

Implementierung eines VPN zwischen Cisco-Routern & Windows 2000-Clients

von Enno Rey, erey@security-academy.de

1. Einleitung

Das vorliegende Papier beschreibt, wie ein VPN zwischen Windows 2000-Rechnern (seien es mobile User oder Heimarbeitsplätze) und Cisco-Routern installiert werden kann.

Ausgangspunkt war zunächst die Überlegung, wie mit möglichst einfachen, standardisierten Mitteln¹ eine Lösung realisiert werden kann, die

- die Integrität der übertragenen Daten gewährleistet
- die Vertraulichkeit der übertragenen Daten durch Verschlüsselung schützt
- die Authentizität idealerweise nicht nur des Client-Systems, sondern auch des Users sicherstellt²
- dem Client eine IP-Adresse aus dem Unternehmensnetz zuweist, damit etwa eine subnetz-basierte Verkehrskontrolle durch die *corporate firewall* stattfinden kann³.
- und gleichzeitig das Ganze möglichst kostengünstig (= > Einwahl der Clients bei beliebigem ISP) gestaltet.

Es ist weiterhin geplant, dieses Paper als Teil einer Schulungsunterlage zum Thema IPsec zu verwenden⁴. Daher werden auch in naher Zukunft weitere dieser Art folgen: in erster Linie eines zur Implementierung eines VPN zwischen *Cisco PIX* und *Check Point Firewall-1*, dann möglicherweise welche zu VPNs zwischen *Symantec Raptor 6.5* und *Bintec X1200*-Routern sowie zu Linux-Clients mit FreeS/WAN⁵ und IPsec-Gateways auf Basis von OpenBSD (jeweils ergänzt um den *I2tpd*⁶).

1.1 Das Problem

Der Zugriff mobiler User auf ein Unternehmens-Netz kann grundsätzlich entweder durch eine dedizierte Provider-Einwahl (mit dediziertem Übergang in ein *corporate network*, etwa über PVCs in einem ATM-Backbone) oder über ein VPN erfolgen, das dabei die oben aufgeführte Funktionalität aufweisen sollte.

Die dedizierte Einwahl ist meist die teurere⁷, Administrations-aufwendigere⁸ sowie schlechter skalierbare Variante und setzt außerdem entsprechende Verträge in allen Ländern voraus, in denen die mobilen User arbeiten. Sie hat allerdings den Vorteil garantierter Bandbreite beim Remote-Zugriff⁹. Des Weiteren ist sie bei Diensten, die (noch) nicht durch IPsec geschützt werden können (z.B. Multicast-Verkehr¹⁰), erste Wahl.

Die VPN-Variante wirft unmittelbar die Frage nach den verwendeten Modulen auf: Transfer-Verfahren, Komponente(n) des Tunnel-Endpunkts & eingesetzte Client-Software.

¹ Ich gehören zu den Netzwerkern, für die „proprietär“ eines der schlimmeren Schimpfworte ist...

² Für den Fall des Diebstahls eines Laptops beispielsweise. Dann müßte vor dem Tunnel-Aufbau zwar irgendwann eine Win2K-Anmeldung stattfinden, was aber dank etwa home.eunet.no/~pnordahl/ntpasswd/index.html kein Problem für einen Übelwollenden sein sollte. Schutz davor bietet u.U. eine schon früh (d.h. beim Boot-Vorgang) einsetzende Festplattenverschlüsselung (unser Favorit ist hier *Pointsec*: www.protectdatasecurity.com/solutions/solutions_pointsec.asp). Die oft anzutreffende Variante der Platten-Verschlüsselung durch's Betriebssystem selbst (z.B. mithilfe des *Encrypting File Systems*, EFS unter Windows 2000) oder darauf aufsetzender Tools (z.B. *PGPdisk*) ist an dieser Stelle wenig hilfreich.

³ Die Clients erhalten dann überhaupt keinen direkten Internet-Zugang, sondern nur einen durch die Unternehmens-Firewall reglementierten und (beispielsweise auf Viren) geprüften.

⁴ Siehe dazu www.antaes.cc.

⁵ www.freeswan.org

⁶ www.marko.net/I2tp

⁷ Das gilt sogar bei Verwendung von 0800er-Einwahl oder ähnlichem.

⁸ Ich muß zusätzlich gestehen, kein Freund von ATM zu sein (weil leitungsvermittelte Übertragung halt jeglicher IP-Philosophie diametral entgegensteht; soviel nur an dieser Stelle dazu).

⁹ Es stellt sich natürlich die Frage, inwieweit die heute üblichen max. 128 Kbit (ISDN, zwei B-Kanäle) mobiler User beim Durchqueren des Internet noch in der Bandbreite beeinträchtigt werden können...

Für Heimarbeits-Plätze mit DSL-Zugang mag das Argument garantierter Bandbreite gewichtiger sein. Das setzt dann aber auch auf Seiten des Providers aufwendigere Technik voraus (Einsatz von DSLAMs).

¹⁰ Vgl. www.ipmulticast.com/community/smug.

Der Gedanke an IPsec als Übertragungs-Verfahren liegt nahe, löst das Problem aber nur partiell. Sämtliche IPsec-basierten Verfahren zur Zuweisung von IP-Adressen (etwa *Mode Config* auf Cisco-Routern¹¹) oder Benutzer-Authentifizierung (beispielsweise *xauth*¹² oder *DIAMETER*¹³) sind entweder Hersteller-proprietär oder noch nicht weit genug im Standardisierungs-Prozeß fortgeschritten, um dem Gebot der Standard-basierten Lösung genügen zu können. IPsec muß deshalb um L2TP ergänzt werden (mehr dazu unten).

Der Tunnel-Endpunkt wird in vielen Netzen gewissermaßen in Personal-Union mit dem Bastion Host realisiert (oft *Check Point FW-1* mit *VPN-1*). Damit wird allerdings massiv gegen einen der wichtigsten Sicherheitsgrundsätze überhaupt: *separation of duties* verstoßen¹⁴, weshalb diese Lösung nicht in Betracht gezogen wurde.

Bleibt nur ein dediziertes IPsec-Gateway in einem eigenem Segment innerhalb der Firewall. Die Wahl fiel hier auf einen Cisco-Router, weil diese 1.) im hier skizzierten Umfeld sowieso vorhanden sind, 2.) stabil und zuverlässig arbeiten und 3.) leicht¹⁵ skaliert werden können¹⁶.

Bei Windows 2000 als vorausgesetztem Client-Betriebssystem¹⁷ fallen folgende Möglichkeiten ein¹⁸:

- *Check Point SecuRemote*¹⁹: zuweilen ein Alptraum für die betroffenen Admins²⁰... und der geneigte Leser wird schon bemerkt haben, daß meine Sympathie für Produkte aus dem Hause *Check Point* nur eingeschränkter Natur ist²¹.
- *Cisco VPN Client*²²: wird nur in Verbindung mit *Cisco* VPN-Devices (*PIX* o. *VPN Concentrator*) angeboten²³ und verwendet zum Adreß-Bezug *mode config* (=> Gateway muß das unterstützen).
- *Conware VPNclient*²⁴: proprietär, da die zugewiesene Client-Adresse in einem UDP-Header transportiert wird, den nur das IPsec-Gateway aus dem eigenen Haus versteht.
- IPsec in Kombination mit L2TP: schränkt die Zahl der möglichen Gateways ein, weil diese L2TP beherrschen müssen, basiert aber auf Standards.

¹¹ Inzwischen liegt eine entsprechendes erstes Dokument zwar vor (www.ietf.org/internet-drafts/draft-ietf-ipsec-dhcp-09.txt), *Mode Configuration* ist aber lange noch nicht einheitlich implementiert.

¹² Auch hier gibt es bislang nur ein IETF-Draft: www.ietf.org/internet-drafts/draft-beaulieu-ike-xauth-01.txt. Ein anderes Verfahren namens *CRACK* (*Challenge/Response for Authenticated Cryptographic Keys*) ist schon wieder vom (Standardisierungs-)Tisch.

¹³ *DIAMETER* wird als der Nachfolger von *RADIUS* gehandelt und ermöglicht AAA-Funktionalität u.a. auch für IPsec-basierte Netze (siehe www.diameter.org oder www.ietf.org/internet-drafts/draft-calhoun-diameter-framework-09.txt).

¹⁴ Der Bastion Host hat sich um Firewall-Funktionalität zu kümmern und nicht um Ver- bzw. Entschlüsselung von Verkehr. Seine Systemstabilität wird dadurch sicher nicht erhöht (im übrigen seine Performance ganz bestimmt auch nicht... wir sprechen schließlich über IPsec). Ein Buffer Overflow im IPsec-Stack sollte nicht zur Kompromittierung der Unternehmens-Firewall führen... es reicht schon, wenn das IPsec-Gateway in die Hände eines Angreifers fällt. Um das nochmals deutlich zu sagen: ein Bastion Host hat nicht die Aufgabe, Pakete zu verschlüsseln. Er soll Traffic regulieren & leiten.

¹⁵ Es gibt inzwischen auch IPsec-Accelerator für die 36er-Serie: www.cisco.com/warp/public/cc/pd/rt/2600/prodlit/kaos_ds.htm.

¹⁶ Denkbar wäre auch ein IPsec-Gateway auf OpenBSD-Basis, insbesondere wg. der dort eingesetzten IPsec-Implementierung, die als eine der besten & stabilsten gilt (und weil im Sicherheits-Umfeld OpenBSD sowieso das Betriebssystem ist). Hier ist dann aber die Skalierbarkeit eingeschränkter (solange OpenBSD noch nicht Multiprozessor-fähig ist: www.openbsd.org/smp.html). Dazu wird es, wie schon angedeutet, eventuell ein anderes Paper geben (mit Linux-Clients).

¹⁷ Ich gehe einfach davon aus, daß die Mehrzahl der *corporate laptops* mit einem Windows-Derivat ausgestattet ist. Linux-basierte Clients (mit FreeS/WAN) werden eben vielleicht noch an anderer Stelle behandelt (s.o.) und IPsec-fähige *Macintosh*-Powerbooks sind nicht gerade zahlreich (zumindest in meinem Umfeld...).

¹⁸ Es gibt eine Reihe weiterer; ich bin für entsprechende Hinweise immer dankbar. Einige sind auch im Vergleichstest von VPN-Produkten genannt, der in der aktuellen Ausgabe (April 2001) des *Windows 2000 Magazine* enthalten ist (www.win2000mag.com/Articles/Index.cfm?ArticleID=20068).

¹⁹ www.checkpoint.com/products/vpn1/securemoteds.html; inzwischen ist auch der *SecureClient*, der zusätzlich noch die Funktionalität einer Personal Firewall hat, für Win2K verfügbar (www.checkpoint.com/products/vpn1/secureclient.html).

²⁰ Inwieweit man bei *SecuRemote* von einem stabilen, funktionalen, ausgereiften Produkt sprechen kann, überlasse ich dem Urteil derer, die es in der täglichen Praxis administrieren...

²¹ Das hat viel mit dem – sagen wir mal: problematischen – Design ihres Flaggschiffs zu tun. An dieser Stelle verweise ich auf die Datenbank von SecurityFocus (www.securityfocus.com/vdb). Man wähle dort als Hersteller *Check Point* und betrachte allein das Jahr 2000... Schon die schiere Anzahl sollte zu denken geben. Wer außerdem wie ich seine Firewall-Sozialisation noch maßgeblich aus der ersten Ausgabe von *CHAPMAN/ZWICKY* aus dem Jahre 1995 erfahren hat, konnte sich nur erstaunt die Augen reiben, wieviele der ‚Todsünden aus der kleinen Schule für Firewaller‘ viele Jahre später in ebendieser Liste zu finden sind (Umgang mit Fragmenten, mangelhafte Input-Prüfung, kein eigener stabiler IP-Stack usw.). Auch die Lektüre von www.dataprotect.com/bh2000/blackhat-fw1.html sollte Ihr Interesse verdienen...

²² www.cisco.com/univercd/cc/td/doc/product/vpn/client/clierel.pdf

²³ So zumindest mein Kenntnisstand (der ggf. per Mail korrigiert werden kann...).

²⁴ www.conware.de/seiten/inhalt/frontend/gruppe.php3?action=kurzbeschreibung&id=33

1.2 Die vorgeschlagene Lösung

Am Bastion Host wird ein eigenes Segment eingerichtet²⁵, in dem sich als einzige Komponente der *Cisco*-Router befindet²⁶, der als IPsec-Gateway und LNS (*L2TP Network Server*, s.u.) dient.

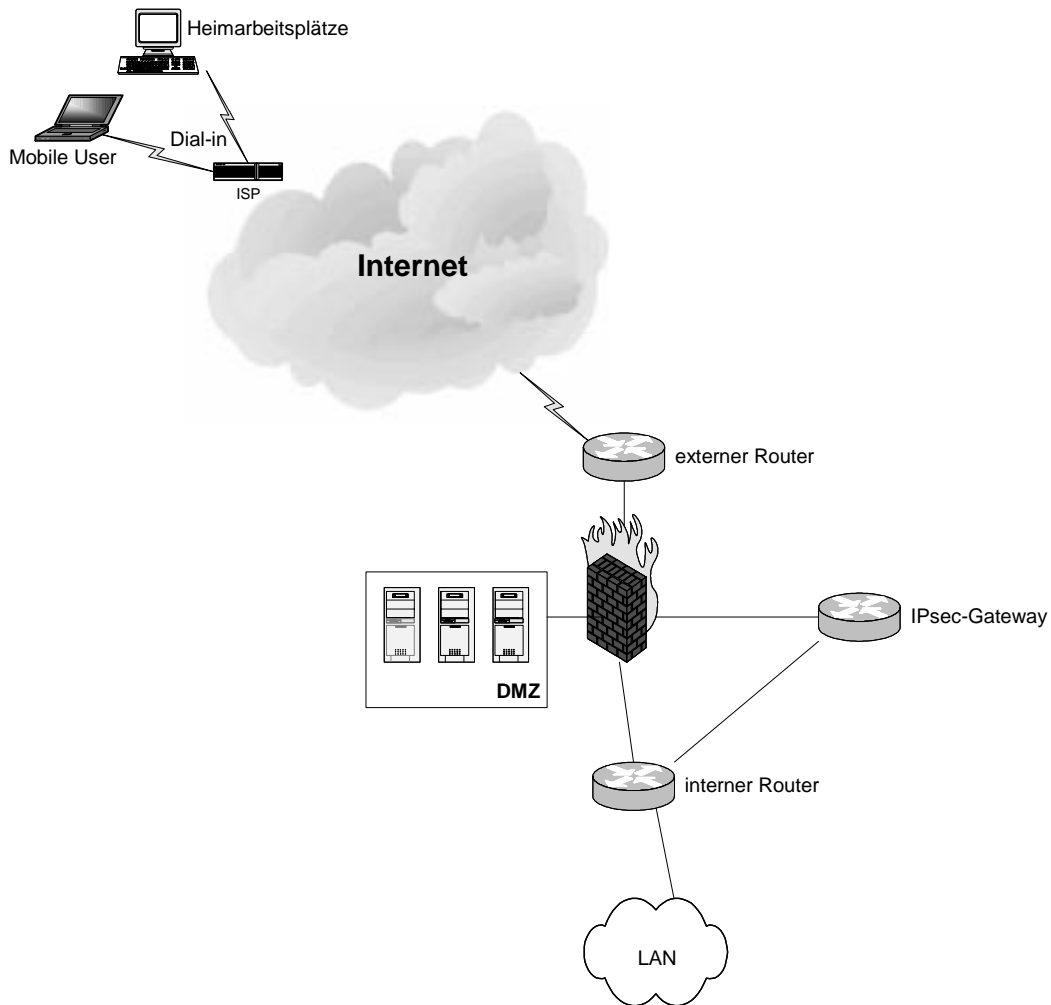


Abb. 1: Skizze d. vorgeschlagenen Lösung

Das ist im Beispiel ein *Cisco 3640* (16/128 MB), auf dem „c3640-jk2o3s-mz.121-5.T5.bin“²⁷ läuft. Die Verschlüsselung findet folglich mit Triple-DES statt. Im produktiven Betrieb ist einfaches DES **immer ungenügend**²⁸ und sollte daher nie eingesetzt werden. Beachten Sie außerdem, daß Windows 2000 in der Export-Version aufgrund (ehemaliger) Krypto-Exportbeschränkungen kein Triple-DES unterstützt, dies aber weitgehend nicht kenntlich macht (es kann – nur scheinbar – 3DES eingestellt werden)²⁹! Verwenden Sie deshalb unbedingt das *High Encryption Pack*³⁰.

²⁵ Wir bevorzugen prinzipiell, sofern technisch machbar, den Ansatz, alle direkt mit dem Bastion Host verbundenen Geräte in eigenen Segmenten zu platzieren (d.h. ein Segment für den/jeden Webserver, eines für den/jeden Mail-Relay, den/jeden DNS-Server usw.).

²⁶ Die Redundanz dieser Komponente soll hier nicht im Fokus stehen. Sie kann beispielsweise durch eine Installation, die routerseitig auf HSRP (*Hot Standby Router Protocol*) basiert und mit kaskadierten Switches sowie etwa *Intel* NICs mit *Advanced Networking Services* (ANS) am Bastion Host arbeitet, gewährleistet werden.

²⁷ Mir sind die grundsätzlichen Bedenken gegen den Einsatz von T-Images bekannt. Sie sind allerdings die einzigen, die Remote-Zugriff auf Cisco-Router über SSH gestatten...

²⁸ Wg. www.eff.org/descracker kombiniert mit www.intel.com/intel/museum/25anniv/hof/moore.htm.

²⁹ Ein entsprechender Eintrag im (Anwendungs-) Eventlog ist der einzige Hinweis. Siehe auch www.securityportal.net/topnews/weekly/microsoft20000522.html.

³⁰ Erhältlich unter www.microsoft.com/windows2000/downloads/recommended/encryption/default.asp. Berücksichtigen Sie auch, daß allein die Installation des *Internet Explorers 5.5* auf Windows 2000-Systemen dazu **nicht** ausreicht (siehe www.microsoft.com/windows/ie/download/128bit/intro.htm).

Die Regeln auf dem Bastion Host werden so modifiziert, daß Verkehr zu diesem Router nur über IP-Protokoll 50 (ESP)³¹ und über UDP Port 500 (ISAKMP) möglich ist³². Sie sollten zusätzlich bedenken, daß der Router auch DNS-Clientfunktionalität haben sollte³³.

Eine weitere Schnittstelle des Routers wird mit dem inneren Router der Firewall verbunden. Das Einwahl-Segment wird so mit dem *corporate network* verbunden, zu dem es per Adresse ja auch gehört. Die Paketfilter an diesem Router sind entsprechend den Anforderungen der mobilen User anzupassen³⁴.

Der mobile Client wählt sich zunächst bei einem Provider seiner Wahl ein, der ihm gewissermaßen nur die physikalische Plattform für die weitere Verbindung zur Verfügung stellt.

Dann stellt er einen Tunnel zum IPsec-Gateway her, in dem sich die beiden Geräte gegenseitig über Zertifikate authentifizieren. Damit wird sichergestellt, daß nur „zugelassene“ Laptops überhaupt einen Tunnel initiieren können. Aller Verkehr, der über diesen Tunnel läuft (und das ist bei richtiger Konfiguration der komplette Verkehr), wird ab jetzt verschlüsselt.

Innerhalb dieses Tunnels wird nun eine L2TP-Verbindung (also eine getunnelte PPP-Verbindung, s.u.) aufgebaut, für deren Zustandekommen eine normale PPP-Authentifizierung (etwa über MS-CHAP [RFC 2433]) notwendig ist (*User-Authentifizierung*) und die im Gegenzug eine IP-Adresse zuweist (klassische Funktionalität von PPP im Rahmen des Sub-Protokolls IPCP [RFC 1332], Option 03).

Diese Benutzer-Authentifizierung kann natürlich via RADIUS [RFC 2138/2139] von einem beliebigen Verzeichnisdienst durchgeführt werden³⁵ oder zukünftig eventuell Smartcard-basiert (über das *Extensible Authentication Protocol*, EAP [RFC 2284]) stattfinden³⁶. Auch eine Integration von *RSA SecurID* ist damit (RADIUS) denkbar³⁷.

So wird eine kostengünstige (Einwahl bei beliebigem ISP), verschlüsselte (IPsec), mit sowohl Geräte- (IPsec) wie auch User-Authentifizierung (L2TP) geschützte Verbindung mit einer Adresse aus dem Unternehmensnetzwerk (L2TP) realisiert.

1.3 Vorkenntnisse, die Sie mitbringen sollten

Ich setze voraus, daß Sie grundsätzlich wissen, wie ein Cisco-Router konfiguriert wird. Ich kann und will hier keine entsprechende Einführung bieten. Sollte diesbezüglich Nachholbedarf bestehen, erwerben Sie entweder etwas wie *Cisco Router Konfiguration*³⁸, besuchen Sie eine entsprechende Schulung³⁹ oder surfen Sie ein wenig⁴⁰.

Die Arbeit mit Windows 2000 hinsichtlich der Konfiguration von Protokollen & Dial-Interfaces und zugehöriger Fehlersuche sollte Ihnen vertraut sein. Sie würden aber sonst wohl auch nicht dieses Paper lesen...

Gute PPP-Kenntnisse sind auf jeden Fall beim Troubleshooting hilfreich (schließlich ist L2TP ein Protokoll zum Tunneln von PPP). Ich verweise an dieser Stelle auf das am Schluß genannte Standardwerk zu PPP von JAMES CARLSON.

³¹ IP-Protokoll 51 (*Authentication Header*, AH) spielt im vorgesehenen Szenario keine Rolle (weil ja zwingend verschlüsselt werden soll). Bei anderen Anforderungen, die zum Einsatz von AH führen, müsste es dann auch freigeschaltet werden.

³² Ergänzt durch entsprechende Paketfilter auf dem Interface des Routers.

³³ Sein Resolver also mit irgendeinem DNS-Server (der auch Kenntnis der mobilen Clients hat) sprechen können muß. Das kann verkehrsmäßig über den Bastion Host geschehen, ist aber wohl geschickter durch (direkten) Kontakt zu einem der internen DNS-Server gelöst (insbesondere, wenn Split-DNS implementiert ist).

³⁴ Der Verkehr des Einwahlsegments könnte auch wiederum über den Bastion Host geleitet werden. Dem liegt jedoch die (eigentlich unzutreffende) Vorstellung zugrunde, daß das Traffic „von außen“ sei. Bei korrekter Einrichtung der reisenden Laptops (niemals direkte Kommunikation mit dem Internet möglich durch entsprechende IPsec-Konfiguration und gegebenenfalls Personal Firewalls [wir empfehlen hier üblicherweise eine Kombination von *Norton Personal Firewall 2001*, www.symantec.com/sabu/nis/npf, und *Network ICE BlackICE Defender*, www.networkice.com/products/blackice_defender.html) können diese Geräte ebenso behandelt werden wie Systeme innerhalb des LANs. Ich teile aber Bedenken, die darauf gründen, daß diese Rechner immerhin physikalisch mit dem Internet verbunden sind. Inwieweit sie dann einer zusätzlichen Verkehrskontrolle zu unterworfen sind, muß im Einzelfall durch die Security Policy geregelt werden.

³⁵ Wenn wir im Windows 2000-Umfeld bleiben, würde sich der *Internet Authentication Service* (IAS) anbieten. Die entsprechende Funktionalität gibt es aber auch für die NDS (z.B. *Steel-Belted Radius* von *Funk Software*, www.funk.com/sbr_ee.html) oder OpenLDAP (z.B. *Radiator* von *Open System Consultants*, www.open.com.au/radiator). Ich verweise auch auf das RFC 2809.

³⁶ Sobald IOS das *Extensible Authentication Protocol* unterstützt...

³⁷ Vgl. www.rsasecurity.com/support/impguides/category.asp?CatID=4&RSAProd=SecurID.

³⁸ ALLAN LEINWAND, BRUCE PINSKY, MARK L. CULPEPPER: *Cisco Router Konfiguration. Der praxisnahe Einstieg in Cisco IOS.* (ISBN 3827259371).

³⁹ www.antares.cc

⁴⁰ Bspw. zu www.cisco.com/warp/public/779/smbiz/service/knowledge/general/tutorial.htm.

2. Die eingesetzten Protokolle

2.1 IPsec

IPsec ist eine standardisierte Protokollfamilie (Basis-RFC ist das RFC 2401) zur Sicherung von IP-Paketen. Sie beinhaltet Mechanismen zur Wahrung der Integrität, Vertraulichkeit und Authentizität von Traffic und zum Schutz vor wiederholtem Senden von Paketen (*anti-replay*). IPsec setzt sich aus drei Hauptkomponenten zusammen: dem Schlüsselaustausch-Verfahren *Internet Key Exchange* (IKE, RFC 2409)⁴¹ und den Protokollen *Encapsulation Security Payload* (ESP, RFC 2406, bietet alle o.g. Schutzmechanismen) sowie *Authentication Header* (AH, RFC 2402, bietet keine Verschlüsselung). Es können Pakete inklusive IP-Header verschlüsselt werden (man spricht dann vom *Tunnel-Modus*, der für den Gateway-zu-Gateway Einsatz, meist den Schutz kompletter Netze bei Verbindung über ein unsicheres Medium, vorgesehen ist), es kann jedoch auch nur Verkehr oberhalb Layer 3 (mit Beibehaltung einer ‚unbehandelten‘ IP-Adresse) verschlüsselt werden (dies ist der sog. *Transport-Modus*).

Bei Aufnahme einer IPsec-basierten Verbindung zwischen zwei Kommunikationspartnern werden sog. *Security Associations* (SAs) hergestellt. Zunächst wird eine IKE-SA gebildet, innerhalb derer sich die Teilnehmer wechselseitig authentifizieren und sich über die für die weitere Kommunikation verwendeten Schlüssel einig werden. Anschließend werden durch IKE zwei gewissermaßen IPsec-SAs mit neuen Schlüsseln generiert (je eine für jede Richtung), die dann für den konkreten Schutz des Verkehrs (mithilfe von ESP und/oder AH) zuständig sind. Der *Internet Key Exchange* kann also in zwei Teile zerlegt werden: eine *Phase 1*, in der ein sicherer und authentifizierter Kommunikationskanal aufgebaut wird⁴², und eine *Phase 2*, in der dieser Kommunikationskanal genutzt wird, um die konkreten Parameter der nachfolgenden gesicherten Verbindung auszuhandeln⁴³.

Ein erfolgreicher Ablauf der Phasen setzt jeweils voraus, daß beide Seiten eine Einigung über die je anzuwendenden Parameter (etwa die Authentifizierungsmethode oder das Verschlüsselungsverfahren) erzielt haben, die von IPsec wohlweislich nicht (kaum) vorgeschrieben sind⁴⁴. Die Parameter **müssen** auf beiden Seiten also übereinstimmen (können). Genau das ist die Quelle der meisten Probleme mit IPsec.

In der *Phase 1* werden vor allem verhandelt⁴⁵:

- Authentifizierungsverfahren⁴⁶ (z.B. *pre-shared keys/secret*, Signaturen mit RSA oder DSA⁴⁷ [– Zertifikate])
- Verschlüsselungsverfahren für den IKE selbst (z.B. DES, 3DES, Blowfish oder CAST-128 [RFC 2144])⁴⁸
- Hash-Algorithmus zur Authentifizierung von Nachrichten gemäß RFC 2104 (MD-5, SHA-1 o. Tiger⁴⁹)
- *Diffie-Hellman*-Gruppe (meist nur Gruppe 1 oder 2)⁵⁰
- Lifetime (Gültigkeitsdauer) der IKE-SA (=> des dort generierten Schlüsselmaterials) in Sekunden⁵¹

Es kann nicht oft genug betont werden... wenn die Kommunikationspartner keine Übereinstimmung bzgl. dieser Parameter finden, wird ein IPsec-Verbindungsaufbau fehlschlagen.

⁴¹ Der sich wiederum aus verschiedenen Teilen zusammensetzt, insbesondere einer allgemeinen Regelung (einer Art ‚Sprache‘) eines solchen Austausch (Internet Security Association and Key Management Protocol, ISAKMP [RFC 2408], IP-Protokoll über UDP Port 500) und weiterhin der Austausch-Verfahren selbst (*Oakley* [RFC 2412] und *SKEME* [Secure Key Exchange Mechanism]).

⁴² Das kann im *main mode* oder *aggressive mode* stattfinden, die ich zwar hier nicht erläutern werde, deren Namen Sie aber kennen sollten, um ggf. beurteilen zu können, an welcher Stelle ein Problem aufgetreten ist.

⁴³ Das ist der *quick mode*.

⁴⁴ Um die für den Einsatz neuer Verfahren (z.B. des *Advanced Encryption Standard*, AES) notwendige Flexibilität zu gewährleisten.

⁴⁵ U.U. müssen noch eventuelle *Perfect Forward Secrecy* (Fußnote nächste Seite) und das sog. *Commit Bit* (RFC 2408) beachtet werden.

⁴⁶ Es gibt noch weitere, z.B. RSA-verschlüsselte *nonces* (Zufallszahlen). Die genannten sind jedoch die wichtigsten und schon die werden nicht von allen Implementierungen unterstützt (etwa DSA-Signaturen weder von Win2K noch von IOS).

⁴⁷ *Digital Signature Algorithm* [www.itl.nist.gov/fipspubs/fip186.htm].

⁴⁸ Auch diese werden lange nicht durchgängig unterstützt (in vielen Implementierungen sogar nur DES und 3DES).

⁴⁹ www.cs.technion.ac.il/~biham/Reports/Tiger

⁵⁰ *Diffie-Hellman* [RFC 2631] ist ein (*das*) Verfahren zum Austausch eines Geheimnisses (Schlüssels) über einen nicht-sicheren Kanal. Die Parameter der dafür notwendigen Aushandlung werden durch sog. Gruppen festgelegt. Das RFC 2412 nennt 5 „well-known groups“, ein IETF-Draft schlägt weitere vor (www.ietf.org/internet-drafts/draft-ietf-ipsec-ike-modp-groups-01.txt). Die Gruppen 1 u. 2 verwenden eine ‚traditionelle‘ Exponentiation über einen Prim-Modulus der Länge 768 Bit (Gr. 1) bzw. 1024 Bit.

⁵¹ Nach Ablauf dieser *lifetime* muß ein erneuter *IKE* inkl. Authentifizierung stattfinden. Sie liegt meist zwischen 8 und 24 Stunden. Eine Erhöhung dieses Werts führt zu seltenerer Neu-Initialisierung (=> Performance-Vorteilen), bringt aber eben auch seltenere Re-Authentifizierung mit sich (problematisch etwa bei erfolgtem Zertifikats-Widerruf). Bei unterschiedlichen Vorschlägen beider Partner wird die kürzere gewählt.

Nach erfolgreichem Abschluß der Phase 1 wird erneut verhandelt, und zwar über die Rahmenbedingungen der IPsec-SAs (die das eigentliche Ziel der Verhandlungen sind⁵²).

Hier wiederum, in der *Phase 2*, sind im wesentlichen⁵³ folgende Parameter (konform) zu konfigurieren:

- der Modus (*Tunnel-* oder *Transport-*Modus, siehe dazu oben)
- die Transforms (welche Sicherheitsprotokolle [ESP/AH] welche Algorithmen verwenden, Beispiele s.u.)⁵⁴
- die Lifetimes (Laufzeiten) d. IPsec-SAs (=>der Schlüssel), Zeit- und/oder Volumenabhängig, in Sek.⁵⁵ o. KB
- ob *Perfect Forward Secrecy* zum Einsatz kommt, d.h. regelmäßig neues Schlüsselmaterial erzeugt wird⁵⁶

Erst wenn diese Einstellungen erfolgreich verhandelt sind, kommt die IPsec-Kommunikation zustande. Prüfen Sie im Fehlerfall immer die Logfiles beider Seiten darauf, inwieweit die einzelnen Teilschritte stattgefunden haben (ein Debug-Beispiel folgt unten), und welche Parameter im Spiel waren.

2.2 L2TP

Das Layer Two Tunneling Protocol (L2TP) ist ein im RFC 2661 spezifiziertes, ursprünglich von *Cisco* und *Microsoft* (auf Initiative der IETF hin) als Nachfolger der jeweils eigenen Tunnel-Protokolle L2F (*Layer Two Forwarding, historic RFC 2431*) und PPTP (*Point-to-Point Protocol, RFC 2637*) entwickeltes Protokoll zum Tunneln von PPP-Verbindungen. Dabei wird das traditionelle Modell einer physikalischen PPP-Verbindung zwischen PPP-Client und NAS (*Network Access Server*) in ein virtuelles überführt. Anstelle einer physikalischen (meist Wähl-) Verbindung der beiden Endpunkte wird UDP-basiert (Port 1701) – also über IP – ein Kommunikationskanal zwischen einem sog. *L2TP Access Concentrator* (LAC, der „PPP-Client“) und einem *L2TP Network Server* (LNS, der „PPP-Server“) aufgebaut, innerhalb dessen dann eine normale PPP-Verbindung mit allen PPP-immanenten Mechanismen wie Authentifizierung oder Adress-Zuweisung stattfindet (über virtuelle PPP-Interfaces). So können beliebige IP-basierte Hosts unabhängig vom physikalischen Standort PPP-Verbindungen unterhalten.

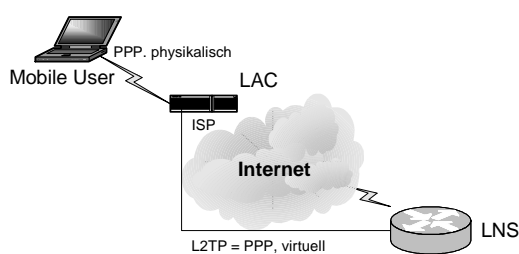


Abb. 2: L2TP, mandatory tunnel

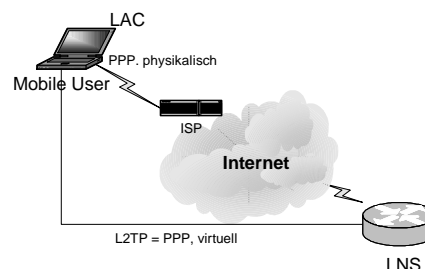


Abb. 3: L2TP, voluntary tunnel

Wählt sich der Client direkt in einen NAS ein, der (meist) ohne Kenntnis des Clients die Verbindung an einen LNS weitergibt und somit als LAC agiert, spricht man von einem *mandatory* (o. *compulsory*) *tunnel* (weil der Client evtl. nichts davon weiß und v.a. auch nicht eingreifen kann). Ist dagegen der Client selbst der (L2TP- und damit PPP-) Endpunkt (= unser Szenario), ist die Rede von einem *voluntary tunnel*.

⁵² Mittels IKE können aufgrund seiner allgemeinen Struktur auch die Sicherheitsdienste anderer Protokolle verhandelt werden, etwa die von OSPF o. RIPv2.

⁵³ Weitere Parameter sind äußerst selten zu definieren. Mir fällt hier nur Länge des sog. Initialisierungsvektors bei der ‚alten‘ ESP-Implementierung [RFC 1829] ein.

⁵⁴ Das ist die wohl wichtigste und grundlegendste Einstellung; nicht zu verwechseln mit der vergleichbaren beim IKE!

⁵⁵ Die SA (+ die zugehörigen Schlüssel) läuft ab, sobald einer der Werte erreicht wird: entweder die Zeit in Sekunden oder die übertragenen Datenmenge in Kilobytes. Kurz [30 Sek. oder 256 KB] vor diesem Ereignis wird eine neue SA verhandelt. Es wird bei der Aushandlung der je kürzere Wert der beiden Partner verwendet. Beachten Sie: die Implementierung dieser Parameter ist nicht durchgängig stringent! Unter Umständen dürfen sie nicht manuell konfiguriert werden (s.u. bei Win2K)!

⁵⁶ Mit Hilfe des in der *Phase 1* erzeugten (IKE-) Schlüssels werden in der *Phase 2* die dort verwendeten (IPsec-) Schlüssel generiert. Auch die nach Ablauf der Lifetime notwendigen Schlüssel können aus diesem Master-Key erzeugt werden (man spricht bei der dann notwendigen, neuen Schlüssel-Aushandlung vom sog. *Re-Keying*). Gelingt es einem Angreifer, den Master-Key zu knacken, kann er alle daraus folgenden Keys der IPsec-SAs leicht ermitteln. Schutz davor bietet sog. *Perfect Forward Secrecy* (PFS). Sie erfordert, für jede SA neues Schlüssel-Material zu generieren. Es besteht dann kein innerer Zusammenhang zwischen den nacheinander verwendeten Schlüsseln. Beachten Sie: PFS benötigt u.U. als Parameter eine Diffie-Hellman-Gruppe (die muß übereinstimmen...).

3. Die Implementierung

3.1 Notwendige Vorarbeiten

Vor der eigentlichen Implementierung müssen noch diverse Rahmenbedingungen geschaffen werden.

3.1.1 Bereitstellung einer Zertifikats-Struktur

IPsec-Authentifizierung mithilfe von manuell auf beiden Seiten eingetragenen Kennwörtern (den *pre-shared secrets*) sollte wo immer möglich vermieden werden. Sie ist schlecht skalierbar und war ursprünglich nur als Hilfsmethode bei simplen Gateway/Gateway-Konfigurationen vorgesehen⁵⁷.

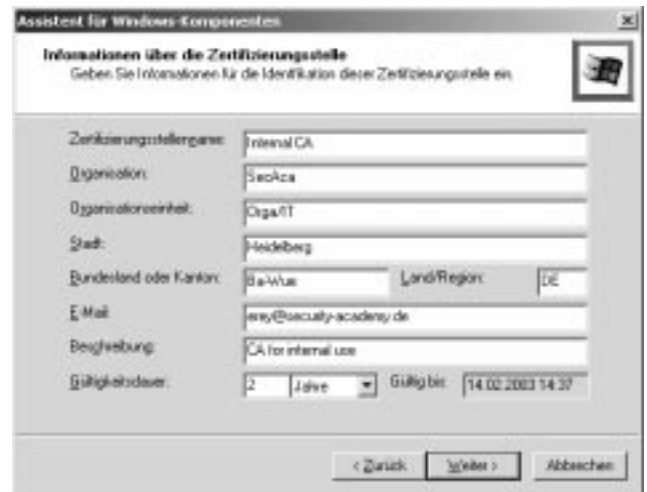
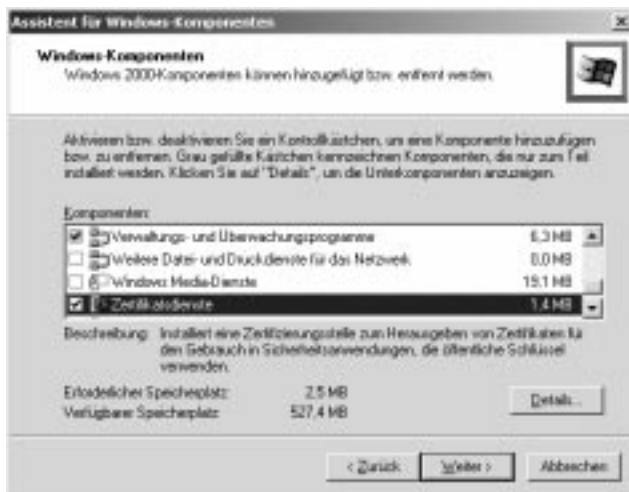
Zertifikat-basierte Authentifizierung ist auf jeden Fall vorzuziehen, weshalb auch hier damit gearbeitet wird. Dazu ist dann aber eine entsprechende Infrastruktur mit mind. einer *Certificate Authority* (CA) und den zugehörigen Zertifikaten auf Seiten der Kommunikations-Teilnehmer notwendig.

Cisco verwendet zur Verteilung von Zertifikaten (also auch zum Bezug durch die Router) ein eigenes Protokoll: das *Simple Certificate Enrollment Protocol* [SCEP, www.ietf.org/internet-drafts/draft-nourse-scep-04.txt]. Die CA muß dieses natürlich unterstützen⁵⁸. Nachdem ich von einer irgendwie vorhandenen Win2K-Landschaft ausgehe, wurden einfach die *Certificate Services* von Windows 2000 herangezogen, für die es im *Resource Kit* ein undokumentiertes (S)CEP-Addon gibt (*/apps/cep/cepsetup.exe*⁵⁹). Es wäre jedoch ebenso jede andere (S)CEP-fähige CA-Implementierung denkbar und selbstredend können Sie auch allein mit kommerziell bezogenen Zertifikaten arbeiten⁶⁰.

Das Simple Certificate Enrollment Protocol, (S)CEP

ist ein Protokoll zum Zertifikats-Management, das gemeinsam von Cisco⁶¹ und Verisign⁶² entwickelt wurde und eine frühe Implementierung der *Certificate Request Syntax*⁶³ darstellte. Es regelt, wie ein Gerät mit einer CA kommuniziert, wie etwa der *public key* der CA abgerufen wird, wie das Gerät selbst ein Zertifikat erhält, wie die *Certificate Revocation List* (CRL) abgerufen wird usw. Es basiert auf den beiden von RSA definierten *Public-Key Cryptography Standards* (PKCSs, www.rsasecurity.com/rsalabs/pkcs) Nr. 7⁶⁴ u. 10⁶⁵.

Nach der Installation und Initial-Konfiguration der *Certificate Services*



⁵⁷ Der *main mode* der Phase 1 (der die Verhandlung in drei Schritten mit insgesamt sechs Nachrichten durchführt, und neben besserem Schutz vor Denial-of-Service Angriffen auch den Schutz der Identität der Teilnehmer ermöglicht) basiert etwa bei Einsatz von *pre-shared keys* auf den IP-Adressen der Teilnehmer, weshalb bei dynamischer IP-Adresse (eines Einwahl-Clients beispielsweise) der weniger sichere *aggressive mode* zum Tragen kommen muß (zumindest solange mit *pre-shared secrets* gearbeitet wird!).

⁵⁸ Einige der wichtigsten kommerziellen CAs, z.B. VeriSign o. Entrust, tun das (ich halte es, nebenbei gesagt, fast für meine Pflicht, bei jeder Nennung von VeriSign auch immer den *MS Security Bulletin MS01-017* zu erwähnen...). Auch die Telekom-Tochter Telesec, die ich im nationalen Maßstab als CA schätze, bietet das an (so zumindest mein Kenntnisstand nach Mail von Andreas Eichstaedt/T-Nova [andreas.eichstaedt@t-systems.de] an mich).

⁵⁹ Siehe auch Q249125.

⁶⁰ Entrust bietet kostenlos Zertifikate (die 60 Tage gültig sind) zum Download per CEP an: freecerts.entrust.com/vpncerts/cep.htm.

⁶¹ Das entsprechende *White Paper* von Cisco finden Sie unter www.cisco.com/warp/public/cc/pd/sqsw/tech/scep_wp.htm.

⁶² siehe Fußnote Nr. 58...

⁶³ Ein ehemaliger Versuch, Zertifikats-Anfragen zu standardisieren, der nach ersten Drafts (siehe casl.csa.iisc.ernet.in/Standards/internet-drafts/draft-ietf-smime-crs-00.txt) in das RFC 2511 mündete.

⁶⁴ *Cryptographic Message Syntax Standard*, RFC 2630

⁶⁵ *Certification Request Syntax Standard*, RFC 2314

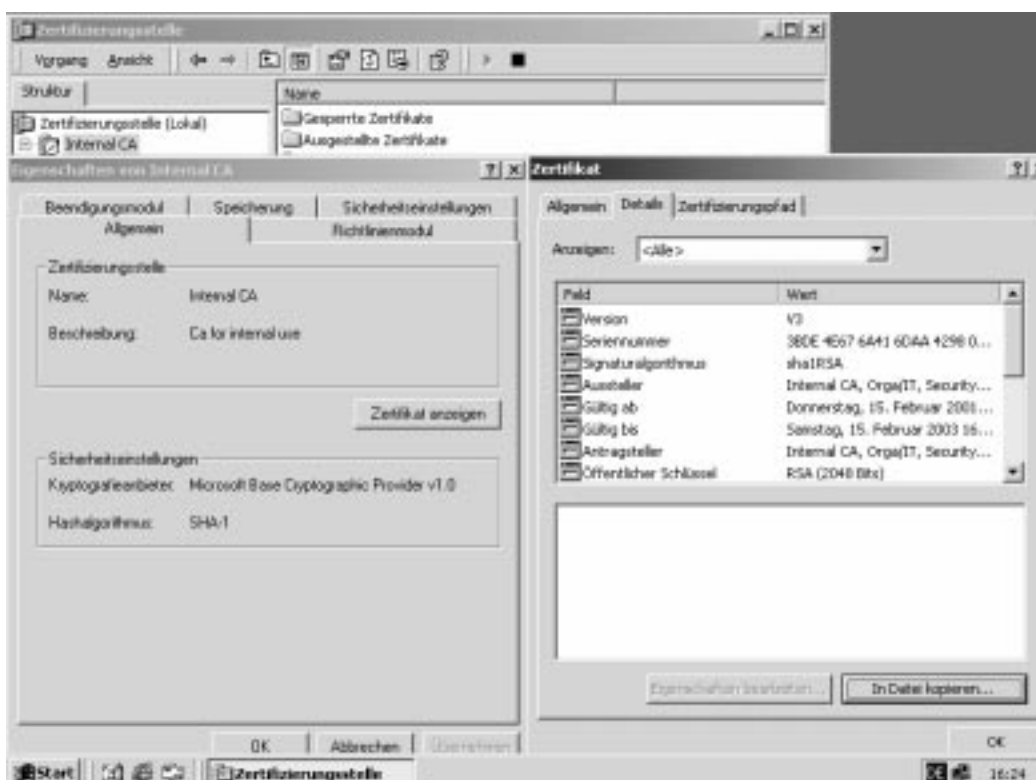
muss noch die besagte (S)CEP-Implementierung aus dem *Resource Kit* installiert werden, was ein weitgehend unspektakulärer Vorgang ist⁶⁶:



Vermeiden Sie bei der Benennung der CA nicht-alphanumerische Zeichen (d.h. Sonderzeichen)! CEP kann damit u.U. nicht umgehen und Sie werden Router-seitig Fehlermeldungen erhalten, die auf fehlgeschlagenen Zertifikatsbezug hinweisen.

Und verwenden Sie für das eigene Schlüsselpaar der CA keine Schlüssellänge > 2048 Bit! Auch das kann dazu führen, daß der Router keine Zertifikate empfangen kann.

Im Anschluß an die Einrichtung der CA müssen Sie deren eigenes Zertifikat exportieren, um es beim Client in die Liste der anerkannten Zertifizierung-Stellen aufnehmen zu können.



⁶⁶ Die einzige Dokumentation zu diesem Add-On erhalten Sie mithilfe eines Browsers unter <http://SERVERNAME/certsrc/mscep/mscep.dll>. Sollten Sie Probleme mit dem Enrollment von Zertifikaten des Routers haben (s.u.), verzichten Sie hier auf die SCEP-Challenge.

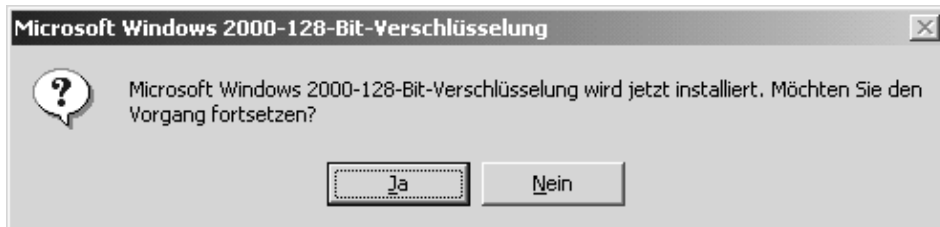
3.1.2 DNS

Funktionierendes DNS ist meist eine der Grundlagen für eine funktionale Zertifikats-Struktur (weil das ‚Subject‘ eines Zertifikats oft ein DNS-Name ist). Ich halte überdies eine effektive DNS-Struktur für ein Merkmal gelungenen Netz-Designs⁶⁷ und schließlich arbeiten wir ja mit Windows 2000, wo DNS sowieso gewissermaßen die Grundlage aller Kommunikation ist.

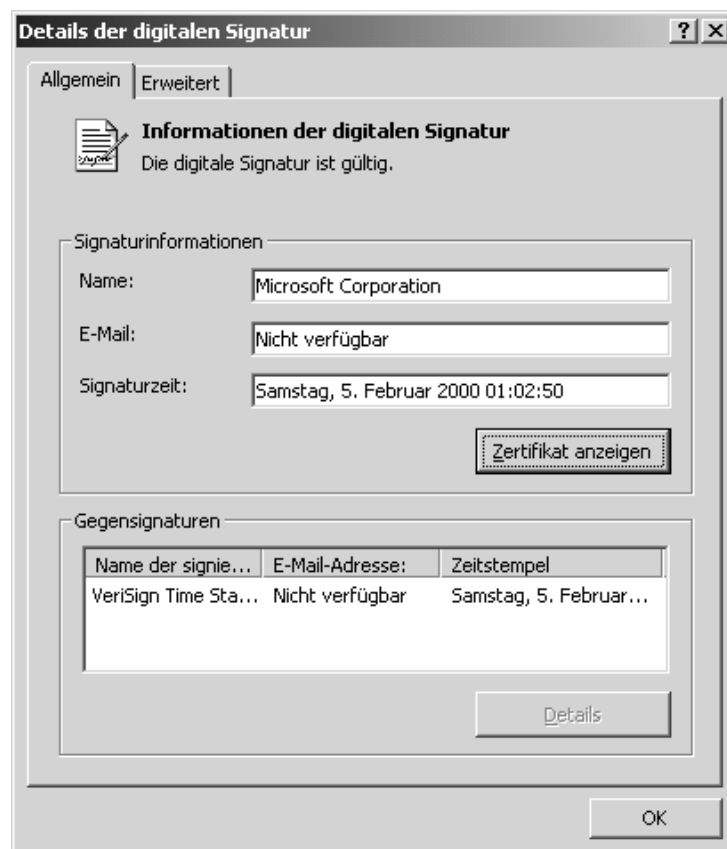
Soll heißen: DNS muß für alle Teilnehmer korrekt implementiert sein, damit das Szenario funktioniert.

3.1.3 Installation des High Encryption Pack

Das High Encryption Pack muß auf jeden Fall installiert werden, damit 3DES-Verschlüsselung möglich ist.



Sollte es der von Ihnen eingesetzten Version nicht auf Diskette beiliegen, kann es unter der o.g. URL downgeloadet werden. Selbstverständlich hätten Sie die dann notwendige Integritäts-Prüfung (Aufruf der *Eigenschaften* der betreffenden Datei – Digitale Signaturen – Details, s.u.) nicht vergessen⁶⁸...



⁶⁷ Erinnern Sie sich an meine Konnotation des Attributs „proprietär“? WINS ist proprietär...

⁶⁸ Nachdem Sie das ja auch für jeden von Microsoft bezogenen Patch und jedes Service Pack so machen... und jedes Mal prüfen, ob das von Verisign ausgestellte Zertifikat auch in die richtigen Hände gelangt ist...

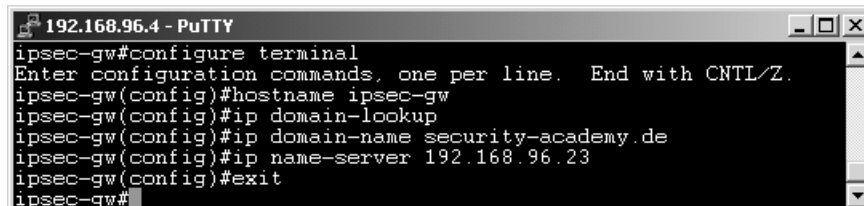
3.2 Konfiguration des IPsec-Gateways (des Routers)

3.2.1 Generelle Maßnahmen

Auch hier sind wieder verschiedene Schritte im Vorfeld notwendig.

3.2.1.1 DNS

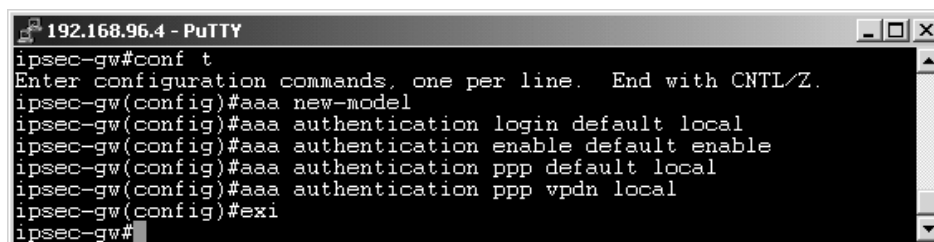
Der Router muß einen DNS-Namen haben und die am Vorgang beteiligten DNS-Namen auflösen können⁶⁹. Wir konfigurieren daher⁷⁰



```
192.168.96.4 - PuTTY
ipsec-gw#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ipsec-gw(config)#hostname ipsec-gw
ipsec-gw(config)#ip domain-lookup
ipsec-gw(config)#ip domain-name security-academy.de
ipsec-gw(config)#ip name-server 192.168.96.23
ipsec-gw(config)#exit
ipsec-gw#
```

3.2.1.2 Regelung der Authentifizierung⁷¹

AAA⁷²-Funktionalität muß vorhanden sein. Im Beispiel findet lokale Authentifizierung statt; besser ist natürlich der Einsatz entsprechender Authentifizierungs-Server. Benötigt wird⁷³:



```
192.168.96.4 - PuTTY
ipsec-gw#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ipsec-gw(config)#aaa new-model
ipsec-gw(config)#aaa authentication login default local
ipsec-gw(config)#aaa authentication enable default enable
ipsec-gw(config)#aaa authentication ppp default local
ipsec-gw(config)#aaa authentication ppp vpdn local
ipsec-gw(config)#exi
ipsec-gw#
```

Nach der generellen Aktivierung von AAA (*aaa new-model*) wird konfiguriert, daß der Zugriffs-Login anhand der lokal (auf dem Router) definierten User durchgeführt wird, beim Wechsel in den privilegierten Modus das Enable-Kennwort erforderlich ist und PPP- wie auch L2TP-Verbindungen ebenso lokal geprüft werden.

3.2.2 Herstellung des Kontakts zur CA und Bezug des Router-Zertifikats

Zunächst muß auf dem Router die CA definiert und authentifiziert werden. Dann müssen Schlüssel generiert werden und ein Zertifikat zu deren Beglaubigung angefordert werden.

3.2.2.1 Adressierung der CA⁷⁴

```
ipsec-gw(config)#crypto ca identity internalca
ipsec-gw(ca-identity)#enrollment mode ra
ipsec-gw(ca-identity)#enrollment url http://internalca.security-academy.de/certsrv/mscep/mscep.dll
Translating "internalca.security-academy.de"...domain server (192.168.96.21) [OK]

ipsec-gw(ca-identity)#crl optional
ipsec-gw(ca-identity)#exi
```

Es wird eine CA namens *internalca* angesprochen, mit der unter einer bestimmten URL – (S)CEP arbeitet über HTTP... – kommuniziert werden kann (*enrollment url*), die über eine *Registration Authority* (RA⁷⁵)

⁶⁹ Daher auch die oben (unter 1.2) genannte DNS-Regel.

⁷⁰ Der aufmerksame Leser wird bemerken, daß ich zuweilen Kommandos **demonstriere**, die offensichtlich schon vorher stattgefunden haben müssen [so in diesem Screenshot, wo 1.) der *hostname* schon konfiguriert ist und 2.) SSH ja schon läuft [= > *domain-name* und anderes erforderlich].

⁷¹ Kommando-Syntax & -Funktionalität: www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt1/scdathen.htm.

⁷² *Authentication, Authorization, Accounting*

⁷³ Es handelt sich hier – aus Gründen der Übersichtlichkeit – um eine absolute Minimalkonfiguration, die in dieser Form wohl selten produktiv auftreten wird. Außerdem wird die streng genommen erst später benötigte *vpdn*-Authentifizierung (L2TP) schon hier vorgenommen.

⁷⁴ Siehe auch www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt4/scdinter.htm.

⁷⁵ = Das Modul einer CA, das die Validierung der Requests durchführt

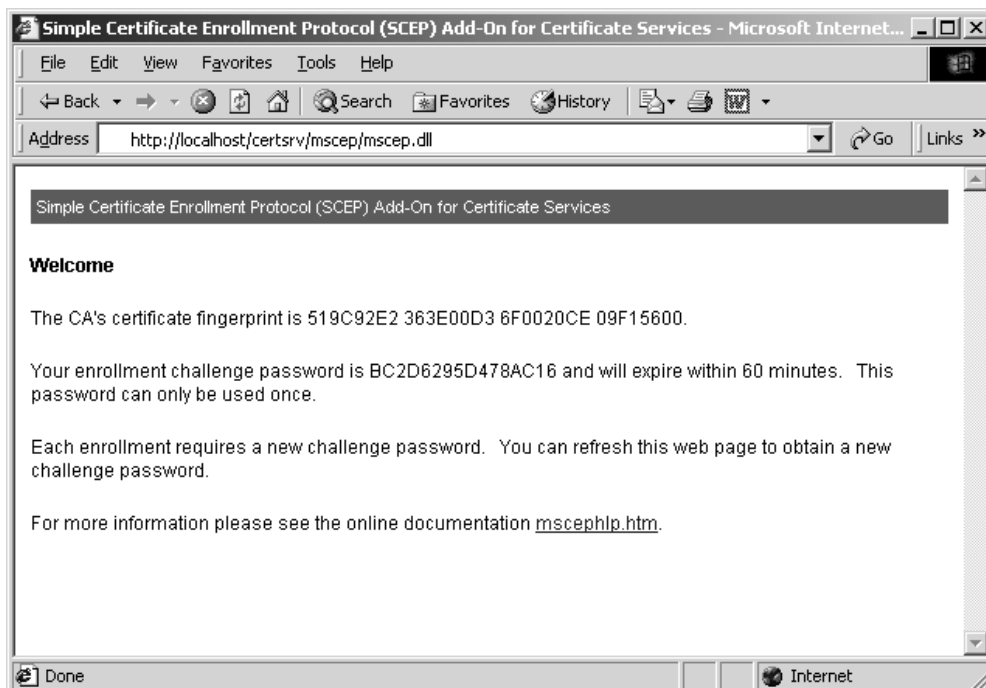
verfügt (*enrollment mode ra*) und bei deren Nicht-Erreichbarkeit Zertifikate trotz potentieller Ungültigkeit⁷⁶ akzeptiert werden (*crl optional*; dies ist auch die Default-Einstellung).

3.2.2.2 Authentifizierung der CA

Anschließend muß der Router den öffentlichen Schlüssel der CA erhalten (in Form ihres eigenen Zertifikats), um Zertifikate, die ihm von späteren Kommunikationspartnern ‚vorgelegt‘ werden, auf ihre Echtheit prüfen zu können⁷⁷

```
ipsec-gw(config)#crypto ca authenticate internalca
Translating "internalca.security-academy.de"...domain server (192.168.96.21) [OK]
Certificate has the following attributes:
Fingerprint: 519C92E2 363E00D3 6F0020CE 09F15600
% Do you accept this certificate? [yes/no]: y
ipsec-gw(config)#
```

Vergleichen Sie diesen Fingerprint ggf. ‚manuell‘ mit dem des Zertifikats der CA, um sicherzustellen, daß es sich um dasselbe Zertifikat handelt...



In einem Dokument zum Thema Cisco-VPN⁷⁸, das ich während des Verfassens dieses Papers in den Händen hatte, steht an dieser Stelle:

If you've made it this far, you're definitely past the hard part.

Ich kann das bestätigen⁷⁹...

⁷⁶ Zur Wechselwirkung mit dem Kommando *query url* siehe die in Fußnote 73 genannte URL.

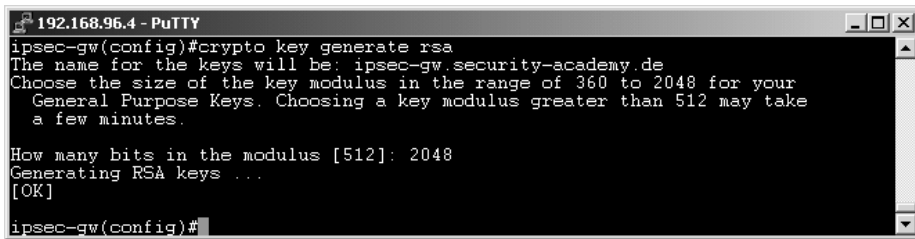
⁷⁷ Diese sind ja mit dem privaten Schlüssel der CA signiert.

⁷⁸ download.nai.com/products/media/pgp/pdf/literature/cisco.pdf

⁷⁹ Es geht übrigens wie folgt weiter: „If you experienced any difficulties obtaining the certificate, you might want to use a Sniffer to make sure everything is being sent correctly or ask Verisign to determine what they are seeing.“ (z.B. ob Sie echte Microsoft-Mitarbeiter erkennen können...).

3.2.2.3 Generierung der Schlüssel

Jetzt wird ein eigenes Schlüsselpaar des Routers generiert...



```
192.168.96.4 - PuTTY
ipsec-gw(config)#crypto key generate rsa
The name for the keys will be: ipsec-gw.security-academy.de
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 2048
Generating RSA keys ...
[OK]
ipsec-gw(config)#
```

3.2.2.4 Beantragung & Erhalt des Zertifikats

...und der öffentliche Teil davon in ein Zertifikat unserer CA gegossen...

```
ipsec-gw(config)#crypto ca enroll internalca
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will be: ipsec-gw.security-academy.de
% Include the router serial number in the subject name? [yes/no]: n
% Include an IP address in the subject name? [yes/no]: y
Interface: FastEthernet0/1
Request certificate from CA? [yes/no]: y
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.

ipsec-gw(config)#    Fingerprint:  0A44D310 93C70A05 1F40A3CF 60C2D0A2

Apr 15 02:45:48: %CRYPTO-6-CERTRET: Certificate received from Certificate Authority
ipsec-gw(config)#
```

Achten Sie auf die Konsole-Meldung, daß das Zertifikat auch überhaupt erhalten wurde...

3.2.2.5 Troubleshooting

Überprüfen Sie das System-Datum des Routers dahingehend, ob es innerhalb des Gültigkeits-Zeitfensters des Zertifikats liegt (siehe dazu auch 5.1).

Vergewissern Sie sich, daß die Länge des öffentlichen Schlüssels der CA 2048 Bit nicht überschreitet.

Mithilfe von „show crypto ca certificate“ (im privilegierten Modus) können Details der Zertifikate des Routers angezeigt werden.

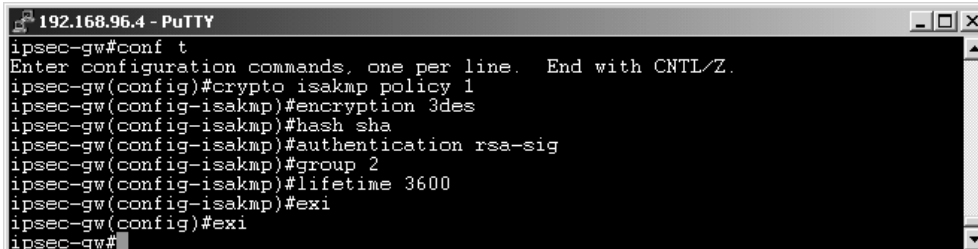
3.2.3 Konfiguration von IPsec

Sie besteht aus zwei Teilen: der Konfiguration (und Aktivierung) des Schlüsselaustausches und der Konfiguration des dann zu verschlüsselnden Verkehrs.

3.2.3.1 Der Schlüsselaustausch (IKE)⁸⁰

Bedenken Sie immer die oben genannten Kern-Parameter des *Internet Key Exchange*.

Wir verwenden: Authentifizierung mit RSA-Signatur (hier mithilfe der Zertifikate), Verschlüsselung des IKE mit 3DES, Hash-Verfahren SHA-1, DH-Gruppe 2 und eine Lifetime von einer Stunde (3600 Sek.)⁸¹.



```
192.168.96.4 - PuTTY
ipsec-gw#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ipsec-gw(config)#crypto isakmp policy 1
ipsec-gw(config-isakmp)#encryption 3des
ipsec-gw(config-isakmp)#hash sha
ipsec-gw(config-isakmp)#authentication rsa-sig
ipsec-gw(config-isakmp)#group 2
ipsec-gw(config-isakmp)#lifetime 3600
ipsec-gw(config-isakmp)#exi
ipsec-gw(config)#exi
ipsec-gw#
```

Der Schlüsselaustausch **muß** dann noch mit „crypto isakmp enable“ [im Konfigurations-Modus] generell aktiviert werden⁸².

3.2.3.2 Konfiguration der Verkehrs-Verschlüsselung⁸³

Hier sind verschiedene Schritte notwendig. Zunächst muß definiert werden, *welcher* Verkehr überhaupt verschlüsselt werden soll⁸⁴. Dann wird durch ein *transform* festgelegt, *wie* (d.h. mit welchen Verschlüsselungs- und/oder Hash-Algorithmen) diese Pakete geschützt werden sollen. Und schließlich werden diese Einstellungen unter dem Dach einer *crypto map* zusammengefasst, die dann wiederum auf ein Interface angewendet wird.

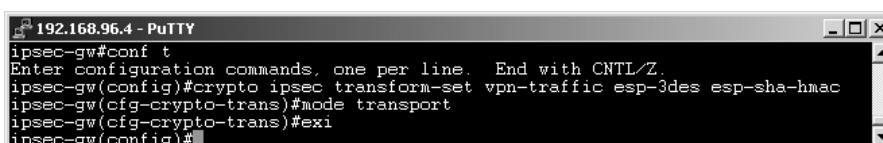
Auf welchen Verkehr IPsec angewandt wird, regelt eine *crypto access-list*. *Crypto access-lists* sehen syntaktisch aus wie reguläre *access-lists*, haben aber eine gänzlich andere Funktion: alle Pakete, die darin unter ein *permit*-Statement fallen, sollen verschlüsselt werden.

Initiale IPsec-Pakete (IKE), die den Schlüsselaustausch durchführen (ISAKMP-Verkehr, UDP Port 500), werden unverschlüsselt zugelassen⁸⁵. Sonstiger UDP-Verkehr (und damit L2TP) wird gewissermaßen IPsec unterworfen (mittels eines *permit*-Statements!)⁸⁶.

```
access-list 101 deny    udp any any eq isakmp
access-list 101 permit udp any host 195.145.236.253
```

Achten Sie peinlichst auf korrekte *access-lists*!⁸⁷

Anschließend wird mittels einer Transformation (eines *transforms*) definiert, welche Sicherheitsprotokolle mit welchen Algorithmen zur (Verhandlungs-) Auswahl stehen. Wir beschränken uns auf ESP mit 3DES als Verschlüsselungs- sowie SHA-1 als Hash-Algorithmus und arbeiten im *transport mode*.



```
192.168.96.4 - PuTTY
ipsec-gw#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ipsec-gw(config)#crypto ipsec transform-set vpn-traffic esp-3des esp-sha-hmac
ipsec-gw(cfg-crypto-trans)#mode transport
ipsec-gw(cfg-crypto-trans)#exi
ipsec-gw(config)#
```

⁸⁰ Kommando-Referenz: www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgr/ secur_r/srprt4/srdike.htm.

⁸¹ Einige dieser Werte sind in der Konfig nicht sichtbar, weil es sich um Default-Werte handelt.

⁸² Das erscheint nicht in der *running* oder *startup config*.

⁸³ Kommando-Referenz: www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgr/ secur_c/scprt4/scdipsec.htm.

⁸⁴ Eigentlich müßte hier stehen: „welcher Verkehr überhaupt durch IPsec geschützt werden soll“. Es wäre ja auch (beim Einsatz von AH) denkbar, nur die Integrität und Authentizität des Verkehrs zu sichern, nicht aber dessen Vertraulichkeit. Im Szenario wird aber nur mit ESP gearbeitet.

⁸⁵ Sowohl eingehender wie ausgehender Verkehr werden durch **eine** *access-list* erfaßt (siehe dazu auch die o.g. Referenz-URL).

⁸⁶ Wir setzen weder RIP noch SNMP in diesen Segmenten ein und auch sonst wird nur wenig UDP-Verkehr an diesem Interface eintreffen... ich gebe aber zu, dass diese *crypto access list* noch exakter gefaßt werden könnte...

⁸⁷ Die *Phase 1* findet auch ohne zutreffende *access-lists* statt... und Sie werden den Fehler dann nicht hier suchen... Die Debug-Meldung „IPSec policy invalidated proposal“ ist ein Hinweis auf falsche *access-lists*.

Die *crypto access-list* und der *transform* werden jetzt verknüpft durch eine *crypto map*. Eine solche *crypto map* regelt, welcher Verkehr geschützt wird (in Form der *access-list*), an welche Gegenstelle dieser Traffic geschickt wird (in Form der Angabe eines o. mehrerer *peers*), welche Sicherheits-Protokolle mit welchen Algorithmen dafür akzeptabel sind (via *transform*) und ggf. wie Schlüssel bzw. SAs verwaltet werden.

Sind diese Informationen nicht im voraus bekannt (wie im Fall einer dynamischen IP-Adresse des Clients), kommt eine *dynamic map* in's Spiel. Dabei handelt es sich um eine Art Template, das variabel angewendet werden kann. Das Ganze sieht dann in etwa so aus:

```
192.168.96.4 - PuTTY
ipsec-gw(config)#crypto dynamic-map vpn 1
ipsec-gw(config-crypto-map)#set transform-set vpn-traffic
ipsec-gw(config-crypto-map)#set pfs group2
ipsec-gw(config-crypto-map)#match address 101
ipsec-gw(config-crypto-map)#exit
ipsec-gw(config)#crypto map vpn-map 1 ipsec-isakmp dynamic vpn
ipsec-gw(config)#interface FastEthernet0/1
ipsec-gw(config-if)#crypto map vpn-map
ipsec-gw(config-if)#exit
ipsec-gw(config)#exit
ipsec-gw#
```

Erstellt wurden hier eine *dynamic map* namens **vpn** mit verschiedenen Parametern (*transform*, *access-list*, PFS mit DH-Gruppe 2 aktiviert) und eine *crypto map* namens **vpn-map**, die auf das dynamische Template ‚vpn‘ zurückgreift. Diese *crypto map* wird dann an einem Interface angewendet.

3.2.3.3 Troubleshooting

Überprüfen Sie die Übereinstimmung aller wichtigen Parameter mit der Gegenstelle!

Das wichtigste Debug-Kommando für IPsec auf Cisco-Routern ist „debug crypto isakmp“. Es erzeugt einen umfangreichen Output insbesondere der Verhandlungsphase (Sie finden im Anhang ein Beispiel). Ergänzen Sie es ggf. um „debug crypto ipsec“ und/oder „debug crypto engine“, die aber – so zumindest meine Wahrnehmung – nur wenig zusätzlich hilfreiche Information liefern.

Es gibt des weiteren einen im Hause *Matsushita* entwickelten, dedizierten IPsec-Protokollanalyser (den *NetCocoon-Analyzer*⁸⁸). Ich hatte allerdings noch keine Gelegenheit, das Produkt zu evaluieren⁸⁹.

Gegebenenfalls können Sie ihr Problem auch an die Mailing-Liste (ipsec@lists.tislabs.com⁹⁰) der IPsec-Charter der IETF posten. Sie werden zwar einerseits unfreundliche Antworten erhalten, dort würde nur über Standards und nicht etwa über Hersteller-spezifische Problemchen diskutiert, andererseits verdanke ich entscheidende Hinweise einem Teilnehmer dieser Liste (der es mit der Begrenzung auf Spezifikationsfragen nicht so genau nahm)...

Und schließlich sollten Sie sich an den Hersteller der Komponente (hier also das *Cisco Technical Assistance Center*) wenden. IPsec ist, wie gesagt, noch nicht umfassend standardisiert. Möglicherweise unterscheidet sich die Implementierung eines Devices von der einer Gegenstelle in einem vermeintlich nebensächlichen – die Kommunikation im konkreten Fall aber verhindernden – Detail (von dessen Existenz Sie erst bei Nachhaken beim Hersteller überhaupt erfahren).

Hilfreich ist auch www.cisco.com/networkers/nw00/pres/2405.pdf

⁸⁸ www.mew.co.jp/e-netcocoon/analyzer.html

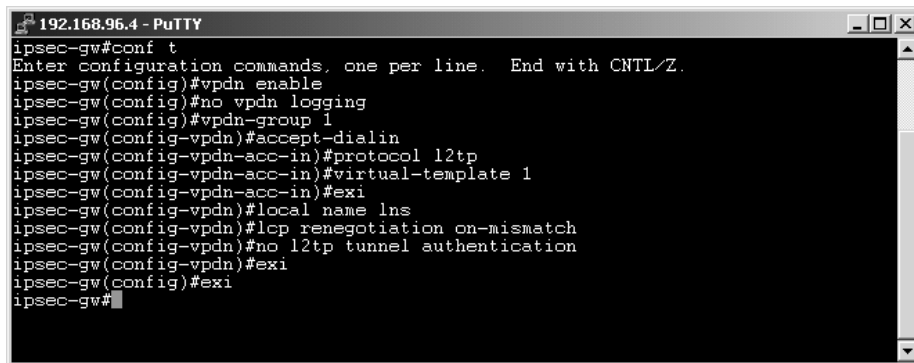
⁸⁹ Ich wäre aber für diesbezügliche Erfahrungsberichte sehr dankbar... Eine Evaluierungs-Version ist übrigens durch direkten (Mail-) Kontakt zum Entwickler-Team erhältlich.

⁹⁰ Zum *subscribe* siehe: www.ietf.org/html.charters/ipsec-charter.html.

3.2.4 Konfiguration von L2TP⁹¹

Die Einrichtung von L2TP auf dem *Cisco*-Router besteht aus verschiedenen Teilen. L2TP muß generell aktiviert werden; dann werden die Parameter des *VPDN* (Virtual Private Dialup Networking, unter diesem Terminus werden bei *Cisco* L2TP und PPTP subsummiert) in einer *vpdn-group* definiert und die Einstellungen der dabei erzeugten virtuellen Interfaces (samt Adress-Pool) konfiguriert.


3.2.4.1 Die generelle L2TP-Konfiguration



```
ipsec-gw#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ipsec-gw(config)#vpdn enable
ipsec-gw(config)#no vpdn logging
ipsec-gw(config)#vpdn-group 1
ipsec-gw(config-vpdn)#accept-dialin
ipsec-gw(config-vpdn-acc-in)#protocol l2tp
ipsec-gw(config-vpdn-acc-in)#virtual-template 1
ipsec-gw(config-vpdn-acc-in)#exit
ipsec-gw(config-vpdn)#local name lns
ipsec-gw(config-vpdn)#lcp renegotiation on-mismatch
ipsec-gw(config-vpdn)#no l2tp tunnel authentication
ipsec-gw(config-vpdn)#exit
ipsec-gw(config)#exit
ipsec-gw#
```

VPDN wird aktiviert, das Logging dafür aber (aus Gründen der Übersichtlichkeit der Logfiles) ausgeschaltet. Dann wird eine entsprechende *vpdn-group* eingerichtet, die Verbindungswünsche entgegennimmt (*accept dialin*), L2TP als Protokoll verwendet und die virtuellen Interfaces gemäß des *virtual-template 1* konfiguriert. Der LNS präsentiert sich (kreativerweise...) unter dem Namen ‚lns‘, das *link control protocol* (Teil von PPP) wird unter Umständen neu-verhandelt und der Tunnel wird nicht als solcher authentifiziert (es findet ja eine User-Authentifizierung bei der Erstellung des virtuellen Interfaces statt). Die (L2TP-) Tunnel-Authentifizierung – die mir in einem Mail angeraten wurde – ist nicht zwingend notwendig und würde überdies auf Seiten des (Windows 2000-) Clients einen Registry-Eingriff erfordern⁹².

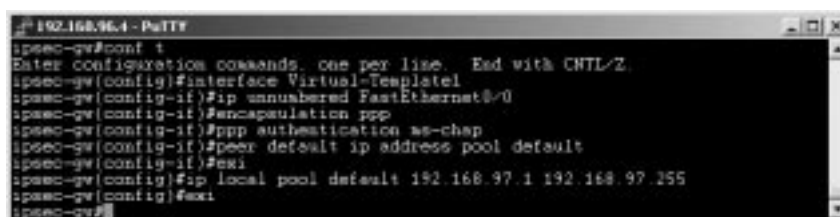
Beachten Sie außerdem, daß der *username* LNS konfiguriert werden muß (trotz, wie mir scheint, anderslautender Aussage der Cisco-Dokumentation). Ohne ihn findet kein ordentlicher L2TP-Verbindungsaufbau statt.



```
ipsec-gw#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ipsec-gw(config)#username lns password brute_force_this!
ipsec-gw(config)#exit
ipsec-gw#
```

3.2.4.2 Konfiguration des *virtual-templates*⁹³

Für alle virtuellen Interfaces wird bei ihrer ‚Ausstattung‘ (etwa mit einer IP-Adresse) eine Vorlage verwendet, die dann pro Verbindung geclont wird. Die virtuellen Schnittstellen erhalten in unserem Beispiel keine eigenen IP-Adressen (‚ip unnumbered‘; sie leihen sich ihre Adresse quasi vom anderen Ethernet-Interface). Die natürlich notwendige Zuteilung einer Adresse an den jeweiligen Client erfolgt aus einem dafür definierten *pool*. Auf dem virtuellen Interface wird PPP mit Authentifizierung durch *MS-CHAP* eingesetzt⁹⁴.



```
ipsec-gw#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ipsec-gw(config)#interface Virtual-Template1
ipsec-gw(config-if)#ip unnumbered FastEthernet0/0
ipsec-gw(config-if)#encapsulation ppp
ipsec-gw(config-if)#ppp authentication ms-chap
ipsec-gw(config-if)#ppp default ip address pool default
ipsec-gw(config-if)#exit
ipsec-gw(config)#ip local pool default 192.168.97.1 192.168.97.255
ipsec-gw(config)#exit
ipsec-gw#
```

⁹¹ Kommando-Referenz: www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/l2tpt.htm und www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgr/dial_r/drdrvp.htm.

⁹² Ein REG_SZ namens ‚password‘ müßte unter ‚HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\WAN Miniport (L2TP) <Device-number (000n)>‘ gesetzt werden. Schlagen Sie dazu ggf. in der *regentry.chm* des RK nach.

⁹³ Kommando-Referenz: www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgr/dial_c/dcvprof.htm.

⁹⁴ Ansonsten sind hier (fast) alle Befehle möglich, die auf seriellen Schnittstellen verwendet werden können.

3.2.4.3 Troubleshooting

Neben den dedizierten Debug-Befehlen für L2TP

```
192.168.96.4 - PuTTY
ipsec-gw#debug wpdn ?
error          VPDN Protocol errors
event          VPDN event
l2tp-sequencing L2TP sequencing
l2x-data       L2F/L2TP data packets
l2x-errors     L2F/L2TP protocol errors
l2x-events     L2F/L2TP protocol events
l2x-packets    L2F/L2TP control packets
packet         VPDN packet
pppoe-data     PPPoE data packets
pppoe-errors   PPPoE protocol errors
pppoe-events   PPPoE protocol events
pppoe-packets  PPPoE control packets

ipsec-gw#debug wpdn
```

ist insbesondere das PPP-Debugging mit „debug ppp negotiation“ hilfreich⁹⁵:

```
192.168.96.4 - PuTTY
ipsec-gw#debug ppp negotiation
PPP negotiation debugging is on
ipsec-gw#show
ipsec-gw#
Apr 16 21:33:18: OCSPTO-4-SECND_PKT_INF_SPL: decaps: rec'd IPSEC packet len 156
vll4 spi len
Apr 16 21:33:21: Vll4-3-UPDOWN: Interface Virtual-Access1, changed state to up
Apr 16 21:33:21: Vll4 PPP: Using mtu 1473
Apr 16 21:33:21: Vll4 PPP: Creating connections as a callee
Apr 16 21:33:21: Vll4 PPP: Phase is ESTABLISHING, Passive Open (8 secs, 8 load)
Apr 16 21:33:22: Vll4 LCP: State is Listen
Apr 16 21:33:23: Vll4 LCP: I CONFREQ [Listen] id 1 len 27
MagicNumber 0x2E1E74E2 (0x5062E1E74E2)
FCF (0x8762)
ACFC (0x8802)
Callback 0 (0x1E306)
Apr 16 21:33:23: Vll4 LCP: O CONFREQ [Listen] id 1 len 25
AuthProto MS-CHAP (0x038C2200)
MagicNumber 0x31E1CC42 (0x50601E1CC42)
Apr 16 21:33:23: Vll4 LCP: I CONFREQ [Listen] id 1 len 7
Callback 0 (0x1E306)
Apr 16 21:33:23: Vll4 LCP: I CONFACK [PENDING] id 1 len 10
AuthProto MS-CHAP (0x038C2200)
MagicNumber 0x31E1CC42 (0x50601E1CC42)
Apr 16 21:33:23: Vll4 LCP: I CONFREQ [Accepted] id 2 len 14
MagicNumber 0x2E1E74E2 (0x5062E1E74E2)
FCF (0x8762)
ACFC (0x8802)
Apr 16 21:33:23: Vll4 LCP: State is Open
Apr 16 21:33:23: Vll4 PPP: Phase is AUTHENTICATING, by this end (0 secs, 8 load)
Apr 16 21:33:23: Vll4 MS-CHAP: O CHALLENGE id 1 len 21 from "ipsec-gw"
Apr 16 21:33:23: Vll4 LCP: I IDENTIFY [Open] id 3 len 18 magic 0x2E1E74E2 MSCHAPv1
id
Apr 16 21:33:23: Vll4 LCP: I IDENTIFY [Open] id 4 len 22 magic 0x2E1E74E2 MSCHAPv1
-REQIDLE
Apr 16 21:33:23: Vll4 MS-CHAP: I RESPONSE id 3 len 68 from "arag"
Apr 16 21:33:23: Vll4 MS-CHAP: O SUCCESS id 3 len 4
Apr 16 21:33:23: Vll4 PPP: Phase is UP (0 secs, 0 load)
Apr 16 21:33:23: Vll4 IPCP: O CONFREQ [Listen] id 1 len 10
Address 176.188.236.253 (0x0308C191E0FD)
Apr 16 21:33:23: Vll4 CCP: I CONFREQ [Sec negotiated] id 0 len 16
MS-FCF supported bits 0x81800001 (0x120818000001)
Apr 16 21:33:23: Vll4 LCP: O PROTRNS [Open] id 2 len 13 protocol CCP (0x88FD0188
0x8120601888801)
Apr 16 21:33:23: Vll4 IPCP: I CONFREQ [PENDING] id 0 len 24
Address 0.0.0.0 (0x030818800000)
Apr 16 21:33:23: Vll4 IPCP: PrimaryDNS 0.0.0.0 (0x818600008888)
Apr 16 21:33:23: Vll4 IPCP: PrimaryVINE 0.0.0.0 (0x812600008888)
Apr 16 21:33:23: Vll4 IPCP: SecondaryDNS 0.0.0.0 (0x812600008888)
```

⁹⁵ Weitere PPP-Debugkommandos erhalten Sie durch „debug ppp?“ [im privil. Modus]. „deb ppp nego“ ist aber das bei weitem wichtigste.

3.3 Der Windows 2000-Client

3.3.1 Umgehung des in Q276360 beschriebenen IPsec-Problems

Der *Knowledge Base*-Artikel Q276360 dokumentiert, daß *Microsoft* mit dem SP1 für Windows 2000 verschiedene Änderungen am IPsec-Stack vorgenommen hat; darunter eine, die die Zusammenarbeit mit Cisco-Routern unter Umständen beeinträchtigt⁹⁶. Und zwar dergestalt, daß L2TP über IPsec nicht mehr funktioniert (was ich auch beobachten konnte: die letzte PPP-Phase [IPCP] wurde dann nicht korrekt abgeschlossen => der Client beendete die PPP-Aushandlung nicht erfolgreich).

Als Lösung kommen in Betracht: Einsatz von W2K ohne Service Pack (unter Sicherheits-Gesichtspunkten unschön), Einspielen des im Artikel genannten Patches⁹⁷ oder eben Warten auf SP2.

Ich entschied mich für die erste Variante (Arbeit *ohne* SP1), weil SP2 zum Zeitpunkt der Erstellung dieses Papers (März 2001) noch nicht verfügbar war und weil der Erhalt nicht downloadbarer Patches bei *Microsoft* traditionell mit viel Aufwand (vor allem administrativer Art) verbunden ist⁹⁸.

Diese Mühe sollten Sie aber beim produktiven Einsatz auf sich nehmen! Es sei denn, Sie installieren alle sicherheits-relevanten Patche, die in SP1 enthalten sind⁹⁹, gewissermaßen manuell auf den Client-Geräten (und verzichten auch sonst auf alle SP1-Annehmlichkeiten...).

3.3.2 Import des Zertifikats der CA

Das unter 3.1.1 exportierte, eigene Zertifikat der CA muß beim Client noch importiert werden, damit diese (unsere) CA während der IPsec-Konfiguration überhaupt als vertrauenswürdig bekannt ist¹⁰⁰. Dazu wird das Snap-In *Zertifikate (Lokaler Computer)* der Management-Konsole verwendet¹⁰¹:



⁹⁶ Das sog. *Padding* (Auffüllen, um Blöcke bestimmter Größe zu erhalten) bei bestimmten Algorithmen innerhalb des ESP-Protokolls [des CBC-Modus von DES o. 3DES] wurde so verändert, daß für empfangene Pakete nur noch max. 7 Bytes *Padding* gestattet sind, im Ggs. zu 9 (ohne SP1). Diesen Hinweis verdanke ich einem *Microsoft*-Mitarbeiter.

⁹⁷ auf den auch in anderen KB-Artikeln (etwa Q272173) verwiesen wird...

⁹⁸ Und das, obwohl ich für einen *MS Solution Provider* arbeite. Ich kann die dahinterstehende Politik auch nicht recht nachvollziehen (und ebenso wenig die Unterscheidung frei erhältlicher vs. „Contact SSP“-Patche); vielleicht kann da jemand von *Microsoft* gelegentlich zu meiner Erhellung beitragen...

⁹⁹ Zu finden unter www.microsoft.com/security/bulletins...

¹⁰⁰ Es soll an dieser Stelle weder über Zertifikats-Hierarchien noch darüber, ob unsere CA tatsächlich zu den ‚Vertrauenswürdigen Stammzertifizierungsstellen‘ gehört, diskutiert werden...

¹⁰¹ Die genannten Snap-Ins erhalten Sie durch Aufruf einer ‚nackten‘ Management-Konsole (Start -> Ausführen: „mmc“) und anschließendem *Konsole – Snap-In hinzufügen/entfernen...*

3.3.3 Erhalt eines IPsec-Zertifikats von der CA

Der Client benötigt natürlich selbst noch ein IPsec-Zertifikat, das im nächsten Schritt angefordert wird:



Wir wünschen ein Zertifikat mithilfe der *Erweiterten Anforderung*. Beachten Sie, daß Sie beim *beabsichtigten Zweck* ‚IPsec-Zertifikat‘ aktivieren und für dieses Zertifikat einen **Lokalen Speicherplatz verwenden**.



Es muß dann noch auf Seiten der CA abgesegnet werden¹⁰² und beim Client anschließend im Browser über ‚Auf ein ausstehendes Zertifikat überprüfen‘ installiert werden.



¹⁰² Sie können auch in den Eigenschaften der CA konfigurieren, daß allen Anforderungen ohne Prüfung durch einen Admin stattgegeben wird.

3.3.4 Konfiguration von IPsec

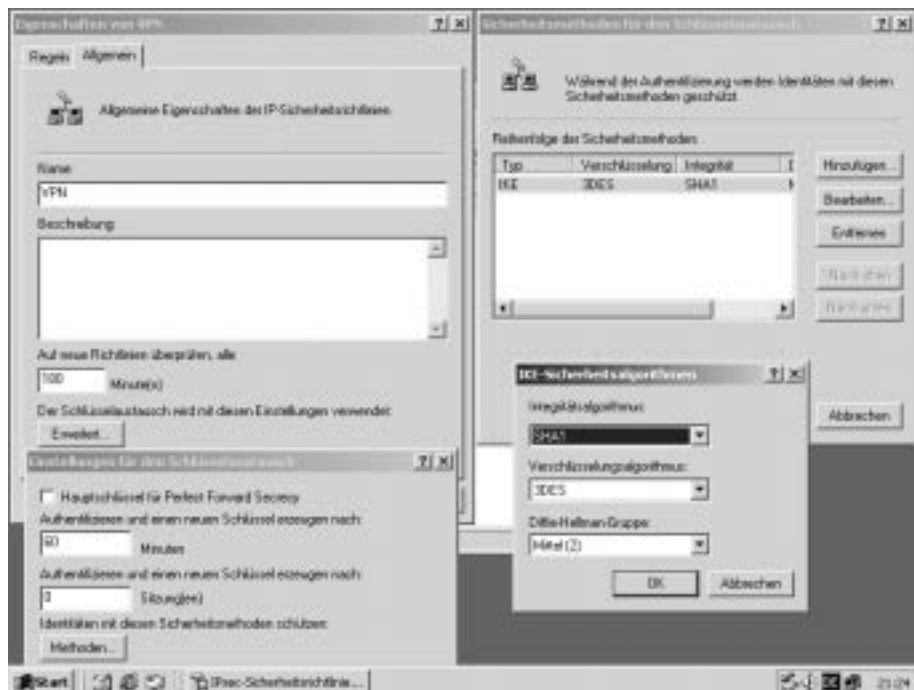
Die Konfiguration der IPsec-Richtlinien wird mit dem Snap-In *IP-Sicherheitsrichtlinien auf lokalem Computer* durchgeführt¹⁰³. Alle bestehenden Richtlinien werden gelöscht und eine neue Richtlinie namens ‚VPN‘ erstellt¹⁰⁴. Rufen Sie dann als erstes ‚IP-Sicherheitsrichtlinie erstellen‘ auf. Wir nennen die Richtlinie *VPN* und arbeiten mit der *Authentifizierungsmethode* Zertifikat (von unserer eigenen CA):



Diese Richtlinie („VPN“) wird anschließend bearbeitet. Zunächst die

3.3.4.1 Eigenschaften des Schlüsselaustausches (IKE)

Diese werden unter *VPN – Eigenschaften – Allgemein – Erweitert – Methoden* definiert. Sie beschreiben nur die Parameter der initialen Schlüsselaushandlung (siehe oben) und **müssen** mit den auf dem *Cisco* unter 3.2.3.1 konfigurierten übereinstimmen (können). Wir konfigurieren wie folgt:



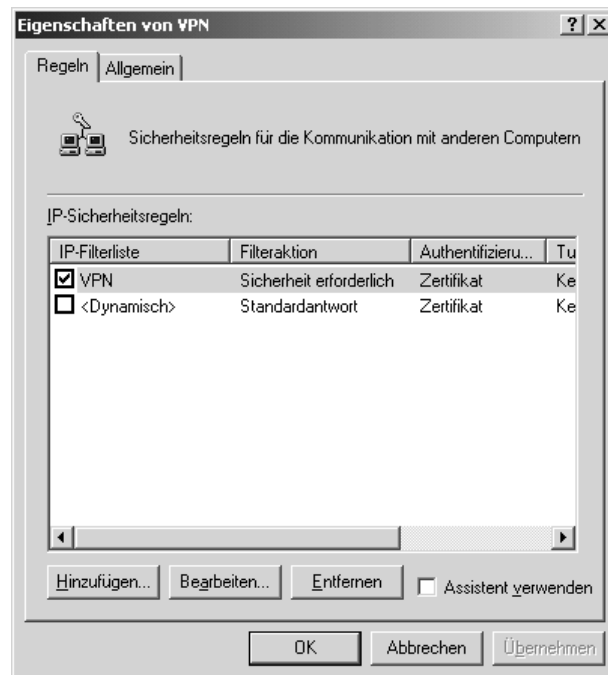
¹⁰³ Alternativ ist eine Konfiguration über die *Lokale Sicherheitsrichtlinie* möglich. Ich bevorzuge aber das dedizierte Snap-In.

¹⁰⁴ Es wird so je nach weiterer Konfiguration die Möglichkeit direkter Internet-Kommunikation (mit allen negativen Sicherheits-Implikationen) weitgehend ausgeschlossen. Sie sollten das aber bei gleichzeitiger Nutzung des Laptops im LAN bedenken... und für diesen Zweck dann ggf. weitere Richtlinien erstellen und eine von diesen aktivieren. Die User sollten das **nicht** selbst tun können (ich gehöre zu denen, die nicht der Meinung sind, daß User administrative Rechte an ihren [mobilen] Rechnern haben sollten. Diese Dinge sind aber ja bestimmt so oder so in Ihrer Security Policy geregelt...). Sollten die Nutzer entsprechende Befugnisse haben, ist eine Quarantäne-Station für mobile Geräte bei „Rückkehr in's LAN“ unverzichtbar (die im übrigen auch sonst hilfreich ist...).

3.3.4.2 Die Eigenschaften des IPsec-Kommunikation selbst, d.h. der *Security Associations*

... wiederum werden unter *VPN – Eigenschaften – Regeln* parametrisiert. Die folgenden Einstellungen **müssen** mit denen auf dem Router unter 3.2.3.2 definierten übereinstimmen (können).

Zunächst wird eine *IP-Sicherheitsregel*¹⁰⁵ hinzugefügt, die (schon wieder...) *VPN* genannt wird.



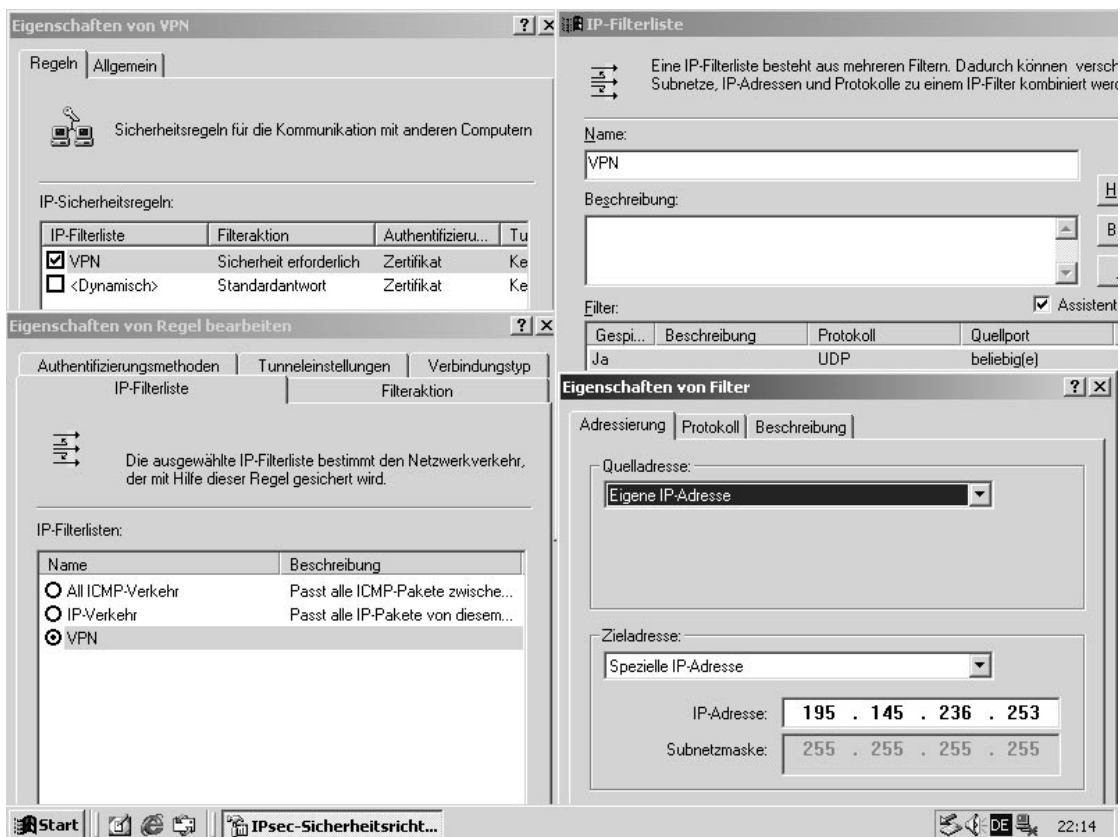
Sie definiert *keinen Tunnel*, gilt für *RAS-Verbindungen* u. arbeitet mit einer IP-Filterliste¹⁰⁶ namens ... *VPN*



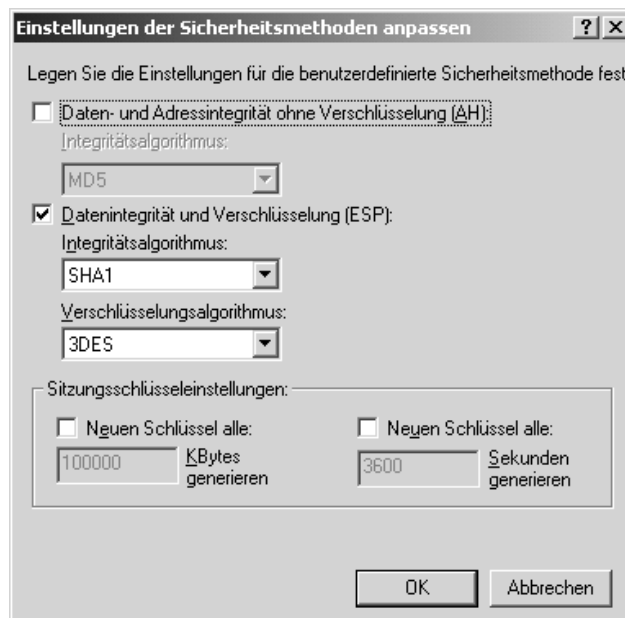
¹⁰⁵ Eine Sicherheitsregel vereint, ähnlich einem *transform*, die Information, welcher Verkehr wie zu handhaben ist. Diese auch *Policy* genannte Regel wird erstellt, um die von L2TP sonst automatisch erstellte Policy (die wir deaktivieren, s.u.) zu ersetzen.

¹⁰⁶ ... die hinzugefügt wird. Eine solche *Filterliste* entspricht einer *crypto access list* auf d. Cisco. Sie regelt, *welcher* Verkehr v. IPsec zu behandeln ist.

Darin wiederum wird konfiguriert, daß UDP-Verkehr (auch das könnte feiner gefaßt werden...) zur IP-Adresse 195.145.236.263 (dem IPsec-Gateway) von dieser Liste erfaßt wird:



Die *Filteraktion*¹⁰⁷ (was soll denn mit dem eben gekennzeichneten UDP-Verkehr zu 195.145.236.253 überhaupt passieren) wird auf *Sicherheit erforderlich* eingestellt (= > zwangsweise IPsec unterworfen), und zwar mit folgenden Rahmenbedingungen (*Sicherheitsmethoden*):



Beachten Sie, daß Sie auf keinen Fall unter *Sitzungsschlüsseinstellungen* eine KB-basierte Lifetime („Neuen Schlüssel alle: ... KBytes generieren“) aktivieren sollten. Die Sitzungsaushandlung („proposal“) mit dem Cisco wird sonst fehlschlagen¹⁰⁸.

¹⁰⁷ ... regelt, wie denn mit dem Verkehr zu verfahren ist.

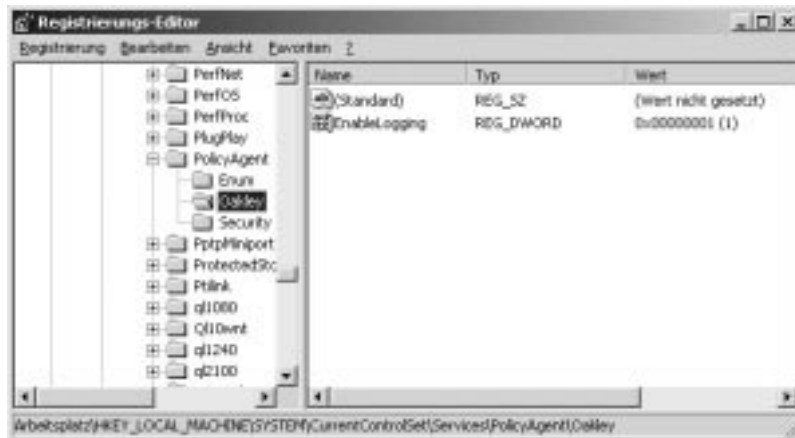
¹⁰⁸ Diesen Hinweis verdanke ich Christian Franzen (mail@christian.franzen.org), der gerade seine Diplomarbeit zum Thema „VPN Interoperability“ verfaßt.

3.3.4.3 Troubleshooting

Der von *Microsoft* selbst immer wieder zum IPsec-Troubleshooting in's Spiel gebrachte *ipsecom* erweist sich als wenig hilfreich, weil damit die Verhandlungsphase selbst nicht weiter beleuchtet werden kann.

Überprüfen Sie zunächst die Übereinstimmung aller wichtigen Parameter mit der Gegenstelle und die Gültigkeit der Zertifikate (Datum!).

Des Weiteren kann ein dediziertes IPsec-Logging aktiviert werden, indem in der Registry unter *HKLM – SYSTEM – CurrentControlSet – Services – PolicyAgent* ein *Schlüssel hinzugefügt* (mithilfe des *regedt32*) wird mit dem Namen *Oakley*, der einen Wert namens *EnableLogging* (ein *REG_DWORD* mit Wert 1) enthält.



Nach einem Neustart des *IPSEC-Richtlinienagenten* (unter *Verwaltung – Dienste*) wird ein umfangreiches Logfile (*oakley.log*) unter *%Systemroot%\Debug* angelegt, das den Verlauf der Aushandlungsphase genauer dokumentiert und Hinweise auf Gründe des Nichtzustandekommens einer IPsec-Verbindung liefern kann. Vergleichen Sie dieses Logfile ggf. mit dem Debug-Output des *Cisco* (bei synchroner Systemzeit der beiden!).

3.3.4 Konfiguration von L2TP

Die Konfiguration von L2TP gestaltet sich dann vergleichsweise simpel. Richten Sie ein Dial-Interface der Variante „Verbindung mit einem privaten Netzwerk über das Internet herstellen“ ein. Auf die Anfangsverbindung sollten Sie verzichten und die Provider-Anwahl manuell durchführen (wg. Verzögerung durch den IKE, s.u.), als Zielsystem der Router (hier: 195.145.236.253) eingetragen

Die *Netzwerk-Eigenschaften* dieser Verbindung werden wie folgt konfiguriert:



Außerdem **muß** noch die von L2TP unter Win2K sonst immer angelegte L2TP-Policy¹⁰⁹ **deaktiviert** werden, weil sie nur einfaches DES verwendet. Fügen Sie dazu in der Registry unter *HKLM\SYSTEM\CurrentControlSet\Services\Rasman\Parameters* den Wert *ProhibitIPsec* hinzu (*REG_DWORD*, auf 1 setzen)¹¹⁰.

¹⁰⁹ Siehe Q248750.

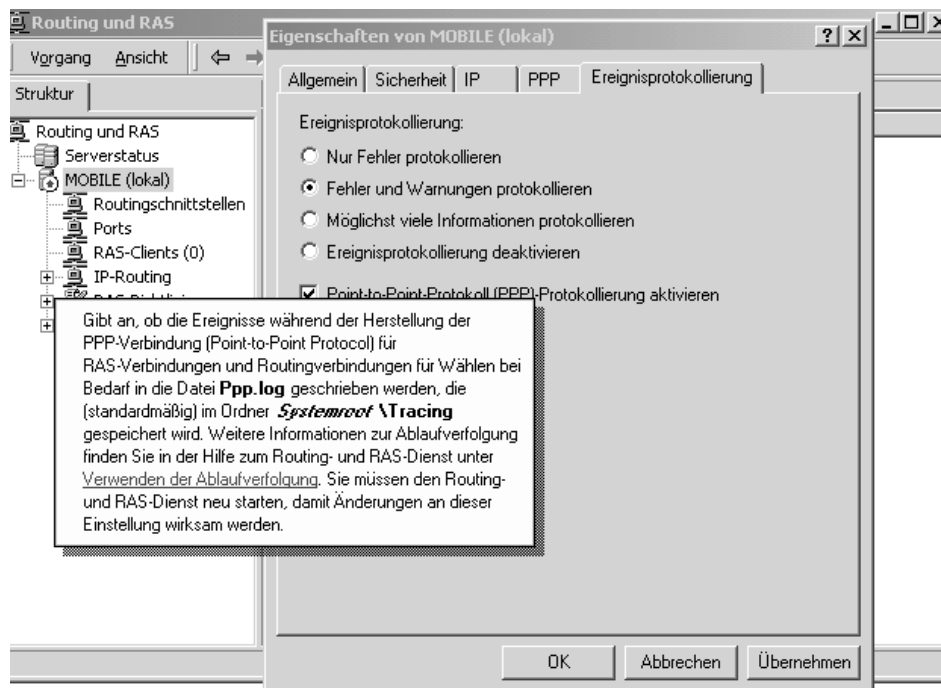
¹¹⁰ Siehe Q258261. Reboot erforderlich...

Unter Umständen ist auch eine Konfiguration des PPP-Authentifizierungsprotokolls & der Adresse des virtuellen Interfaces notwendig (im Beispiel nicht, weil MS-CHAP und Bezug der IP-Parameter durch den Server [beides gehört zu den Default-Einstellungen] verwendet werden).

Der zur Anwahl verwendete Benutzername („erey“ mit Kennwort „1cisco-Router!“) muß natürlich durch den Router authentifiziert werden können, sei es lokal (das ist hier der Fall) oder per RADIUS¹¹¹.

3.3.4.1 Troubleshooting

Um evtl. PPP-Problemen auf die Spur zu kommen, empfiehlt sich, die L2TP-Schnittstelle vorübergehend als Demand-Dial-Interface („Schnittstelle für Wählen bei Bedarf“) im RRAS („Manuell konfigurierter Server“) hinzuzufügen. Bei aktiviertem PPP-Logging:



wird bei manuellem Aktivieren des Demand-Dial-Interfaces („Verbinden“) unter %Systemroot%Tracing eine Log-Datei (PPP.LOG) angelegt, die detailliert Auskunft über eventuelle PPP-Probleme gibt.

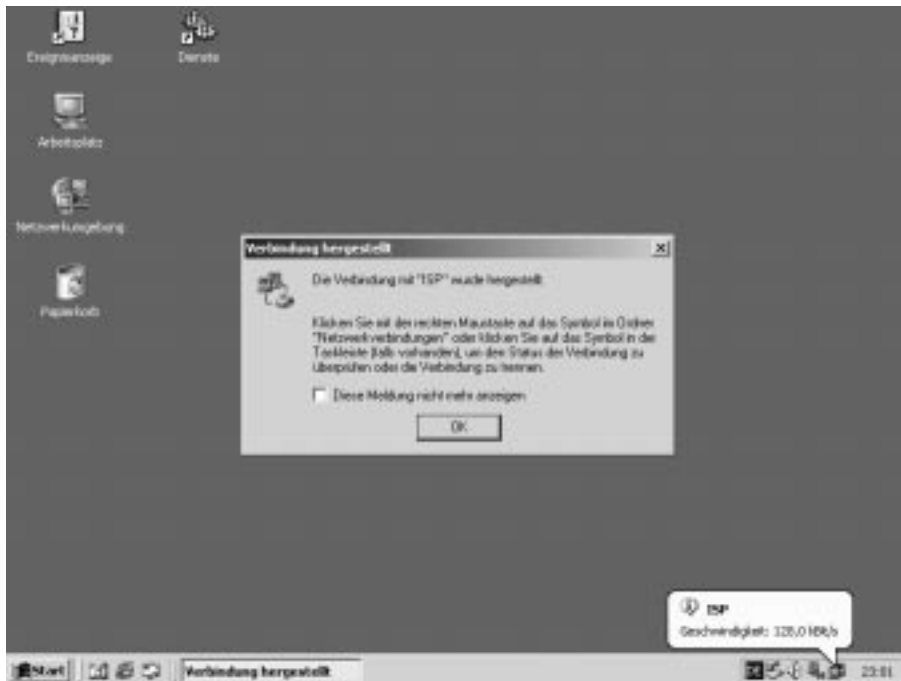
Vergessen Sie nicht, den RRAS anschließend wieder zu deaktivieren...

Wenn Sie die Vermutung haben, IPsec sei für das Nichtzustandekommen einer L2TP-Verbindung verantwortlich, kann L2TP auch ohne IPsec ausgeführt werden (die L2TP Default-Policy ist ja deaktiviert). Beachten Sie, daß dabei notwendiger Authentifizierungsverkehr unverschlüsselt über's Kabel läuft!

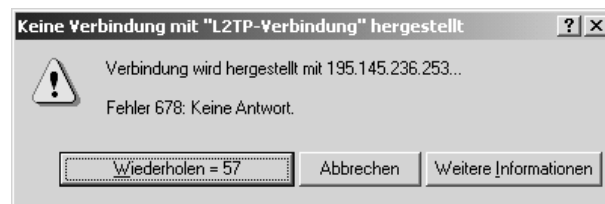
¹¹¹ Meinetwegen auch über TACACS+, das ich wegen geringerer OS-Unterstützung und vor allem seit der kritischen Analyse durch *Solar Designer* (www.openwall.com/advisories/OW-001-tac_plus.txt) nicht gerne einsetze.

4. Das Ergebnis

Nach manueller Provider-Einwahl ...



wird ein erster Verbindungsaufbau mit L2TP versucht, der aber wg. der Dauer des IKE in einen Timeout läuft¹¹²:



Ein erneuter Aufbau (**nicht** „Wiederholen“!, sondern über *Start – Einstellungen – ...*) führt jedoch zu:



¹¹² Hier ist, wie man sieht, noch etwas Feintuning erforderlich...

Ein Blick auf die IP-Parameter zeigt:

```
C:\> netstat -rn

Routingstabelle
=====
Schnittstellenliste
0x1 ..... MS TCP Loopback interface
0x1000003 ...00 d0 59 0d 46 5c ..... Intel 8255x-based Integrated Fast Ethernet
0x10000004 ...00 53 45 00 00 00 ..... WAN (PPP/SLIP) Interface
0x11000005 ...00 53 45 00 00 00 ..... WAN (PPP/SLIP) Interface
=====
Aktive Routen:
  Netzwerkziel   Netzwerkmaske   Gateway   Schnittstelle   Anzahl
  0.0.0.0        0.0.0.0         192.168.97.1  192.168.97.1    1
  0.0.0.0        0.0.0.0         212.120.33.205 212.120.33.205 2
  127.0.0.0      255.0.0.0       127.0.0.1     127.0.0.1       1
  192.168.97.1   255.255.255.255 127.0.0.1     127.0.0.1       1
  192.168.97.255 255.255.255.255 192.168.97.1  192.168.97.1   1
  194.121.133.6  255.255.255.255 212.120.33.205 212.120.33.205 1
  195.145.236.253 255.255.255.255 212.120.33.205 212.120.33.205 1
  195.145.236.253 255.255.255.255 192.168.97.1  192.168.97.1   1
  212.120.33.205 255.255.255.255 127.0.0.1     127.0.0.1       1
  212.120.33.255 255.255.255.255 212.120.33.205 212.120.33.205 1
  224.0.0.0      224.0.0.0       192.168.97.1  192.168.97.1   1
  224.0.0.0      224.0.0.0       212.120.33.205 212.120.33.205 1
  255.255.255.255 255.255.255.255 192.168.97.1  192.168.97.1   1
Standardgateway: 192.168.97.1
=====
Ständige Routen:
Keine
```

und Verbindungen in's interne Netz sind problemlos möglich:

```
C:\> ipconfig

Windows 2000-IP-Konfiguration

Ethernetadapter "LAN-Verbindung":

    Medienstatus. . . . . : Kabel nicht angeschlossen

PPP-Adapter "ISP":

    Verbindungsspezifisches DNS-Suffix:
    IP-Adresse. . . . . : 212.120.33.205
    Subnetzmaske. . . . . : 255.255.255.255
    Standardgateway . . . . . : 212.120.33.205

PPP-Adapter "@":

    Verbindungsspezifisches DNS-Suffix:
    IP-Adresse. . . . . : 192.168.97.1
    Subnetzmaske. . . . . : 255.255.255.255
    Standardgateway . . . . . : 192.168.97.1

C:\> net use y: \\192.168.96.11\service
Der Befehl wurde erfolgreich ausgeführt.

C:\> _
```

Unser Client befindet sich also virtuell im LAN (physikalisch weit entfernt davon...); die Verbindung ist mit 3DES verschlüsselt und mehrfach authentifiziert (Rechner-basiert per Zertifikat und User-basiert via PPP-Login). Und alles mithilfe von Standards und ohne kostenintensive, proprietäre Zusätze!

5. Zum Schluß

5.1 nochmals die wichtigsten Tips zur Vermeidung von Fehlern bei der Implementierung:

- 1.) Sorgen Sie für eine synchrone Zeit aller beteiligten Komponenten¹¹³. Zertifikate enthalten ein Zeitfenster, das ihre Gültigkeit definiert. Ist die Zeit eines Systems vor oder nach dieser Periode, werden Zertifikate als ungültig zurückgewiesen¹¹⁴.
- 2.) Vermeiden Sie bei der Benennung & Konfiguration der CA auf alle Sonderzeichen!
- 3.) Verwenden Sie für das eigene Schlüsselpaar der CA keine Schlüssellänge > 2048 Bit!
- 4.) Achten Sie auf die exakte Formulierung der *crypto access-lists*.
- 5.) Umgehen Sie Q276360.
- 6.) Vergeben Sie auf keinen Fall bei den *Sitzungsschlüsseleinstellungen* auf dem Windows-Client eine KB-basierte Lifetime.
- 7.) Und nochmals: Achten Sie auf eine synchrone Zeit aller Komponenten (Datum, Uhrzeit, Zeitzone)!

5.2 Danksagungen

Michael Thumann (mthumann@security-academy.de, webmaster@ids-guide.de) für sein stets offenes Ohr und allen sonst von mir per Mail genervten IPsec-Interessierten (siehe Fußnoten), insbesondere Christian Franzen und Ben Nagy.

5.3 Ceterum censeo

... daß auf Border-Routern, wann immer möglich¹¹⁵, *Network Ingress Filtering* gemäß RFC 2827 implementiert werden sollte. Wenn alle das täten, wäre die IT-Landschaft ein klein wenig sicherer (nämlich gegen Angriffe mit gespoofen Adressen, z.B. Denial-of-Service Attacken).

5.4 Literatur:

Carlson, James: PPP Design, Implementation and Debugging. Second Edition, Boston 2000 (Addison-Wesley Pearson Education, ISBN 0201700530). [Ausführliche, technische Darstellung von PPP mit gutem Debugging-Kapitel. Gehört in den Bücherschrank jeden WAN-Admins.]

Shea, Richard: L2TP Implementation and Operation, Reading/Massachusetts 1999 (Addison-Wesley Longman, ISBN 0201604485). [Das wohl einzige dedizierte L2TP-Buch. Gut & umfangreich, für unsere Zwecke hier aber nicht zwingend notwendig, da eher für Entwickler & Netzwerk-Designer gedacht.]

Tiller, James S.: A Technical Guide to IPsec Virtual Private Networks, Boca Raton 2001 (Auerbach Publications, ISBN 0849308763). [Das **beste** Praktiker-Buch zu IPsec, das ich kenne! Anschaffung dringend empfohlen.]

5.5 Disclaimer

Alle im Dokument genannten Produkte sind Warenzeichen der jeweiligen Hersteller.

Ich übernehme keinerlei Haftung oder Garantie für das Gelingen der beschriebenen Implementierung oder Folgen derselben oder eines Fehlschlags. Halt einfach keine Gewährleistung irgendeiner Art.

Über Berichtungen, Hinweise, Kommentare, Feedback gleich welcher Art bin ich immer erfreut.

5.6. OpenContent License

Das Papier steht unter der OpenContent License (www.opencontent.org/opl.shtml) und kann entsprechend verteilt, ergänzt, zitiert, etc. werden.

¹¹³ Das gilt überhaupt für viele Authentifizierungsverfahren. Auch bei Kerberos oder SecurID ist eine synchrone Zeit elementar.

¹¹⁴ Ich mußte einen meiner Testrouter gelegentlich ausschalten (wg. eines noch zu untersuchenden Log-Überlaufs an der Konsole, der weiteren Zugriff unmöglich machte). Machmal vergaß ich danach ein erneutes „clock set“... und wunderte mich dann über fehlgeschlagene Authentifizierungsvorgänge.

¹¹⁵ D.h. eigentlich immer, solange nicht asymmetrisch geroutet wird. Und selbst dann, falls die Security Policy der Vermeidung von gespoofen Adressen aus dem eigenen Netz eine höhere Priorität als permanenter Verfügbarkeit einräumen würde...

Anhang A: die komplette Konfig¹¹⁶

```
!  
! Last configuration change at 01:18:53 berlin Tue Apr 17 2001  
! NVRAM config last updated at 23:32:06 berlin Mon Apr 16 2001 by erey  
!  
version 12.1  
no service single-slot-reload-enable  
service timestamps debug datetime  
service timestamps log datetime  
service password-encryption  
!  
hostname ipsec-gw  
!  
logging rate-limit console 10 except errors  
aaa new-model  
aaa authentication login default local  
aaa authentication enable default enable  
aaa authentication ppp default local  
aaa authentication ppp vpdn local  
enable secret 5 $l$4E0k$0V.3Sb51yigwkCyLJ88Vh1  
!  
username erey password 7 1354141B180F0B67192B3D27303052  
clock timezone berlin 1  
clock summer-time berlin recurring  
ip subnet-zero  
!  
!  
no ip finger  
ip domain-name security-academy.de  
ip name-server 192.168.96.23  
!  
ip audit notify log  
ip audit po max-events 100  
ip ssh time-out 120  
ip ssh authentication-retries 3  
vpdn enable  
no vpdn logging  
!  
vpdn-group 1  
! Default L2TP VPDN group  
  accept-dialin  
  protocol l2tp  
  virtual-template 1  
  local name lns  
  lcp renegotiation on-mismatch  
  no l2tp tunnel authentication  
!  
!  
crypto ca identity internalca  
  enrollment mode ra  
  enrollment url http://internalca.security-academy.de:80/certsrv/mscep/mscep.dll  
  crl optional  
crypto ca certificate chain internalca  
certificate 614CFCAD00000000000E  
  308205C6 308204AE A0030201 02020A61 4CFCAD00 00000000 0E300D06 092A8648  
  86F70D01 01050500 30819F31 27302506 092A8648 86F70D01 09011618 65726579  
  40736563 75726974 792D6163 6164656D 792E6465 310B3009 06035504 06130244  
  45310F30 0D060355 04081306 42612D57 75653113 30110603 55040713 0A486569  
  64656C62 65726731 19301706 0355040A 13105365 63757269 74792041 63616465  
  6D793110 300E0603 55040B13 074F7267 612F4954 31143012 06035504 03130B49  
  6E746572 6E616C20 4341301E 170D3031 30343134 32333535 31325A17 0D303230  
  34313530 30303531 325A304D 311E301C 06092A86 4886F70D 01090813 0F313935  
  2E313435 2E323336 2E323533 312B3029 06092A86 4886F70D 01090213 1C697073  
  65632D67 772E7365 63757269 74792D61 63616465 6D792E64 6530819F 300D0609
```

¹¹⁶ Berücksichtigen Sie dabei, daß auf fast alle für das Szenario nicht zwingend notwendigen Kommandos verzichtet wurde. Wir verwenden normalerweise vorgefertigte Konfigs, die eine Reihe von sicherheits-relevanten Einstellungen vornehmen [Deaktivierung von Funktionalitäten, sichere Konfiguration von Interfaces, Logging, NTP usw. In etwa das, was in www.cisco.com/warp/public/707/21.html und *Phrack 55-10* (www.insecure.org/news/P55-10.txt) beschrieben ist]. Dies alles ist hier nicht enthalten, um Ihnen ein eventuelles Troubleshooting durch Vergleich mit der funktionierenden Konfiguration zu erleichtern.

2A864886 F70D0101 01050003 818D0030 81890281 8100A7BC B7853068 01F989C3
F60D01E1 1B365A76 9CEC5146 C99046B6 56A35D5C 629D801B 28A18D4A 7939DA44
59BDD779 51694D1A CF3B3E22 A703A53B 05A78154 C2CAF692 F41A6412 C22B47F0
4D1ED6D2 7840FA73 2E8B394E A0A3BBFE 77C6531A ED02F6E4 57BD36CC 6EB0F8E1
3EODACCA 74734FA8 34B6EB54 8114C77A 90D42576 922B0203 010001A3 8202D730
8202D330 0B060355 1D0F0404 030205A0 301D0603 551D0E04 16041403 3801CD6C
B5270550 35ACBFD9 7BC9D41A CC1A9830 81DB0603 551D2304 81D33081 D080148A
ABC7B542 19CEB227 71DA2014 28124712 79D01EA1 81A5A481 A230819F 31273025
06092A86 4886F70D 01090116 18657265 79407365 63757269 74792D61 63616465
6D792E64 65310B30 09060355 04061302 4445310F 300D0603 55040813 0642612D
57756531 13301106 03550407 130A4865 6964656C 62657267 31193017 06035504
0A131053 65637572 69747920 41636164 656D7931 10300E06 0355040B 13074F72
67612F49 54311430 12060355 0403130B 496E7465 726E616C 20434182 103BDE4E
676A416D AA42980A 675AC0C2 D8303006 03551D11 0101FF04 26302482 1C697073
65632D67 772E7365 63757269 74792D61 63616465 6D792E64 658704C3 91ECFD30
81A10603 551D1F04 81993081 963048A0 46A04486 42687474 703A2F2F 696E7465
726E616C 63612E73 65637572 6974792D 61636164 656D792E 64652F43 65727445
6E726F6C 6C2F496E 7465726E 616C2532 3043412E 63726C30 4AA048A0 46864466
696C653A 2F2F5C5C 696E7465 726E616C 63612E73 65637572 6974792D 61636164
656D792E 64655C43 65727445 6E726F6C 6C5C496E 7465726E 616C2532 3043412E
63726C30 81F00608 2B060105 05070101 0481E330 81E0306D 06082B06 01050507
30028661 68747470 3A2F2F69 6E746572 6E616C63 612E7365 63757269 74792D61
63616465 6D792E64 652F4365 7274456E 726F6C6C 2F696E74 65726E61 6C63612E
73656375 72697479 2D616361 64656D79 2E64655F 496E7465 726E616C 25323043
412E6372 74306F06 082B0601 05050730 02866366 696C653A 2F2F5C5C 696E7465
726E616C 63612E73 65637572 6974792D 61636164 656D792E 64655C43 65727445
6E726F6C 6C5C696E 7465726E 616C6361 2E736563 75726974 792D6163 6164656D
792E6465 5F496E74 65726E61 6C253230 43412E63 7274300D 06092A86 4886F70D
01010505 00038201 01005336 2DBBE8CC A157BE3C 97DD5C90 E7BC6416 36876518
276AD913 5261F475 D914958A CB0E42F8 DDEDED527 C0EEC6E9 F9C1CE38 CD3D7A32
CE9F1F27 979508F6 7EA390F6 915FA0E9 AB3000D5 1F738A0A B12A7851 0C40839A
61719C37 AB50E0A6 F15ECA02 9D899D89 87879FB0 BC3DE19B 1DEB09F7 51949D8F
AA6A917E 2A5BC0AD B5CA29E6 1E5BC579 59A97702 4613F48D 7480927E ACE441C2
195B5B3A 05593EF0 774212E3 95180F4A 94CB4C7A 5BB97514 EA61F086 3E8A4713
E1A2B640 0D964416 74855FD0 D0C56E07 45B2DC74 35672DC7 02331B4A DF74720E
BBDEBFBF A6D17BE8 5935FA51 FDD606AC 415DD368 8DD3BF9D 146D2EA3 F28D6218
BA3B4753 0F2856FA 5EA7

quit

certificate ra-sign 612F8A2A000000000009

308205F4 308204DC A0030201 02020A61 2F8A2A00 00000000 09300D06 092A8648
86F70D01 01050500 30819F31 27302506 092A8648 86F70D01 09011618 65726579
40736563 75726974 792D6163 6164656D 792E6465 310B3009 06035504 06130244
45310F30 0D060355 04081306 42612D57 75653113 30110603 55040713 0A486569
64656C62 65726731 19301706 0355040A 13105365 63757269 74792041 63616465
6D793110 300E0603 55040B13 074F7267 612F4954 31143012 06035504 03130B49
6E746572 6E616C20 4341301E 170D3031 30343134 32323239 30345A17 0D303230
34313432 32333930 345A3081 92312730 2506092A 864886F7 0D010901 16186572
65794073 65637572 6974792D 61636164 656D792E 6465310B 30090603 55040613
02444531 0F300D06 03550408 13064261 2D577565 31133011 06035504 07130A48
65696465 6C626572 67310F30 0D060355 040A1306 53656341 63613110 300E0603
55040B13 074F7267 612F4954 3111300F 06035504 03130845 6E6E6F20 52657930
819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100 C7517034
8CF3CCA0 DEBAEC24 9BF94CEE EB18E278 5E3F3599 597611C2 BADA2C97 270D052E
CFE472CD 6AFBF891 E1F3016E E0B53119 761838CE 2F62FB6A A5799B0D 36209B5F
DD6EC145 5F8F2699 C3BAEF72 4ABE8783 0A210B17 863AE557 B7C3F723 6609DFC0
14BE65BC 8861F11D E2855756 9CC57015 005FFF05 9D5AF166 DE432869 02030100
01A38202 BF308202 BB300E06 03551D0F 0101FF04 04030206 C0301506 03551D25
040E300C 060A2B06 01040182 37140201 301D0603 551D0E04 16041436 ACAD66BF
A01F1E60 C282F6EA 27A65E3F F2A22630 81DB0603 551D2304 81D33081 D080148A
ABC7B542 19CEB227 71DA2014 28124712 79D01EA1 81A5A481 A230819F 31273025
06092A86 4886F70D 01090116 18657265 79407365 63757269 74792D61 63616465
6D792E64 65310B30 09060355 04061302 4445310F 300D0603 55040813 0642612D
57756531 13301106 03550407 130A4865 6964656C 62657267 31193017 06035504
0A131053 65637572 69747920 41636164 656D7931 10300E06 0355040B 13074F72
67612F49 54311430 12060355 0403130B 496E7465 726E616C 20434182 103BDE4E
676A416D AA42980A 675AC0C2 D83081A1 0603551D 1F048199 30819630 48A046A0
44864268 7474703A 2F2F696E 7465726E 616C6361 2E736563 75726974 792D6163
6164656D 792E6465 2F436572 74456E72 6F6C6C2F 496E7465 726E616C 25323043
412E6372 6C304AA0 48A04686 4466696C 653A2F2F 5C5C696E 7465726E 616C6361
2E736563 75726974 792D6163 6164656D 792E6465 5C436572 74456E72 6F6C6C5C
496E7465 726E616C 25323043 412E6372 6C3081F0 06082B06 01050507 01010481
E33081E0 306D0608 2B060105 05073002 86616874 74703A2F 2F696E74 65726E61
6C63612E 73656375 72697479 2D616361 64656D79 2E64652F 43657274 456E726F

6C6C2F69 6E746572 6E616C63 612E7365 63757269 74792D61 63616465 6D792E64
655F496E 7465726E 616C2532 3043412E 63727430 6F06082B 06010505 07300286
6366696C 653A2F2F 5C5C696E 7465726E 616C6361 2E736563 75726974 792D6163
6164656D 792E6465 5C436572 74456E72 6F6C6C5C 696E7465 726E616C 63612E73
65637572 6974792D 61636164 656D792E 64655F49 6E746572 6E616C25 32304341
2E637274 300D0609 2A864886 F70D0101 05050003 82010100 781DB545 72E01B4C
1F44F584 522BCEF0 2965FAF2 E5BA33A9 3D1AED76 7E4C787B 4162DC28 C0CA6DE9
B8D39CA3 EBA3D620 68B8E22E 17959F65 3A239ECD C8C3119A 490E380D D713101E
773FCFAE 4C7BFD8D F20A0983 9C75E43C F9BF4867 F712FD22 D4F2BCCE 5A5C2735
E7CF5B81 76F5904D DABDCB59 986D1F6C 8890CAA5 C0508DDE C9F69F22 4030E4B5
0B4395ED 8955BB5D 3BF1FCB0 6FDF36BD 4E3F10F0 7A3CC247 C1600310 7ED3DAF8
CE7A82DE C57B2E69 B2872082 B36259A5 22EDA53C 2F3BFCEB C3442B53 ADF79C60
09A85E68 88BA3AEB D73A489A 711E1515 7797D5FA EAF37815 B3237BA0 CA91195B
7091666E C89586A0 99FDBB5D 464B73F1 4F3323D7 00457A0F

quit

certificate ca 3BDE4E676A416DAA42980A675AC0C2D8

308204C1 308203A9 A0030201 0202103B DE4E676A 416DAA42 980A675A C0C2D830
0D06092A 864886F7 0D010105 05003081 9F312730 2506092A 864886F7 0D010901
16186572 65794073 65637572 6974792D 61636164 656D792E 6465310B 30090603
55040613 02444531 0F300D06 03550408 13064261 2D577565 31133011 06035504
07130A48 65696465 6C626572 67311930 17060355 040A1310 53656375 72697479
20416361 64656D79 3110300E 06035504 0B13074F 7267612F 49543114 30120603
55040313 0B496E74 65726E61 6C204341 301E170D 30313032 31353135 30343134
5A170D30 33303231 35313531 3330385A 30819F31 27302506 092A8648 86F70D01
09011618 65726579 40736563 75726974 792D6163 6164656D 792E6465 310B3009
06035504 06130244 45310F30 0D060355 04081306 42612D57 75653113 30110603
55040713 0A486569 64656C62 65726731 19301706 0355040A 13105365 63757269
74792041 63616465 6D793110 300E0603 55040B13 074F7267 612F4954 31143012
06035504 03130B49 6E746572 6E616C20 43413082 0122300D 06092A86 4886F70D
01010105 00038201 0F003082 010A0282 010100D0 7169DC76 1F5AFB19 ECB7EB8F
CDC7286F 47447ECE 812336FA FD62E8B2 87B2944C DCBB0EC3 C4A0D27E 49258489
993B48DD 042F61FB A87BF24D 6F93C15D 3DDA101C 458642D3 89928EDC FD9479EA
F436FCC0 0E2ABFD9 952E9EF8 8437415F 500DE0A8 50D1483B DCF A2104 24D9B148
4AD9D40C 98A769EA B191917D 113C9ACB 95EF6AC4 6E021C26 EB4BFCDC 957D1177
C65F9576 40244FFF F6F81332 DEADE1AD 4B8CCB78 396F1CD8 DA5F04BA E312D10A
50760EA0 B20866A0 0FB6231 EC625BA8 5825FED6 666134C3 56C73BF0 E54057E2
CBC713A3 4BAFE58D CF09B28A E519C395 7C6755F2 71509C31 2B4CF439 5E7662BB
DBEB0730 B4E0DD64 5E9AFE7B E6E01354 FC205F02 03010001 A381F630 81F3300B
0603551D 0F040403 0201C630 0F060355 1D130101 FF040530 030101FF 301D0603
551D0E04 1604148A ABC7B542 19CEB227 71DA2014 28124712 79D01E30 81A10603
551D1F04 81993081 963048A0 46A04486 42687474 703A2F2F 696E7465 726E616C
63612E73 65637572 6974792D 61636164 656D792E 64652F43 65727445 6E726F6C
6C2F496E 7465726E 616C2532 3043412E 63726C30 4AA048A0 46864466 696C653A
2F2F5C5C 696E7465 726E616C 63612E73 65637572 6974792D 61636164 656D792E
64655C43 65727445 6E726F6C 6C5C496E 7465726E 616C2532 3043412E 63726C30
1006092B 06010401 82371501 04030201 00300D06 092A8648 86F70D01 01050500
03820101 0051799F 03123381 C664F3BF 17D7697D 85EA83E4 7C822145 78258F60
BEE3F60E B827633F 1D93D5D4 B768F8CC 3B403BDB 108C9DE0 323E56E6 C3A46A29
8ACBA3F5 02896365 9BDEAD7F 44EF4C9D DEFA0F48 B2C92CBB C4269E26 A876B453
5CAE1760 FBF73515 25DFCE73 DE29522D E650AAB7 779C0219 61F329DC 4ECEB986
C6805F31 F735B509 0E59CD0F D9FCC703 4DDC608F 23788886 7D371B0E 1C2796B2
E554D938 EAC0334A 98D828AA 86705846 C518E724 64EAACA0 54B8CFB3 82D54D8F
5E03E5F6 B58B275F E90E81E5 16CA96F8 BB806495 C2ECA536 ACC10344 ECC2D27A
E14038CC 42FCF125 BF8CB99A EB EA5186 DEC3BFB6 53E64611 76A69C87 684AE050
6EE0F235 C3

quit

certificate ra-encrypt 612F8EED00000000000A

308205F4 308204DC A0030201 02020A61 2F8EED00 00000000 0A300D06 092A8648
86F70D01 01050500 30819F31 27302506 092A8648 86F70D01 09011618 65726579
40736563 75726974 792D6163 6164656D 792E6465 310B3009 06035504 06130244
45310F30 0D060355 04081306 42612D57 75653113 30110603 55040713 0A486569
64656C62 65726731 19301706 0355040A 13105365 63757269 74792041 63616465
6D793110 300E0603 55040B13 074F7267 612F4954 31143012 06035504 03130B49
6E746572 6E616C20 4341301E 170D3031 30343134 32323239 30355A17 0D303230
34313432 32333930 355A3081 92312730 2506092A 864886F7 0D010901 16186572
65794073 65637572 6974792D 61636164 656D792E 6465310B 30090603 55040613
02444531 0F300D06 03550408 13064261 2D577565 31133011 06035504 07130A48
65696465 6C626572 67310F30 0D060355 040A1306 53656341 63613110 300E0603
55040B13 074F7267 612F4954 3111300F 06035504 03130845 6E6E6F20 52657930
819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100 C2546946
B084AC11 4E1FA370 4F94F36B E8C8EDF8 E3937194 01ADBF45 115DC411 153F222A
59AE1CEB F5F3589C 49D9FC01 DDB59130 0C2FCC09 220D2D92 F32BF705 82B0931E
FD987FF9 467CFF63 469A01E6 9C3224E3 40D2629D 638E1BD8 AA795FBC 5EE28C12

```

C6A77AD1 41FBBC68 CC20A613 7A269E3B 67C55EF8 AF4B2159 E0CE350D 02030100
01A38202 BF308202 BB300E06 03551D0F 0101FF04 04030204 30301506 03551D25
040E300C 060A2B06 01040182 37140201 301D0603 551D0E04 16041402 EF628FF6
9F20D3CD D8141E45 7237F95E 3ADE5530 81DB0603 551D2304 81D33081 D080148A
ABC7B542 19CEB227 71DA2014 28124712 79D01EA1 81A5A481 A230819F 31273025
06092A86 4886F70D 01090116 18657265 79407365 63757269 74792D61 63616465
6D792E64 65310B30 09060355 04061302 4445310F 300D0603 55040813 0642612D
57756531 13301106 03550407 130A4865 6964656C 62657267 31193017 06035504
0A131053 65637572 69747920 41636164 656D7931 10300E06 0355040B 13074F72
67612F49 54311430 12060355 0403130B 496E7465 726E616C 20434182 103BDE4E
676A416D AA42980A 675AC0C2 D83081A1 0603551D 1F048199 30819630 48A046A0
44864268 7474703A 2F2F696E 7465726E 616C6361 2E736563 75726974 792D6163
6164656D 792E6465 2F436572 74456E72 6F6C6C2F 496E7465 726E616C 25323043
412E6372 6C304AA0 48A04686 4466696C 653A2F2F 5C5C696E 7465726E 616C6361
2E736563 75726974 792D6163 6164656D 792E6465 5C436572 74456E72 6F6C6C5C
496E7465 726E616C 25323043 412E6372 6C3081F0 06082B06 01050507 01010481
E33081E0 306D0608 2B060105 05073002 86616874 74703A2F 2F696E74 65726E61
6C63612E 73656375 72697479 2D616361 64656D79 2E64652F 43657274 456E726F
6C6C2F69 6E746572 6E616C63 612E7365 63757269 74792D61 63616465 6D792E64
655F496E 7465726E 616C2532 3043412E 63727430 6F06082B 06010505 07300286
6366696C 653A2F2F 5C5C696E 7465726E 616C6361 2E736563 75726974 792D6163
6164656D 792E6465 5C436572 74456E72 6F6C6C5C 696E7465 726E616C 63612E73
65637572 6974792D 61636164 656D792E 64655F49 6E746572 6E616C25 32304341
2E637274 300D0609 2A864886 F70D0101 05050003 82010100 2607E823 FA0A2B2F
6F7CBE73 01EB78DD 2E3DC53F E6961836 43AD4443 D0590E32 A40B4575 29D93B05
1FE46DB9 A2ED0564 15C14469 2F5DF1C0 4802B3E3 EB5FAF2C 5A0BD926 609D7AE7
A697F77C 80D11F5F F5A242CB 0F3ACB8A 32907C89 9C9B1F3C BF49D451 6D0EA0A8
E2EC302A 6C10F03E 2BCB082B D85D65E5 90AAE212 40910C87 C78C91C6 E97A295B
1EF3E2A8 3CF4315A F23C1EA2 D316141C F2AC7E11 664BC21F 9C08DC98 1BFF593E
D9D9B3BC 4C64BBA5 39A2F794 20859568 81AF36F0 DC99A646 48138339 14EF6A11
31B48EEB A411BD49 A56D2583 70DDF72A 40AF29CF 7EAF0EC5 F765C3A6 46A257E9
722F2D12 210B2C1F EC75AB36 8CE7B2CC 775A3AA1 0CF1E9BF
quit
!
crypto isakmp policy 1
  encr 3des
  group 2
  lifetime 3600
!
!
crypto ipsec transform-set vpn-traffic esp-3des esp-sha-hmac
  mode transport
!
crypto dynamic-map vpn 1
  set transform-set vpn-traffic
  set pfs group2
  match address 101
!
!
crypto map vpn-map 1 ipsec-isakmp dynamic vpn
!
call rsvp-sync
cns event-service server
!
!
!
!
!
!
!
!
interface FastEthernet0/0
  ip address 192.168.96.4 255.255.255.0
  no ip mroute-cache
  speed 100
  full-duplex
!
interface FastEthernet0/1
  ip address 195.145.236.253 255.255.255.248
  no ip mroute-cache
  speed 10
  full-duplex
  crypto map vpn-map

```

```
!  
interface Virtual-Templat1  
  ip unnumbered FastEthernet0/1  
  peer default ip address pool default  
  ppp authentication ms-chap  
!  
ip local pool default 192.168.97.1 192.168.97.255  
ip kerberos source-interface any  
ip classless  
ip route 0.0.0.0 0.0.0.0 195.145.236.249  
no ip http server  
!  
access-list 101 deny  udp any any eq isakmp  
access-list 101 permit udp any host 195.145.236.253  
!  
!  
dial-peer cor custom  
!  
!  
!  
!  
line con 0  
  transport input none  
line aux 0  
line vty 0 4  
  transport input ssh  
!  
end
```

Anhang B: Debug-Output¹¹⁷

```
ipsec-gw#
Apr 16 23:08:40: ISAKMP (0:0): received packet from 212.120.33.205 (N) NEW SA
Apr 16 23:08:49: ISAKMP: local port 500, remote port 500
Apr 16 23:08:49: ISAKMP (0:2): processing SA payload. message ID = 0
Apr 16 23:08:49: ISAKMP (0:2): Checking ISAKMP transform 1 against priority 1 policy
Apr 16 23:08:49: ISAKMP: encryption 3DES-CBC
Apr 16 23:08:49: ISAKMP: hash SHA
Apr 16 23:08:49: ISAKMP: default group 2
Apr 16 23:08:49: ISAKMP: auth RSA sig
Apr 16 23:08:49: ISAKMP: life type in seconds
Apr 16 23:08:49: ISAKMP: life duration (VPI) of 0x0 0x0 0xE 0x10
Apr 16 23:08:49: ISAKMP (0:2): atts are acceptable. Next payload is 0
Apr 16 23:08:49: ISAKMP (0:2): processing vendor id payload
Apr 16 23:08:49: ISAKMP (0:2): SA is doing RSA signature authentication using id type ID_IPV4_ADDR
Apr 16 23:08:49: ISAKMP (0:2): sending packet to 212.120.33.205 (R) MM_SA_SETUP
Apr 16 23:08:49: ISAKMP (0:0): received packet from 212.120.33.205 (N) NEW SA
Apr 16 23:08:58: ISAKMP: local port 500, remote port 500
Apr 16 23:08:58: ISAKMP (0:0): received packet from 212.120.33.205 (N) NEW SA
Apr 16 23:09:07: ISAKMP: local port 500, remote port 500
Apr 16 23:09:07: ISAKMP (0:0): received packet from 212.120.33.205 (N) NEW SA
Apr 16 23:09:16: ISAKMP: local port 500, remote port 500
Apr 16 23:09:16: ISAKMP (0:2): received packet from 212.120.33.205 (R) MM_SA_SETUP
Apr 16 23:09:16: ISAKMP (0:2): processing KE payload. message ID = 0
Apr 16 23:09:16: ISAKMP (0:2): processing NONCE payload. message ID = 0
Apr 16 23:09:16: ISAKMP (0:2): SKEYID state generated
Apr 16 23:09:16: ISAKMP (0:2): sending packet to 212.120.33.205 (R) MM_KEY_EXCH
Apr 16 23:09:16: ISAKMP (0:2): received packet from 212.120.33.205 (R) MM_KEY_EXCH
Apr 16 23:09:16: ISAKMP (0:2): phase 1 packet is a duplicate of a previous packet.
Apr 16 23:09:16: ISAKMP (0:2): retransmission skipped for phase 1 (time since last transmission 4)
Apr 16 23:09:16: ISAKMP (0:2): received packet from 212.120.33.205 (R) MM_KEY_EXCH
Apr 16 23:09:16: ISAKMP (0:2): phase 1 packet is a duplicate of a previous packet.
Apr 16 23:09:16: ISAKMP (0:2): retransmission skipped for phase 1 (time since last transmission 4)
Apr 16 23:09:16: ISAKMP (0:2): received packet from 212.120.33.205 (R) MM_KEY_EXCH
Apr 16 23:09:16: ISAKMP (0:2): phase 1 packet is a duplicate of a previous packet.
Apr 16 23:09:16: ISAKMP (0:2): retransmission skipped for phase 1 (time since last transmission 4)
Apr 16 23:09:16: ISAKMP (0:2): received packet from 212.120.33.205 (R) MM_KEY_EXCH
Apr 16 23:09:16: ISAKMP (0:2): phase 1 packet is a duplicate of a previous packet.
Apr 16 23:09:16: ISAKMP (0:2): retransmission skipped for phase 1 (time since last transmission 4)
Apr 16 23:09:17: ISAKMP (0:2): received packet from 212.120.33.205 (R) MM_KEY_EXCH
Apr 16 23:09:17: ISAKMP (0:2): processing ID payload. message ID = 0
Apr 16 23:09:17: ISAKMP (0:2): processing CERT payload. message ID = 0
Apr 16 23:09:17: ISAKMP (0:2): processing a CT_X509_SIGNATURE cert
Apr 16 23:09:17: ISAKMP (0:2): cert approved with warning
Apr 16 23:09:17: ISAKMP (0:2): processing SIG payload. message ID = 0
Apr 16 23:09:17: ISAKMP (0:2): processing CERT_REQ payload. message ID = 0
Apr 16 23:09:17: ISAKMP (0:2): peer wants a CT_X509_SIGNATURE cert
Apr 16 23:09:17: ISAKMP (0:2): peer want cert issued by CN = Internal CA, OU = Orga/IT, O = Security Academy, L = Heidelberg, ST = Ba-Wue, C = DE, EA =<16>erey@security-academy.de
Apr 16 23:09:17: ISAKMP (0:2): SA has been authenticated with 212.120.33.205
Apr 16 23:09:17: ISAKMP (2): ID payload
    next-payload : 6
    type          : 1
    protocol      : 17
    port          : 500
    length        : 8
Apr 16 23:09:17: ISAKMP (2): Total payload length: 12
```

¹¹⁷ Ich habe nach einiger Überlegung darauf verzichtet, ihn zu kommentieren. Ich denke, er erläutert sich weitgehend selbst. Sollten Sie Fragen haben oder selbst an einer Stelle in Ihrer Implementierung ‚hängen‘, mailen Sie mir einfach (erey@security-academy.de).

```

Apr 16 23:09:17: ISKAMP: growing send buffer from 1024 to 3072
Apr 16 23:09:17: -Traceback= 6153F060 615476E0 61547A44 6153DA08 61537C3C 615388A4
6039714C 60397138
Apr 16 23:09:18: ISAKMP (0:2): sending packet to 212.120.33.205 (R) QM_IDLE
Apr 16 23:09:18: ISAKMP (0:2): received packet from 212.120.33.205 (R) QM_IDLE
Apr 16 23:09:18: ISAKMP (0:2): phase 1 packet is a duplicate of a previous packet.
Apr 16 23:09:18: ISAKMP (0:2): retransmitting due to retransmit phase 1
Apr 16 23:09:18: ISAKMP (0:2): retransmitting phase 1 QM_IDLE ...
Apr 16 23:09:19: ISAKMP (0:2): received packet from 212.120.33.205 (R) QM_IDLE
Apr 16 23:09:19: ISAKMP (0:2): processing HASH payload. message ID = 1979848979
Apr 16 23:09:19: ISAKMP (0:2): processing SA payload. message ID = 1979848979
Apr 16 23:09:19: ISAKMP (0:2): Checking IPsec proposal 1
Apr 16 23:09:19: ISAKMP: transform 1, ESP_3DES
Apr 16 23:09:19: ISAKMP:   attributes in transform:
Apr 16 23:09:19: ISAKMP:     encaps is 2
Apr 16 23:09:19: ISAKMP:     authenticator is HMAC-SHA
Apr 16 23:09:19: ISAKMP:     group is 2
Apr 16 23:09:19: ISAKMP (0:2): atts are acceptable.
Apr 16 23:09:19: ISAKMP (0:2): processing KE payload. message ID = 1979848979
Apr 16 23:09:19: ISAKMP (0:2): processing NONCE payload. message ID = 1979848979
Apr 16 23:09:19: ISAKMP (0:2): processing ID payload. message ID = 1979848979
Apr 16 23:09:19: ISAKMP (2): ID_IPV4_ADDR src 212.120.33.205 prot 17 port 0
Apr 16 23:09:19: ISAKMP (0:2): processing ID payload. message ID = 1979848979
Apr 16 23:09:19: ISAKMP (2): ID_IPV4_ADDR dst 195.145.236.253 prot 17 port 0
Apr 16 23:09:19: ISAKMP (0:2): asking for 1 spis from ipsec
Apr 16 23:09:19: ISAKMP (0:2): retransmitting phase 1 QM_IDLE ...
Apr 16 23:09:19: ISAKMP (0:2): incrementing error counter on sa: retransmit phase 1
Apr 16 23:09:19: ISAKMP (0:2): no outgoing phase 1 packet to retransmit. QM_IDLE
Apr 16 23:09:19: ISAKMP: received ke message (2/1)
Apr 16 23:09:19: ISAKMP (0:2): sending packet to 212.120.33.205 (R) QM_IDLE
Apr 16 23:09:19: %CRYPTO-4-RECV_PKT_INV_SPI: decaps: rec'd IPSEC packet has invali
lid spi for
    destaddr=195.145.236.253, prot=50, spi=0x843020FD(-2077220611)
Apr 16 23:09:19: ISAKMP (0:2): received packet from 212.120.33.205 (R) QM_IDLE
Apr 16 23:09:19: ISAKMP (0:2): Creating IPsec SAs
Apr 16 23:09:19:   inbound SA from 212.120.33.205 to 195.145.236.253
    (proxy 212.120.33.205 to 195.145.236.253)
Apr 16 23:09:19:   has spi 0x843020FD and conn_id 2006 and flags 21
Apr 16 23:09:19:   outbound SA from 195.145.236.253 to 212.120.33.205 (proxy
195.145.236.253 to 212.120.33.205 )
Apr 16 23:09:19:   has spi 1512938038 and conn_id 2007 and flags 21
Apr 16 23:09:19: ISAKMP (0:2): deleting node 1979848979 error FALSE reason "quick
mode done (await())"
Apr 16 23:10:09: ISAKMP (0:2): purging node 1979848979
Apr 16 23:10:18: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
Apr 16 23:10:22: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1,
changed state to up

```