, wenn es um Wachstum, Innovation und Marktführung geht. Die Dienstleistungen Growth Partnership Services und Growth Consulting helfen dem Kunden, innovative Wachstumsstrategien zu entwickeln, eine auf Wachstum ausgerichtete Kultur zu etablieren und entsprechende Strategien umzusetzen. Seit 50 Jahren in unterschiedlichen Branchen und Industrien tätig, verfügt Frost & Sullivan über einen enormen Bestand an Marktinformationen und unterhält mittlerweile mehr als 40 Niederlassungen auf sechs Kontinenten. Der Kundenstamm von Frost & Sullivan umfasst sowohl Global-1000-Unternehmen als auch aufstrebende Firmen und Kunden aus der Investmentbranche. Weitere Informationen zum Thema Growth Partnerships unter http://www.frost.com.