

White Paper

VPN-Entscheidungsleitfaden

Entscheidungskriterien für IPSec oder SSL VPNs

Roslyn Rissler
Direktor - Produkt Marketing

Sarah Sorensen
Produkt Marketing Manager



Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
+1 408 745 2000 oder 888 JUNIPER
www.juniper.net

Artikelnummer: 350037-001 Apr 2004

Inhalt

Inhalt	2
Einsatzbereich	4
Network Layer VPNs	4
Was ist ein SSL VPN?	5
IPSec oder SSL VPN?	6
Total Cost of Ownership	8
Sicherheit	8
Netzwerkzugriff	8
Zugriff auf Applikationen	9
Zugriffs-Management	9
Zusammenfassung	10
Checkliste - Entscheidungskriterien SSL contra IPSec	11
IT-Umgebung	11
Anwenderkreis	11
Client-seitiges Netzwerk und Devices	11
Applikationen und Inhalt	12

Einsatzbereich

Sicherer Zugriff auf Unternehmensressourcen ist mittlerweile eine Notwendigkeit für Unternehmen geworden, und ist oft sogar erfolgsentscheidend. Alle Anwender, egal ob sie in einem Remote Office oder im Hotelzimmer arbeiten, müssen problemlos auf Unternehmensressourcen zugreifen, um ihre Arbeit produktiv erledigen zu können. Darüber hinaus benötigen Geschäftspartner und Kunden immer häufiger Echtzeitzugriff auf Unternehmensressourcen und -Applikationen.

Anfang der Neunzigerjahre gab es nur begrenzte Möglichkeiten, um die Verfügbarkeit des Unternehmensnetzwerks über die Grenzen der Unternehmenszentrale hinaus auszudehnen. Es handelte sich dabei meist um extrem teure und unflexible private Netzwerke und Standleitungen. Mit zunehmender Verbreitung des Internets wurde jedoch ein alternatives Konzept entwickelt, nämlich Virtual Private Networks (oder VPNs). Die meisten dieser Lösungen nutzten den kostenlosen/öffentlichen IP-Transportservice und das bewährte IPSec-Protokoll, um flexiblere, kostengünstigere Lösungen für einen sicheren Zugriff zu bieten. VPNs erfüllen effektiv den Bedarf an festen Site-to-Site Netzwerkverbindungen. Für mobile Anwender waren sie jedoch in vieler Hinsicht nach wie vor zu kostspielig. Bei Geschäftspartnern oder Kunden wiederum konnten sie nicht installiert werden. In dieser Umgebung kamen schließlich die SSL VPNs ins Spiel. Sie bieten Remote/Mobile Anwendern, Geschäftspartnern und Kunden den benötigten problemlosen, sicheren Zugriff auf Unternehmensressourcen. Gemeinsam können IPSec und SSL VPNs Remote Offices und Anwendern sichere, uneingeschränkte Verfügbarkeit des Unternehmensnetzwerks bieten und somit zum Geschäftserfolg beitragen.

Dieses Dokument beleuchtet die Unterschiede zwischen IPSec und SSL VPNs. Außerdem werden die Kriterien untersucht, die bei der Entscheidung, welche Technologie sich am besten für die jeweiligen Geschäftsanforderungen eignet, eine Rolle spielen.

IPSec Network Layer VPNs

IPSec VPNs (Network Layer VPNs) bieten Unternehmen eine einfache, kostengünstige Möglichkeit, Kommunikation zwischen verschiedenen Standorten zu verteilen. Sie liefern leistungsstarke Konnektivität und Ausfallsicherheit, um den Anforderungen anspruchsvoller Netzwerkumgebungen gerecht zu werden. Sie wurden als preiswerte Alternative zu Private Networks oder Standleitungen geschaffen. Unternehmen können damit die Internet-Infrastruktur nutzen, um das Private Network schnell auf geographisch verteilte Standorte auszudehnen.

Aus technischer Sicht entsprechen Network Layer VPNs der Anforderung, das Internet (das nur mit dem IP-Protokoll arbeitet und Text normalerweise unverschlüsselt überträgt) als Transportmedium für vertraulichen Multi-Protocol Traffic zu nutzen. Network Layer VPNs bieten eine Kombination aus Verschlüsselungs- und Tunneling-Funktionen, um diesen Anforderungen gerecht zu werden. Sie arbeiten mit Peer Negotiation-Protokollen wie IPSec, um die Daten in einem IP „Wrapper“ gekapselt über das Internet zu übertragen. Diese gekapselten Daten werden vom Network Layer VPN Gateway empfangen, „entpackt“, entschlüsselt und an den Empfänger weitergeleitet. Traffic vom VPN Gateway wird so behandelt, als ob er von einem Anwender im LAN kommen würde. Somit bieten Network Layer VPNs Anwendern denselben permanenten Zugriff auf das Netzwerk, wie über eine physikalische Verbindung. Eine normale Kommunikation und gemeinsame Nutzung von Ressourcen durch Anwender in geographisch getrennten Büros und eine unternehmensweite Produktivitätssteigerungen lassen sich damit leichter realisieren.

In bestimmten Fällen ist ein derart umfassender Zugriff jedoch gar nicht notwendig. Mobile Anwender, die beispielsweise nur ihre E-Mails lesen oder bestimmte Dokumente vom Intranet abrufen möchten, benötigen keine dedizierte Pipeline zu sämtlichen Ressourcen im Netzwerk. Außerdem könnte ein derart umfassender Zugriff ein Sicherheitsrisiko darstellen, wenn der „Endpunkt“ von dem aus der Zugriff erfolgt, nicht sicher oder leicht zu manipulieren ist. PCs innerhalb eines LANs lassen sich problemlos absichern. Die Implementierung von Sicherheitsfunktionen für Remote PCs in unmanaged Netzwerken ist jedoch schwierig und kostspielig. Deshalb sollten bei Verbindungen, die nicht von einem dedizierten Endpunkt ausgehen, der vom Unternehmen kontrolliert wird, die Ressourcen möglichst beschränkt werden. Die Verbindung sollte außerdem nicht ununterbrochen bestehen bleiben, um die Gefahr von Angriffen zu senken. Remote Anwender, die von einem untrusted Netzwerk aus auf Applikationen oder Ressourcen zugreifen, benötigen eine einfache, preiswerte Möglichkeit, um dies zu tun. Der Zugriff sollte jedoch nur auf die Applikation bzw. Ressourcen beschränkt sein und nicht für das gesamte Corporate-LAN erteilt werden. Gleichermaßen kann Geschäftspartnern von einem unmanaged Gerät aus Zugriff auf bestimmte Ressourcen gewährt werden, jedoch keine LAN-weite Konnektivität.

Ein weiterer Faktor, der bei IPSec VPNs berücksichtigt werden muss, sind die Management Ressourcen, die für die Installation und Wartung zur Verfügung stehen. Alle Remote- oder Mobile Anwender, die nicht über einen Aggregationspunkt zugreifen, müssen Client-Software auf ihrem Remote PC installiert haben. Für Unternehmen, die Hunderten oder sogar Tausenden von mobilen Anwendern Remote Access ermöglichen wollen, kann die Installation, Aktualisierung und Verwaltung all dieser Clients sehr zeit- und kostenaufwändig werden. Sollen externe Partner oder Kunden angebunden werden, vervielfachen sich diese Probleme noch. Für regionale Büros, Branch und Remote Offices, in denen das Unternehmen zuverlässige, hoch verfügbare Konnektivität benötigt und nur wenige Netzwerk VPN-Devices verwalten muss, ist dies eine notwendige und angemessene Investition. IPSec-Clients eignen sich von den Kosten her nur bedingt, um dem Bedarf von Remote/Mobile Mitarbeitern, Geschäftspartnern oder Kunden gerecht zu werden. Da beispielsweise eine VPN Client-Software notwendig ist, um Remote Anwender anzubinden, sind diese Anwender auf Geräte beschränkt, auf denen die Software installiert ist, d. h. Corporate-Laptops. Dadurch sind andere Zugriffsmethoden ausgeschlossen, wie z. B. Internet Kiosks, PDAs, etc., die für mobile Anwender häufig wesentlich komfortabler sind. Auch Geräte, die Geschäftspartner oder Kunden in ihrem eigenen Netzwerk nutzen, bleiben außen vor.

In dieser Umgebung haben SSL VPNs Einzug gehalten. Sie stellen eine benutzerfreundliche Lösung für mobile Anwender, Geschäftspartner oder Kunden dar und ergänzen die zuverlässige, leistungsstarke Kommunikationsinfrastruktur, die IPSec VPNs für Site-to-Site Verbindungen bieten.

Was ist ein SSL VPN?

Der Begriff SSL VPN bezeichnet eine neue und schnell wachsende Produktkategorie, die verschiedene Technologien nutzt. Will man grundlegend definieren, welche Produkte und Technologien zu dieser Kategorie gehören, könnte man mit dem Begriff „VPN“ selbst beginnen. VPN, oder Virtual Private Network, ist die Nutzung eines öffentlichen Netzwerks, wie das Internet, für die Übertragung vertraulicher Daten. Bis 2001 wurde VPN von der IT nur selten mit dieser Bezeichnung versehen, da fast alle der damals zur Verfügung stehenden VPNs mit Network Layer Transport arbeiteten. Im Bereich VPN war das IP Security Protocol (IPSec) einer der ersten Standards, auch wenn manche Hersteller andere Verfahren einsetzen, wie z. B. Layer 2 Tunneling Protocol (L2TP) und Point-to-Point Tunneling Protocol (PPTP).

SSL VPNs setzen auf eine völlig andere Methode beim Transport vertraulicher Daten über das Internet. Statt sich darauf verlassen zu müssen, dass der Endanwender einen konfigurierten Client auf einem Corporate-Laptop installiert hat, nutzen SSL VPNs SSL/HTTPS als sicheren Transportmechanismus, der ohne zusätzliche Softwareinstallation bei allen standardmäßigen Web-Browsern zur Verfügung steht. Bei einem SSL VPN wird die Verbindung zwischen dem mobilen Anwender und der internen Ressource über eine Web-Verbindung auf Applikationsebene hergestellt, und nicht über den offenen „Tunnel“ auf Netzwerkebene wie bei den IPSec VPNs. Der Einsatz von SSL ist aus folgenden Gründen ideal für mobile Anwender:

- SSL braucht nicht auf das für den Zugriff verwendete Gerät heruntergeladen zu werden.
- SSL braucht vom Endanwender nicht konfiguriert zu werden.
- SSL steht bei jedem normalen Web-Browser zur Verfügung. Die Anwender brauchen somit kein Corporate-Laptop.

Fast alle Anwender sind mit SSL vertraut, auch wenn sie über kein technisches Hintergrundwissen verfügen. Es ist bereits auf allen Internet-fähigen Geräten installiert, die einen standardmäßigen Web-Browser verwenden. Eine Konfiguration erübrigt sich. SSL arbeitet auf Applikationsebene, unabhängig vom Betriebssystem. Änderungen am Betriebssystem erfordern somit keine Aktualisierung der SSL-Implementierung. Und da SSL VPNs auf Applikationsebene arbeiten, kann eine differenzierte Zugriffssteuerung für Applikationen realisiert werden. Sie eignen sich somit hervorragend für mobile Mitarbeiter und Anwender, die über ungesicherte Endpunkte zugreifen.

IPSec oder SSL VPN?

Vielen Anwendern fällt die Entscheidung schwer, welche Technologie sie einsetzen sollen. Wie fügen sich IPSec- und SSL VPNs in die Security Policies Ihres Netzwerks ein, und welche Probleme lassen sich mit welcher der beiden Technologien lösen? Was ist eigentlich für die Installation und Verwaltung eines IPSec- und SSL VPN alles notwendig?

Die Diskussionen bzgl. IPSec und SSL drehen sich hauptsächlich um die technischen Details der Protokolle und nicht darum, was das wichtigste Entscheidungskriterium bei diesen Methoden sein sollte - nämlich die Nutzungsszenarien an sich. Dadurch wird nicht unbedingt mehr Klarheit geschaffen. In der Tat schließen sich IPSec und SSL nicht gegenseitig aus. Sie können in ein- und demselben Unternehmen installiert werden - was auch oft der Fall ist. Der entscheidende Faktor zwischen den beiden liegt nicht darin, was die einzelnen Protokolle leisten können, sondern was mit der jeweiligen Installation erreicht werden soll. Betrachtet man den Kosten/Nutzen der jeweiligen Installationsart sowie die Frage, welche Probleme sich damit lösen lassen, wird klarer, welche Installation gewählt werden sollte.

Weiterführende Informationen zu IPSec VPNs

Weitere Informationen finden Sie im White Paper von Juniper Networks „Dynamic VPNs Achieving Scalable, Secure Site-to-Site Connectivity: *How to replace WAN connections with a more reliable communication infrastructure*“ und in der Application Note „*How Different Approaches to Site-to-Site VPNs Affect Scalability and Connectivity*“.

Administratoren, die hohe Performance und redundante Site-to-Site Konnektivität erreichen müssen, sind mit den IPSec VPN-Lösungen gut bedient. Diese wurden erstellt, um Mitarbeitern auf der ganzen Welt sichere „Always-On“ Verbindungen zur Verfügung zu stellen, damit sie auf Unternehmensressourcen zugreifen und eine optimale Produktivität erzielen können. Seit Jahren liefern IPSec VPNs die ausfallsichere, zuverlässige Konnektivität, die für eine störungsfreie Kommunikation zwischen Kollegen in verschiedenen Standorten unerlässlich ist. IPSec VPNs bieten Anwendern an verschiedenen Standorten die gleiche Funktionalität, als wenn sie in der Unternehmenszentrale arbeiten würden. Sie können problemlos auf sämtliche Netzwerkressourcen zugreifen, die ihnen auch im LAN zur Verfügung stehen würden. Bei den meisten Applikationen hat die Verwaltung des Control Traffic (Anforderung von Dateien oder Server Advertisements) direkte Auswirkung auf den Datenverkehr. Wenn interne Anwender Dateien nicht gleich finden, werden sie diese wahrscheinlich auch nicht laden. Das ist nicht unerheblich, da sich Applikationen von Fall zu Fall anders verhalten. Selbst wenn nur Datenverkehr identifiziert werden kann, kann eine Regelung dieses Traffics durch Policies die Auswirkungen von Downloads auf anderen Traffic effektiv begrenzen.

Administratoren, die mobilen Mitarbeitern und anderen Anwendern, die nicht von „trusted“ (vom Unternehmen kontrollierten) Endpunkten kommen, Zugriff auf bestimmte Unternehmensressourcen bieten möchten, sind mit SSL VPNs gut bedient. Diese sind auf den Bedarf von Remote/Mobile Mitarbeitern sowie von Partnern oder Kunden abgestimmt, die von überall aus sicheren Zugriff auf bestimmte Unternehmensressourcen benötigen. SSL VPNs ermöglichen Administratoren die Implementierung einer sehr differenzierten Zugriffskontrolle. Dabei wird auf URL-, Datei- oder Serverebene festgelegt, auf welche Applikationen Anwender zugreifen dürfen. Diese Funktionalität senkt das Risiko, das mit Zugriffen von ungeschützten Endpunkten aus, über ein untrusted Netzwerk oder durch unbefugte Anwender verbunden ist. SSL VPNs bieten den Anwendern somit eine bequeme Möglichkeit, ortsunabhängig über ein beliebiges Web-fähiges Gerät auf Unternehmensressourcen zuzugreifen.

Führende Analysten prognostizieren, dass SSL in den nächsten Jahren die maßgebliche Zugriffsmethode für Remote und Mobile Anwender sein wird.

<i>Applikationstyp</i>	<i>PC-Typ</i>	<i>Remote Network Security</i>	<i>Verbindungstyp</i>	<i>VPN-Typ</i>
<i>Remote Office/ Branch Office</i>	<i>Corporate</i>	<i>Managed, Trusted</i>	<i>Fest</i>	<i>IPSec</i>
<i>Mobiler Mitarbeiter</i>	<i>Corporate oder Non-Corporate</i>	<i>Unmanaged, Untrusted</i>	<i>Mobil</i>	<i>SSL VPN</i>
<i>Partner/Kunden- Extranet</i>	<i>Non-Corporate</i>	<i>Unmanaged, Untrusted</i>	<i>Mobil</i>	<i>SSL VPN</i>

Total Cost of Ownership

Total Cost of Ownership ist eine wichtige Überlegung bei der Entscheidung, welche VPN-Technologie eingesetzt werden soll. Fassen wir noch einmal zusammen: Um diese Entscheidung treffen zu können, muss man sich unbedingt den Einsatzzweck ansehen und nicht die Technologie. Bei Bedarf an Site-to-Site Konnektivität, beispielsweise in einem Remote Office oder einem Branch Office, sind IPSec VPNs die logische und kostengünstigste Lösung. Anwender können in diesem Fall alle benötigten LAN-Funktionen nutzen, ohne verschiedene Clients verwalten zu müssen. Wenn jedoch Konnektivität für Remote/Mobile Anwender, Geschäftspartner oder Kunden erforderlich ist, die über ständig wechselnde Geräte und Netzwerke zugreifen, sind SSL VPNs die kostengünstigste Lösung. Administratoren können bestehende Investitionen in Authentifizierungs-Stores nutzen, differenzierte Rollen-/Ressourcen-basierte Policies erstellen und Zugriff für unterschiedlichste Anwendergruppen in wenigen Stunden ermöglichen. Dazu ist es nicht erforderlich, einzelne Software-Clients zu installieren, zu konfigurieren oder zu verwalten.

Sicherheit

Vergleiche zwischen IPSec und SSL enden häufig in der Diskussion „Welches Protokoll ist sicherer?“. In der Realität haben diese Diskussionen kaum eine Bedeutung für die Entscheidung zwischen SSL und IPSec für Remote Access und Site-to-Site VPNs. Diese Protokolle haben ähnliche Ziele. Sie sorgen für einen sicheren

Schlüsselaustausch und bieten starke Datensicherheit während des Transports. Trotz beträchtlicher Unterschiede bei den Protokollen arbeiten IPSec und SSL auf einem vergleichbar hohen Niveau. Beide Technologien sichern Netzwerk-Traffic effektiv. Und beide haben bestimmte Vorteile, so dass sie sich für unterschiedliche Anwendungen eignen. Die Implementierung der Protokolle erfolgt zwar unterschiedlich, doch weisen die beiden Systeme zahlreiche Gemeinsamkeiten auf. Dazu gehören die leistungsfähige Verschlüsselung und Authentifizierung sowie Protokoll-Session Keys, die auf ganz ähnliche Weise festgelegt werden. Jedes Protokoll unterstützt die führenden

Verschlüsselungs-, Datenintegritäts- und Authentifizierungstechnologien: 3-DES, 128 Bit RC4, AES, MD5 oder SHA-1.

IPSec VPNs schützen IP-Pakete, die zwischen Remote Networks oder Hosts und einem IPSec Gateway am Edge des privaten Netzwerks ausgetauscht werden. SSL VPN-Produkte schützen Applikation-Streams von Remote Anwendern zu einem SSL Gateway. Mit anderen Worten, IPSec verbindet Hosts mit ganzen privaten Netzwerken, SSL VPNs verbinden Anwender mit Diensten und Applikationen innerhalb dieser Netzwerke.

Netzwerkzugriff

IPSec VPNs sollen eine virtuelle Erweiterung des Corporate-LAN oder der darin enthaltenen VLANs ermöglichen. Diese Art von Zugriff ist für Remote Offices besonders wichtig, deren Mitarbeiter ungehinderten Zugriff benötigen, um effektiv arbeiten zu können. Anwender, die mit Site-to-Site Installationen arbeiten, unterliegen denselben Sicherheitsvorkehrungen wie im Corporate-LAN, inklusive unternehmenseigener und managed Devices und einer trusted Netzwerk-Topologie. Somit stellt dies kein größeres Sicherheitsrisiko dar als die LAN-Installation selbst. Diese Sicherheitsvorkehrungen lassen sich jedoch nicht effektiv auf mobile Anwender, Geschäftspartner oder Kunden ausdehnen, die von verschiedenen Geräten und Netzwerken aus auf Ressourcen zugreifen möchten. Für solche Einsätze kann ein SSL VPN die Zugriffsrisiken auf kostengünstige Weise mindern.

SSL ist in die Kritik geraten, da es über viele verschiedene Geräte Zugriff ermöglicht, darunter auch solche ohne Corporate Management, und weil es sich für eine Reihe verschiedener Endanwender problemlos bereitstellen lässt. In der Praxis ist diese Kritik jedoch nicht gerechtfertigt. Viele SSL VPN-Implementierungen bieten jetzt Methoden, um Endpoint Security durchzusetzen. Außerdem bieten sie Möglichkeiten, um PCs von allen Informationen zu „bereinigen“, die während einer Session heruntergeladen wurden.

Zugriff auf Applikationen

IPSec VPNs können alle IP-basierten Applikationen unterstützen - für ein IPSec VPN-Produkt sind alle IP-Pakete gleich. Somit sind sie die logische Wahl bei Site-to-Site Einsätze, bei denen es nicht akzeptabel wäre, wenn eine Ressource oder Applikation auf das Corporate-LAN beschränkt wäre.

SSL VPN Applikations-Services sind ganz unterschiedlich, da jeder Hersteller und jedes Produkt auf andere Weise die Client-Oberflächen über Browser darstellt, Applikations-Streams über das Gateway überträgt und die Integration in Zielsever im privaten Netzwerk vornimmt. SSL ist in die Kritik geraten, da früher jede Applikation Web-fähig sein musste. Dazu mussten neue Funktionen entwickelt und neue Software verteilt werden. Dieses Problem wurde von den führenden SSL VPN-Herstellern aus der Welt geschafft. Sie bieten jetzt Client-losen Webzugriff sowie einen Client Proxy für Client/Serveranwendungen oder uneingeschränkten Netzwerkzugriff. SSL VPNs können somit von verschiedensten Anwendern für einen sicheren Zugriff auf fast alle Applikationen genutzt werden.

Um es nochmals zu verdeutlichen: Wenn die Installation allen Anwendern uneingeschränkten Netzwerkzugriff von managed Geräten in trusted Netzwerke bieten soll, sind IPSec VPNs ideal. Soll jedoch mobilen Mitarbeitern oder Anwendern, die über unkontrollierbare Endpunkten zugreifen, wie z. B. Geschäftspartner oder Kunden, kontrollierten Zugriff auf bestimmte Unternehmensressourcen möglich sein, sind SSL VPNs ideal.

Zugriffs-Management

Eine weitere Überlegung ist die Zugriffskontrolle. IPSec-Standards unterstützen Selektoren auf Paketfilterbasis. In der Praxis gewähren viele Unternehmen Hosts jedoch Zugriff auf ganze Subnetze statt für jede IP-Adressänderung oder neue Applikation Selektoren erstellen bzw. ändern zu müssen. Wenn trusted User Groups Zugriff auf private Server und Subnetze erhalten sollen, sind IPSec VPNs eine hervorragende Lösung. Andererseits ist ein SSL VPN die optimale Wahl, wenn eine Zugriffskontrolle auf Anwender-/Gruppen- oder Ressourcenbasis benötigt wird. Kontrollen dieser Art lassen sich problemlos einrichten, da SSL VPNs auf Applikationsebene arbeiten. Neue Zugriffs-Management Funktionen können eine dynamische Authentifizierung und Rollenzuweisung sowie eine flexible und ausdrückliche Ressourcen-basierte Autorisierung ermöglichen. Damit lassen sich die Sicherheits-Policies eines Unternehmens auf sehr kostengünstige Weise durchsetzen.

Zusammenfassung

Noch wichtiger als das „bessere“ Transportverschlüsselungsprotokoll ist folgende Frage: „Welche Sicherheitstechnologie wird den Anforderungen an eine Remote Access-Lösung am besten gerecht?“ Da sich IP-Traffic mit Hilfe von IPSec absichern lässt und sich SSL für Traffic auf Applikationsebene zugeschnitten ist, eignet sich IPSec besonders gut für langfristige Verbindungen, bei denen umfassende und andauernde Zugriffe auf Netzwerkebene erforderlich sind. SSL eignet sich hingegen für Anwendungen, bei denen das System individuelle Anwender mit Applikationen und Ressourcen verbinden muss.

Checkliste

Entscheidungskriterien SSL contra IPSec

IT-Umgebung:	IPSec VPN	SSL VPN
Verbindungstyp	Feste Verbindung	Vorübergehende Verbindung
Gerätetyp	Managed Corporate Device	Verschiedene Geräte
Zugriffsart	Site-to-Site	Externer Mitarbeiter, Geschäftspartner, Kunde
Zugriffskontrolle		Ermöglicht Durchsetzung einer Access Management-Policy

Anwenderkreis:	IPSec VPN	SSL VPN
Mitarbeiter im Remote Office	x	
IT-Personal		x
Mobile Mitarbeiter		x
Day Extender		x
Berater		x
Kunden		x
Geschäftspartner		x

Client-seitiges Netzwerk und Gerät:	IPSec VPN	SSL VPN
Gerätetyp	Managed Corporate Device	Unmanaged
Netzwerktyp	Trusted	Untrusted
Spezifische Anwendungsfälle	Remote Office oder Branch Office	Internet-Zugang im Hotel, öffentliches Terminal (z. B. Kiosks oder Internet Café), PC des Kunden oder Geschäftspartners, Heim-Netzwerk

Applikationen und Inhalt:	IPSec VPN	SSL VPN
Voice Over IP	x	
Komplette Subnetze, die keine Zugriffskontrolle für Applikationen erfordern	x	
Netzwerke, inklusive Intranets und Extranets, die Zugriffskontrolle erfordern		x
Web-Applikationen	x	x
Client/Serveranwendungen	x	x
Intranet Inhalt	x	x
E-Mail	x	x
File Server	x	x
Server Socket-abhängige Applikationen	x	x

Copyright © 2004 Juniper Networks, Inc. Alle Rechte vorbehalten.

Juniper Networks, das Juniper Networks-Logo, NetScreen, NetScreen Technologies, Neoteris, Neoteris-Secure Access, Neoteris-Secure Meeting, NetScreen-SA 1000, NetScreen-SA 3000, NetScreen-SA 5000, IVEGigaScreen und das NetScreen-Logo sind eingetragene Marken von Juniper Networks, Inc. NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC und NetScreen ScreenOS sind Marken von Juniper Networks, Inc. Alle anderen Marken und eingetragenen Marken sind Eigentum der jeweiligen Unternehmen.

Änderungen der Angaben in diesem Dokument vorbehalten.

Kein Teil dieses Dokuments darf in irgendeiner Form oder mit irgendwelchen Mitteln (elektronisch oder mechanisch) zu irgendeinem Zweck reproduziert oder übertragen werden ohne schriftliche Genehmigung von:

Juniper Networks, Inc.

1194 N. Mathilda Ave. Sunnyvale, CA 95014 ATTN: General Counsel