IPSEC Protokoll - Einsatz, Aufbau, benötigte Ports und Begriffserläuterungen

ANLEITUNG SICHERHEIT VERSCHLÜSSELUNG & ZERTIFIKATE

spacyfreak (Level 2)
08.11.2007, aktualisiert am 30.01.2010

IPSEC nutzt fast jede Firma - doch kaum einer weiss was es damit auf sich hat.

Erklärungen gibt es dazu viele, doch leider auch zu viele unverständliche oder zu ausführliche, die keiner versteht.
Das Problem liegt nicht nur an der Komplexität des IPSEC Protokolls, sondern zu allem Übel an den verschiedenartigsten Möglichkeiten, wie man IPSEC konfigurieren kann. Dadurch kann der Eindruck entstehen, verschiedene IPSEC- Erklärungen die man im Internet findet, würden gegensätzliches aussagen - dabei gehen die Erklärungen oft einfach nur von verschiedenen IPSEC Konfigurationsvarianten aus.

Ich will versuchen, die wichtigsten Merkmale und Begrifflichkeiten rund um IPSEC zu erklären ohne zu sehr auf jedes einzelne Detail einzugehen, da IPSEC mit allen Einzelheiten wohl Bände füllen könnte.
Da es jedoch selbst für einen Administrator spannenderes gibt als jedes Detail von IPSEC zu verstehen, dürften die unten stehenden Informationen für geschätzte 99,9% aller Administratoren ausreichen, um IPSEC zu VERSTEHEN.
Wie man es konfiguriert ist wieder eine Wissenschaft für sich und hängt vom Hersteller ab, auf dessen Gerätschaft man IPSEC konfigurieren soll. Vor dem Konfigurieren kommt aber das Verstehen, und darum geht es in diesem Tutorial.

Falls sich fachliche Fehler eingeschlichen haben sollten oder man das eine oder andere noch einfacher erklären kann freue ich mich über kompetenten Input.

Inhaltsverzeichnis

Welche Ports muss man öffnen um IPSEC machen zu können?

Kommt ganz darauf an! Je nachdem, wie der VPN Server konfiguriert ist, brauchen wir

- **UDP Port 500 und IP-Protokoll ESP (Obacht: ESP hat keine Ports, es ist ein L3 Protokoll! Guggst du!)**

oder

- **UDP Port 500 und UDP Port 4500 (Wenn ESP via NAT-T in UDP gekapselt wird)**

oder

- **TCP Port 10.000 (Wenn IKE und ESP in TCP gekapselt werden)**

Auf der sicheren Seite ist man, wenn also die Ports UDP500, UDP4500 und TCP10.000 und IP Protokoll ESP zwischen den VPN Partnern offen sind.

Erläuterungen zu den Ports und was es mit den einzelnen Varianten auf sich hat - siehe unten!

IPSEC BLITZ-ERKLÄRUNG FÜR SCHNELLENTSCHLOSSENE!

IPSEC ist eine Protokollsuite die IP-Verbindungen sicherer machen soll.
Es wird vor allem für VPN Verbindungen eingesetzt und ist das verbreitetste VPN Protokoll.

IPSEC besteht im wesentlichen aus den Protokollen IKE und ESP.

IKE ist die technische Umsetzung des ISAKMP Frameworks. IKE nutzt UDP Port 500.

IKE Phase 1 baut einen sicheren Verbindungs-Kanal auf. Dabei findet auch die "Authentisierung" zwischen den VPN Partnern statt, die mit Zertifikaten oder Pre-Shared Keys (Passwörtern) erfolgen kann.

Dieser sichere Verbindungskanal wird dann genutzt, um die Parameter aus Phase 2 sicher zwischen den VPN Partnern aushandeln zu können.

IKE Phase 2 handelt die Verschlüsselungs- und Integritätsparameter aus, mit denen die eigentlichen Daten gesichert werden.

Nach Aushandlung der SAs (Security Assotiations) in IKE Phase 2 wird das Protokoll ESP benutzt, um letztendlich die verschlüsselten Daten zu transportieren. ESP hat keinen Port, da es ein OSI Layer 3 Protokoll ist.

Bei Einsatz von NAT-Traversal (auch NAT-Transparency genannt), um auch über PAT-Router ESP Verbindungen aufbauen zu können, braucht man Port UDP4500. Dabei wird ESP in UDP gekapselt, da ESP keine Ports benutzt und dadurch nicht "gepattet" werden kann.

Bei Einsatz von IPSEC-over-TCP braucht man nur Port TCP10.000. Dabei werden IKE als auch ESP in TCP gekapselt, und über diesen einen Port TCP10.000 geleitet. **Geheim-TIP:** Man kann den Port am VPN Server auch von TCP10.000 aúf einen anderen ändern (z. B. TCP80), so dass ein IPSEC Tunnel auch von Lokationen aus aufgebaut werden kann, die nur wenige Ports geöffnet haben - z. B. in WLAN Hotspots. Dies funktioniert aber nur, wenn zwischen den VPN Endpunkten keine Firewall auf Applikationsebene die Art des TCP Verkehrs filtert und z. B. "Nicht-HTTP-Traffic" erkennt und verwirft.

Im IPSEC Tunnelmode werden IP-Pakete in andere IP-Pakete gekapselt (getunnelt). Dadurch kann ein zugreifender Client eine "virtuelle" IP aus dem IP-Bereich des Firmen-Netzes bekommen und sich netzwerktechnisch mit dem Firmen-Intranet verbinden, als wäre er im Büro.

Detailiertere Erklärung zu IPSEC

Begrifflichkeiten rund um IPSEC

- Tunnelmode. Im Tunnelmode wird ein komplettes IP-Paket (welches die virtuelle Firmen-Netz-IP-Adresse enthält die der Client bei VPN Aufbau sowie die Daten enthält) in ein anderes Paket (welches die "realen" IPs des Clients u. VPN Servers enthält) gekapselt. Damit kann der Remote Access Benutzer eine "virtuelle" IP aus dem Firmen-Intranet verpasst bekommen, und im Firmen-Intranet von daheim aus agieren, als wäre er im Büro. Wird vor allem für Remote-Access VPN Verbindungen (Client zu Server) verwendet.

- Transportmode. Im Transportmode werden die Daten verschlüsselt, der IP-Header bleibt jedoch erhalten. Wird vor allem bei Site-to-Site VPN Verbindungen verwendet. Hat einen geringeren "Protokoll Overhead" als der Tunnelmode und ist daher etwas performanter.

- ISAKMP (Internet Security Associations and Key Management Protocol): Framework, das die Authentisierung u. Schlüsselaustausch zwischen den VPN Partnern beschreibt, jedoch die eigentliche Technik wie dies zu realisieren ist, nicht festlegt. Dadurch sind verschiedenste Schlüssel-Austauschverfahren anwendbar.

- IKE (Internet Key Exchange). Hybrid-Protokoll (bestehend aus Teilen von Oakley u. SKEME) das den sicheren Austausch von Schlüsseln sowie Sicherheits-Parametern für de VPN Tunnel über ein unsicheres Netz ermöglicht. IKE stellt quasi die technische Umsetzung des ISAKMP Frameworks zum Austausch von Parametern und Schlüsseln für den auf diesen Parametern und Schlüsseln basierenden IPSEC Tunnel dar, der wiederum per ESP realisiert wird. IKE nutzt UDP Port 500.

- SKME & Oakley: Teile dieser Protokolle werden innerhalb des IKE Protokolls verwendet zur Verschlüsselung per "public key" und rasche Erneuerung ablaufender Schlüssel; Einsatz sogenannter "nonces" (Zufallszahlen)

- Diffie-Hellman: Public-Key-Algorithmus der innerhalb des IKE Protokolls zum sicheren asymetrischen Austausch von Schlüsseln und Aushandlung eines symetrischen Schlüssels verwendet wird. Es gibt 7 verschiedene Varianten von Diffie-Helman Algorithmen, die sich in der Schlüsselstärke unterscheiden.

- IKE Main Mode. Im IKE Main Mode werden für die einzelnen Schritte (Schlüsselaustausch etc) einzelne Verbindungen nacheinander aufgebaut.

- IKE Aggressive Mode. Im Aggressive Mode werden einzelne Schritte des Mainmode zusammengefasst (schneller, aber rein theoretisch weniger sicher).

- ESP (Encapsulating Security Payload). (Protokoll-Type 50 auf Layer 3), welches verschlüsselt Daten zwischen zwei VPN Partnern überträgt. ESP hat mit NAT keine Probleme - mit PAT allerdings schon. ESP ist das Transportmedium, das letztendlich die Daten zwischen den VPN Partnern transportiert, basierend auf den in IKE Phase2 ausgehandelten Verschlüsselungs- und Hashparametern. Die aus der IKE Phase2-Aushandlung resultierenden SAs werden im SPI (Security Parameter Index) in jedem ESP Paket mitgesendet.

- AH (Authentication Header). Nicht mehr eingesetztes Variante, die von ESP weitgehend abgelöst wurde. AH konnte nicht über NAT Router verwendet werden. AH stellt die Datenintegrität sicher - verschlüsselt jedoch nicht.

- AES, 3DES, DES. Dies sind Verschlüsselungsverfahren. AES ist performant und sicher (128,192 oder 256 bit). 3DES (168bit) gilt als sicher, aber nicht so performant wie AES. DES(56bit) sollte man nicht einsetzen, wird (wohl) nur noch aus Kompatibilitätsgründen angeboten, falls die "gegenstelle" nur DES unterstützt.

- SHA1, MD5. Hash-Algorithmen. Diese werden innerhalb IPSEC benutzt, um die "Datenintegrität" zu gewährleisten. Durch Prüfsummen, die in jedem IPSEC Paket mitgesendet werden, wird gewährleistet, dass die Daten nicht auf dem Wege verändert wurden, da veränderte Daten eine andere Prüfsumme ergeben würdem auf dem Ziel-VPN-Server, und nicht akzeptiert werden würden.

- HMAC: Mechanismus, der SHA1 oder MD5 zur Gewährleistung der Datenintegrität verwendet.

- SA (Security Assotiation): Ausgehandelte Sicherheits Parameter zwischen zwei VPN-Partnern (z. B. Verschlüsselung, Hash, lifetime).

- SPI (Security Parameter Index). Zahl, die in Verbindung mit der IP-Adresse und dem Sicherheitsprotokoll die Sicherheitsassoziation identifiziert. Anhand des SPI stellt der VPN Server fest, welche Sicherheitsparameter zuvor ausgehandelt wurden.

- PFS (Perfect-Forward-Secrecy): Das Brechen eines einzelnen Schlüssels liefert nur Zugang zu den Daten der betroffenen Nachricht, nicht aber zu anderen Nachrichten oder Schlüsseln. Ein Verschlüsselungssystem er- reicht dies, indem es die Schlüssel oft wechselt, wobei einzelne Schlüssel nicht voneinander abgeleitet sein dürfen.

- Replay-Protection: Schützt vor erneutem Verwenden von abgehörten Datenpaketen durch einen Angreifer. Damit wäre ein Denial-of-Service Angriff möglich durch Erschöpfung der CPU Ressourcen des VPN Servers.

- Split-Tunneling: Wenn man Split-Tunneling "disabled", also deaktiviert, werden alle Daten, die ein VPN Client über das Netzwerk senden will, in den VPN Tunnel geschickt. Kein anderer PC kann mit dem Client kommunizieren, ausser PCs die am "anderen Ende des Tunnels" sind. Damit soll verhindert werden, dass ein eventueller Angreifer über den VPN Client PC Zugang zum Firmen-Intranet erhält. Ist Split-Tunneling "enabled", kann der VPN Client auch andere Verbindung gleichzeitig starten, während der VPN Tunnel aufgebaut ist. Nachteilig wirkt sich das Abschalten von Split-Tunneling vor allem aus, wenn der Benutzer lokale Netzwerkdrucker verwenden will. Diese sind nicht erreichbar, so lange der VPNTunnel aufgebaut ist, wenn Split-Tunneling ausgeschaltet ist.

- NAT-Traversal (auch NAT Transparency genannt): Einkapselung von ESP in UDP Pakete um auch über PAT-Router IPSEC machen zu können. Nutzt Port UDP 4500.

- NAT Keepalives. Kleine Dateibrocken die regelmässig gesendet werden, um bei Einsatz von NAT-Traversal (udp) den prinzipbedingten Tunnelabbruch durch Einsatz von UDP zu verhindern. UDP Verbindungen haben im Gegensatz zu TCP Verbindungen eine kurze Lebensdauer.

Cisco-spezifische Ausdrücke rund um IPSEC

- IPSEC-over-TCP: Einkapselung von IKE und ESP in TCP. Braucht NUR Port TCP 10.000

- "ISAKMP": Im Cisco Jargon bezeichnet isakmp die Konfiguration von IKE Phase 1.

- "IPSEC": Im Cisco Jargon bezeichnet IPSEC die Konfiguration von IKE Phase 2.

- "Transformsets": Im Cisco Jargon bezeichnet dies die ausgewählten Security Assotiations für IKE Phase 2 (z. B. AES256bit / SHA1)

- "Crypto Map": Im Cisco Jargon die Zusammenfassung der eingestellten Parameter. Die Crypto Map wird an das Interface gebunden, das als Tunnel-Endpunkt dienen soll.

- "Interesting Traffic": Traffic, der basierend auf einer konfigurierten Access Liste in den Tunnel geschickt werden soll. Die zu konfigurierende Access-Liste (in Verbindung mit der Crypto Map) definiert also beispielsweise, dass jeglicher Traffic, der zu einem bestimmten Netz (z. B. das Subnetz der Partner-Site) geroutet werden soll, per IPSEC geschützt wird.

Einsatz von VPNs

VPNs (Virtual Private Networks) dienen dazu, zwei Netze miteinander zu verbinden über einen virtuellen Tunnel, der die Daten schützt, und somit sensible Daten auch über "unsichere" Netze (z. B. Internet) transportieren zu können.

Site-to-Site VPNs

Während man natürlich zwei Netze (zum Beispiel zwei Standorte einer Firma) mit Standleitungen verbinden kann, stellen VPNs eine sichere und weitaus kostengünstigere Methode dar, Firmen-Netze miteinander verbinden zu können.
Im Gegensatz zum Remote Access VPN müssen die Client Rechner bei dieser Variante keinen speziellen "VPN Client" installieren, da der VPN Tunnel zwischen zwei VPN Servern (z. B. Cisco PIX, ASA oder VPN Concentrator, oder in kleineren Firmen auch Draytec oder Netgear) aufgebaut wird, und der Traffic von einem der Standorte zum anderen Standort automatisch über den VPN

Tunnel geschleust wird. Der Benutzer merkt im Grunde garnicht, dass seine Daten, die er eventuell zum anderen Standort sendet, über einen VPN Tunnel gesendet werden.

Remote Access VPNs

Damit reisende Mitarbeiter oder Homeoffice-Benutzer auf Firmen-Intranet Ressourcen zugreifen können, kann man eine VPN Remote Access Lösung einsetzen. Dazu muss der Benutzer einen VPN Client auf seinem PC installieren, den VPN Client starten und sich authentisieren, um auf die Firmen-Ressourcen zuzugreifen. Wenn der Client den Tunnel aufgebaut hat, hat er in aller Regel eine "virtuelle" IP-Adresse aus dem Firmen-IP-Bereich, den ihm der VPN Server verpasst (Tunnelmode). Damit ist der PC des Benutzers auf Netzwerkebene in das Firmen-LAN integriert, als wäre er in seinem Büro.

IPSEC ist der defacto Standard in Sachen VPN Protokolle. Man verwendet dieses Protokoll vor allem für Site-to-Site Verbindungen beispielsweise zwischen zwei Niederlassungen einer Firma, oder als Remote-Access Lösung für reisende Mitarbeiter oder Homeoffice-Benutzer, die eine sichere Verbindung ins Firmennetz benötigen. IPSEC wurde eigentlich für Site-to-Site VPNs designt, setzte sich jedoch auch im Remote Access Bereich durch. IPSEC "könnte" in den nächsten Jahren im Remote Access Bereich durch SSL VPNs abgelöst werden - doch das ist ein anderes Thema.

Wie der Name bereits andeutet, sichert IPSEC Daten auf dem OSI Layer 3 (Network bzw. IP Ebene).
Im sogenannten "Tunnelmode" wird das gesamte IP-Paket in ein anderes IP-Paket gekapselt, daher die Bezeichnung "Tunnel".

IPSEC ist eine Protokollsuite, die aus einer Vielzahl von Unterprotokollen besteht. Dies macht IPSEC recht kompliziert.
Es ist eventuell gar eines der kompliziertesten Netzwerkprotokolle überhaupt.

Was ist der Vorteil von IPSEC?

IPSEC versucht eine Vielzahl von Anforderungen, die man an eine "sichere" Verbindung über ein unsicheres Netzwerk (Internet) stellt, zu erfüllen. Ferner hat sich IPSEC als sicheres, performantes und stabiles VPN Protokoll durchgesetzt.

Diese Anforderungen die IPSEC erfüllen will:

- Verschlüsselung:

Die "sensiblen" Firmen-Daten dürfen nicht für Dritte lesbar sein. Darum werden sie verschlüsselt.

Als derzeit "sicher" und gleichzeitig "performant" gilt AES (128, 192 oder 256Bit) Verschlüsselung. Je höher die Bit-Stärke, desto "sicherer" die Verschlüsselung - doch damit steigt auch die CPU Belastung des VPN Servers.
Alternativen zu AES wären 3DES (168Bit) oder DES(56bit).

3DES gilt ebenfalls als sicher, aber langsamer als AES. DES dagegen gilt als unsicher und sollte nicht verwendet werden.

- Daten Integrität:

Die Daten dürfen auf dem Weg zwischen Absender und Empfänger nicht verändert werden können.
Um die Daten Integrität zu gewährleisten, werden Hash-Algorithmen verwendet.
Derzeit gilt SHA1 als (noch halbwegs) sicher, während MD5 zwar schneller, aber weniger sicher ist.

- Sichere Authentisierung:

Damit sich bei einer Site-to-Site VPN Verbindung nur autorisierte VPN Server miteinander einen Tunnel aufbauen können, muss eine sichere Authentisierung integriert sein. Hier hat man die Auswahl zwischen Zertifikaten oder so genannten Preshared Keys (Passwörter).
Bei Remote Access Verbindungen von Mitarbeitern authentisiert sich der Benutzer meist mit einem Passwort. Sicherer sind Zertifikate oder Einmal-Passwörter (z. B. RSA SecurID Token). Hier muss individuell abgewägt werden was man benötigt, um einen Kompromiss zwischen Sicherheitsbedarf, benutzerfreundlicher Handhabung und Kosten zu finden.

Protokoll Aufbau von IPSEC

IKE (Internet Key Exchange)
IKE ist quasi gleichbedeutend mit ISAKMP (Internet Security Association and Key Management Protocol).
Es dient zum einen zum sicheren Austausch von Schlüsseln über ein unsiches Netzwerk, wofür der Difi-Hellman Algorithmus verwendet wird. Zum anderen dient IKE zur "Aushandlung" von Sicherheits Parametern, wie Verschlüsselungs-Variante und Stärke, Hash-Algorithmus (zur Datenintegrität, sprich Gewährleistung dass die Daten nicht auf dem Weg zum Empfänger verändert wurden) sowie Authentisierung (per Zertifikaten oder Preshard Keys / Passwörtern).

IKE Phase 1
Die IKE Phase 1 dient prinzipiell zum **Aufbau eines "sicheren" Kanals** zwischen den zwei VPN-Servern, oder zwischen Remote-Benutzer und VPN Server. Dabei wird auf UDP Port 500 mit dem VPN Server kommuniziert.
In IKE Phase 1 werden - worauf der Name bereits hinweist - "Schlüssel ausgetauscht".

Zum Schlüsselaustausch wird der **Diffi-Hellman Algorithmus** verwendet. Diese geniale Erfindung stellt eine sichere Methode dar, Schlüssel über ein unsicheres Medium zu übertragen und einen symetrischen Schlüssel zu berechnen, der nur für die jeweilige Session gültig ist. Mittels diesen Schlüssels wird die Kommunikation dann verschlüsselt.

Der **Lifetime** Parameter bestimmt nur dann die Lebenszeit des Administrators, wenn er die

Lifetime auf beiden VPN Servern einer Seite-to-site Verbindung UNTERSCHIEDLICH konfiguriert. Die lifetime muss auf beiden identisch sein, da der Tunnel ansonsten in regelmässiger Unregelmässigkeiten abbricht und man sich beim Troubleshooting den Wolf sucht.

IKE Phase 2
In der IKE Phase 2 handeln die VPN Partner aus, **welche Verschlüsselungsvariante und -Stärke, mit der die eigentlichen Daten verschlüsselt werden sollen**, sowie die "lifetime" (Lebensdauer des ausgehandelten Schlüssels). Die Aushandlung aus Phase1 betrifft also nur die Parameter zum Aufbau des "sicheren Kanals".

Die Aushandlung der Parameter in Phase2 betrifft nur die Sicherungs-Parameter für den Datenkanal!

Man könnte die Sache auch so interpretieren, dass die Designer des IPSEC Protokolls recht paranoid waren, dass sie so viel Sicherheit eingebaut haben - zumal dies das Protokoll beliebig kompliziert und damit fehleranfällig und angreifbar macht. Dies zumindest Bruce Schneiers (Sicherheits-Guru) Meinung zu IPSEC - "zu kompliziert um sicher zu sein". Nichts desto trotz gilt IPSEC als das sicherste VPN Protokoll das man derzeit einsetzen kann - vor allem wenn man AES und SHA1 verwendet, ist der Tunnel an sich, zumindest momentan, quasi nicht zu knacken. In Verbindung mit einer sicheren Authentisierungsmethode (Zertifikate, oder RSA Tokens bei User-Zugriff) ist das Ding als sicher zu betrachten.

Die ausgehandelten Parameter (also Verschlüsselungsvariante- und Stärke, Hash-Algorithmus sowie lifetime) nennt man auch **SAs (Security Assoitiation)**. Die SAs stellen also die "Policy" dar die die beiden VPN Partner ausgehandelt haben. Die Möglichkeit, dass beide VPN Partner die einzelnen Parameter, die für den IPSEC Tunnel verwendet werden sollen, aushandeln können macht IPSEC recht flexibel, und ermöglicht auch die Zusammenarbeit zwischen VPN Servern verschiedener Hersteller.

Zumindest eines der verfügbaren Varianten (Schlüssel, Hash) müssen also beide VPN Server die zusammen einen VPN Tunnel aufbauen wollen, beherrschen.

Beispiel: Kann VPN Server 1 nur AES, und VPN Server 2 nur 3DES, kann kein VPN Tunnel zwischen beiden Servern aufgebaut werden. Beherrscht VPN Server 1 jedoch AES und DES, der zweite jedoch AES und 3DES, werden sich die beiden VPN Server auf AES "einigen".

Nach IKE Phase 2 (Aushandlung von SAs) kommt das Protokoll **ESP (Encapsulating Security Payload)** zum Einsatz, das die Daten verschlüsselt zwischen den VPN Servern transportiert. IPSEC nutzt im Tunnelmode **ESP, um die Daten in einem IP-Paket, das in ein anderes IP-Paket "eingekapselt" bzw. "getunnelt" wird, zu transportieren und zu verschlüsseln**.

ESP (Encapsulating Security Payload)
ESP nutzt keinen "Port", da es ein reines Layer 3 Protokoll ist (wie IP oder auch ICMP) und kein

Transportprotokoll wie UDP oder TCP (Layer 4), welche prinzipiell Ports nutzen um eine Verbindung aufzubauen.

Hintergrund-Wissen zum ESP Protokoll, NAT-Traversal und IPSEC-over-TCP

ESP hat jedoch den Nachteil, dass es bei Netzwerken, die **PAT Router (Port Address Translation)** benutzen (wie gängige Heim-Router), Einschränkungen unterliegt. Im Grunde kann nur EIN PC im Heimnetz einen VPN Tunnel in die Firma aufbauen - würde es gleichzeitig ein zweiter versuchen, würde dies prinzipbedingt scheitern, da ESP keine Ports benutzt, die man "patten" könnte.

Aus diesem Grunde wurde **NAT-Traversal** erfunden.
Dabei wird ESP in UDP gekapselt, und auf UDP Port 4500 über den NAT-Router (der aber in Wahrheit allermeist ein PAT-Router ist) gesendet.

Mit NAT hat ESP keine Probleme, das Problem liegt am PAT und an der Port-losigkeit des ESP Protokolls.

Dies hat wiederum jedoch einen Nachteil, da UDP Verbindungen (im Gegensatz zu TCP Verbindungen) eine recht kurze Lebensdauer haben, und der IPSEC Tunnel dadurch - wenn der Benutzer beispielsweise keine Daten über den Tunnel sendet - abrupt abbrechen kann.
Um dies zu verhindern, wurden die **NAT-Keepalives** eingeführt, die regelmässig kleine Datenbrocken über die Leitung senden um den Abbruch des UDP Tunnels zu verhindern.

Aus dieser UDP-NAT-Traversal Problematik heraus (UDP-Tunnel-Abbruch) hat Cisco alternativ **IPSEC-over-TCP** erfunden, welches wie der Name sagt TCP verwendet, und sowohl IKE Phase1 als auch ESP über TCP Port 10000 zum benachbarten VPN Server schleust. Dies ist die bevorzugte Variante, die man nutzen sollte, wenn der VPN Server es unterstützt.

Nachteile von IPSEC

- Sind die benötigten Ports nicht offen (z. B. wenn eine Firewall zwischen Client-PC und VPN-Server Port UDP 500 blockt) kommt kein IPSEC Tunnel zustande
- Recht kompliziert und nicht einfach zu konfigurieren und troubleshooten

Hilfreiche Seiten mit noch mehr IPSEC-Details

Detailiertere Erklärung zu IPSEC (Englisch): http://www.unixwiz.net/techtips/iguide-ipsec.html
Detailiertere Erklärung zu IKE (Deutsch):http://net.informatik.uni-tuebingen.de/fileadmin/RI/teaching/seminar_ii ...

Alternativen zu IPSEC

- PPTP
- SSL-VPN
- L2TP

Content-Key: 73117
Url: https://administrator.de/contentid/73117
Ausgedruckt am: 05.01.2022 um 10:01 Uhr

---

10 Kommentare

brammer 09.11.2007 um 08:49:42 Uhr

Hallo,

Super Tutorial!

brammer

Dani 11.11.2007 um 19:55:57 Uhr

Hallo ihr beiden,
kann mich Brammer nur anschließen. Einfach super...
Endlich habe ich alles dazu auf einer Seite. Schön zusammengefasst und verständlich. Kein so blödes IT-Deutsch. 😄 Dank dir viel mals...

Grüße
Dani

RavenX2 19.11.2007 um 18:02:54 Uhr

Sehr schön gemacht! Wenn man bedenkt was MS dazu in den Fachbüchtern schreibt, ist dein Beitrag knapp und präzise zusammengefasst.

TuXHunt3R 19.11.2007 um 21:54:40 Uhr

Sehr schönes Tutorial, werde es meinem Netzwerktechnik-Lehrer als Lehrmittel vorschlagen. Kein Witz!

---

spacyfreak 20.11.2007 um 13:10:59 Uhr

> Sehr schönes Tutorial, werde es meinem Netzwerktechnik-Lehrer als Lehrmittel vorschlagen. Kein Witz!

Ich kapiere auch nicht weshalb es kaum einer schafft, die "ach so komplexen" Netzwerkprotokolle "easy und einfach" zu vermitteln.
Ich denke oft genug habens (zumindest einige) Lehrer selber nicht kapiert, darum können sie vieles auch nicht verständlich vermitteln.
Oder sie verlieren sich in Details und achten nicht darauf, ob die Schüler überhaupt das "grobe" schon verinnerlicht haben.
Macht halt wenig Sinn, sich an Details zu wagen, ohne zu wissen worum es überhaupt geht. 😄

TuXHunt3R 20.11.2007 um 20:38:26 Uhr

> Ich kapiere auch nicht weshalb es kaum einer schafft, die "ach so komplexen" Netzwerkprotokolle > "easy und einfach" zu vermitteln.
> Ich denke oft genug habens (zumindest einige) Lehrer selber nicht kapiert, darum können sie
> vieles auch nicht verständlich vermitteln.

Stimme zu! Obwohl der betreffende Lehrer das Thema schon gut vermitteln kann, im Gegensatz zu seinem Vorgänger.....

Der konnte nicht mal den Unterschied zwischen geraden und Crossover-Kabeln einigermassen erklären.....

gnarff 15.12.2007 um 19:47:27 Uhr

Sehr schönes Tutorial, man hätte vllt. noch erwähnen sollen, dass das Schlüsselaustausch-Protokoll Diffie-Hellmann gegen **Manipulationen der Datenpakete** bei einem Man-In-The-Middle-Angriff sicherheitsanfällig ist.

Um das Schlüsselaustausch-Verfahren nach Diffie-Hellman besser abzusichern bedient man sich des **STS-Protokolls** um die ausgetauschten Nachrichten authentisieren zu können.

Das STS-Protokoll ist seinerseits anfällig für **Unknown Key Share Angriffe**; hier ist das schön auf englisch erklärt...:D
Das Dokument gibt es auch als **PS-Datei**

saludos
gnarff

LoveZilla 04.09.2008 um 20:19:49 Uhr

Sehr gut erklärt. Habe überall nachgeschlagen um die einzelnen Definitionen zu finden. Hilft mir dabei meinen VPN Router zu konigurieren. Danke.

---

osze90 23.07.2015 aktualisiert um 14:41:17 Uhr

> ^^Zitat von @spacyfreak: Der Lifetime Parameter bestimmt nur dann die Lebenszeit des Administrators, wenn er die Lifetime auf beiden VPN Servern einer Seite-to-site Verbindung UNTERSCHIEDLICH konfiguriert. Die lifetime muss auf beiden identisch sein, da der Tunnel ansonsten in regelmässiger Unregelmässigkeiten abbricht und man sich beim Troubleshooting den Wolf sucht.

Hallo verstehe nicht ganz wie das gemeint ist. Ich möchte einen IPsec Verbindung mit Site-To-Site via zwei Routern herstellen.

Verstehe dabei nicht ganz die Lifetime muss somit auf jedem der 2 Router anders konfiguriert werden.? Weiter steht unten das die Lifetime identisch sein muss. Das ist ein wiederspruch in sich. Handelt es sich hier also um einen Fehler?

Bezüglich SKME & Oakley und Diffi-Hellmann habe ich noch Fragen wofür genau ist das public key? Ich habe doch bereits AES welches für die Verschlüsselung verantwortlich ist und als Algorithmus entweder SHA1 oder MD5 oder was es da noch alles gibt...

brammer 23.07.2015 um 14:41:51 Uhr

Hallo,

nach 7 Jahren solltest du bitte einen neuen Beitrag im Forum schreiben und nicht auf einen alten Antworten....

brammer
