

indev:s Technologie Information: SSL VPN und IPSec VPN

Remote Access: IPSec oder SSL VPN?

Unternehmen und Organisationen haben heutzutage gegensätzliche Aufgaben zu erfüllen, wenn es darum geht die Produktivität zu verbessern, Gewinne zu steigern und Risiken zu minimieren.

Zum einen wird zunehmend verlangt, dass die IT Systeme einem bestimmten Benutzerkreis, von Mitarbeitern zu Vertragspartnern und von Lieferanten zu Kunden, jederzeit einen "immer und überall" Zugriff auf Informationen ermöglichen. Die Entwicklung der Technologie von Virtuellen Privaten Netzen (VPN) hat diese Verfügbarkeit von Informationen ermöglicht. Die Weiterentwicklung von beidem, Netzwerk-Layer (IPSec) und Application-Layer (SSL) ermöglicht einen einfachen und effizienten "Site-to-site" und "User-to-site" Zugriff.

Zum anderen wird verlangt, dass interne Ressourcen und Systeme geschützt sind durch intelligente Technologie, je mehr Remote Access zur Anwendung kommt. Die veröffentlichten Horrorszenarien bei denen Hacker auf fremde Systeme zugreifen und sich fremde Identitäten ergaunern, zwingen Unternehmen ihre elektronisch gespeicherten Informationen vor unberechtigtem Zugriff zu schützen. Es ist tatsächlich so, dass es in vielen Fällen nicht schwerer ist für einen Hacker, sich einen Zugang zu verschaffen als es für einen autorisierten Benutzer ist.

Die indevis GmbH bietet verschiedene Technologien und Lösungsansätze führender Hersteller um einen wirklich sicheren Remote Access über SSL VPN und IPSec zu ermöglichen. Dieses Paper zeigt Ihnen die Unterschiede zwischen beiden Möglichkeiten auf und geht auch auf die Lösung der Problematik der sicheren Authentisierung solcher Systeme ein.

Inhalt

1. Einleitung

Warum SSL VPN
Fokus Sicherheit

2. SSL VPN vs. IPSec: Was ist besser?

Kosten und Administration
Flexibilität

3. RSA SecurID vs. Passwörter

Das Problem von Passwörtern

4. Schlussfolgerung

1. Einleitung

Immer mehr mobilen Benutzern muss ein Umfeld zur Verfügung gestellt werden, das ihre Produktivität auch außerhalb des Unternehmens sicherstellt. Anfangs haben Unternehmen versucht Benutzer mit Netzwerk Applikationen zu verbinden. Der ursprüngliche Weg – Einwahl Lösungen und Standleitungen - war langsam und teuer. Anfang der 90er Jahre wurde die VPN Technologie entwickelt. Sie ermöglichte den Transport privater Daten über das öffentliche Internet. Netzwerk-Layer VPNs verwenden eine Verbindungssoftware wie IPSec, die auf einem Client PC installiert wird, um Daten zu verschlüsseln und zu versenden. Die Daten werden dann als verschlüsselte Datenpakete über das Internet transportiert und auf der Gegenseite entschlüsselt. Traffic der am VPN Gateway von außen ankommt wird weitergeleitet als käme er aus dem internen Netzwerk, was dem Benutzer draußen den Eindruck vermittelt er befände sich im Netz (LAN). IPSec VPN ist somit ideal um Standorte miteinander zu verbinden. Sie sind ebenso eine gangbare Lösung, wenn eine Organisation nur einem sehr kleinen Benutzerkreis einen Zugang ermöglichen möchte. Die Einschränkungen einer solchen Lösung für einen großflächigen Einsatz sind folgende:

- Aufwendige Installation und Pflege von Software auf jedem Client PC
- Die Benutzer sind an die Firmen-PC Hardware gebunden, was ziemlich unpraktisch sein kann
- Dadurch dass IPSec VPN einen vollständigen LAN Zugriff ermöglicht, können sensible Informationen erlangt werden

Warum SSL VPN?

IPSec VPN ist eine gute Lösung für eine kleine Anzahl von vertrauenswürdigen Benutzern, die Zugriff auf das LAN von unternehmenseigenen PCs haben. Zunehmend werden Benutzer aber aus verschiedensten Umgebungen kommen: von Zuhause, Kunden, aus dem Hotel, etc. Sie werden verschiedenste Systeme nutzen (Laptops, PDA und Web-Telefone), und sie werden verschiedenen Benutzer-Gruppen angehören (Mitarbeiter, Vertragspartner, Lieferanten, Kunden). In diesen Fällen - und bei Organisationen mit vielen hundert oder tausend Remote Benutzern oder im Fall, dass die Organisation nicht die Kontrolle über die Client PCs hat (z.B. Lieferanten) wird es teuer, schwer zu administrieren oder gar unmöglich Client Software zu installieren.

Aufgrund dieser Herausforderungen kam eine neue Variante VPN hervor: SSL VPN. SSL VPNs benutzen das Secure Socket Protokoll, welches Bestandteil von allen Web Browsern ist und den sicheren Transport von Informationen über das Internet (wie beim Online Banking) anstelle von individueller Client Software sicherstellt. Dadurch dass SSL VPNs lediglich einen Web Browser und eine Internetverbindung benötigen, sind sie sehr

flexibel. Sie sind aber wiederum keine ideale Lösung, wenn es darum geht Standorte miteinander zu vernetzen.

Fokus Sicherheit

Weil VPNs darauf ausgelegt sind Zugang zu internen Informationen zu ermöglichen, werden Sicherheit und Zugriffskontrolle zu einem zentralen Punkt der Aufmerksamkeit. Sowohl IPsec als auch SSL VPN unterstützen Verschlüsselung um Vertraulichkeit und Integrität der Daten beim Netztransfer über das Internet sicher zu stellen. Dies stellt sicher, dass die Daten die gesendet wurden auch die Daten sind die erhalten werden. Es stellt jedoch noch nicht sicher, dass der Benutzer in einem IPsec oder SSL VPN Umfeld auch derjenige ist der er vorgibt zu sein. Bei IPsec VPN muss Client Software auf dem PC installiert sein. Dadurch, dass auf jedem Client PC Software installiert werden muss erweckt das den Eindruck, dass IPsec VPNs "vertrauenswürdiger" sind, obwohl dies nicht wirklich stimmen muss. Client Software kann kostenlos und einfach aus dem Internet heruntergeladen werden und Hacker-Methoden entwickeln sich ebenfalls weiter. SSL VPNs können einem größeren und auch "unbekanntem" Nutzerkreis Datenzugriff erlauben, da keinerlei Software auf dem Client PC installiert werden muss. Als Tatsache bleibt festzuhalten, dass jede Zugriffslösung ein System zur Benutzerauthentisierung benötigt. indevis empfiehlt hier eine starke Authentisierung von RSA Security.

2. SSL VPN vs. IPsec: Was ist besser?

Sowohl SSL als auch IPsec VPN sind effiziente Remote Zugriffslösungen. Beide haben sich in der Praxis bewährt. Sie sind beide gleich leistungsfähig und verschlüsseln auch gleich stark. Es ist aber so, dass sich IPsec und SSL VPN nicht gegenseitig

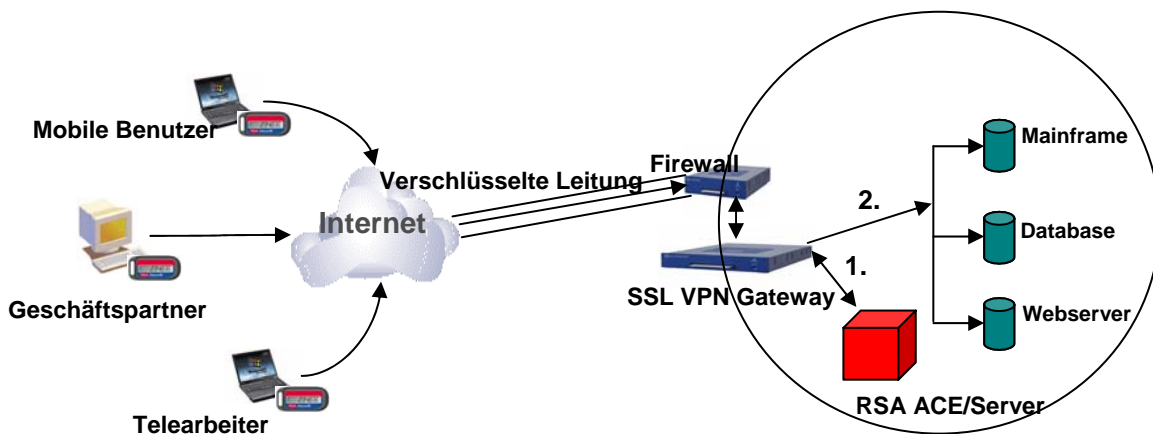
ausschließen - oft werden beide Lösungen gleichzeitig in Unternehmen eingesetzt. Jede hat seine Stärken die sie für bestimmte Einsatzgebiete prädestinieren. Beispielsweise sind IPsec VPNs ideal, für statische, langfristige Verbindungen zwischen Büros, während SSL VPNs bei Zugängen für eine große Benutzerzahl von mobilen Mitarbeitern und Geschäftspartnern im Rahmen von Extranet Umgebungen zum Einsatz kommen. Eine Einzelbetrachtung in den Schlüsselbereichen Kosten, Administration und Flexibilität folgt.

Kosten und Administration

Für einen echten Netzwerkzugriff und "site-to-site" Verbindungen bleiben IPsec VPNs das Mittel der Wahl. Sie eignen sich auch für den Remote-Zugriff, aber sie setzen auch voraus, dass auf jedem Client PC ein Software Client installiert und konfiguriert wird, der wenn nötig von Zeit zu Zeit erneuert werden muss. Bei einigen wenigen Anwenderzahlen ist dies ein gangbarer Weg. Bei Organisationen in denen eine größere Anzahl von mobilen Benutzern auf verschiedenste Systeme zugreift, wird das verteilen, konfigurieren und managen der Client Software eine administrative und finanzielle Belastung. Wenn zum Beispiel Geschäftspartnern oder Kunden ein Zugriff auf eigene IT-Systeme ermöglicht werden soll, ist die Verteilung von Client-Software oftmals gar nicht möglich. In solchen Fällen, bei denen eine Organisation keinen Zugriff auf die Client PCs hat, ist SSL VPN die bessere Wahl. Bei der Technologie von SSL VPN muss auf den Client PCs (oder PDAs, oder Mobiltelefonen) keine Client-Software installiert werden. Das spart Kosten. Zudem besteht bei SSL VPN die Verbindung zwischen dem Benutzer und dem Unternehmen auf Applikationsebene. Das SSL VPN System ist damit unabhängig. Wenn sich beispielsweise das Betriebssystem auf einem Client PC ändert, müssen in einem SSL VPN Umfeld keine



SSL VPN und RSA SecurID



Änderungen vorgenommen werden, während bei IPSec die Client Software erneuert und konfiguriert werden muss. Dadurch, dass es keine Client Software gibt, sind die Verteilungskosten sowie die Gesamtkosten einer solchen Lösung bei großen Benutzerzahlen deutlich niedriger.

Flexibilität

Auf teure Standleitungen kann zunehmend verzichtet werden. Verbunden mit dem Internet bieten IPSec VPNs eine günstige und flexible Verbindungsmöglichkeit. Im Rahmen einer Standortverbindung leisten IPSec VPNs die gleichen Dienste wie Standleitungen, aber erheblich günstiger. Für Remote User ist ein IPSec VPN eingeschränkt auf den PC auf dem die Clientsoftware installiert und konfiguriert wurde. Wenn eine Organisation die Kontrolle über jeden einzelnen Remote PC hat, ist IPSec ein möglicher Weg, der aber bei wachsenden Benutzerzahlen schwer zu administrieren ist. Wenn die IT keine Kontrolle über jeden einzelnen Remote PC hat, wie bei Geschäftspartnern, mobilen Mitarbeitern, Kunden, etc., dann ist SSL die sehr viel flexiblere Lösung. Bei SSL ist der Browser der "Client" - wie beim Online Banking. SSL VPNs sind damit sehr viel mehr skalierbar und bieten einen "immer und überall" Zugriff für jede definierte Benutzergruppe und ihre Rolle. Dadurch lässt sich sowohl die Produktivität, Kundenzufriedenheit und -service und Vertriebsaktivitäten steigern.

Beide VPNs sind effizient und ergänzen sich

IPSec und SSL VPN bieten Netzwerkzugriff für Remote User und stellen Standortvernetzungen sicher. Beide Varianten haben in verschiedenen Szenarien ihre Vorteile und zahlreiche Organisationen werden Einsatzgebiete für beide Lösungen haben. Beide sind - bezogen auf Ihr Einsatzgebiet und ihren Einsatzzweck - gleich gut. Dadurch dass beide Methoden einen sicheren Datenverkehr ermöglichen, kommt der Benutzerauthentisierung eine besondere Bedeutung zu. Der Benutzer der Datenzugriff erlangen möchte muss auch der Benutzer sein, der er vorgibt zu sein.

3. RSA SecurID vs. Passwörter

Trotz aller Annehmlichkeiten, die ein VPN bietet, gibt es mögliche Risiken. IPSec VPNs werden eingerichtet, um eine virtuelle Erweiterung des Firmennetzwerks zu ermöglichen. Ein gerouteter Tunnel zwischen dem Client und dem VPN Gateway (Firewall) verbindet die Client-Maschine mit dem Netzwerk. Wenn ein solcher Client PC in einem IPSec Netzwerk durch einen Wurm oder einen Virus befallen wird, sind das Netzwerk und die Server dadurch ebenfalls gefährdet. Weil SSL VPNs eine Verbindung auf Applikationsebene herstellen, ist das Netzwerk niemals im selben Rahmen bedroht. Trotzdem sind SSL VPNs verwundbar, weil auch das Internet verwundbar ist. Obwohl SSL eine Datenverschlüsselung bietet, wird meist nur

ein einfaches Passwort zum Schutz der sensiblen Daten eingesetzt, um nicht autorisierte Benutzer am Netzwerkzugriff zu hindern.

Das Problem von Passwörtern

Der Passwortschutz ist die verbreitetste Authentisierungsmethode um VPNs zu schützen, obwohl ein einfaches Passwort nur einen schwachen Schutz bietet. Dafür gibt es mehrere Gründe:

- Passwörter können verloren gehen, vergessen werden oder unberechtigten zugänglich sein
- Passwörter können erraten oder gehackt werden
- Schwache Passwort-Regeln (z.B. nicht regelmäßig geändertes Passwort, kein alphanumerisches Passwort, etc.) halten einer Sicherheitsüberprüfung nicht stand
- Starke Passwort-Regeln haben unbeabsichtigte Konsequenzen (z.B. Aufschreiben des Passworts) und erhöhte Helpdesk Kosten wenn Benutzer ihr Passwort vergessen

Passwörter sind nur eine "einfache" Authentisierung. Ein Benutzer benötigt nur ein korrektes Passwort um Datenzugriff zu erhalten. Sehr viel sicherer ist dagegen eine "Starke" Authentisierung, bei der ein Passwort oder eine PIN mit einer anderen Authentisierungsmethode kombiniert werden. Die Technologie von RSA Security zum Beispiel arbeitet mit sogenannten "Token" um eine Zwei-Faktor Authentisierung zu gewährleisten. Wenn Benutzer Zugang zu einem SSL VPN erlangen möchten, werden Sie nach ihrer PIN und dem zufällig generierten "Token Code" gefragt, der sich alle 60 Sekunden auf dem Token ändert. Erst wenn beides zueinander passt erhält der Benutzer Datenzugriff. Die PIN bzw. der Token allein sind wertlos - die korrekte Kombination von beidem ist erforderlich.

4. Schlussfolgerungen

Die Technologie von RSA SecurID ist effizient, flexibel und hat sich in der Praxis bewährt. Einfache Passwörter sind damit nicht zu vergleichen. RSA SecurID Token werden von weltweit mehr als 18 Millionen Benutzern eingesetzt. Durch ihre Flexibilität und technische Unabhängigkeit lassen sie sich perfekt im Umfeld von SSL VPN einsetzen. Trotzdem ist eine starke Authentisierung nicht nur auf SSL VPN zu beschränken, wenn ein erhöhtes Sicherheitsbedürfnis auch im IPSec Umfeld zu erkennen ist. Die Token gibt es in Form von Schlüsselanhängern und Kreditkarten. Software Token gibt es für Microsoft Windows Workstations, Pocket PC, Palm und Blackberry PDAs.

Bei der Auswahl und Beratung zu der für Ihre Organisation geeigneten VPN- und Authentisierungslösung und Technologieauswahl stehen Ihnen die IT Sicherheits-Spezialisten von indevis jederzeit gerne zur Verfügung:

www.indevis.de
info@indevis.de