DAFTAR ISI

DAFTAR ISI **1**
BAB 1 ..... **3**
VPN—Virtual Private Network **3**
Cabang yang dibutuhkan oleh Dedicated Line 3
Broadband Access Internet dan VPN 5
VPN merupakan : 5
Bagaimana VPN bekerja? 6
VPN digunakan untuk apa ? 8
Networking Concepts—Protocols dan Lapisan 9
Tunneling dan Overhead 12
VPN Concepts—Overview 13
Standart tujuan dari Tunneling 13
Implementasi Protocol pada Layer 2 14
Implementasi Protokol Layer 3 15
Implementasi Protokol Pada Layer 4 (Transport) 16
OpenVPN-SSL/TLS-Solusi 17
Ringkasan 17
BAB 2 ..... **18**
VPN SECURITY **18**
VPN Security 18
Privacy – proses enkripsi suatu traffic 19
Symmetric Encryption and Pre-Shared Keys 20
Reliability and Authentication 21
Masalah Kompleksitas Pada VPN Klasik 21
Asymmetric Encryption dengan SSL/TLS 22
SSL/TLS Security 23
Memahami SSL/TLS Certificates 24
Trusted Certificates 25
Self-Signed Certificates 26
SSL/TLS Certificates dan VPNs 28
Ringkasan 29
BAB 3 ..... **30**
OpenVPN **30**
Keuntungan OpenVPN 30
Sejarah OpenVPN 32
OpenVPN Versi1 33
OpenVPN Versi 2 36
Jaringan dengan OpenVPN 37
OpenVPN dan Firewall 39
Mengkonfigurasi OpenVPN 41
Permasalahan dengan OpenVPN 42
Perbandingan OpenVPN dengan IPSec VPN 43
Sumber Bantuan dan Dokumentasi 44
Komunitas Proyek 44
Dokumentasi di dalam Paket Software 45
Ringkasan 46

Bab 4 ..... **47**
Menginstal OpenVPN **47**
Memperoleh Software 48
Instalasi OpenVPN pada Windows 49
Download dan Memulai Instalasi 50
Memilih Komponen dan Lokasi 51
Menyelesaikan Instalasi 53
Uji Instalasi – tampilan pertama Applet 54
Menginstal OpenVPN pada Debian 55
Menginstal Paket-Paket Debian 57
Menggunakan keserasian untuk mencari dan menginstall Paket 60
OpenVPN – File-file terinstall pada Debian 62
Ringkasan 62
BAB 5 ..... **63**
Konfigurasi OpenVPN dengan Tunnel Pertama **63**
OpenVPN pada Microsoft Windows 63
Membangkitkan kunci statistic openVPN 64
Membuat contoh koneksi 66
Mengadopsi Kelengkapan contoh konfogurasi file oleh OpenVPN 68
Memulai dan mengetest Tunnel 71
Perintah pada interface jaringan windows openVPN 73
Menghubungkan windows dengan Linux 74
Merubah file diantara Windows dan Linux 74
Menginstall WinSCP 75
Mentransfer file key dari windows ke linux dengan WinSCP 77
Pitfall kedua –membawa kembali/ tujuan akir pada baris 78
Konfigurasi sistem linux 79
Mengetest Tunnel 81
Melihat pada interface Linux 82
Menjalankan secara otomatis OpenVPN 82
OpenVPN sebagai server Windows 83
OpenVPN sebagai Server pada Linux 83
Menggunakan runlevel dan init untuk merubah dan mengecek Runlevel 84
Kontrol system untuk Runlevel 84
Mengatur Script init 85
Troubleshooting Firewall Issues 87
Menonaktifkan Firewall 87
Ringkasan 89
BAB 6 ..... **90**
Troubleshooting dan Monitoring **90**
Uji konektivitas jaringan 90
Mengecek interface, routing dan koneksi pada server VPN 93
Debugging dengan tcpdump dan IPTraf 97
Menggunakan Protokol OpenVPN dan File Status untuk Debugging 100
Scanning server dengan Nmap 102
Tool monitoring 103
Petunjuk untuk Tool lainnya 105
Ringkasan 106

BAB 1

VPN—Virtual Private Network

Bab ini akan mulai dengan solusi jaringan yang digunakan di masa lalu untuk menghubungkan beberapa cabang dari suatu perusahaan. Kemajuan teknologi seperti jalur lebar Internet akses menyempurnakan berbagai kemungkinan baru dan konsep baru untuk isu ini, salah satunya disebut Virtual Private Network (VPN). Di dalam bab ini, kamu akan belajar tentang peralatan VPN, bagaimana kemajuannya selama akhir dekade, kenapa penting bagi perusahaan modern, dan bagaimana prinsip kerja VPN. Konsep dasar jaringan adalah diperlukan untuk memahami variasi VPN solusi dibahas di dalam bab ini.

Cabang yang dibutuhkan oleh Dedicated Line

Di waktu dulu, menukar informasi antar cabang dari suatu perusahaan sebagian besar dilaksanakan oleh pos, telepon, dan kemudiannya oleh fax. Tetapi hari ini ada empat tantangan utama untuk perusahaan modern:

1. Proses akselerasi bisnis yang umum dan peningkatan kebutuhan yang cepat, fleksibel menukar informasi antar semua cabang dari suatu perusahaan telah menjadikan "model kuno" mengeposkan dan bahkan jasa fax nampak terlalu melambat untuk kebutuhan modern.
2. Teknologi seperti Groupware, Customer Relationship Management (CRM), dan Enteprise Resourse Planning (ERP) digunakan untuk memastikan kerjasama sekelompok produktif dan tiap-tiap karyawan diharapkan untuk bekerja sama.
3. Hampir tiap-tiap perusahaan mempunyai beberapa cabang di dalam lokasi berbeda dan para pekerja rumah. Semua ini harus dimungkinkan untuk mengambil bagian di dalam internal menukar informasi dengan segera.
4. Semua jaringan komputer harus memenuhi standart keamanan ke tingkat tinggi untuk memastikan dataintegritas, keaslian, dan stabilitas.

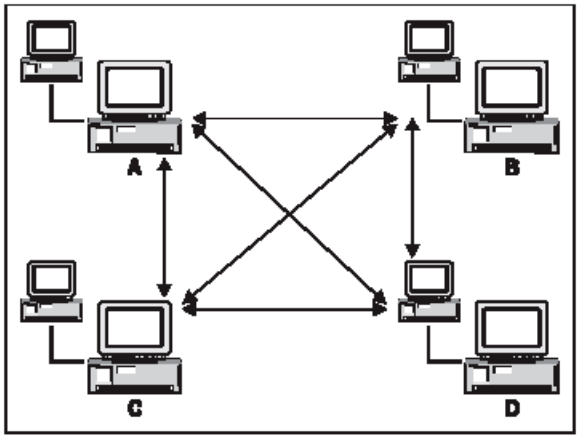
Empat faktor ini sudah mendorong kebutuhan tentang solusi jaringan canggih antar suatu perusahaan di seluruh penjuru dunia. Dengan jaringan komputer yang

menghubungkan semua desktop di dalam satu penempatan, kebutuhan akan koneksi antar lokasi telah menjadi semakin banyak mendesak.

Sejak awal, kamu hanya bisa membeli jalur resmi antar lokasi mu dan sangat mahal, dan hanya perusahaan besar yang mampu untuk menghubungkan cabang mereka untuk memungkinkan perusahaan di seluruh duniabekerjasama. Untuk menjangkau tujuan ini, kecepatan dan ahalnya koneksi telah diinstall di dalam tiap-tiap lokasi, penetapan biaya jauh lebih dibanding perusahaan normal Internet akses.

Konsep di belakang disain jaringan ini didasarkan pada suatu jaringan riil antar cabang perusahaan. Suatu penyedia diperlukan untuk menghubungkan tiap-tiap penempatan, dan suatu sambungan kabel riil antar semua cabang dibentuk. Seperti jaringan telepon, jalur yang menghubungkan dua mitra yang digunakan untuk komunikasi.

Keamanan untuk garis ini dicapai dengan menyediakan suatu koneksi di setiap jaringan antar cabang telah diinstall dengan suatu jalur. Karena suatu perusahaan dengan empat cabang (A, B, C, dan D), enam jalur yang menjadi penting.



Lagipula, Remote Access Servers (RAS) digunakan untuk para pekerja rumah atau bidang yang hanya menghubungkan untuk sementara kepada jaringan perusahaan itu. Orang ini harus lebih dulu menggunakan dial-in khusus koneksi (dengan suatu modem atau suatu jalur ISDN, dan perusahaan bertindak seperti suatu penyedia internet. Karena tiap-tiap pekerja remote suatu dial-in harus diatur dan para pekerja bidang bisa hanya

menghubungkan di atas garis ini. Perusahaan telepon menyajikan orang untuk jalur untuk tiap-tiap dial-up, dan cabang yang pusat harus lebih dulu meyakinkan bahwa cukup bentuk telepon selalu tersedia.

Dengan melindungi kabel dan dial-in server, suatu jaringan pribadi riil diinstall pada biaya-biaya sangat tinggi. Keleluasaan pribadi di dalam jaringan perusahaan yang memutar berbagai cabang dicapai oleh pengamanan jalur dan menyediakan jasa hanya untuk koneksi hard-wired. Hampir semua keamanan dan tugas ketersediaan diserahkan kepada penyedia jasa pada biaya-biaya sangat tinggi. Tetapi dengan menghubungkan lokasi secara langsung, perpindahan kecepatan kecepatan data yang lebih tinggi bisa dicapai dibanding dengan "normal" Internet koneksi pada waktu itu.

Sampai pertengahan tahun 1990, bentuk dedicated line dan dial-in akses server digunakan untuk memastikan kelompok kerja antar para pekerja bidang dan cabang berbeda dari perusahaan besar.

Broadband Access Internet dan VPN

Pada pertengahan tahun 1990, kenaikan internet dan peningkatan kecepatan untuk Internet dengan menyiapkan jalur koneksi teknologi baru. Banyak pengembang, pengurus, dan tidak berlangsung tetapi paling sedikit, para manajer telah menemukan bahwa di sana mungkin ada solusi lebih baik dibanding belanjaan beberapa beratus-ratus dolar, jika bukan beribu-ribu dolar, pada akses jalur dial-up.

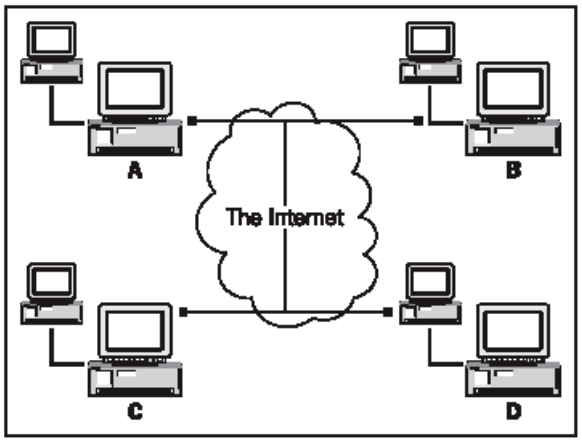
Gagasan akan menggunakan Internet untuk komunikasi antar cabang dan pada waktu yang sama memastikan kerahasiaan dan keselamatan mentransfer data. Singkatnya: menyediakan keamanan koneksi antar cabang perusahaan dengan biaya murah menggunakan Internet. Ini adalah suatu uraian sangat mendasar dari VPN.

VPN merupakan :

1. Virtual, karena tidak ada koneksi jaringan yang langsung riil antaradua atau lebih komunikasi, tetapi hanya suatu koneksi sebetulnya yang disajikan oleh VPN Perangkat lunak, sadari secara normal di atas publik Internet koneksi.

2. Private, karena hanya anggota dari perusahaan yang dihubungkan oleh VPN Perangkat lunakdiijinkan untuk membaca data ditransfer.

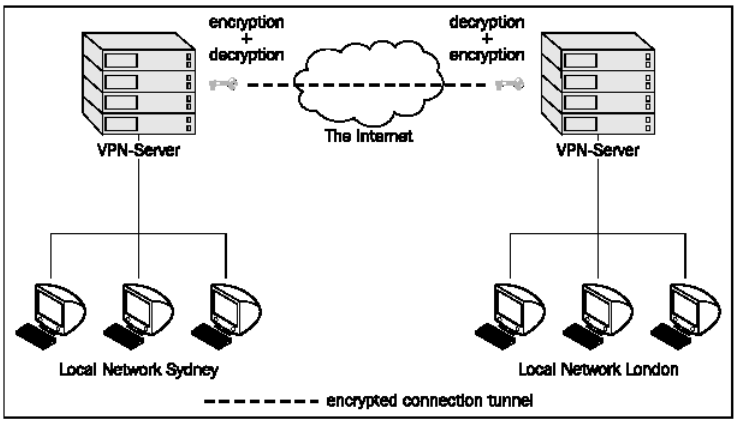
Dengan VPN, staff mu di Sydney dapat bekerja dengan Kantor London seolah-olah kedua-duanya di dalam lokasi yang sama. Perangkat lunak VPN menyediakan suatu jaringan koneksi internet antar lokasi dengan biaya murah. Jaringan ini sebenarnya hanya koneksi jaringan riil.



VPN dapat juga diuraikan sebagai satuan koneksi logis yang dijamin aman oleh perangkat lunak khusus yang menetapkan keleluasaan pribadi dengan perlindungan koneksi endpoints. Hari ini Internet adalah jaringan medium, dan keleluasaan pribadi dicapai oleh metoda cryptographic modern.

Bagaimana VPN bekerja?

Mari kita menggunakan suatu contoh untuk menjelaskan bagaimana VPN bekerja. Virtual Entity Networks Inc. (VEN Inc.) mempunyai dua cabang, London dan Sydney. Jika cabang Australian di Sydney memutuskan untuk mengontrak penyalur, kemudian kantor London harus mengetahui langsung. Bagian utama dari infrastruktur IT disediakan di London. Di Sydney ada duapuluh orang yang pekerjaannya tergantung pada ketersediaan data menjadi tuan rumah pada Server London.

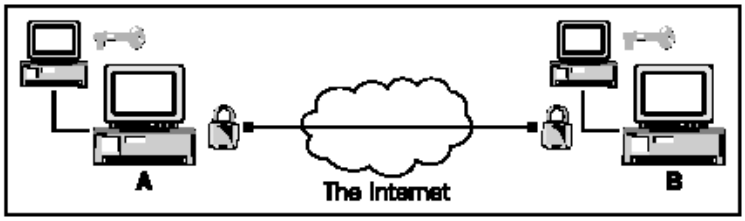


Kedua lokasi dilengkapi dengan suatu jalur internet permanen. Suatu Internet router gateway adalah di-set sampai menyediakan Internet mengakses untuk staff itu. Penerus ini diatur untuk melindungi jaringan yang lokal lokasi dari akses tidak syah dari sebelah, yang mana adalah itu "kejahatan" internet. Penerus seperti itu menyediakan untuk menghalangi lalu lintas khusus dapat disebut suatu firewall dan harus ditemukan di dalam tiap-tiap cabang yang dikira untuk ambil bagian dalam VPN itu.

Perangkat lunak VPN harus diinstall pada firewall ini atau suatu server atau alat yang dilindungi oleh itu. Banyak firewall peralatan modern dari pabrikan seperti Cisco atau Bintec meliputi corak ini, dan ada VPN Perangkat lunak untuk semua perangkat keras dan lunak platform.

Pada langkah berikutnya, VPN Perangkat lunak harus diatur untuk menetapkan koneksi pada sisi lainnyasebagai contoh VPN server London harus menerima koneksi dari Sydney server, dan Sydney server harus menghubungkan ke London atau sebaliknya.
Jika langkah ini berhasil diselesaikan, perusahaan mempunyai suatu Virtual Network. Kedua cabang dihubungkan dengan internet dan dapat bekerja sama seperti di dalam suatu jaringan riil. Di sini, kita mempunyai suatu VPN tanpa keleluasaan pribadi, sebab banyak roter internet antar London dan Sydney dapat membaca pertukaran data. Suatu pesaing yang memperoleh kendali pada suatu roter internet bisa membaca semua relevan data bisnis jaringan yang sebetulnya itu.

Maka bagaimana cara kita membuat Virtual Network Private? Solusinya adalah enkripsi. Jalur VPN antar dua cabang dikunci dengan kunci khusus, dan hanya para orang atau komputer yang memiliki kunci ini yang dapat membuka dan nampak di data pengirim.



Semua data dikirim dari Sydney ke London atau dari London ke Sydney harus terenkripsi sebelum dan didekripsi setelah transmisi. Encryption melindungi data di dalam koneksi seperti dinding dari suatu terowongan melindungi kereta dari gunung di sekitar itu. Ini menjelaskan mengapa VPN sering dikenal sebagai terowongan (tunnel) atau VPN tunneling, dan teknologinya sering disebut tunneling—even jika tidak ada mekanika kwantum lain yang melibatkan.

Metoda encryption yang tepat dan menyediakan kunci bagi semua partisi melibatkan salah satu dari faktor pembeda utama antar VPN solusi yang berbeda.

Suatu koneksi VPN yang secara normal dibangun antara dua akses router internet yang dilengkapi dengan suatu firewall dan perangkat lunak VPN. Perangkat lunak harus di-set sampai menghubungkan pada VPN partner, firewall harus di-set sampai bisa mengakses, dan menukar data antara VPN partner dengan encryption. Encryption kunci harus disajikan untuk semua VPN partner, sedemikian sehingga data yang ditukar hanya dapat dibaca oleh VPN partner yang diberi hak.

VPN digunakan untuk apa ?

Pada contoh sebelumnya, kita sudah membahas beberapa skenario untuk penggunaan teknologi VPN. Tetapi satu VPN solusinya harus ditambahkan di sini: Semakin banyak penawaran pelanggannya atau teman bisnis akses dilindungi ke data

relevan untuk hubungan bisnis mereka, seperti data pemesanan kaus kaki. Ini kita mempunyai tiga skenario untuk VPN solusi di dalam perusahaan modern:

1. Intranet yang diputar di atas beberapa lokasi dari suatu perusahaan.
2. Akses dial-up untuk para pekerja bidang atau rumah dengan mengubah hak akses.
3. Extranet rekan mitra bisnis atau pelanggan.

Masing-Masing tipe skenario memerlukan susunan dan pertimbangan keamanan khusus. Yang eksternal para pekerja rumah akan memerlukan akses berbeda ke server di dalam perusahaan dibanding pelanggan dan rekan bisnis. Sesungguhnya, mengakses untuk pelanggan dan rekan bisnis harus terbatas.

Sejak mengetahui bagaimana suatu VPN dapat dengan aman menghubungkan suatu perusahaan dalam cara yang berbeda, kita akan mengetahui cara kerja dari suatu VPN. Untuk memahami fungsinya, beberapa konsep jaringan dasar perlu untuk dipahami.
Semua pertukaran data di dalam jaringan komputer didasarkan pada protokol. Protokol seperti bahasa yang harus digunakan antar komunikasi di dalam jaringan. Tanpa penggunaan protokol yang benar, komunikasi gagal.

Networking Concepts—Protocols dan Lapisan

Ada sejumlah besar protokol dilibatkan dalam berbagai aksi yang kamu ambil ketika kamu Mengakses Internet atau suatu PC dalam jaringan lokal mu. Jaringan Mu Menghubungkan Kartu (NIC) yang akan berkomunikasi dengan suatu hub, switch, atau router; aplikasi mu akan berkomunikasi dengan suatu server pada PC yang lain, dan banyak lagi prosedur komunikasi protocol-based yang diperlukan untuk menukar data.

Oleh karena ini Open System Interconnection (OSI) spesifikasi diciptakan. Tiap-Tiap protokol digunakan di dalam jaringan masa kini dapat digolongkan oleh rencana ini.
Spesifikasi OSI menggambarkan tujuh lapisan pertukaran datai, yang mana mulai pada Lapisan 1 (physical layer) tentang dasar media jaringan (electrical, optical, atau sinyal radio) dan memutar ke Lapisan 7 (lapisan aplikasi), di mana aplikasi pada PC berkomunikasi satu sama lain.

Lapisan DARI OSI adalah:

1. Physical Layer: Mengirimkan dan menerima melalu perangkat keras.
2. Data Link Layer: Mengarahkan komunikasi antara alat jaringan dengan medium yang sama.
3. Network Layer: Routing, addressing, error handing, dll.
4. Transport Layer: End-To-End error dan flow control.
5. Session Layer: Membuat koneksi dan koneksi antar aplikasi.
6. Presentation Layer: Penterjemah antara format jaringan dan format data aplikasi.
7. Aplikation Layer: Protocol untuk aplikasi tertentu.

Satuan lapisan ini adalah hirarkis dan tiap-tiap lapisan sedang melayani lapisan di atas dan lapisan di bawah. Jika protokol dari lapisan phisik bisa komunikasi dengan sukses, kemudian kendali disampaikan untuk lapisan yang berikutnya, Data Link Layer. Hanya jika semua lapisan, 1 sampai 6, dapat berkomunikasi dengan sukses, dapat menukar data antara aplikasi pada Lapisan 7 dicapai.

Di dalam Internet, bagaimanapun pendekatan yang sedikit berbeda digunakan.
Internet sebagian besar didasarkan pada Internet Protokol (IP).

Lapisan dari IP adalah:

1. Link Layer: Penggabungan OSI Layer 1 dan 2 (Phisical dan Data Link).
2. Network Layer: Menjadi anggota Network Layer dari OSI.
3. Transport Layer: Meliputi protokol seperti Transmission Control Protocol (TCP) dan User Datagram Protocol (UDP), yang merupakan basis untuk protokol Aplikation Layer.
4. Aplication Layer: Penggabungan OSI Lapisan 5 sampai 7 (Sesi, Presentation, dan Aplication Layer). Protokol di dalam Transport Layer adalah basis untuk protokol Aplication layer (Lapisan 5 sampai Lapisan 7) seperti HTTP, FTP, atau yang lain.

Paket jaringan terdiri dari dua komponen: header dan data. Header adalah sejenis label yang berisi metadata pada pengirim, penerima, dan informasi administratif untuk perpindahan itu. Pada tingkat jaringan dari suatu Ethernet jaringan, paket ini disebut

bingkai. Dalam konteks IP paket ini disebut datagram, Internet datagrams, IP datagrams, atau sederhananya paket.

Lalu apa yang dilakukan VPN? VPN Perangkat lunak mengambil IP paket atau Ethernet membingkai dan membungkusnya ke dalam paket yang lain . Ini nampak sulit, tetapi ini merupakan suatu cara sangat sederhana, seperti yang berikut:

Contoh 1: Pengiriman parsel tanpa nama

Kamu ingin mengirimkan suatu parsel kepada seorang teman yang hidup di dalam suatu masyarakat dengan orang asing, yang kamu tidak percaya. Parsel mu mempunyai label alamat dengan data penerima dan pengirim seperti suatu Internet paket. Jika kamu tidak ingin orang lain mengetahui bahwa kamu mengirim teman mu suatu parsel, tetapi pada waktu yang sama kamu ingin teman mu untuk sadari ia membuka itu, apa yang kamu akan lakukan? Hanya embungkus keseluruhan parsel di dalam paket yang lain dengan suatu label alamat berbeda (contoh tanpa informasi pengirim mu) dan tak seorangpun akan mengetahui bahwa parsel ini adalah dari kamu. Tetapi teman mu akan membongkar lapisan dasar dan lihat parsel masih dibongkar, dan dengan suatu label alamat dari kamu.

Contoh 2: Pengiriman suatu parsel yang dikunci

OK, sekarang mari kita mencurigai komune yang masih ada lagi. Kekuatan seseorang ingin membuka parsel dalam urutan untuk menemukan apa yan ada di dalam. Untuk mencegah ini, kamu akan menggunakan suatu kunci. Ada dua kunci untuk kunci, satu untuk kamu dan satu untuk teman mu. Hanya kamu dan teman mu yang dapat membuka kunci dan lihat isi dalam paket itu.

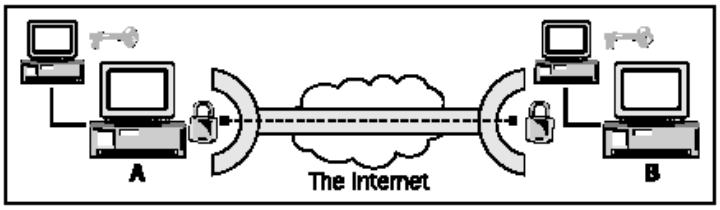
VPN Perangkat lunak menggunakan suatu kombinasi yang lebih awal dua contoh:

1. Paket jaringan utuh (bingkai, datagrams) terdiri dari header dan data yang dibungkus ke dalam paket baru.
2. Semua data yang mencakup metadata seperti pengirim dan penerima encrypted.
3. Paket yang baru diberi label dengan header baru yang berisi meta-information tentang VPN dan menunjukkan VPN.

Semua sistem VPN perangkat lunak berbeda dalam cara membungkus dan mengunci data itu.

Tunneling dan Overhead

Kita sudah mempelajari teknologi VPN yang sering disebut terowongan (tunneling), sebab data dalam koneksi VPN dilindungi dari Internet sebagai dinding dari suatu jalur atau tunnel rel melindungi lalu lintas di dalam tunnel dari orang banyak batu gunung di atas. Mari kita sekarang memperhatikan bagaimana VPN Perangkat lunak mengerjakan ini:



VPN perangkat lunak dalam lokasi A dan B encrypts (kunci) dan decrypts (membuka kunci) data dan mengirimkannya melalui tunnel itu. Seperti mobil atau kereta dalam uatu terowongan, data tidak bisa meninggalkan tetapi terowongan yang lain endpoint.
Berikut yang dipasang dan dibungkus ke dalam satu paket baru:

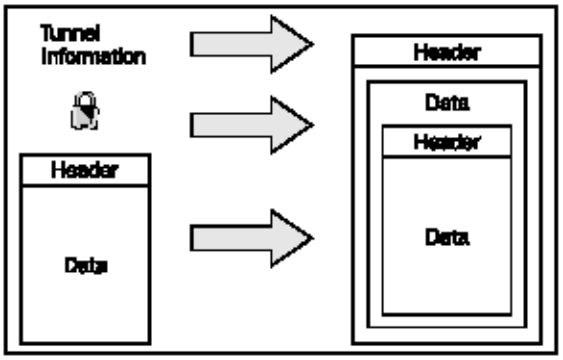
a. Informasi tunnel (seperti alamat dari endpoint lain)
b. Encryption data dan metoda
c. IP paket Yang asli (atau bingkai jaringan)

Paket yang baru kemudian mengirim kepada tunnel endpoint yang lain. Muatan penghasil untung dari paket ini sekarang menjaga IP paket yang lengkap (atau membungkus jaringan), tetapi di dalam format encrypted dan begitu menarik untuk seseorang yang tidak memiliki kunci. Header baru dari paket yang sederhana berisi alamat pengirim dan penerima dan metadata lain yang penting dan yang disajikan oleh VPN perangkat lunak.

Barangkali kamu sudah mencatat bahwa jumlah pengiriman data bertambah sepanjang proses " pembungkusan". Tergantung pada penggunaan software VPN, ini bernama overhead dapat menjadi suatu faktor sangat penting. Overhead adalah perbedaan antara data pengiriman pada software tunnel dan pengiriman data gross melalui tunnel oleh software VPN. Jika suatu file 1 MB dikirim dari user A ke user B, dan file ini menyebabkan 1.5 MB kepadatan di dalam tunnel, kemudian overhead akan menjadi

50%, setingkatan sangat tinggi. Overhead disebabkan oleh softwareVPN yang tergantung pada jumlah data yang terorgasisasi dan menggunakan encryption. Sedangkan yang pertama tergantung hanya pada penggunaan software VPN, yang akhirnya merupakan

suatu pilihan antara keamanan dan kecepatan. Dengan kata lain, makin baik encryption yang digunaan, semakin banyak overhead yang akan dihasilkan. Kecepatan melawan keamanan adalah pilihan mu.



VPN Concepts—Overview

Sepanjang terakhir sepuluh tahun, banyak VPN konsep berbeda sudah meningkatkan. Kamu mungkin telah mencatat bahwa aku

selalu menambahkan " bingkai jaringan" di dalam kurungan ketika aku membangun tunnel IP paket. Ini menjadi perlu, sebab pada prinsipnya, membangun tunnel bisa dilakukan pada hampir semua lapisan OSI model.

Standart tujuan dari Tunneling

General Routing Encapsulation (GRE) menyediakan standard untuk pembangunan tunnel data, yang digambarkan di tahun 1994 di Request for Comments (RFC) 1701 dan 1702. Barangkali, karena definisi ini tidak merupakan suatu definisi protokol, tetapi kurang lebih suatu proposal standard pada bagaimana cara data tunnel, implementasi ini telah menemukan caranya dalam banyak alat dan menjadi basis untuk protokol lain.

Konsep GRE adalah sederhana. Suatu protokol header dan suatu penyerahan header ditambahkan pada paket asli dan muatan penghasil untungnya adalah encapsulasi dalam paket yang baru itu. Tidak ada encryption dilaksanakan.

Keuntungan dari model ini hampir dipastikan menawarkan banyak berbagai kemungkinan, ketransparanan memungkinkan penerus dan pengurus untuk melihat di dalam paket dan keputusan yang didasarkan pada jenis pengiriman muatan penghasil untung . Dengan membuat maka, aplikasi khusus dapat diistimewakan.

Ada banyak implementasi untuk GRE yang membangun software tunnel di bawah Linux; hanya kernal yang sangat penting, yang mana dipenuhi oleh distribusi paling modern.

Implementasi Protocol pada Layer 2

Paket encapsulasi pada OSI Lapisan 2 mempunyai suatu keuntungan penting: tunnel bisa memindahkan protokol non-IP. IP adalah suatu standard yang digunakan secara luas dalam Internet dan dala) Ethernet jaringan.

Bagaimanapun, ada standard yang berbeda juga. Sistem Netware, sebagai contoh, menggunakan Internetwork Packet Exchange (IPX) protokol untuk komunikasi. VPN teknologi yang terdapat pada Lapisan 2 secara teoritis banyak jenis tunnel. Dalam banyak kasus, sebenarnya suatu Point-To-Point Protokol (PPP) memutuskan alat yang mana digunakan untuk menghubungkan pada tunnel yang endpoint.

Empat Layer 2 yang diketahui adalah teknologi VPN, yang digambarkan oleh RFCS, menggunakan encryption metoda dan menyediakan pengesahan pemakai:

1. Poin-to-point Tunneling Protoocol (PPTP), yang dikembangkan dengan bantuan Microsoft, adalah suatu perluasan PPP dan terintegrasi dalam semua Microsoft sistem operasi. PPTP menggunakan GRE untuk encapsulation dan tunnel dapat IP, IPX, dan paket lain di Internet itu. Kerugian Yang utama adalah pembatasan yang hanya dapat satu tunnel serentak antar komunikasi.

2. Layer 2 Forwarding (L2F) dikembangkan hampir pada waktu yang sama oleh perusahaan seperti Cisco dan yang lain dan penawaran lebih berbagai kemungkinan dibanding PPTP, terutama mengenai pembangunan tunnel jaringan dan berbagai multipel simulasi tunnel.
3. Layer 2 Tunneling Protocol (L2Tp) diterima sebagai suatu standard industri dan digunakan secara luas oleh Cisco dan pabrikan lain. Suksesnya didasarkan pada fakta bahwa itu kombinasi keuntungan dari L2F dan PPTP tanpa mendapatkan kerugian. Sungguhpun itu tidak menyediakan mekanisme keamanan, dapat dikombinasikan dengan teknologi yang menawarkan mekanisme seperti seperti IPsec.
4. Layer 2 Securitty Protocol (L2Sec) dikembangkan untuk menyediakan suatu solusi pada kekurangan keamanan IPsec. Sungguhpun overheadnya agak besar, mekanisme keamanan aman digunakan, sebab sebagian besar SSL/TLS digunakan.

Faktor pembeda lain antar protokol dan sistem tersebut adalah:

1. Ketersediaan mekanisme pengesahan
2. Mendukung untuk keuntungan jaringan seperti Network Address Translation (NAT)
3. Alokasi IP dinamis untuk tunnel dalam dial-up gaya
4. Mendukung untuk Public Key Infrastructure (PKI)

Corak ini akan dibahas di dalam bab kemudiannya.

Implementasi Protokol Layer 3

IPsec banayak digunakan pada teknologi tunnel. IPsec adalah suatu kompromi yang diterima dengan suatu komisi pengawas. Alat-alat IPsec dapat digunakan dalam banyak lingkungan dan susunan berbeda, memastikan kecocokan, tetapi hampir tidak aspek tentangnya menawarkan kemungkinan solusi terbaik.

IPsec dikembangkan sebagai suatu Standard Keamanan Internet pada Lapisan 3, dan telah distandardisasi oleh Internet Engineering Task Force (IETF) sejak 1995. IPsec dapat digunakan untuk encapsulasi data pada lapisan aplikasi, tetapi tidak ada lalu lintas lapisan jaringan yang lebih rendah. Bingkai jaringan, IPX paket, maupun

penyampaian pesan dapat ditransfer, dan terjemahan alamat jaringan yang mungkin dengan pembatasan.

Keuntungan IPsec yang utama digunakan di mana-mana. Administrator dapat memilih dari suatu jumlah berlimpah-limpah perangkat keras alat dan perangkat lunak implementasi untuk menyediakan jaringannya dengan suatu mengamankan tunnel.

Pada dasarnya ada dua relevan metoda penggunaan IPsec:

1. Tunnel Mode: mode tunnel bekerja seperti contoh pendaftaran, keseluruhan IP paket dan dienkapsulasi di dalam suatu paket baru dan mengirim kepada tunnel pada endpoint, di mana software VPN membongkarnya dan ke depannya kepada penerima itu. Dengan cara ini IP alamat penerima dan pengirim, dan semua metadata lain dilindungi juga.
2. Trasport Mode: Dalam transport mode, hanya muatan pada data yang dilakukan enkripsi dan enkapsulasi. Dengan membuat, maka overhead lebih kecil dibanding tunnel mode, tetapi dapat dengan mudah dibaca dan berkomunikasi. Bagaimanapun, data telah dienkripsi dan oleh karena itu terlindungi.

Implementasi Protokol Pada Layer 4 (Transport)

Ini mungkin untuk menetapkan tunnel VPN hanya pada lapisan aplikasi. Secure Sockets Layer (SSL) dan Transport Layer Security (TLS) solusi mengikuti pendekatan ini. Pemakai dapat mengakses jaringan VPN dari suatu perusahaan melalui suatu browser koneksi antar kliennya dan VPN server di perusahaan itu. Suatu koneksi sederhananya dimulai dengan pembukuan ke dalam suatu HTTPS-SECURED website dengan suatu browser. Sementara itu, ada beberapa peluang produk tersedia, seperti SSLEXPLORER dari http://3sp.com/showSslExplorer.do, dan produk seperti penawaran ini fleksibilitas dikombinasikan dengan keamanan dan susunan yag mudah. Menggunakan pengamannan koneksi penawaran browser, para pemakai dapat menghubungkan jaringan dan mengakses jasa di jaringan yang remote itu. Keamanan adalah yang dicapai dengan encrypting lalu lintas menggunakan SSL/TLS mekanisme, yang sudah terbukti sangat dapat dipercaya dan untuk selamanya ditingkatkan dan diuji.

OpenVPN-SSL/TLS-Solusi

Openvpn adalah suatu solusi VPN terkemuka. Implements koneksi Lapisan 2 atau Lapisan 3, menggunakan standard industri SSL/TLS untuk encryption, dan berkombinasi hampir semua jenis solusi VPN tersebut. Kerugian utama bahwa masih ada sedikit perangkat keras pabrikan yang mengintegrasikannya dalam solusi mereka.

Ringkasan

Di dalam bab ini, kamu sudah mempelajari sekitar teknik digunakan dalam perusahaan menggunakan jaringan komputer pada beberapa cabang. Kamu sudah mempelajari dasar jaringan seperti protokol, lapisan networking, OSI, dan solusi VPN. Kamu sudah membaca bagaimana pembangunan tunnel, bagaimana kerjanya, dan bagaimana perbedaan penerapan solusi VPN.

BAB 2
VPN SECURITY

Dalam bab ini, kita akan mendiskusikan sasaran dan teknik-teknik mengenai keamanan VPN. Dua terminologi ini terhubung bersama dengan sangat rahasia. Tanpa Security, suatu VPN tidak akan private lagi.

Oleh karena itu, pertama kita akan melihat pokok persoalan keamanan dan menciptakan solusi yang akan dipakai dalam suatu perusahaan. Informasi dalam metoda-metoda kunci symmetric dan asymmetric, teknik merubah kunci, dan permasalahan dari keamanan dibandingkan dengan kemudahan untuk menyiapkan jalan bagi keamanan SSL/TLS dan melihat dengan teliti pada sertifikat SSL. Setelah selesai membaca bab ini, anda diharapkan dapat memahami pokok-pokok yang mendasari keamanan/security dari OpenVPN (dan solusi VPN yang lain).

VPN Security

Keamanan IT dan VPN dijelaskan oleh tiga sasaran yang harus dicapai, antara lain:

1. Privacy (Confidentiality) : Data yang dikirim hanya akan tersedia untuk yang berhak.
2. Reliability (Integrity): Data yang dikirim tidak harus dirubah pada sisi pengirim dan penerima.
3. Availability: Data yang dikirim harus tersedia ketika diperlukan.

Semua sasaran ini harus dicapai dengan menggunakan perangkat lunak (software), perangkat keras (hardware), Internet Service Providers (ISP), dan kebijakan-kebijakan keamanan. Suatu kebijakan keamanan menegaskan pertanggung jawaban, prosedur-prosedur standart, kerugian dan perbaikan dari yang terburuk. Mengerti kerusakan maksimum dan biaya-biaya dari kerugian yang terburuk yang mungkin dapat memberi suatu gagasan berapa banyak biaya harus dikeluarkan untuk persoalan keamanan. Kebijakan keamanan juga perlu menetapkan pertanyaan-pertanyaan organisasi seperti:

1. Siapa yang mempunyai kunci untuk server ketika administrator sedang berlibur?
2. Siapa yang diizinkan untuk membawa laptop pribadi?
3. Bagaimana suatu kabel dilindungi?
4. Bagaimana suatu wireless LAN (WLAN) dilindungi?

Ada sejumlah online dokumen yang sempurna di mana anda dapat membaca lebih banyak tentang dasar keamanan bahwa perlu juga dibahas di dalam perusahaan Anda. Saya hanya ingin menyebutkan dua mereka di sini:

IT Baseline Protection seperti yang diterbitkan oleh BSI Jerman dan IT-Sec Handbook yang berisi petunjuk keamanan dan sering dikutip sebagai material acuan untuk semua persoalan keamanan di dalam perusahaan yang modern. Anda dapat menemukan mereka di sini:
mailto:http://www.bsi.bund.de/english/gshb/index.html
mailto:http://www.cccure.org/Dokuments/HISM/ewtoc.html

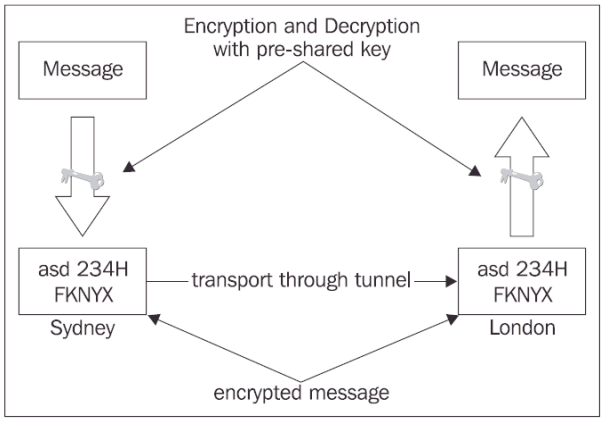
VPN security dapat dicapai dengan melindungi traffic dengan metoda-metoda enkripsi yang modern, kuat, mengamankan teknik-teknik pengesahan, dan pengendalian firewall traffic ke dan dari tunnels. Dan hanya enkripsi traffic itu tidaklah cukup; ada perbedaan sangat besar di dalam keamanan tergantung pada metoda yang digunakan. Bagian-bagian yang berikut akan berhubungan dengan persoalan mengenai kerahasiaan dan integritas, sedangkan pendekatan untuk memastikan ketersediaan dibahas di dalam bab yang berikutnya.

Privacy – proses enkripsi suatu traffic

Sering kali password atau kunci enkripsi digunakan untuk enkripsi data. Jika kedua sisi menggunakan kunci yang sama untuk enkripsi dan dekripsi data, ini disebut enkripsi symmetric. Kunci enkripsi itu harus dtempatkan di semua mesin yang diduga untuk ambil bagian dalam koneksi VPN.

Symmetric Encryption and Pre-Shared Keys

Siapapun yang mempunyai kunci ini dapat dekripsi traffic. Jika satu penyerang dapat memegang kunci ini, ia dapat dekripsi semua traffic dan semua sistem mengambil bagian dalam VPN, sampai semua sistem disediakan bersama dengan kunci lain Itu hanyalah soal waktu untuk satu penyerang menemukan dan membaca kunci, atau bahkan lebih buruk, mengubah data.



Oleh karena itu, Software VPN seperti IPsec merubah kunci di dalam interval yang digambarkan. Setiap kunci akan tetap untuk suatu periode waktu tertentu, yang disebut kunci seumur hidup. Suatu kombinasi yang baik dari kunci seumur hidup dan panjangnya kunci memastikan bahwa satu penyerang tidak bisa merubah kunci tetap tersebut. Jika VPN Software itu sedang mengubah kunci, lalu penyerang harus cepat, atau kunci yang diperoleh tidak akan berguna.

Meskipun demikian, jika software VPN adalah untuk mengubah kunci selamanya, suatu metoda dari kunci akan merubah antara partner komunikasi yang harus digunakan sehingga kedua sisi menggunakan kunci enkripsi yang sama pada waktu yang sama. Pertukaran kunci ini harus dijamin aman, dan mengikuti prinsip-prinsip yang sama seperti sebelumnya. Selama dekade yang terakhir banyak kunci telah ditemukan dengan metode yang berbeda, sangat canggih, dan telah banyak yang sudah membuktikan. Pada

dasarnya, pertukaran kunci ini menambahkan suatu lapisan dari kompleksitas pada software VPN, yang cenderung mengalami kegagalan.

IPsec, kebanyakan memakai teknologi VPN dengan membawa protokol sendiri untuk menukarkan kunci enkripsi. Protokol ini disebut Internet Key Exchange (IKE) Protokol dan telah berkembang sejak pertengahan 90-an dan masih belum selesai. Banyak diskusi tentang keamanan dari protokol ini ditemukan lewat Internet dan meskipun IKE kelihatannya memiliki beberapa persoalan keamanan, IKE tetap saja digunakan (dengan IPsec) di dalam banyak perusahaan.

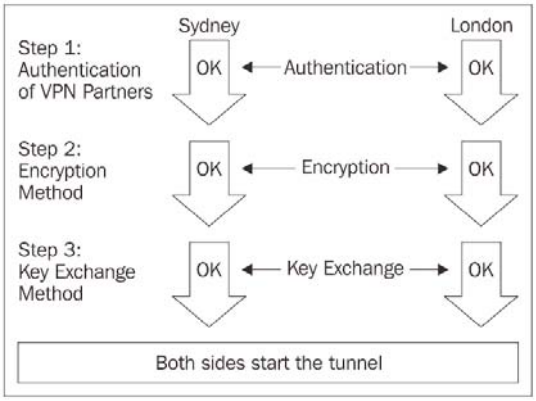
Reliability and Authentication

Bahaya man-in-the-middle Another atau yang disebut dengan serangan, atau yang lebih kita kenal dengan eavesdropping. Di dalam skenario ini, suatu hacker menginterupsi semua traffic data antara pengirim dan penerima, mengkopi dan meneruskanya pada tujuan yang benar. Pengirim maupun penerima akan mengenali bahwa data sedang diinterupsi. Man-in-the-middle itu dapat menyimpan salinan, meneliti, dan bahkan memodifikasi traffic yang didapat. Ini mungkin jika penyerang dapat menginterupsi dan menurangi kunci ketika mereka dipakai untuk enkripsi

Masalah Kompleksitas Pada VPN Klasik

Dengan VPNs klasik yang menggunakan kunci symmetric, ada beberapa lapisan-lapisan pengesahan, pertukaran kunci enkripsi, dan encryption/decryption. Ada tiga langkah pertama dari VPNs dengan enkripsi yang symmetric:

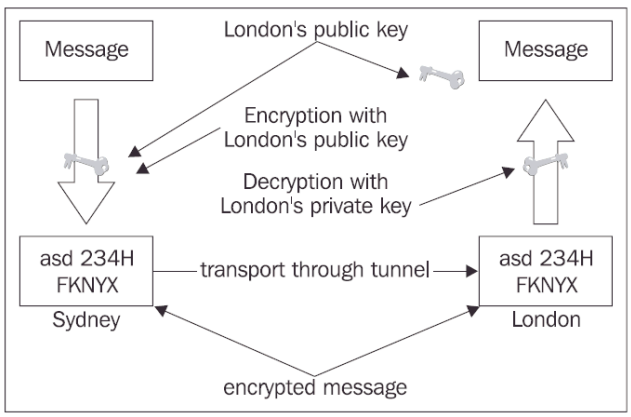
1. Para mitra itu harus membuktikan keaslian satu sama lain.
2. Mereka harus setuju metoda-metoda enkripsi.
3. kemudian mereka harus setuju dengan perubahan metode pertukaran kunci yang digunakan



Mengapa teknologi VPN sering dikenal sebagai teknologi yang kompleks dan sulit. Paragraph terakhir sudah menggambarkan kurang lebih teknik dasar di mana banyak solusi-solusi VPN modern bekerja. Singkat cerita, pendekatan yang berbeda, pertukaran kunci, dan pengesahan para mitra VPN membuat bagian utama dari perbedaan antara solusi VPN.

Asymmetric Encryption dengan SSL/TLS

SSL/TLS menggunakan salah satu teknologi enkripsi terbaik yang disebut enkripsi asimetric untuk memastikan identitas dari mitra VPN. Keduan mitra enkripsi memiliki dua kunci masing-masing: satu publik dan yang lain, pribadi. Kunci publik itu diserahkan kepada mitra komunikasi, untuk meningkatkan datanya. Oleh karena algoritma mathematical yang terpilih digunakan untuk menciptakan pasangan kunci public/private, hanya kunci pribadi penerima itu yang dapat mengurangi data yang disandikan oleh kunci publiknya.



Kunci pribadi harus dirahasiakan dan untuk kunci publik harus ditukarkan.

Pada contoh di atas, suatu pesan teks dienkripsi pada Sydney dengan kunci publik dari London. Kode acak dikirim kepada London, di mana hal itu dapat diuraikan menggunakan kunci pribadi London. Hal ini bisa dilakukan sebaliknya untuk data dari London ke Sydney, yang dienkrypsi oleh kunci publik Sydney di London dan hanya dapat dideskripsikan oleh kunci pribadi Sydney di Sydney.

Suatu prosedur yang serupa dapat juga digunakan untuk tujuan pengesahan: London mengirim suatu nomor acak yang besar kepada Sydney, di mana nomor ini disandikan dengan kunci pribadi dan dikembalikan. Di London, kunci publik Sydney dapat memecahkan kode nomor. Jika nomor yang dikirim dan dideskripsi sesuai, kemudian pengirim harus memiliki kunci pribadi Sydney. Ini disebut tanda tangan digital.

SSL/TLS Security

Library SSL/TLS dapat digunakan untuk pengesahan dan tujuan enkripsi. Library ini merupakan bagian dari OpenSSL Software yang diinstall di setiap sistem operasi yang modern. Jika tersedia, Dasar sertifikat pengesahan SSL/TLS dan enkripsi akan selalu menjadi pilihan pertama untuk setiap tunnel yang dibuat.

SSL juga yang dikenal sebagai TLS, adalah suatu protokol yang awalnya dirancang oleh Netscape Communications Corporation untuk memastikan integritas data dan keaslian untuk perkembangan Internet di dalam 1990s. Semua orang yang menggunakan browser modern dapat mengambil bagian di dalam komunikasi yang diencrypsi. SSL/TLS adalah satu teknologi yang terkemuka yang sedang digunakan di mana-mana Web untuk perbankan, e-commerce, atau aplikasi di mana keleluasaan pribadi lain manapun dan keamanan diperlukan. Itu sedang pasti terkendali, debugged, yang diuji, dan yang diperbaiki oleh kedua-duanya pengembang sumber dan kepemilikan yang terbuka dan banyak korporasi.

Selama SSL/TLS berada di bawah protokol aplikasi, itu dapat digunakan hampir pada setiap aplikasi. Setiap surfer telah memberitahukan URL dimulai dengan https:// sebagai ganti http://, yang menandakan satu koneksi yang dienkripsi. Point pada suatu situs web dienkripsi dengan https://, seperti `https://packpub.com`

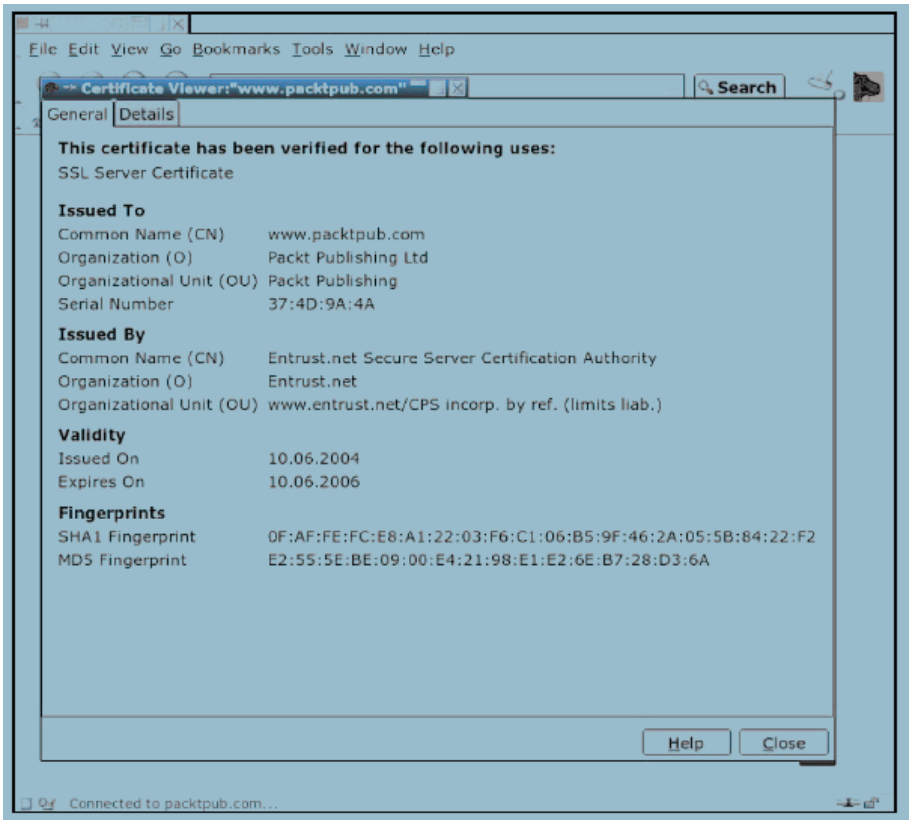
Dimanapun anda menunjuk browser anda seperti pada halaman untuk pertama kali, anda harus mengesahkan sertifikat SSL. Biasanya, browser anda mengerjakan hal ini ketika sertifikat itu dapat dipercaya. Screenshot di atas menunjukkan jendela Mozilla, yang akan diterima ketika ada error di dalam sertifikat. Biasanya, ini merupakan satu dari penekanan tombol OK, selama surfing tanpa perhatian lebih lanjut.

Memahami SSL/TLS Certificates

Dengan diterimanya suatu sertifikat (penekanan OK), sebuah browser itu diberitahu untuk mempercayai persoalan (situs web bahwa menyediakan sertifikat) dan anda setuju untuk menggunakan sertifikat ini untuk enkripsi komunikasi dengan server ini. Ketika anda sedang menggunakan Mozilla, Firefox, atau Konqueror, anda dibisikkan jika anda ingin menerima sertifikat. Klik di tombol View Certificate, dan anda akan melihat suatu layar seperti itu yang ditunjukkan di halaman sebelah screenshot di dalam bagian di Trusted Certificates.

Trusted Certificates

Di dalam screenshot yang berikut, anda dapat melihat informasi yang aman pada sertifikat SSL. Informasi di dalam field Issued To dan Issued By mungkin yang yang paling penting. Jika anda menemukan suatu organisasi yang terpercaya di sini, haruslah aman untuk mempercayai sertifikat ini. Makna terpercaya beberapa organisasi dengan sertifikat, dengan demikian menjamin identitas pemilik dari sertifikat.



Dengan suatu sertifikat yang ditandatangani oleh pemilik dari sertifikat itu dapat membuktikan (bahwa) dia adalah yang ia atau dia menyatakan diri sebagai, siapapun yang mempercayai sertifikat otorisasi.

Setiap penelusur TLS-Enable berisi daftar organisasi-organisasi yang terpercaya yang berhak atas sertifikat-sertifikat tanda dan kunci-kunci itu perlu mengkonfirmasikan hal ini.

Klik tombol dan yang lain memperhatikan window—CloseSecuras yang pertama Error. Itu ada di fakta suatu peringatan. Sertifikat itu mula-mula dikeluarkan karena www.packtpub.com dan bukan untuk packtpubcom, dimana itu diterima, dan klien Mozilla SSL hanya memperingatkan tentang fakta ini. www.packtpub.com adalah suatu

subdomain dari packtpub.com, jadi perbedaan ini tidak terlalu penting. Bagaimanapun, jika anda menerima suatu peringatan tentan suatu sertifikat untuk domain A mula-mula dikeluarkan untuk daerah B, anda seharusnya menjadi curiga.

Hal ini yang disebut rencana third-party-authentication. Informasi ini hanyalah valid untuk suatu waktu yang tertentu dan bisa ditelusur balik kepada penerbit efek. Hampir semua orang yang lain, perusahaan, atau organisasi bersandar pada informasi ini. Prinsip-prinsip ini adalah juga diterapkan di dalam banyak mekanisme-mekanisme pengesahan yang modern seperti Kerberos atau SSL/TLS.

Self-Signed Certificates

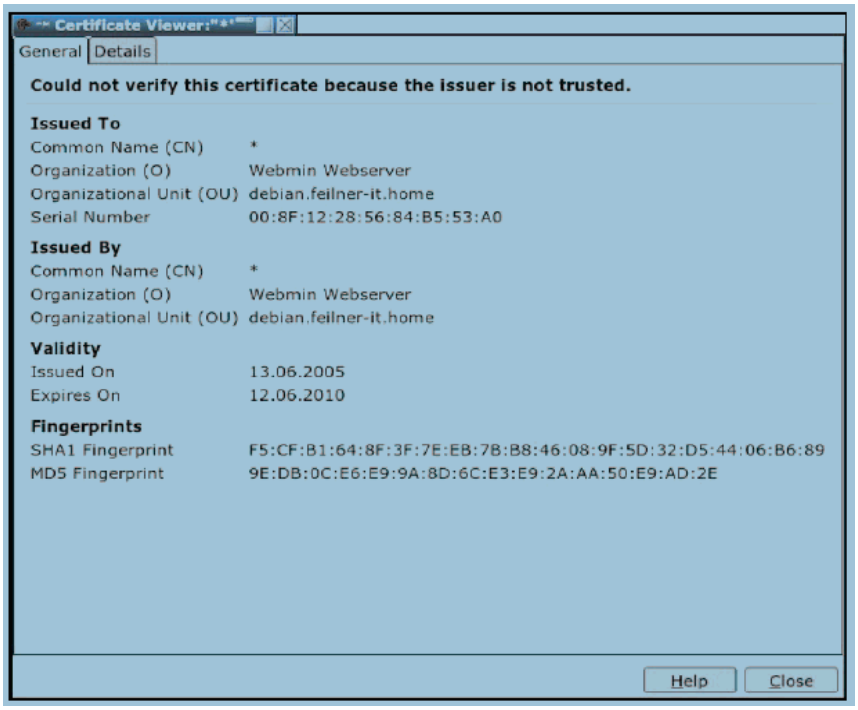
Ini juga mungkin untuk menggunakan sertifikat-sertifikat yang tidak ditandatangani oleh penguasa tersebut di atas, hanya oleh suatu local Certificate Authority (CA).

Di dalam kehidupan nyata, jika seorang teman yang baik memperkenalkan kita pada suatu seorang temannya yang dapat dipercaya, kita cenderung untuk mempercayai dia. hanya oleh karena rekomendasi. Tetapi kita tidak akan mempercayai seseorang yang tidak kita kenal. Jika anda menunjuk Mozilla pada suatu lokasi dengan suatu sertifikat yang ditandatangani hanya oleh suatu CA yang lokal, anda akan menerima peringatan yang berikut:

Peringatan berarti: "Berhati-hati, aku tidak mengetahui penerbit efek dari sertifikat ini, atau aku mengetahui seseorang yang menjamin identitas penerbit efek."

Setiap klien SSL/TLS memberi anda suatu peringatan ketika suatu klien menginginkan untuk menetapkan satu koneksi yangdienkripsi dengan satu sertifikat pribadi yang tidak ditandatangani. Mozilla membuka Window Website Certified oleh satu Unknown Authority.

Klik pada tombol Examine Certificateto menunjukkan rincian dari suatu sertifikat di Mozilla:



Pada screenshot ini, anda melihat suatu sertifikat yang dibangun untuk mengamankan administrasi Webmin interface di suatu sistim lokal. Mozilla melaporkan: Tidak bisa memverifikasi sertifikat ini karena penerbit efek itu tidak dipercaya. Darimana sertifikat datang?

Solusi itu adalah sederhana: paket software OpenSSL, yang berisi perangkat lunak enkripsi, juga menyediakan program-program untuk menciptakan sertifikat-sertifikat dan untuk tanda mereka. Sertifikat seperti itu menyebut diri sendiri menandatangani sertifikat, dan hanya dapat mempertimbangkan ketika penerbit efek atau CA itu dikenal dan yang dipercaya oleh klien. Kemudian dalam buku ini, anda akan belajar bagaimana caranya menciptakan, tanda, dan mengatur sertifikat-sertifikat seperti itu.

sertifikat-sertifikat Self-signed sering digunakan untuk tujuan pengujian atau di dalam jaringan lokal karena pendaftaran (penandatanganan) sertifikat pada penguasa sertifikat sangat mahal dan bukan hal yang terlalu penting di dalam banyak skenario. Bagaimanapun, kebijakan keamanan dari suatu perkumpulan perlu berisi definisi-definisi yang sesuai dengan pemakaian sertifikat-sertifikat tidak ditandatangani dan yang ditandatangani di server-server.

SSL/TLS Certificates dan VPNs

Sertifikiat SSL/TLS bekerja sama dengan sertifikat otorisasi VPNs—digambarkan atau yang diciptakan dan semua sertifikat yang valid yang dikeluarkan oleh otoritas ini diterima untuk VPN. Setiap klien harus mempunyai suatu sertifikat yang valid yang dikeluarkan oleh CA ini dan kemudian diizinkan untuk menetapkan suatu koneksi kepada VPN.

Suatu Penarikan Certificate Return List (CRL) dapat digunakan untuk menarik kembali sertifikat-sertifikat klien. bahwa harus diizinkan untuk disambungkan ke VPN lebih lama lagi. Hal ini bisa dilakukan tanpa bentuk pada setiap klien, dengan hanya menciptakan satu penarikan kembali yang sesuai mendaftar di server. Ini adalah sangat bermanfaat ketika suatu laptop dicuri atau dikompromikan.

Suatu organisasi yang menggunakan kunci yang dibagi bersama harus menaruh kunci ini di setiap sistim untuk disambungkan ke server VPN. Kunci yang harus diubah di semua sistem jika satu sistim tunggal atau kunci lenyap. Tetapi jika anda sedang menggunakan sertifikat-sertifikat dengan penarikan kembali mendaftar, anda hanya harus menaruh sertifikat dari laptop yang dicuri di CRL server itu. Ketika klien ini mencoba untuk sambungkan ke server, akses akan ditolak. Tidak ada kebutuhan untuk interaksi di dengan setiap klien.

Koneksi-koneksi akan ditolak jika:

1. Tidak ada sertifikat yang diperkenalkan
2. Suatu sertifikat dari suatu CA yang salah diperkenalkan
3. Suatu sertifikat yang ditarik kembali diperkenalkan

Sertifikat-sertifikat seperti itu dapat digunakan untuk banyak tujuan. HTTPS dan OpenVPN hanyalah dua aplikasi dari suatu variasi yang berkelimpahan dari berbagai kemungkinan. VPN System lain(seperti IPsec), server web, server surat, dan hampir semua aplikasi server yang lain dapat menggunakan sertifikat-sertifikat ini untuk membuktikan keaslian klien-klien. Jika anda sudah memahami dan menerapkan teknologi ini secara benar, anda sudah mencapai suatu derajat tingkat yang sangat tinggi dari keamanan.

Ringkasan

Di dalam bab ini, anda sudah pelajari konsep-konsep keamanan dasar (yang) penting bagi teknologi VPN. Ada beberapa situs web dengan material yang sempurna pada IT persoalan keamanan. Anda sudah menerima satu ringkasan dari keamanan dan enkripsi dasar mengeluarkan dan mengetahui mengapa kompleksitas merupakan suatu musuh dari keamanan. Dengan keying symmetric, kedua mitra enkripsi menggunakan kunci yang sama, tetapi jika keying asimetris digunakan, kunci enkripsi itu berbeda dari satu yang digunakan untuk decrypsi data. Library SSL/TLS menggunakan asimetris keying dan menyediakan sertifikat-sertifikat yang digunakan oleh berjuta-juta situs web. Sertifikat-sertifikat itu dapat ditandatangani oleh penguasa resmi seperti pasport - pasport kita(kami atau ID kartu-kartu, atau diri sendiri yang ditandatangani oleh suatu otoritas yang lokal. Ini menyebut pengesahan pihak ketiga karena suatu sertifikat yang ditandatangani oleh pihak ketiga dipercaya.

BAB 3
OpenVPN

Pada bab ini, kita akan membahas OpenVPN. Kita akan memulai dengan fitur-fitur dan sejarah nya, termasuk dasar konsep networking dan konfigurasi pertama kali. Pada akhir bab ini, OpenVPN dibandingkan dengan IPSec, quasi-standard dalam teknologi VPN.

Keuntungan OpenVPN

OpenVPN termasuk generasi baru VPN. Ketika solusi VPN yang lain sering menggunakan proprietary atau mekanisme non-standard, OpenVPN mempunyai konsep modular baik underlying security maupun networking. OpenVPN menggunakan keamanan, kestabilan, dan mekanisme SSL/TLS untuk autentikasi dan enkripsi. OpenVPN sangat komplek yang tidak terdapat pada impelmentasi VPN lainnya seperti market leader IPSec. Pada saat yang bersamaan, OpenVPN menawarkan kemungkinan untuk keluar dari lingkup implementasi VPN lainnya:

1. Layer 2 dan Layer 3 VPN : OpenVPN menawarkan 2mode dasar yang bekerja baik pada layer 2 ataupun layer 3 VPN. Kemudian tunnel OpenVPN mengirim Ethernet Frames, IPX paket, dan Windows Networking Browsing pakets (NETBIOS).
2. Menjaga dengan menggunakan internal firewall : Field worker dikoneksikan dengan sentral cabang dari perusahaan dengan tunnel VPN yang dapat mengubah setup network pada laptop nya, jadi jalur jaringan nya dikirim melalui tunnel. Sekali OpenVPN dibangun dengan sebuah tunnel, sentral firewall pada cabang sentral perusahaannya dapat menjaga laptop, walaupun bukan mesin local. Hanya satu port jaringan harus dibuka untuk jaringan local (missal, pelanggan) oleh field worker. Pengusaha dijaga oleh sentral firewall ketika dia dikoneksikan ke VPN.

3. Koneksi OpenVPN di tunnel melalui hampir setiap firewall: jika kamu mempunyai akses internet dan jika kamu dapat mengakses website HTTP, tunnel OpenVPN seharusnya bekerja.
4. Konfigurasi proxy dan pendukungnya: OpenVPN mempunyai proxy pendukung dan dapat di konfigurasikan untuk bekerja sebagai TCP atau UDP, dan sebagai server atau client. Sebagai server, OpenVPN menunggu hingga koneksi permintaan client. Sebagai client, OpenVPN mencoba untuk mendirikan sebuah koneksi meliputi konfigurasinya.
5. Satu port pada firewall harus dibuka mengikuti koneksi yang dating.
   Sejak openVPN 2.0, mode server yang special mengikuti koneksi multiple incoming pada port TCP atau UDP, yang mana masih menggunakan konfigurasi yang berbeda untuk setiap koneksi single.
6. Interface virtual mengikuti jaringan specific dan rules firewall : semua rules,restriction, mekanisme forwarding dan konsep seperti NAT dapat digunakan dengan tunnel OpenVPN.
7. Flexibility tinggi dengan posibiliti catatan extensive : OpenVPN menawarkan jumlah point selama koneksi set up untuk memulai script individual. Script ini dapat digunakan untuk varietas dengan tujuan dari autentifikasi untuk failover dan lebih.
8. Transparent, mendukung performance tinggi untuk Ip dynamic : Dengan menggunakan openVPN, disana tidak membutuhkan apapun untuk menggunakan IP statistic pada sisi lainnya pada tunnel. Antara tunnel endpoint dapat mempunyai akses DSL yang murah dengan IP dynamic dan pengguna akan mencatat dengan jarang perubahan pada IP di sisi lain. Antara terminal server session windows dan session Secure Shell (SSH) hanya akan kelihatan untuk hang untuk beberapa detik, tetapi tidak akan diakiri dan akan membawa permintaan aksi setelah pause short.
9. Tidak masalah dengan NAT : antara server OpenVPN dan client didalam jaringan menggunakan alamat IP private. Setiap firewall dapat digunakan untuk mengirim traffic tunnel untuk tunnel endpoint lainnya.
10. Instalasi simple pada tiap platform : antara instalasi dan penggunaan incredibly simple. Untuk spesialnya, jika kita telah berusaha men set up koneksi IPsec

dengan implementasi yang berbeda, kamu akan menemukan OpenVPN yang menarik.

11. Design Modular : Design modular dengan antara high degree pada simplicity antara disecurity dan networking adalah outstanding. Tidak ada solusi openVPN dapat menerima range yang sama pada possibility pada level security.

Sejarah OpenVPN

Menurut interfiew pada http://linuxsecurity.com diplubikasikan di 2003, James Yonan akan traveling pada central Asia di hari 9/11, 2001 dan mengkoneksikan ke kantor mereka melebihi Asia atau kepemilikan internet Rusia.

Fakta bahwa koneksi akan dibangun oleh server di negara dengan kondisi keamanan yang meragukan membuatnya lebih dan lebih sadar akan dan perhatian terhadap isu keamanan. Risetnya membawa pengertian yang mendalam bahwa terdapat dua main stream pada VPN teknologi, yang satu mempromosikan keamanan dan yang lainnya kemudahan penggunaan. Tidak satu pun dari solusi-solusi tersediapada saat itu ditawarkan suatu ideal blend dari kedua obyektif. IPsec dan keseluruhan dari implementasi itu sulit untuk di-set up, tetapi ditawarkan keamanan yang dapat diterima. Tetapi struktur yang komplek membuatnya peka terhadap penyerangan, bugs, dan kekurangan keamanan. Oleh karena itu, jaringan mendekati Yonan ditemukan pada beberapa solusi penggunaan terlihat lebih rasional, menuntunnya pada suatu modul jaringan modular menggunakan perangkat jaringan virtual TUN/TAP yang disediakan oleh kernel Linux.

“Setelah beberapa study pada open source VPN, kesimpulanku adalah “usability first” camp merupakan ide yang tepat tentang jaringan dan inter-network tunneling, dan SSH, SSL/TLS, dan IPsec mempunyai level yang sesuai dari keseriusan ke arah isu crypto. Ini adalah konsep dasar starting point untuk pekerjaanku pada OpenVPN.”

James Yonan pada sebuah linuxsecurity interview, 10 November 2003.

(http://www.linuxsecurity.com/content/view/117363/49/)

Pemilihan perangkat TUN/TAP sebagai networking model dengan seketika menawarkan fleksibilitas dimana solusi VPN yang lain tidak bisa menawarkan. Sementara SSL/TLS berbasis VPN perlu suatu browser untuk menetapkan koneksi,

Openvpn akan menyiapkan hampir riil (namun sebetulnya) perangkat jaringan, terpasang dimana hampir semua aktivitas networking bisa dilakukan.
Yonan kemudian memilih nama Openvpn berkenaan dengan library dan program Openssl proyek dan oleh karena pesan yang jelas ini adalah open source dan software cuma-cuma.

OpenVPN Versi1

OpenVPN memasukkan peristiwa dari solusi-solusi VPN hanya pada 13 Mei 2001 dengan sebuah inisial pelepasan yang awalnya bisa hampir tidak ada celah untuk IP Packets di atas UDP dan hanya encrypt dengan kode Blowfish dan tanda SHA HMAC (agak mengamankan enkripsi dan menandai metoda-metoda). Versi ini telah dinomori 090 yang kelihatannya ambisius, karena hanya versi (091) mengikuti dalam 2001, menawarkan dan memperluas dukungan enkripsi. Karena dukungan SSL/TLS, para pemakai mau tidak mau harus menunggu hampir satu tahun setelah pelepasan; pembebasan yang pertama. Versi 10 diluncurkan pada bulan Maret 2002 dan menyediakan SSL/TLS-based pengesahan dan pergantian kunci. Versi ini adalah juga pertama untuk berisi dokumentasi dalam suatu manpage.
Lalu, OpenVPN dikembangkan dengan mengambil kecepatan. Hanya lima hari kemudian, versi 1.0.2 diluncurkan , yang adalah versi yang pertama dengan adaptasi-adaptasi untuk Redhat Package Manager (sistem RPM)-BASED. Dari versi ini peluncuran ini kemudian diterbitkan hampir secara teratur setiap empat sampai delapan minggu.
Tabel berikut ini memberi satu ikhtisar dari peluncuran dan daftar tanggal dari versi-versi ketika fitur pilihan ditambahkan kepada versi 1x OpenVPN. Untuk detil dapat dilihat di dalam bagian-bagian Changelog situs web OpenVPN pada http://openvpn.net/changelog.html dan pelepasan; pembebasan mencatat pada http://openvpn.net/relnotes.html

Tanggal	Versi	Kejadian penting
13 – 5 - 2001	0.90	Pelepasan awal, dengan hanya sedikit fungsi-fungsi seperti protokol internet (di) atas UDP, dan hanya dengan satu mekanisme encrypsi
26 –12 -2001	0.91	Penambahan mekanisme encrypsi
23-3-2002	1.0	Pengesahan dan penambahan kunci penukaran TLS-BASED pada halaman manual pertama.
28-3-2002	1.0.2	Bugfixes dan perbaikan-perbaikan, terutama karena sistem yang rpm-based seperti Redhat
9-4-2002	1.1.0	Dukungan diperluas untuk TLS/SSL Pengetaman lalu lintas ditambahakn Pertama kali OpenBSD port Perlindungan pengulangan diperluas membuat OpenVPN lebih terjamin
22-4-2002	1.1.1	Perbaikan lebih lanjut Documentation (manpage) Pilihan-pilihan untuk konfigurasi yang otomatis suatu jaringan OpenVPN
22-5-2002	1.2.0	Ketidakaktifan untuk mengendalikan fitur File konfigurasi mendukung ditambahkan SSL/TLS sebagai latar belakang proses panjang menyetem berbagai port-port ditambahkan (Solaris, OpenBSD, Mac OSX, x64) Memperbaiki situs web, termasuk "howto" Instalasi tanpa automake yang mungkin
12-6-2002	1.2.1	Biner RPM file untuk instalasi di sistem Redhat-based disediakan Perbaikan-perbaikan yang intensive di penanganan isyarat dan manajemen kunci di restart. Dukungan untuk daya penggerak berubah di dalam kemasan-kemasan yang datang/berikutnya seperti IPs dinamis. Dukungan ditambahkan untuk identitas penurunan setelah installation—OpenVPN dapat dijalankan dengan pengguna yang tidak khusus.

10-7-2002	1.3.0	"Housekeeping Releases": Bugfixes, sedikit ditambahkan, dan fitur- fitur baru ;sekarang bekerja dengan OpenSSL 0.9.7 Beta 2
10-7-2002	1.3.0	SAMA
23-10-2002	1.3.2	NetBSD port Dukungan untuk instantiasi inetd/xinetd di bawah Linux Bangunan sederhana sertifikat untuk SSL/TLS ditambahkan. Dukungan untuk IPv6 (di) atas TUN ditambahkan.
7-5-2003	1.4.0	Perbaikan dari perlindungan pengulangan (keamanan) Numerous bugfixes, perbaikan-perbaikan, dan penambahan-penambahan
15-5-2003	1.4.1	Dukungan perbaikan untuk kernel 24
15-7-2003	1.4.2	Pertama kali permulaan port Windows (tetapi kehilanagn Windows kemel driver) Gentoo init script
4-8-2003	1.4.3	Peluncuran Bugfix Penarikan kembali daftar settifikat.
20-11-2003	1.5.0 dan versi 1.4 beta sebelumnya	TCP support Port Windows 2000 dan XP, termasuk Win32 telah diinstal. Peningkatan Check yerhadap jumlah parameter Penambahan proxy support Perluasan fungsi routing Memperbaiki dukungan TLS , fitur kunci dan nol; perluasan kode. Dukungan Proxy SOCKS.

9-5-2004	1.6.0	Berbagai perbaikan-perbaikan di jaringan windows Dinamic Host Configuration Proticol(DHCP). Berbagai bugfixes

OpenVPN Versi 2

Paralel untuk perbaikan dan pengembangan dari versi OpenVPN 1, tempat ujian untuk versi OpenVPN 2 adalah buatan Nopember 2003, dan Pada Bulan Februari 2004, versi 20-test3 pada awalnya mempersiapkan gol dari suatu server multi-client untuk OpenVPN. Server multi-client ini adalah salah satu fitur terkemuka dari OpenVPN hari ini, beberapa klien-klien dapat disambungkan ke server VPN di port yang sama. Di Pebruari 22, 2004, kedua cabang pengembangan 16-beta7 dan 20-test3 digabungkan dan pengembangan lebih lanjut dilanjutkan di dalam versi 2's cabang.

Ada sedikitnya dari 29 versi memberi label sebagai "test" versi-versi, 20 versi beta, dan 21 calon pelepasan, pembebasan, sampai di April 17, 2005, OpenVPN versi 20 bisa dibebaskan; dilepaskan. Ini terjadi karena nomor yang besar dari pengembang-pengembang yang mendukung proyek, bug-bug perbaikan, dan meningkat;kan kinerja dan stabilitas untuk selamanya.

Daftar yang berikut akan memberi suatu ikhtisar yang singkat dari fitur yang baru yang ditambahkan pada versi OpenVPN 2:

1. Multi-client dukungan: OpenVPN menawarkan suatu modus koneksi yang khusus, di mana klien-klien TLS-authenticated (di-blacklist di CRL) disiapkan dalam bentuk DHCP-style dengan IPs dan networking (tunnel) data. Perjalanan

ini, beberapa tunnel (sampai dengan 128) dapat dikomunikaskan di atas port TCP protokol atau UDP yang sama. Sungguh, suatu modus layanan server yang perlu diaktifkan.

2. Push/pull pilihan: susunan Network dari klien-klien dapat dikendalikan oleh server. Setelah susunan suatu tunnel sukses, server itu dapat mengatakan kepada klien (kedua-duanya Windows dan Linux) untuk menggunakan suatu susunan jaringan yang berbeda dengan segera.
3. Suatu antar muka manajemen (Telnet) ditambahkan.
4. Windows driver dan perangkat lunak telah diperbaiki secara luas.

Jaringan dengan OpenVPN

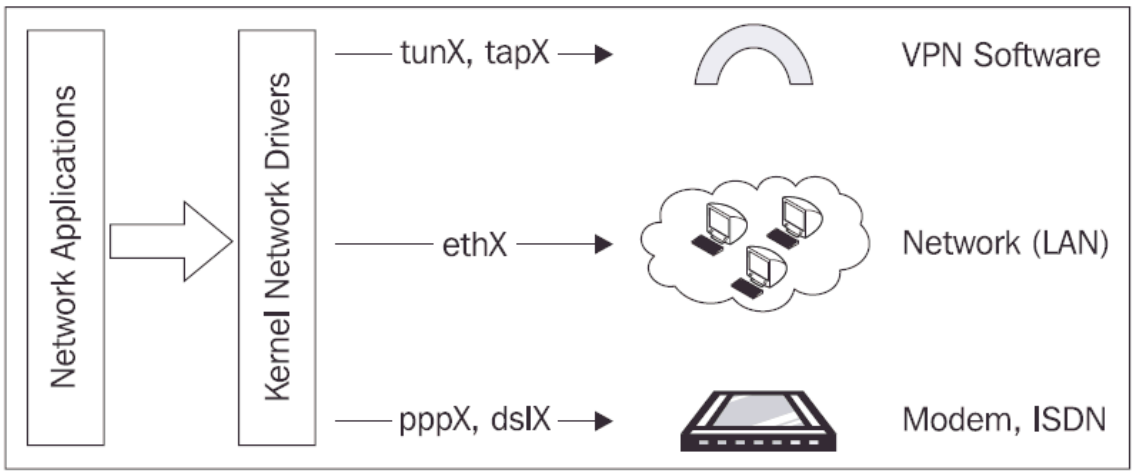
Struktur yang modular dari OpenVPN tidak hanya bisa ditemukan dalam model keamanannya, tetapi terdapat juga di dalam rencana jaringan. James Yonan memilih driver Universal TUN/TAP untuk lapisan networking dari OpenVPN.

TUN/TAP driver adalah sebuah proyek sumber terbuka yang tercakup di semua distribusi-distribusi Linux/UNIX yang modern seperti juga Windows dan Mac OS X. Seperti SSL/TLS yang digunakan di dalam banyak proyek, karena itu dapat memperbaiki dengan baik, dan fitur baru sedang ditambahkan. Dengan menggunakan alat-alat TUN/TAP, dapat menyingkirkan banyak kompleksitas dari struktur OpenVPN. Struktur sederhananya membawa keamanan yang lebih baik dibandingkan dengan solusi-solusi VPN yang lain. Kompleksitas adalah musuh utama dari keamanan. Sebagai contoh, IPSEC mempunyai suatu struktur kompleks dengan modifikasi-modifikasi yang kompleks di dalam kernel dan tumpukan protokol internet, dengan demikian menciptakan banyak lubang kecil di dinding keamanan yang mungkin terjadi.

Universal Driver TUN/TAP dikembangkan untuk menyediakan dukungan Linux kernel untuk membangun terowongan protokol internet lalu lintas. Hal ini merupakan suatu antar muka jaringan maya, yang kelihatan sebagai asli kepada semua aplikasi dan para pemakai, hanya nama tunX atau tapX mencirikan adanya alat-alat lainnya. Setiap aplikasi yang mampu menggunakan suatu antar muka jaringan dapat menggunakan antar muka terowongan. Setiap teknologi yang sedang anda jalankan di dalam jaringan, dapat berjalan di suatu TUN atau TAP.

Driver ini adalah salah satu faktor utama dalam kemudahan memahami pembuatan OpenVPN, mudah dalam pengaturan, dan keamanan pada waktu yang sama.

Gambar berikut menjelaskan tentang OpenVPN menggunakan interface baku:\



Sebuah TUN device dapat digunakan sebagai suatu antar muka point-to-point yang maya, seperti suatu modem atau DSL mata rantai. Ini disebut routed mode, karena rute-rute disiapkan kepada mitra VPN.

Suatu TAP device, bagaimanapun, dapat digunakan seperti suatu adapter Ethernet yang maya. Hal ini memungkinkan mendengarkan daemon yang terhubnug pada Frame eternet, yang bukanlah mungkin dengan alat-alat TUN. Modus ini disebut modus penghubung karena jaringan itu dihubungkan seolah-olah di atas suatu jembatan perangkat keras.

Aplikasi-aplikasi dapat dibaca atau ditulis pada antar muka ini, perangkat lunak (tunnel driver) akan mengambil semua data dan menggunakan pustaka-pustaka yang cryptographic dari SSL/TLS ke encrypt mereka. Data itu dibungkus dan dikirim kepada yang lain yang merupakan akhir dari tunnel. Pengemasan ini dilakukan atas standardisasi UDP atau paket-paket TCP protokol kendali transmisi opsional. UDP merupakan pilihan pertama, tetapi TCP protokol kendali transmisi dapat sangat menolong dalam beberapa hal. Anda hampir dengan sepenuhnya bebas untuk memilih parameter-parameter konfigurasi seperti angka-angka protokol atau port, sepanjang kedua-duanya tujuan tunnel sepakat menggunakan gambar-gambar yang sama.

OpenVPN mendengarkan alat-alat TUN/TAP, mengambil lalu lintas, encryptsnya, dan mengirimkan kepada mitra VPN yang lain, di mana proses OpenVPN yang lain

menerima data, deskripsi, dan menyampaikannya kepada alat jaringan maya, di mana kekuatan aplikasi itu sedang menantikan data.

Sejauh yang saya ketahui, tidak ada VPN Software yang lain yang memungkinkan VPN para mitra untuk memancarkan. Konsep ini menawarkan berbagai kemungkinan berlimpah:

a. Siarkan yang diperlukan karena menelusuri jaringan Windows atau untuk LAN Games
b. Non-ip paket-paket seperti IPX dan hampir semuanya yang ada dalam LAN Anda dapat mengirimkan kepada VPN itu kepada sisi yang lain

Dan karena OpenVPN menggunakan paket-paket jaringan standar, NAT juga tidak bermasalah. Suatu tuan rumah di dalam jaring lokal di Sydney dengan suatu protokol internet lokal dapat memulai suatu tunnel kepada tuan rumah yang lain di dalam jaring yang lokal di London, yang juga dilengkapi dengan protokol internet lokal.

Tetapi ada kelebihan lain. Karena antar muka jaringan dilakukan dengan standardisasi Linux, antar muka jaringan (TUN atau TAP), apapun yang mungkin di satu Ethernet NIC bisa dilakukan di VPN Tunnels:

a. Firewall-firewall dapat membatasi dan mengendalikan lalu lintas.
b. Pengetaman lalu lintas bukanlah hanya yang mungkin, tetapi ini juga suatu fitur bahwa OpenVPN membawa serta.

Jika anda juga menginginkan untuk menggunakan bentuk DSL dengan seringnya menyambung kembali dan secara dinamis menugaskan IPs, OpenVPN akan menjadi pilihan pertama. Menyambung kembali ahan lebih cepat daripada menggunakan segala perangkat lunak VPN yang lain yang sudah diuji, suatu server terminal Windows atau SSH sesi tidak berakhir/mengakhiri selagi salah satu dari para mitra VPN mengubah protokol internetnya, sesi hanya membekukan untuk beberapa detik dan lalu anda dapat melanjutkan. Dapatkah VPN memenuhi itu?

OpenVPN dan Firewall

OpenVPN bekerja dengan sempurna dengan firewall. Ada beberapa solusi VPN untuk dapat memiliki suatu dukungan firewall yang serupa, tetapi tidak ada yang dapat menawarkan yang sama tingkat keamanan.

Apa yang sesungguhnya firewall? Ada suatu definisi sederhana dan yang terkenal: Suatu firewall adalah suatu penerus bahwa tidak mengarahkan. Jika anda mempertimbangkan, menganggap ini sangat tidak menolong, di sini ada suatu definisi yang lebih:

Suatu firewall adalah sekedar penerus untuk mengarahkan data Internet yang terpilih. Firewall memerintah menggambarkan bagaimana caranya menangani data dan lalu lintas spesifik.

Firewall merupakan alat atau perangkat lunak di PC, server-server, atau di alat-alat yang lain. Suatu firewall memperhatikan data yang diterima dan melihatnya lebih dekat. Firewall modern adalah yang disebut penyaringan paket, stateful firewall pemeriksaan. Tergantung pada lapisan OSI mana beroperasi, firewall itu dapat melewati keputusan-keputusan yang didasarkan pada data yang ditemukan di dalam judul dari data paket-paket atau aplikasi. Firewall penyaringan paket biasanya dioperasikan dengan membaca judul data protokol internet, stateful pemeriksaan adalah suatu mekanisme untuk mengingat tempat asal koneksi. Dengan cara ini, jaringan yang internal dapat dilindungi dari jaringan eksternal, dan selagi koneksi-koneksi Internet memulai dari di dalam dapat diizinkan, semua koneksi-koneksi yang tak dikehendaki, yang tidak syah dari luar dapat ditolak. Pada waktu yang sama, data yang datang yang diminta oleh seorang anggota jaringan yang lokal, dapat dilewatkan (karena firewall mengingat status tempat asal dari permintaan).

Di Bawah Linux, kebanyakan firewall didasarkan pada program iptables. Ini adalah ruang bagi pengguna untuk terhubung ke Linux, kemampuan firewall netfilter kernel, dan menawarkan segala firewall modernn yang diperlukan. Mungkin cara terbaik untuk melindungi LAN anda adalah dengan penulisan satu set perintah iptables dengan suatu script. Bagaimanapun, script seperti itu tidaklah sempurna. Kebanyakan pengurus-pengurus menghendaki suatu Graphical User Interface (GUI) karena kendali firewall, dan semua firewall perangkat keras menawarkan hal ini. Satu proyek yang terkemuka untuk tujuan ini dan Linux firewall (iptables) adalah proyek Shorewall (Shoreline Firewall). Itu mengintegrasikan ke dalam Webmin suite yang berbasis web awal dan akhir untuk mengurus Linux sistem dari suatu browser. Proyek Shorewall sudah

menulis suatu petunjuk tentang pengintegrasian tunnel-tunnel OpenVPN ke dalam Shorewall dan lebih jelas dapat dilihat pada http://www.shorewall.net/OPENVPN.html.

IPCOP adalah suatu peluang mandiri, easy-to-configure Linux sistim firewall juga dilengkapi dengan suatu profesional GUI. Standarisasi peng-instalasiani, struktur sederhana, dan pasang tambah modular membuat suatu proyek tumbuh dengan cepat. Beberapa perusahaan sedang mengembangkan alat-alat perangkat keras berdasar pada IPCop, dan proyek open-source Zerina yang berhubungan dengan pengintegrasian OpenVPN: http://home.arcor.de/u.altinkaynak/openvpn.html

Mengkonfigurasi OpenVPN

Hingga kini anda sudah melihat OpenVPN itu mempunyai suatu keaman dan pendekatan keamanan sehingga mudah digunakan dan suatu model jaringan yang fleksibel. Sebagai konsekwensi, suatu sintaksis konfigurasi yang sangat sederhana dan dokumentasi baik menandai antarmuka pengguna OpenVPN. Konfigurasi dilaksanakan dengan editing suatu file teks yang sederhana; sintaksis adalah sama di setiap sistim operasi. Di sini dijelaskan satu contoh dari suatu konfigurasi yang sederhana dari 13 bentuk file yang ada :

```
remote feilner-it.dynalias.net
float
dev tun
tun-mtu 1500
ifconfig 10.79.10.1 10.79.10.2
secret my_secret_key.txt
port 5050
route 10.94.0.0 255.255.0.0 10.79.10.2
comp-lzo
keepalive 120 600
resolv-retry 86400
route-up "/sbin/firewall restart"
log-append /var/log/openvpn/ultrino.log
```

Suatu baris perintah antar muka mengizinkan anda untuk memulai tunnel sesuai keinginan anda, yang sangat bermanfaat ketika anda sedang menguji susunan-susunannya. Parameter-parameter yang sama seperti di file konfigurasi ditambahkan kepada baris perintah, dan tunnel itu dimulai.

Di dalam sebutan modus server, OpenVPN dapat mendorong berbagai data konfigurasi kepada klien-klien melalui tunnel. Tunnel ganda dapat berjalan di port-nya dalam bentuk tunggal, menggunakan protokol UDP atau TCP. OpenVPN dapat di-tunnel melalui firewall dan wakil-wakilnya, jika mereka mengizinkan koneksi0koneksi HTTPS, dan server itu dapat mengatakan kepada klien untuk menggunakan tunnel sebagai rute asli pada Internet.

Hal ini menawarkan suatu variasi yang sangat besar dari berbagai kemungkinan, anda dapat mempunyai satu port yang dapat terhubung ke jaringan manapun mereka disambungkan. Ini adalah port OpenVPN terbiasa dengan sambungkan ke server VPN. Begitu menghubungkan, semua lalu lintas Internet dari sebuah laptop dapat ditaklukkan via jaringan dari sebuah perusahaan, ke tunnel VPN yang disambungkan. Dengan cara ini firewall perusahaan tersebut dapat juga melindungi para pengguna. Seorang pengguna adalah seorang anggota suatu perkumpulan (atau suatu jaringan perusahaan) siapa yang sedang bekerja di luar perusahaan itu dan sambungkan ke koneksi-koneksi jaringan yang sering digunakan yang berbeda via. Suatu pengguna yang khas bisa suatu salesman atau wanita pelayan toko dengan laptop-nya, yang perlu untuk mengakses sumber daya perusahaan itu dari jaringan pelanggan-nya.

Permasalahan dengan OpenVPN

OpenVPN mempunyai beberapa kelemahan-kelemahan:

1. Tidak memiliki IPsec yang dapat dipertukarkan, dan IPsec adalah patokan VPN solusi. Banyak alat-alat seperti Cisco atau Bintec menggunakan IPsec dan dapat disambungkan ke aplikasi-aplikasi lain atau perangkat lunak IPsec klien. Sedikitnya mereka harus bisa, karena dalam praktek banyak pabrik cenderung untuk mengembangkan perluasan-perluasan kepemilikan mereka sendiri pada IPsec, implementasi-implementasi buatan mereka yang pada kenyataannya tidak cocok/bertentangan dengan alat-alat IPsec yang lain.

2. Ada sedikit orang yang mengetahui bagaimana caranya menggunakan OpenVPN, terutama di dalam skenario yang sulit. Maka jika anda membaca, anda dapat memperoleh suatu keahlian yang mahal.
3. Tidak ada kerja GUI untuk administrasi (tetapi ada beberapa proyek-proyek peluang).
4. Dewasa ini, anda hanya dapat disambungkan ke komputer-komputer lain. Tetapi ini sedang mengalamin perubahan, ada beberapa perusahaan yang bekerja di alat-alat dengan klien-klien OpenVPN yang terintegrasi.

Ketika Anda dapat melihat, kelemahan-kelemahan utama dari OpenVPN adalah ketidakcocokan pada IPsec dan ketiadaan pengetahuan publik tentang fitur dan perangkat keras. Pada awalnya mungkin akan tidak berpengaruh, karena arsitektur-arsitektur berbeda terlalu banyak, tetapi yang selanjutnya akan sangat berpengaruh.

Perbandingan OpenVPN dengan IPSec VPN

Meskipun IPsec adalah tidak standard facto, ada banyak argumentasi untuk menggunakan OpenVPN. Jika anda ingin meyakinkan manajemen anda sekitar mengapa cabang dari jaringan anda harus dihubungkan melalui OpenVPN sebagai ganti IPsec VPN, tabel yang berikut dapat membantu argumentasi anda (poin-poin yang didahului oleh "+"adalah keuntungan-keuntungan dan poin-poin yang didahului oleh "-"adalah kerugian-kerugian):

IPsec VPN	OpenVPN
+ The standard VPN technology	- Still rather unknown, not compatible with IPsec
+ Hardware platforms (devices, appliances)	- Only on computers, but on all operating systems. Exception are devices, where embedded UNIXs are running like OpenWrt and similar
+ Well-known technology	- New technology; still growing and rising
+ Many GUIs for administration	- No professional GUI; however, there are some interesting and promising projects
- Complex modification of IP stack	+ Simple technology
- Critical modification of kernel necessary	+ Standardized network interfaces and packets
- Administrator privileges are necessary	+ OpenVPN Software can run in user space, and can be chroot-ed
- Different IPsec implementations of different manufacturers can be incompatible	+ Standardized encryption technologies

IPsec VPN	OpenVPN
- Complex configuration, complex technology	+ Easy, well-structured, modular technology, easy configuration
- Steep learning curve for newbies	+ Easy to learn, fast success for newbies
- Several ports and protocols in firewall necessary	+ Only one port in firewall necessary
- Problems with dynamic addresses on both sides	+ DynDNS works flawlessly, faster reconnects
- Security problems with IPsec technologies	+SSL/TLS as industry-standard cryptographic layer
	+ Traffic shaping
	+ Speed (up to 20 Mbps on a 1Ghz machine)
	+ Compatibility with firewalls and proxies
	+ No problems with NAT (both sides can be in NATed networks)
	+ Possibilities for **road warriors**

Mungkin argumentasi terbaik adalah bahwa anda dapat menggunakan kedua-duanya solusi-solusi VPN di dalam paralel, sedikitnya jika anda sedang menggunakan Linux atau suatu aplikasi Linux-based. Karena pendekatan yang berbeda kepada networking, tidak ada perbedaan antara kedua sistem.

Sumber Bantuan dan Dokumentasi

Jika anda ingin belajar lebih banyak tentang OpenVPN (saya bertaruh anda akan), ada banyak sumber daya di dalam Internet. Situs web, daftar alamat, forum-forum, dan halaman-halaman pribadi dari OpenVPN keluar dapat ditemukan. Google menemukan lebih dari tiga juta yang ada "open vpn". Hal ini daftar kursus tidak bisa melengkapi, tetapi di sini anda akan menemukan sambungan dengan situs web yang sangat menolong saya ketika saya memulai dengan OpenVPN dan di mana saya masih mencari bantuan hari ini.

Komunitas Proyek

OpenVPN proyek mempunyai situs web sendiri, termasuk download-download dari versi-versi dan pembaruan, dokumentasi, howtos, daftar alamat, dan sambungan dengan berbagai VPN-related halaman. Suatu halaman proyek dapat dengan susah menjadi lebih baik dibandingkan dengan OpenVPN. Anda akan menemukannya pada http://openvpn.net/.

Sumber yang paling penting untuk menjadi bantuan adalah daftar alamat: http://openvpn.net/mail.html.

Karena kita sedang menggunakan SSL/TLS untuk enkripsi yang dimaksud, anda pasti ingin memahami toolkit ini. Situs web pustaka-pustaka SSL/TLS Cryptographic menyediakan dokumentasi dan daftar alamat yang terperinci, yang dapat ditemukan pada http://www.openssl.org/.

Situs web dari TLS Charter oleh TLS Working Group menyediakan suatu daftar dengan banyak RFCs dan Internet yang terkait dengan draft anda yang akan dianggap sangat menolong: http://www.ietf.org/html.charter/tls-charter.html.

Driver Universal TUN/TAP dapat downloaded dari halaman yang berikut: http://vtun.sourceforge.net/tun/. Meskipun demikian, ini tidak harus perlu karena setiap distribusi yang modern (dan kernel) perlu mempunyai fitur berikut ini. Tetapi FAQ dari proyek ini bisa sangat menolong untuk berbagai pertanyaan-pertanyaan.

Dokumentasi di dalam Paket Software

Jika anda menginstal OpenVPN dari paket-paket yang biner untuk distribusi anda, anda akan memiliki standard dokumentasi di dalam direktori yang berikut:

Distribution	Path to Documentation
Debian	`/usr/share/doc/openvpn`
SuSE	`/usr/share/doc/packages/openvpn`
Redhat	`/usr/share/doc/openvpn-2.0`
Windows	only online Documentation

Distribusi-distribusi lain mungkin punya lokasi-lokasi yang berbeda; periksa sistem paket manajemen anda secara detail. Sistem RPM-BASED memberi daftar semua file kepunyaan suatu yang spesifik membungkus ketika anda mengetik `"rpm -ql openvpn"` sebagai pengguna yang hebat. Sistem Debian-based (seperti Ubuntu) perlu

memberi informasi yang sama ketika masuk root "`dpkg -L openvpn`". Hanya menggantikan openvpn dengan nama dari paket, anda ingin install.

Paket source program (tarball) berisi beberapa READMEs dan file dokumentasi. Hanya ditelusuri melalui direktori di mana anda menyadap OpenVPN. Dan jika anda tertarik, mempunyai hampir sebagian dari source file program, pengembangan comment bisa merupakan suatu yang besar membantu ke arah memahami kerendahan dari software!

Ringkasan

OpenVPN menawarkan berbagai kemungkinan besar; terutama konsep networking mengizinkan susunan-susunan sangat transparan dengan firewall-firewall atau di dalam konfigurasi-konfigurasi warrior. James Yonan, pendiri sudah membuat keputusan-keputusan sangat baik ketika mempercayai driver jaringan TUN/TAP dan pustaka-pustaka SSL/TLS. OpenVPN pertama diterbitkan dalam 2001; versi 2 muncul dalam 2005 dan fitur penawaran maju lebih jauh dibanding versi-versi sebelumnya. Multi-client dukungan, versi Windows, dan opsi push/pull hanyalah sebagian dari fitur nya. OpenVPN mudah untuk mengatur dan hanya mempunyai beberapa kelemahan-kelemahan, paling serius yang mana ketidakcocokannya pada IPsec. Tetapi untuk menyebut suatu kelemahan ini adalah suatu putusan, jika itu dibandingkan dengan IPsec seperti yang dilaksanakan di dalam bab ini. IPSEC masih ada standard, tetapi OpenVPN mempunyai lebih jauh fitur pada suatu tingkatan keamanan yang jauh lebih baik.

Bab 4
Menginstal OpenVPN

Menerapkan OpenVPN itu mudah dan platform mandiri. Dalam bab ini kita akan menginstalnya pada Windows, Mac OS X, Linux versi berbeda, dan FreeBSD. Lebih dari itu. Lagipula, kita akan mengcompile source code yang disediakan oleh project Openvpn dan memungkinkan jaringan yang dibutuhkan mendukung perangkat TUN/TAP dalam kernel anda. Kita akan mulai dengan instalasi grafis di bawah Windows, Mac OS X, dan SuSE, dan diakhiri dengan membangun OpenVPN versi kita sendiri dari source program, termasuk isyarat untuk konfigurasi dari suatu kernel individu.

Prasyarat

Beberapa prasyarat harus dipenuhi jika anda ingin menginstal Openvpn pada sistem anda. Para pemakai Windows harus menggunakan Windows 2000 atau XP; Mac Os X diperlukan pada platform Apple. Ini semua yang diperlukan untuk sistem operasi ini, tetapi Linux/Unix sistem harus temu permintaan berikut :

1. **Sistem anda harus mendukung untuk driver Universal TUN/TAP :**

   Kernel yang lebih baru dari versi 2.4 dari hampir semua distribusi modern Linux mendukung untuk perangkat TUN/TAP. Hanya jika anda menggunakan suatu distribusi lama atau jika anda telah membangun kernel anda sendiri, anda harus menambahkan support ini ke konfigurasi anda. Bagian dari bab ini Enabling Linux Kernel Support for TUN/TAP Devices, berhadapan dengan masalah ini. Website dari project ini dapat ditemukan pada: http://vtun.sourceforge.net/tun/.

2. **Library OpenSSL harus telah diinstal pada system anda :**

   Saya belum menemukan sistem modern Linux/Unix yang tidak temu kebutuhan ini. Bagaimanapun, jika anda ingin menyusun Openvpn dari source program, paket pengembangan SSL mungkin perlu. Website adalah: http://www.openssl.org/

3. **Library Lempel-Ziv-Oberhumer (LZO) Compression harus diinstal :**

   Dan lagi, sistem Linux/Unix yang paling modern menyediakan paket ini, maka tidak akan ada masalah. LZO adalah suatu library kompresi real-time yang digunakan oleh Openvpn untuk memampatkan data sebelum pengiriman. Paket dapat ditemukan pada http://openvpn.net/download.html, website dari proyek ini adalah: http://www.oberhumer.com/opensource/izo/.

Kebanyakan Linux/Unix tools instalasi sistem bisa memecahkan yang disebut ketergantungan terpasang mereka sendiri, tetapi itu bisa sangat menolong untuk mengetahui di mana untuk mendapatkan perangkat lunak yang diperlukan itu.

Memperoleh Software

Pada dasarnya, instalasi Openvpn bisa dilakukan dalam salah satu cara berikut :

1. Untuk sistem operasi Microsoft Windows, anda harus mendownload file binary. exe dari http://openvpn.net/download.html atau paket berisi graphical user interface dari http://openvpn.se/.
2. Pada Macintosh sistem yang menjalankan Mac OS X, ada suatu graphical installation wizard dan manajemen tool disebut Tunnelblick.
3. Sistem Linux yang paling komersil, seperti Suse, menyediakan tools instalasi seperti Yet Another Setup Tools (Yast) dan berisi versi Openvpn terbaru pada media instalasi (CD atau DVD). Lagipula, sistem yang didasarkan pada software RPM dapat juga menginstal dan mengatur software Openvpn pada command line.
4. Sistem Linux seperti Debian menggunakan paket manajemen canggih yang dapat menginstal perangkat lunak yang disediakan oleh tempat penyimpanan pada server jaringan. Tidak ada media lokal diperlukan; manajemen paket akan memecahkan ketergantungan potensi dirinya sendiri dan menginstal versi Openvpn terbaru atau yang paling aman.
5. FreeBSD (seperti sistem BSD yang lain).
6. Seperti semua project open source, source code Openvpn disediakan untuk download. Kompresan tar.gz atau tar.bz2 dapat didownload dari

http://openvpn.net/download.html dan dibongkar ke suatu direktori lokal. Source code ini harus diatur dan diterjemahkan (di-compile) untuk sistem operasi anda.

7. Anda dapat juga menginstal unstabil, pengembang, atau versi Openvpn yang lebih lama dari http://openvpn.net/download.html. Hal ini mungkin menarik jika anda ingin mengetes fitur baru versi mendatang.
8. Ekstraksi source code daily (unstable) Openvpn dapat diperoleh dari http://sourceforge.net/cvs/?group_id=48978. Di sini anda temukan Concurrent Versions System (CVS) repository, di mana semua Openvpn developer menempatkan perubahan mereka kepada file proyek.

Instalasi OpenVPN pada Windows

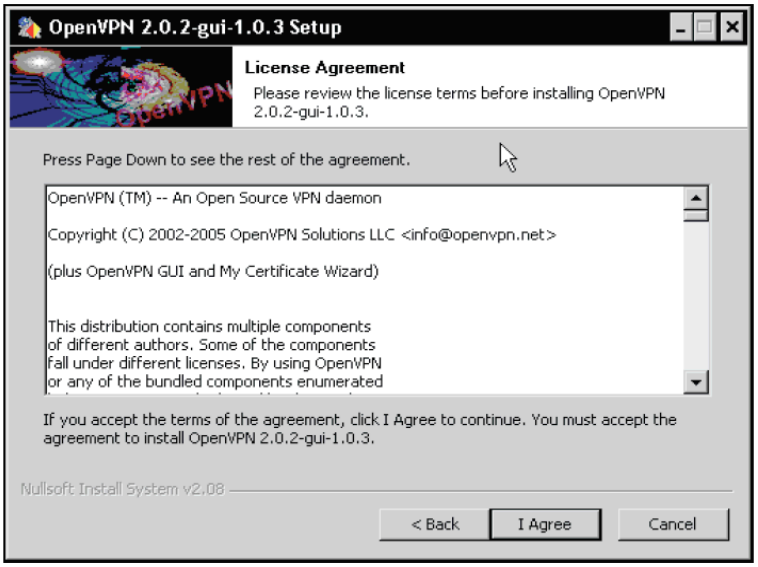
Jika anda ingin menginstall OpenVPN pada Windows, anda harus membuat suatu pilihan sebelum mendownload. Anda dapat menginstall software original OpenVPN dari http://openvpn.net/download.html atau (ini saranku) menginstall GUI OpenVPN dari http://openvpn.se/. Paket ini berisi software OpenVPN plus sebuah GUI untuk membawa atau menurunkan tunnel. Khususnya, jika anda men-set up sebuah client OpenVPN—sebuah laptop atau desktop PC dari pekerja rumahan, dimana dia hanya terkoneksi sementara ke VPN anda—pengguna Windows akan menginginkan suatu interface yang mudah digunakan dan clickable. Bagaimana pun juga, jika anda tidak ingin para pengguna berinteraksi dengan VPN tunnel, software original OpenVPN akan melakukannya.

OpenVPN dapat bekerja sebagai suatu service pada Windows PC, yang berarti OpenVPN dimulai secara otomatis pada startup. Dia dapat dikonfigurasi untuk enable tunnel secara otomatis atau didorong oleh sebuah klik dari mouse. Instalasinya cukup langsung saja dan tidak seharusnya di-pose problem apapun kepada pengguna Windows. Section berikut ini memberi anda suatu proses pemandu instalasi
Jika anda diprompt yang drivernya tidak melewati testing Windows Logo, klik pada **Continue anyway.**

Download dan Memulai Instalasi

Download versi terbaru dari OpenVPN GUI dari http://openvpn.se/ ke drive lokal anda. Log in sebagai administrator atau privileged user dan double-klik pada download file untuk mulai setup wizard. Jika anda menggunakan firewall, anda akan di-promp untuk mengijinkan OpenVPN diinstal dan dikoneksikan ke internet nanti.

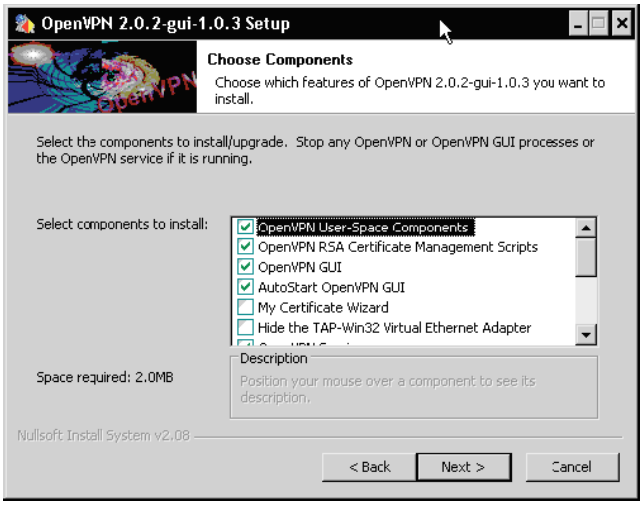
Instalasi wizard OpenVPN GUI, kemungkinan adalah cara paling konvenien untuk menginstal OpenVPN pada Windows, dimulai. Klik Next untuk memproses.



Meski OpenVPN dan OpenVPN GUI tersedia komplit di bawah open source General Public License (GPL), anda harus menerima license agreement. anda harus membaca liense-nya untuk memastikan bahwa rencana anda menggunakan OpenVPN cocok dengannya. Klik pada I Agree untuk melanjutkan.

Memilih Komponen dan Lokasi

Jendela dialog yang berikutnya menawarkan suatu pilihan di komponen OpenVPN, anda boleh menginstal. Dengan demikian pemilihan patokan komponen bisa dipahami di dalam hampir semua kasus-kasus.



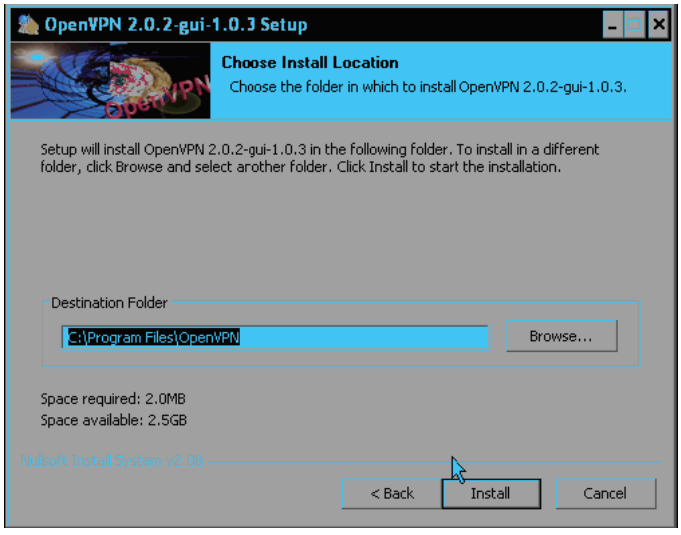
Di dalam dialog ini, anda mempunyai beberapa opsi untuk memilih. Meskipun jika anda secara normal tidak perlu untuk merubah di sini, tabel yang berikut memberi satu ikhtisar dari masukan-masukan dan ketika anda perlu menginstal fitur. Client Install adalah suatu sistem yang berkoneksi ke sistem OpenVPN lain, sedangkan Server Install itu adalah satu sistim OpenVPN yang mengizinkan koneksi-koneksi berikutnya.

Option	Feature	Client Install	Server Install
OpenVPN User-Space Components	The OpenVPN program	x	x
OpenVPN RSA Certificate Management Scripts	easy-rsa for Windows		x
OpenVPN GUI	The graphical user interface	x	
AutoStart OpenVPN GUI	Link for auto start	x	
My Certificate Wizard	Certificate requests for a certificate authority	x	
Hide the TAP-Win32 VEA	Interface is not shown in network setup		
OpenVPN Service	Configure OpenVPN as a service		x
OpenVPN File Associations	Configuration files (*.ovpn) are associated with OpenVPN	x	x
OpenSSL DLLs	Dynamic link libraries	x	x
TAP-WIN32 VEA	Virtual network interface	x	x
Add OpenVPN to PATH	openvpn.exe is in the path of every user's command line	x	x
Add Shortcuts to Start Menu	Shortcut to start menu	x	x

Versi-versi lebih baru juga termasuk opsi OpenSSL Utilities.

Seperti yang Anda lihat, satu-satunya perbedaan adalah RSA Management dan opsi untuk menjalankan OpenVPN sebagai suatu layanan. Keduanya dapat dikonfigurasi dengan makna yang berbeda, seperti file konfigurasi, Windows management sistem, atau software seperti xca dimana kita akan terbiasa untuk menghasilkan dan mengurus sertifikat-sertifikat.

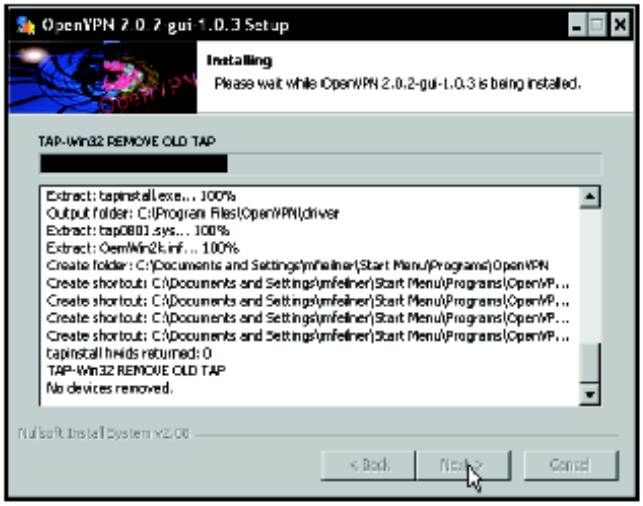
Tekan NEXT untuk melanjutkan instalasi.



Sekarang anda harus memilih satu direktori instalasi untuk OpenVPN. Alur standard instalasi dari OpenVPN under Windows adalah C:\Program Files\OpenVPN, dan ini perlu bekerja bagus di dalam hampir setiap kasus. Bagaimanapun, anda dapat menetapkan alur ini ketika Anda ijinkan. Setelah meng-klik Install, proses instalasi dimulai.

Menyelesaikan Instalasi

Sementara OpenVPN sedang diinstal, anda dapat membaca outputnya di dalam window instalasi dan mengikuti pembuatan folder, file-file, dan shortcut dan instalasi dari driver (TAP) untuk networking.



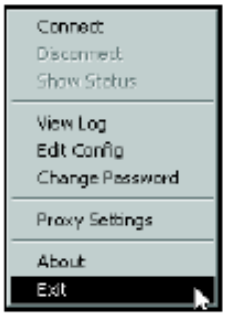
Jika anda telah melangkah sejauh ini, anda telah sukses menginstal OpenVPN pada Windows sistem. Jika ingin membaca file Readme, aktifkan checkbox Show Readme sebelum mengklik Finish.

Uji Instalasi – tampilan pertama Applet

Setelah instalasi OpenVPN GUI, OpenVPN dimulai dan panel applet dibuat. Dalam screenshot di bawah ini, icon yang dekat ke kiri.

Applet ini menyediakan suatu metode yang cocok untuk pengguna Windows untuk mengontrol dan mengkonfigurasi (sebagian) OpenVPN. Meski begitu, ketika tidak ada interface untuk konfigurasi, konfigurasi file hanya dapat diedit oleh editor. Dan sampai suatu konfigurasi dibuat, context menu terlihat miskin. Klik kanan pada panel applet :

Sekali saja anda telah mengkonfigurasi sebuah koneksi pertama, menu ini akan terpopulasi dengan entri baru. Dengan entri Connect dan Disconnect anda dapat mulai dan stop configured tunnels.



Menginstal OpenVPN pada Debian

Mungkin distribusi yang paling mudah yang di atasnya untuk menginstal OpenVPN adalah Debian. Hanya mengetik siap mendapat instal openvpn, jawaban dua pertanyaan-pertanyaan, dan OpenVPN diinstall dan siap untuk digunakan. Debian membungkus sistim manajemen adalah mampu memecahkan semua isu bahwa akan terjadi selama instalasi. Jika sistim anda diatur secara benar, instalasi yang otomatis meliputi langkah-langkah ini:

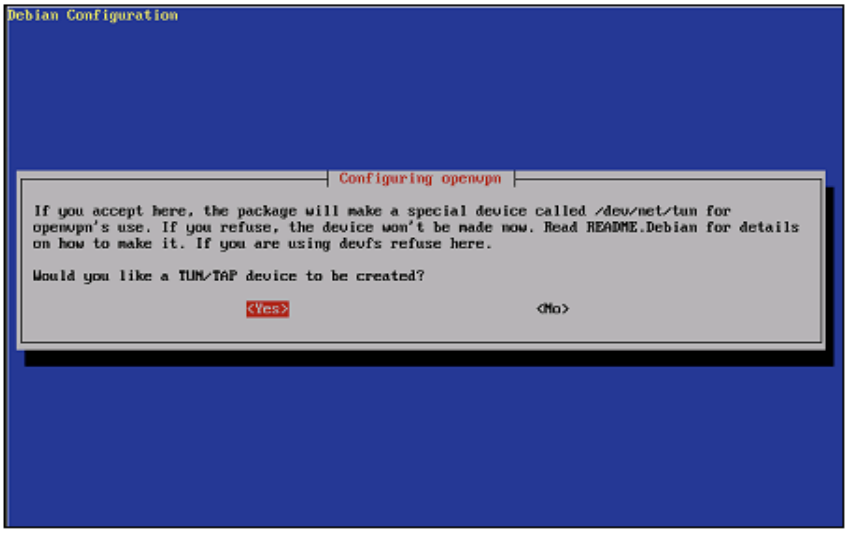
1. Penolong instalasi siap mendapat akan menemukan perangkat lunak di server-server instalasi.
2. Penolong itu akan mendownload paket yang dipilih dan membongkarnya kepada sistim anda yang lokal.
3. Satu script konfigurasi yang interaktip dieksekusi, yang mengatur sistim anda dan perangkat lunak yang baru diinstall untuk pemakaian yang kemudiannya dengan parameter-parameter yang anda masukan.

Ekstrak kode yang berikut adalah keluaran apt-get install openvpn di suatu sistem Debian. Keluaran ini boleh bertukar-tukar tergantung pada pemilihan perangkat lunak anda yang sebelumnya, dan dalam apustaka LZO compression library harus diinstall. Di beberapa sistem siap menginstal OpenSSL Libraries, dalam banyak kasus, apt-get mampu memecahkan semua permasalahan untuk anda.

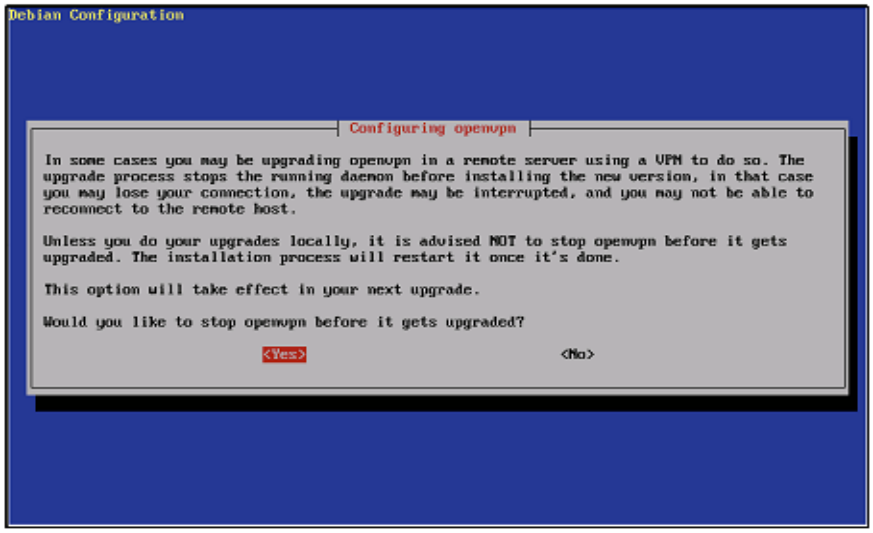
```
debian01:~# apt-get install openvpn
Reading Package Lists... Done
Building Dependency Tree... Done
The following NEW packages will be installed:
openvpn
0 upgraded, 1 newly installed, 0 to remove and 7 not upgraded.
Need to get 293kB of archives.
After unpacking 762kB of additional disk space will be used.
Get:1 http://ftp.uni-erlangen.de testing/main openvpn 2.0-4 [293kB]
Fetched 293kB in 1s (247kB/s)
Preconfiguring packages ...
Selecting previously deselected package openvpn.
(Reading database ... 9727 files and directories currently installed.)
Unpacking openvpn (from .../openvpn_2.0-4_i386.deb) ...
Setting up openvpn (2.0-4) ...
Restarting virtual private network daemon:.
debian01:~#
```

Selama proses ini, anda akan diperintahkan untuk menjawab dua pertanyaan-pertanyaan yang berikut:

1. Anda harus membiarkan apt untuk membuat suatu alat TUN/TAP untuk penggunaan oleh OpenVPN Software. Jika anda memilih nomor, tunnels anda tidak akan diciptakan dan tunnel perangkat lunak terowongan anda tidak akan bekerja.



2. Pertanyaan yang kedua menggunakan keamanan akan kebenaran. OpenVPN Software harus dihentikan selama diperbarui, supaya Anda harus memilih YES dan kerugian kembali.



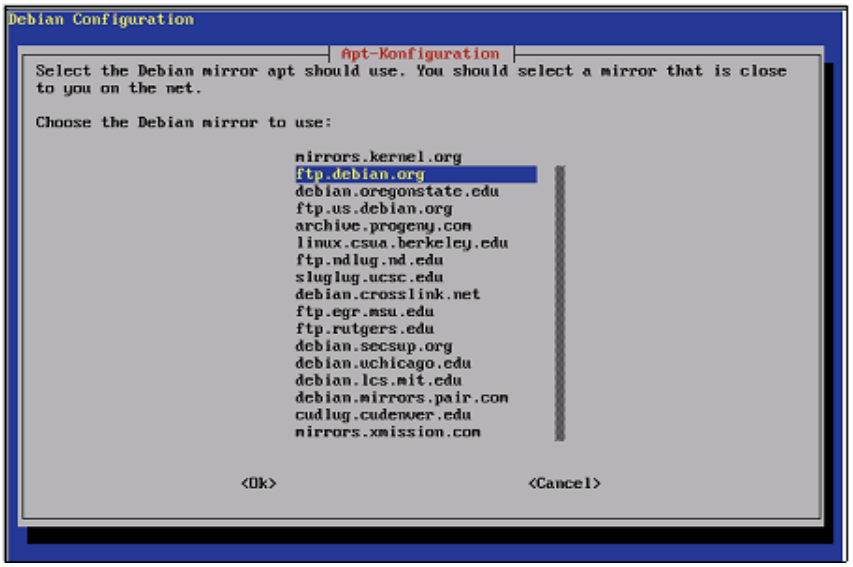
Anda harus memberhentikan tunnel perangkat lunak lama ketika pembaruan sedang dijalankan. Semua pembangunan tunnel akan dihentikan, dan para pemakai anda tidak akan mampu untuk disambungkan ke sistim anda sekarang. Mulai sekarang, semua tunnels diciptakan oleh OpenVPN Software yang baru termasuk tambalan-tambalan dan bugfixes. Ini adalah keamanan untuk perjalanan.

Bagaimanapun, jika anda memilih No, anda mengambil resiko bahwa perangkat lunak dan pustaka-pustaka yang lama masih sedang dijalankan, bahkan setelah instalasi OpenVPN Software yang baru. Bugfixes dan tambalan-tambalan dari versi yang baru tidak berlaku bagi tunnels yang ada dan dimulai lagi; kembali. Anda boleh benar benar menjalankan inconsistencies system anda, jika anda mempunyai beberapa tunnels dan mereka sedang menjalankan versi-versi yang berbeda perangkat lunak anda. Jadi Dengan demikian, lebih aman untuk memiliki suatu waktu yang singkat kapan para pemakai tidak akan mampu untuk menyaambung.

Menginstal Paket-Paket Debian

Paket software untuk sistem Debian disiapkan dalam bentuk yang disebut file .deb dalam format file .DEB biasanya disimpan di dalam tempat penyimpanan yang

online di FTP atau server web dan setiap sistim Debian memegang sebuah daftar tempat penyimpanan untuk digunakan untuk instalasi. Anda akan menemukan daftar ini di /etc/apt/sources.list. Susunan untuk memprogram base-config menyediakan suatu konfigurasi yang berbasis menu menghubungkan untuk apt.



Jika anda ingin menambahkan tempat sumber penyimpanan kepada instalasi Debian anda, jenis base-config dan berubah kepada menu siap mengatur. Pilih tempat yang anda pilih dengan dan tempat penyimpanan dari pilihan anda. Pilih Ok. Sekarang semua paket software dari server ini dapat secara otomatis diinstall di sistim anda, dengan hanya mengetik apt-get install <paket>.

Suatu paket Debian berisi software dan informasi tentang nama, versi, uraian, isi-isi, prasyarat-prasyarat, dependencies dan script-script konfigurasi yang dimulai untuk setelah instalasi.

Sistem Debian menawarkan program-program powerful yang dapat anda mengendalikan software instalasi sangat secara rinci. Mendaftarkan semua program dan opsi akan berhasil di luar lingkup dari buku ini, tetapi di sini adalah suatu ikhtisar yang pendek beberapa paket manajemen yang ringkas:

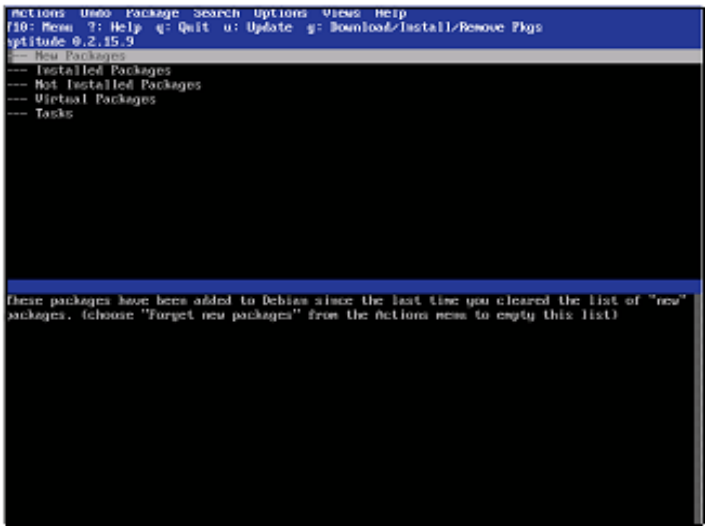
Command	fungsi
apt-get install <package>	Install paket yang terpilih dari daftar tempat penyimpanan /etc/apt/sources.list
apt-get remove <package>	hapus paket yang dipilih dari sistem anda
apt-get update	barui daftar paket-paket yang tersedia di tempat daftar penyimpanan /etc/apt/sources.list
apt-get upgrade	Install dari yang tersedia versi-versi terakhir dari semua software anda yang akan diinstall
apt-get dist-upgrade	Install dari yang tersedia versi-versi terakhir yang berhubungan dengan konfigurasi anda
dpkg-reconfigure	Restarts/Starts script konfigurasi di dalam paket, yang akan dibawa yang berbasis menu dialog dengan cara yang sama seperti setelah instalasi
apt-cache show <package>	Mencetak informasi yang terperinci tentang paket software
dpkg -l <package>	Mencetak informasi tentang paket software yang diinstal
dpkg -L <package>	Daftar semua file yang diinstall oleh paket software
dpkg -i <file>	Instal suatu yang lokal dari file (.deb) kepada sistim anda
dpkg -S <file>	Mencetak informasi tentang pemilikan paket software <file>
apt-cache search <string>	Mencari database siap untuk kemasan-kemasan berisi <string> di dalam nama dan uraian

Program-program ini perlu memecahkan semua pertanyaan-pertanyaan yang mungkin, isu-isu, dan permasalahan sekitar instalasi software di sistem Debian. Hanya mencoba ini perintah dengan kemasan OpenVPN baru saja yang menginstall di sistim anda. Ketik pertunjukan cache siap openvpn untuk menerima informasi tentang paket yang diinstall:

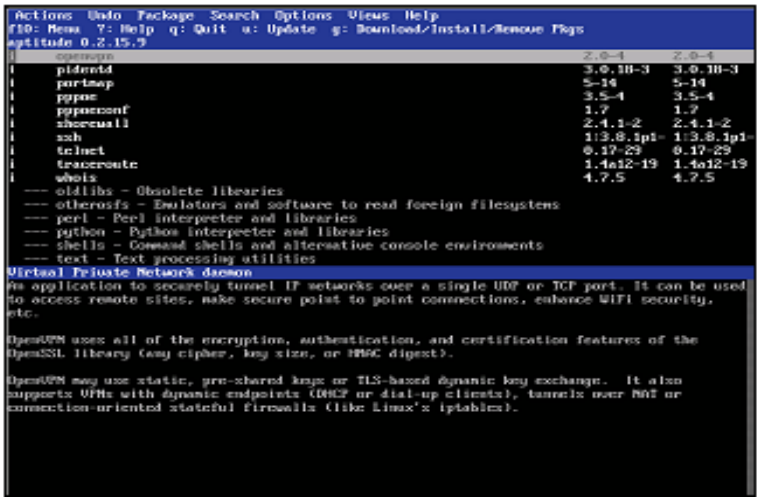
```
debian:~# apt-cache show openvpn
Package: openvpn
Priority: optional
Section: net
Installed-Size: 744
Maintainer: Alberto Gonzalez Iniesta <agi@inittab.org>
Architecture: i386
Version: 2.0-4
Depends: debconf, libc6 (>= 2.3.2.ds1-21), liblzo1, libssl0.9.7
Filename: pool/main/o/openvpn/openvpn_2.0-4_i386.deb
Size: 293492
MD5sum: dcc638e084f7b3143c614a33b26d5750
Description: Virtual Private Network daemon
An application to securely tunnel IP networks over a single UDP or TCP
port.
It can be used to access remote sites, make secure point to point
connnections,
enhance WiFi security, etc.
.
OpenVPN uses all of the encryption, authentication, and certification
features
of the OpenSSL library (any cipher, key size, or HMAC digest).
.
OpenVPN may use static, pre-shared keys or TLS-based dynamic key
exchange. It
also supports VPNs with dynamic endpoints (DHCP or dial-up clients),
tunnels
over NAT or connection-oriented stateful firewalls (like Linux's
iptables).
Tag: security::cryptography, interface::daemon
debian:~#
```

Menggunakan keserasian untuk mencari dan menginstall Paket

Meski alat debian command-line adalah sangat bagus, ada lebih banyak program-program bahwa bantuan anda mendapat kembali dan menginstal software. Software yang paling umum mungkin untuk tujuan ini adalah Aptitude. Jenis ketepatan ini di suatu baris perintah untuk interface instalasi yang berbasis menu.



Aptitude terdiri dari suatu menu ada di puncak dari layar, daftar paket-paket, dan suatu jendela yang mempertunjukkan secara detail di software dan memilih di dalam daftar paket. Jika anda mempunyai dukungan cosole mouse, anda dapat meng-klik pada masukan-masukan menu. Klik pada masukan menu Search, atau tekan F10 dan menjalankan menu Search. Pilih masukan Find. Anda akan diperintahkan dengan suatu simbol pencarian. Masuk openvpn. Sementara anda sedang mengetik, ketepatanuntuk dapat membaharui jendela utama. Klik OK dan lihat keluarannya.



Aptitude akan menemukan versi OpenVPN yang sudah anda install sebelumnya, dan isi menu-menu Actions dan Package membantu anda memilih dan menginstal perangkat

lunak. Tergantung pada pemilihan dan tempat penyimpanan bahwa anda sudah menambahkan kepada sourceslist anda selama instalasi, aptitude dapat juga membantu anda memilih versi-versi yang berbeda pada OpenVPN.

OpenVPN – File-file terinstall pada Debian

Tabel yang berikut memberi satu ikhtisar dari file-file yang diinstall oleh Debian melingkupi sistem manajemen . Sebagian dari file ini akan digunakan di dalam bab-bab yang selanjutnya:

Full Path and File Installed by OpenVPN	Function
/etc/openvpn	Directory containing configuration files
/etc/network/if-up.d/openvpn /etc/network/if-down.d /etc/network/if-down.d/openvpn	Start/stop openvpn when the network goes up/down
/etc/init.d/openvpn	Start/stop script for services
/sbin/openvpn	The binary
/usr/share/doc/openvpn	Documentation files
/usr/share/man/man8/openvpn.8.gz	Manual page
/usr/share/doc/openvpn/examples/sample-config-files	Example configuration files
/usr/share/doc/openvpn/examples/sample-keys	Example keys
/usr/share/doc/openvpn/examples/easy-rsa	easy-rsa—a collection of scripts useful for creating tunnels
/usr/share/doc/openvpn/changelog.Debian.gz /usr/share/doc/openvpn/changelog.gz	Version history
/usr/share/openvpn/verify-cn	verify-cn function (revoke command)
/usr/lib/openvpn/openvpn-auth-pam.so /usr/lib/openvpn/openvpn-down-root.so	Libraries for PAM-Authentication and chroot mode

Ringkasan

Di dalam bab ini yang kita sudah melihat di banyak instalasi-instalasi tentang sistem yang berbeda, instalasi itu OpenVPN adalah sangat gampang. Terlepas dari sistem Linux seperti SuSE, Redhat, Debian, atau FreeBSD, yang menyediakan sistem manajemen instalasi dan kemasan canggih, OpenVPN dapat juga dengan mudah diinstall di sistem yang lain seperti Windows. Dan di sana terdapat berbagai kemungkinan untuk menerapkan OpenVPN dari sumber dan membangitkan instalasi membungkus untuk sistem anda sendiri

BAB 5

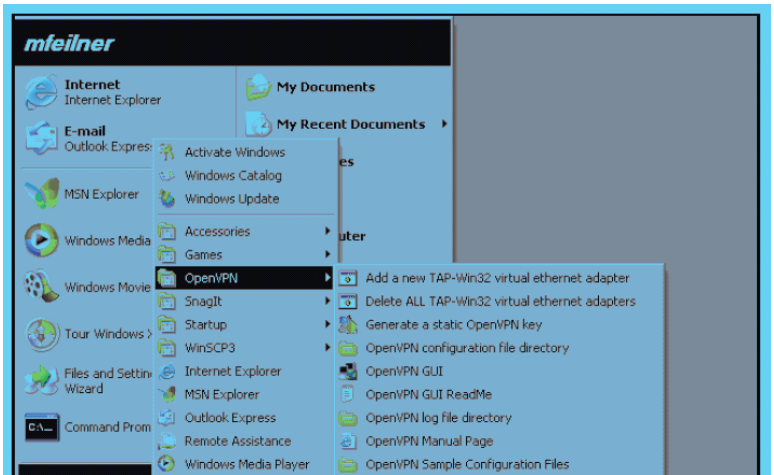
Konfigurasi OpenVPN dengan Tunnel Pertama

Pada bab ini kita akan membuat kunci enkripsi untuk open VPN dan menggunakannya untuk mensetup tunnel open VPN pertama kali diantara dua system window pada jaringan yang sama. Kita telah mengetest lingkungan dimana tidak ada masalah dengan firewall atauu router yang akan interference dengan setup open VPN dan kita dapat konsentrasi pada pelajaran ini bagaimana membuat tunnel.

Pekerjaan kecil pada konfigurasi file membutuhkan untuk dilakukan dan kunci yang dapat merubat diantara system ini. Setelah itu, tunnel akan dimulai dan ditest dengan perintah ping. Kita akan mencopy kunci pada sistem linux dan mengkoneksikan sistem dengan tunnel pada mesin windows pertama kali. Langkah selanjutnya, kita akan memastikan bahwa openVPN akan dijalankan secara otomatis antara sistem dan melihat pada manajer service di windows dan sistem pada linux.

OpenVPN pada Microsoft Windows

Selama proses instalasi pada openVPN yang telah mengisi seperti pada main menu windows dibawah ini :



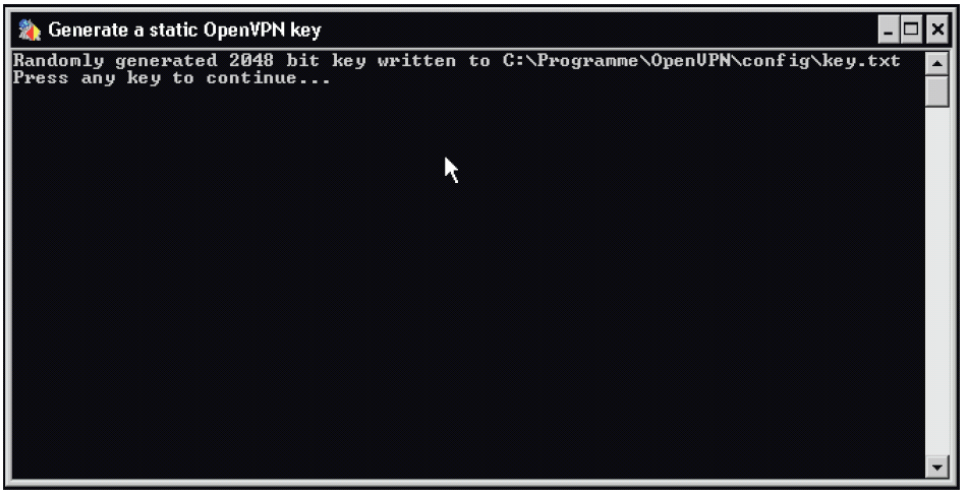
Tergantung pada versi windows dan install program, lokasi sebenarnya pada menu dapat diubah. Pada point ini, hanya pada 5 isi dibawah ini pada enu yang relevan (dimulai dari atas) :

Judul	Fungsi
Membangkitkan kunci statistic OpenVPN	Membuat kunci enskripsi statistic yang dapat digunakan untuk membuat tunnel
Konfigurasi OpenVPN directory file	Membuka windows explorer pada directory C:\Program Files\OpenVPN\Config, dimana konfigurasi data untuk persediaan pada openVPN
OpenVPN GUI	Memulai openVPN GUI yang plug in pada system tray pada taksbar
OpenVPN log directory file	Membuka windows explorer pada directory C:\Program Files\OpenVPN\log, dimana file log untuk menjaga openVPN
Contoh konfigurasi openVPN	Membuka windows explorer pada directory C:\Program Files\OpenVPN\sample-config, dimana contoh konfigurasi file untuk menemukan OpenVPN

Terpisah dari isi, dimana kita akan menemukan informasi pada openVPN di halaman yang online secara manual, membaca file, terhubung ke website dan beberapa isi yang dapat menolong untuk memenage interface jaringan yang membuat openVPN.

Membangkitkan kunci statistic openVPN

Sebelum kita dapat mengkoneksikan dua system dengan tunnel openVPN, kita telah mempunyai kunci statistic yang akan kita gunakan untuk enskripsi pada traffic. Kunci ini harus dilengkapi pada system both karena pada kasus pada enskripsi simetris sisi both akan menggunakan kunci yang sama. Pilih isi yang membangkitkan kunci statistic openVPN pada menu window openVPN.



OpenVPN akan membuka perintah-baris pada window dan membangkitkan kunci enskripsi yang panjangnya 2048 bit. Kunci ini disimpan pada directory konfigurasi standart dengan nama key.txt.kunci ini harusnya hanya digunakan untuk mengetest dan mempelajati tujuan, tetapi untuk semua test setup itu sangat diperlukan.

> Jangan menggunakan kunci ini untuk semuanya tetapi mengetest koneksi OpenVPN.

Proses ini juga dilakukan oleh program openvpn.exe. pada bab selanjutnya kita akan menjelaskan penggunaan pada interface perintah-baris openvpn.

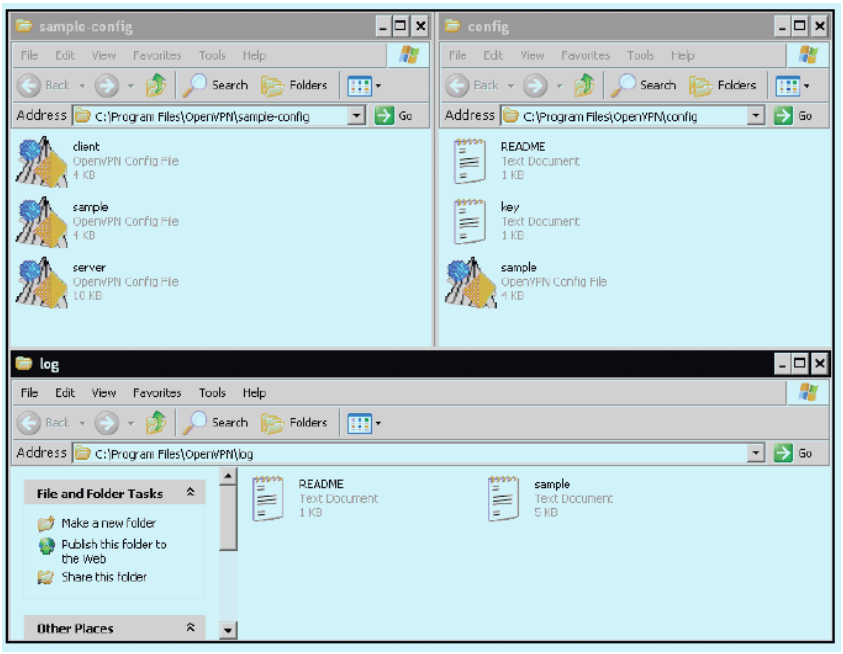
Menu dalam isi openVPN dimulai dari applet panel openVPN. Setelah instalasi applet ini siap dijalankan,jadi pilih isi menu yang hanya membawa window dimulai, openVPN GUI siap dijalankan. Jika GUI dihentikan, isi akan merestart panel applet. Tiga menu isi lainnya pada saat membuka windows explorer ada tiga perbedaan pada directorinya yaitu :

1. Directory C:\Program Files\OpenVPN\Config, adalah default dimana openVPN akan melihat untuk konfigurasi dan kunci file. Telah melihat pada screnshoot

pembangkit generasi berlawanan dan akan melihat bahwa kunci yang kita bangkitkan telah ditulis di C:\Program Files\OpenVPN\Configkey.txt.

2. Pada directory C:\Program Files\OpenVPN\Sample-Config, kita akan menemukan konfigurasi file untuk setup standart. File ini telah diubah menjadi kecil dan kita dapat menggunakan untuk test VPN dengan yang berkaitan.
3. Output pada software tunnel ditulis ke file text pada directory C:\Program Files\OpenVPN\log.

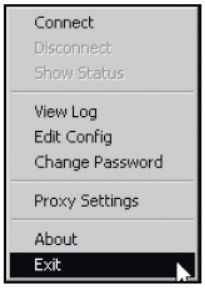
Pada screenshot dibawah ini digambarkan susunan pada windows explorer pada tiga directori :



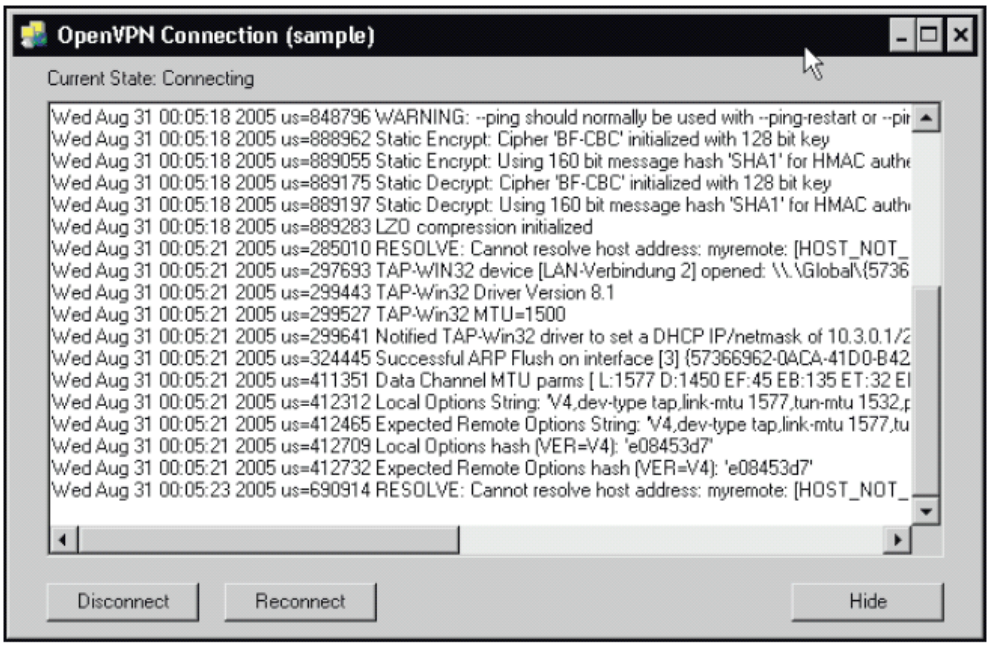
Membuat contoh koneksi

Kita akan mengetahui contoh koneksi VPN untuk melihat bagaimana OpenVPN GUI bekerja. Buka semua tiga directori oleh clicking pada isi di memu main. Copy contoh konfigurasi file dari contoh directory konfigurasi ke dalam directory konfigurasi. Kita dapat menggunakan drag-and-drop untuk menyelesaikannya. Smua konfigurasi openVPN yang baru dapat dimulai via panel applet ---jika jaringan cocok dengan contoh konfigurasi.

Klik kanan pada panel applet. Anda akan melihat menu isi yang memiliki beberapa isi sekarang. Pilih koneksi isi untuk memulai contoh konfigurasi sekarang.

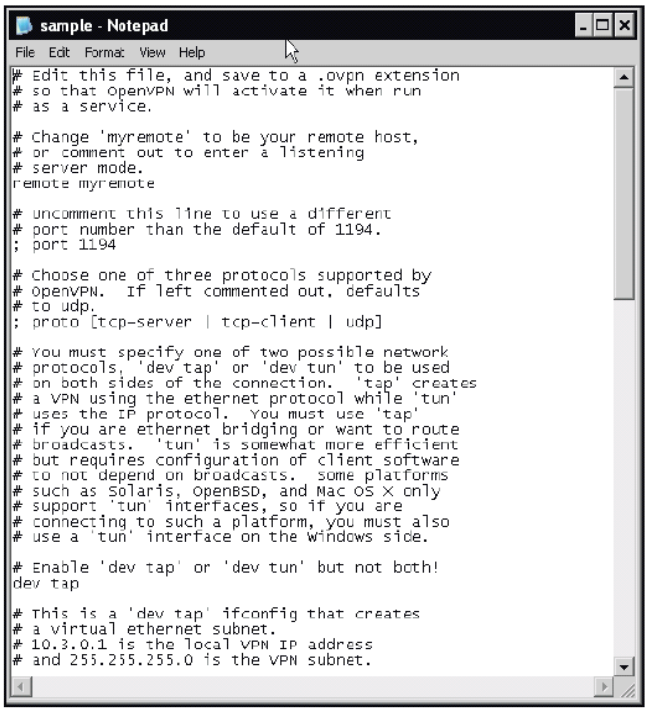


Koneksi window openVPN (contoh) adalah membuka. Pada window ini protocol output pada contoh koneksi, yang mana juga ditulis untuk file lig pada directory log digambarkan. Kita dapat melihat bahwa disana konfigurasi yang sama masih bekerja untuk melakukannya : pada contoh konfigurasi, openVPN adalah koneksi untuk mengontrol server yang disebut myremote. Jika tidak terjadi apa-apa untuk melakukan server openVPN dengan nama pada jaringan local, seharusnya melihat window sebenarnya seperti pada di bawah ini. Ini berarti bahwa software window openVPN anda adalah up dan running tetapi itu tidak dapat membuat tunnel.



Mengadopsi Kelengkapan contoh konfogurasi file oleh OpenVPN

Kita telah merubah semua konfigurasi. Pilih isi konfigurasi file directory OpenVPN dari main menu windows dan klik kanan pada contoh konfigurasi file yang kita copikan disana. Notepad memulai up dan menunjukkan kita contoh konfigurasi file :



Pada file ini, kita merubah atau masuk pada tiga settingan di bawah ini :

a. Nama atau alamat IP pada host VPN lainnya.
b. Nama pada kunci file
c. Alamat IP untuk VPN dan host.

Open VPN membutuhkan alamat IP pada tunnel endpoint lain pada susunan untuk mengetahui dimana kita mengkoneksikannya. Untuk memastikannya antara sisi

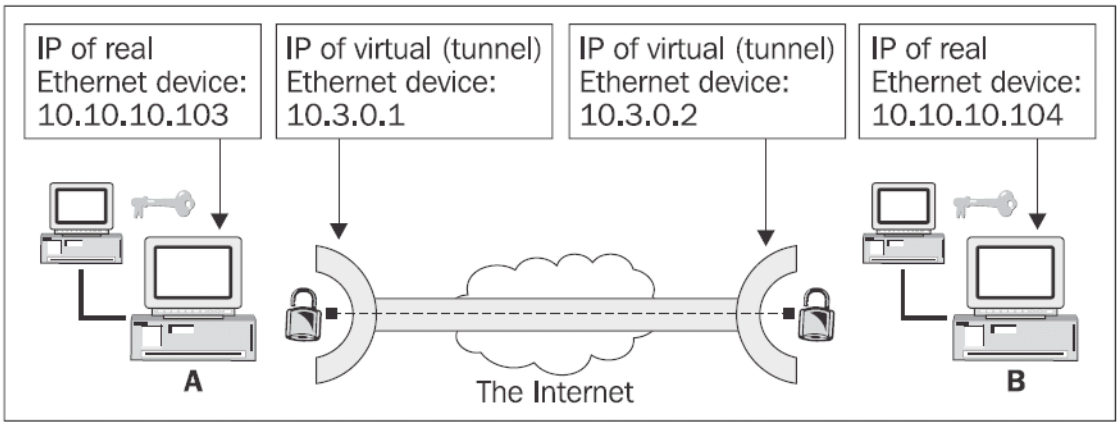
menggunakan enskripsi kunci yang sama, kita harus spesifikasikan file yang mana kunci tetap terjaga. tunnel net harus menjadi eqquipped dengan IP. IP itu menunjukkan ke adapter jaringan virtual.setiap tunnel mempunyai satu adapter jaringan virtual pada tiap sisi, dan sisi lainnya hanya dapat berkomunikasi dengan lainnya jika mempunyai segment jaringan yang sama. Kita memilih alamat Ip untuk tiap host, sebagai contoh menggunakan IP untuk contoh set file 10.3.0.1 dan 10.3.0.2 .

Jika kita memilih rata-rata parameter untuk settimgan, kitadapat dengan mudah mengkoneksikan dua system. Tabel dibawah ini menunjukkan isi konfigurasi file openVPN untuk dua koneksi host via openVPN yang berada pada subnet sama :

Host A (10.10.10.103)	Host B (10.10.10.104)
remote 10.10.10.104	remote 10.10.10.103
ifconfig 10.3.0.1 255.255.255.0	ifconfig 10.3.0.2 255.255.255.0
secret `key.txt`	secret `key.txt`

Hanya tiga parameter file konfigurasi di openVPN yang penting untuk set up semua contoh tunnel.
Remote mendefinisikan end lainnya pada tunnel. Disini dapat diliat isi IP atau DNS.Ifconfig mengeset IP local dan netmask untuk interface tunnel pada openVPN dimana kunci file digunakan,relative untuk directory konfigurasi.

Dibawah ini grafik yang menolong untuk mengklarifikasikan :



Untuk tunnel openVPN terdiri dari empat jaringan. Dua dari mereka adalah ethernet card yang sesungguhnya dan dua lagi lainnya hanya alat tunnel virtual (TUN atau TAP). Alat jaringan yang sesungguhnya mempunyai IP yang menetapkan di bawah sistem yang dapat dicapai pada local net. Alat jaringan virtual mempunyai IP yang menetapkan untuk digunakan set up tunnel.

Host A dengan LAN IP 10.10.10.103 berusaha untuk terkoneksi dengan host B dengan LAN IP 10.10.104. IP pada interface jaringan virtual (pada jaringan tunnel) untuk host A adalah 10.3.0.1, host B mempunyai 10.3.0.2. nama pada file kunci adalah key.txt pada sistem kedua-duanya.

> Open VPN dapat mempunyai nama IP dan DNS sebagai pilihan untuk konfigurasi parameter remote. Jika kamu menggunakan nama DNS, kamu telah membuat bahwa nama domain menetapkan pada sistem konfigurasi. Di lain sebab, kita harus yakin host lainnya dapat dicapai—check DNS,routing dan konfigurasi firewall.

Peringatan bahwa dua host pada semua contoh adalah mempunyai subnet sama. Ini adalah setup yang simple dimana tidak ada routing,DNS atau firewall yang akan memberi tahu interface dengan semua tunnel. Semuanya kita membutuhkan dua PC yang menjalankan OpenVPN.Pilihan remote membutuhkan untuk dirubah kemudian, dimana kita mensetup tunnel diantara dua site internet. Sekarang copi kunci file key.txt ke sisitem kedua, dan edit konfigurasi file sistem. Cara yang paling mudah melakukan itu dalah membuat folder pada salah satu sistem dan memetakannya. Itu sebagai drive jaringan pada sistem lainnya.

Memulai dan mengetest Tunnel

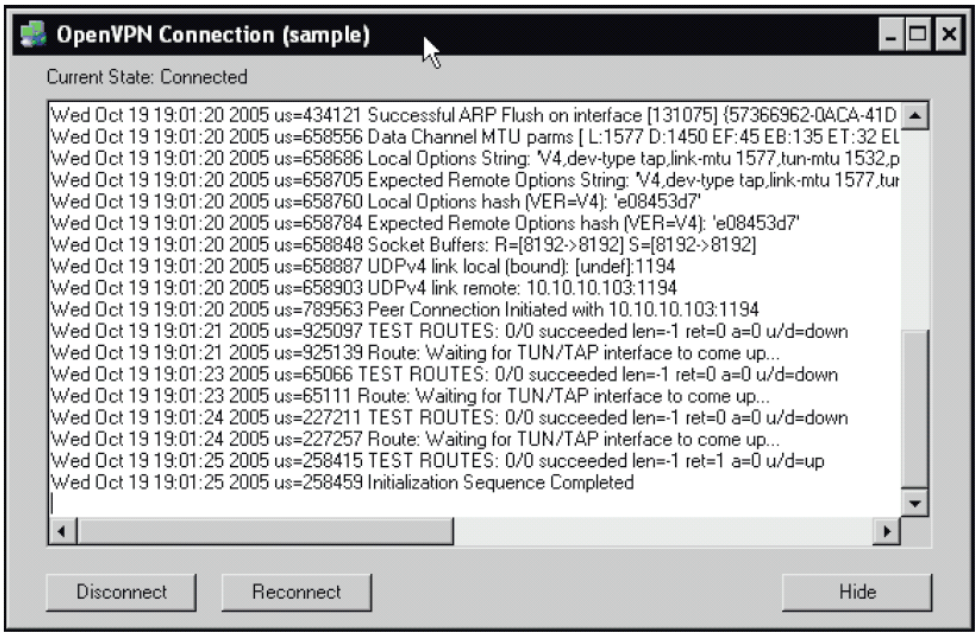
Setelah sistem kedua-duanya direncanakan, mulai openVPN GUI (atau membuat itu berjalan) dan pilih masukan koneksi dari menu pada sistem kedua-duanya.

Jika out bekerja dengan baik, icon openVPN pada sistem kedua-duanya akan berubah ke hijau seperti ini:

Jika anda melihat lampu merah disini, tunnel openVPN tidak terhubung,kuning menggambarkan koneksi baru saja di set up dan pada proses ini berhasil, icon menunjukkan warna hijau.

Bagaimanapun juga,jika kita menggunakan firewall local pada sistem lainnya, yakinkan itu tidak diblok pada paket ini.Frewall windows XP seperti sistem windows lainnya, per default yang paket keluarnya tidak diblok, yang mana berarti bahwa koneksi openVPN harus selalu ditetapkan.

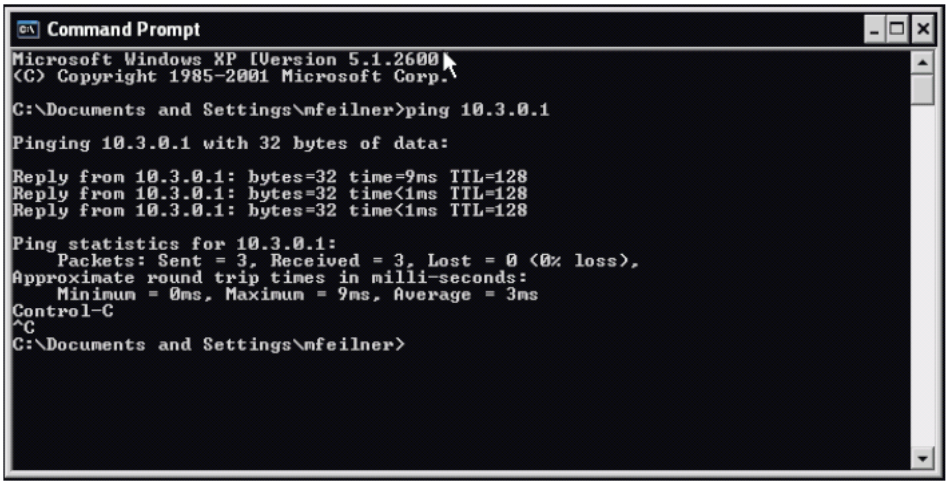
Pilih masukan status dari menu context openVPN GUI untuk menerima secara detail informasi tentang proses pada koneksi.



Untuk sekarang, hanya baris terakir pada output yang penting. Inisialisasi sequence melengkapi kesusesan pesan openVPN. Tunnel up dan running dan sistem kedua-duanya harus digambarkan pesan pada status log.

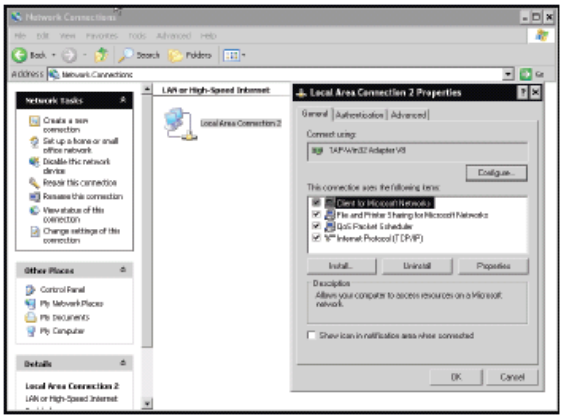
Sekarang kita test tunnel dengan perintah ping. Mulai kerangka DOS dengan memilih main menu windows Run dan masuk cmd.exe. anda akan menggambarkan dengan perintah-line interface sebagai screnshoot yang mengikuti. Tipe ping 10.3.0.2 pada host a untuk mengecek jika paket ping telah benar mentransfer ke host B.pada host B, anda akan memasuki ping 10.3.0.1 jika anda menggunakan alamat jaringan yang sama seperti yang disebutkan contoh sebelumnya.

Jika kamu menerima output seperti screnshot dibawah ini, perintah ping akan berhasil dan tunnel openVPN akan bekerja.



Perintah pada interface jaringan windows openVPN

Pada sistem windows, buka control panel dan rubah koneksi jaringan. Kita akan dapat melihat, untuk setiap tunnel openVPN anda dapat menggambarkan, interface jaringan virtual yang dimasuki.screnshot di bawah ini menggambarkan interface yang aktif—default ketika tunnel up. Muncul seperti interface jaringan sesungguhnya dan dapat digunakan seperti interface lainnya.Jika anda tidak percaya, lihat pada dialog propertis pada content menu pada icon interface. Bagian dari faktanya bahwa interface ini digambarkan sebagai TAP-WIN 32 Adapter V8, setiap settingan mungkin pada adapter jaringan yang nyata dapat ditutup disini juga.



Anda dapat disablekan interface dengan double-click pada icon itu, tetapi jaga bahwa tunnel akan dikoneksikan secara otomatis setelah anda memulai interface lagi. Anda

harus merecconnect lagi secara manual dengan memilih masuk pada context menu openVPN.

Jika anda membutuhkan informasi dengan detail pada interface jaringan , perintah ipconfig / alll akan sangat membantu. Buka kerangka DOS windows dan masuk ipconfig / alll. Windows akan mendaftar semua interface jaringan yang dapat, Ip dan routing data.

Menghubungkan windows dengan Linux

Koneksi diantara dua system hamper sederhana seperti menggambarkan mengulang bagian. Step membutuhkan untuk mengambil data sesungguhnya yang sama, bagaimanapun juga, disana ada dua lubang yang harus kita hindari, dan lubang kedua-duanya dikoneksikan untuk mentransfer file dari windows ke linux (atau kembali)

Merubah file diantara Windows dan Linux

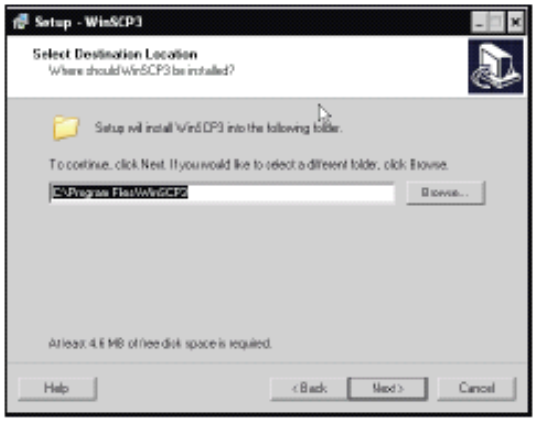
Pada linux, perintah eksekusi remote dan merubah data sepanjang SSH adalah standart. SSH juga digunakan opn SSL, untuk enskripsi, sepeti membuka

OpenVPN,windos,bagaimanapun juga, tidak membutuhkan dukungan untuk merubah enksripsi data.Sistem windows menggunakan protokol **Server Message Block** (**SMB**) untuk berkomunikasi dan merubah data. Linux tidak didukung untuk ini tetapi disana ada server daya yang sesuai yang disebut **Samba,** yang mana dapat digunakan untuk membuat mesin linux tampil seperti PC windows.

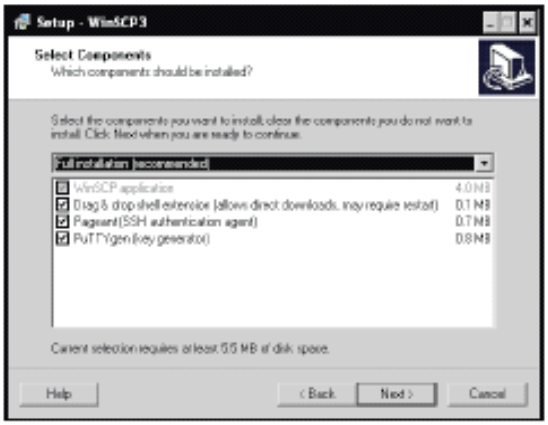
Jadi bagaimana kita mengcopy kunci file dari windows ke server linux? Disana ada dua kemungkinan. Pada saat kita mengset up samba pada linux untuk aksinya sebagai client windows atau server atau kita menginstall software SSH pada windows. Tool yang sangat mudah untuk tujuan **WinSCP**, yang mana dapat digunakan untuk mendownload dengan bebas dari http://winscp.net/. WinSCP yaitu aplikasi Explorer-style yang ditemukan drag-and-drop mengkopi semua koneksi.

Menginstall WinSCP

Download WinSCP dan double-click pada file EXE . Start dan install clicking Next twice.

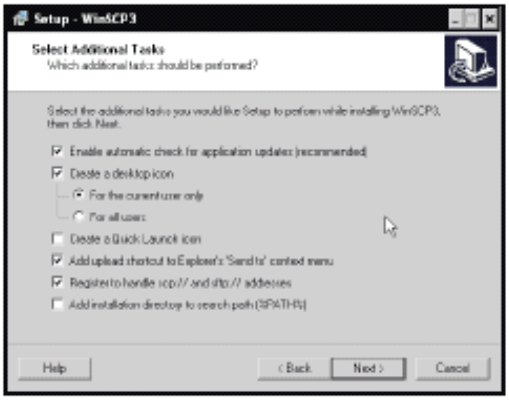


Jika menginginkan lokasi yang berbeda untuk program ini, masuk dan klik pada dialog kedua.

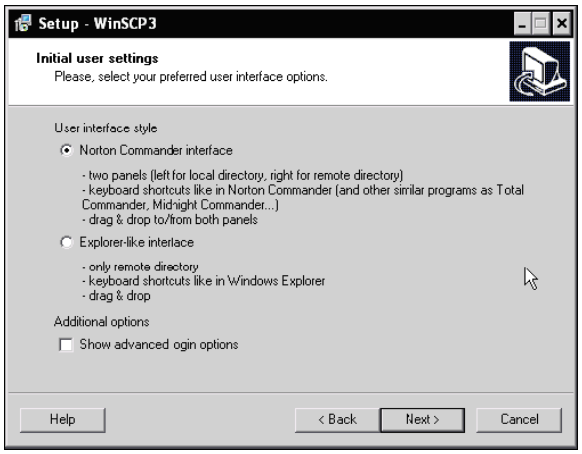


Full instalasi seperti memilih oleh default yang merupakan sebabyang paling baik,tetapi instalasi compact mungkin juga cukip jika kita hanya ingin mengcopy. Full instalasi dilengkapi feature penggunaan keypad untuk enskripsi koneksi seperti membuat kunci enskripsi atau menggunakan kunci yang telah ada.

Klik mext dua kali untuk menerima pilihan dan masuki menu default untuk main menu windows.



WinSCP dapat melakukan tambahan, disamping itu biasanya icon desktop dan updates regular secara otomatis dapat mempunyai isi menu context dan mendukung untuk url seperti scp:// dan sftp:// untuk Windows Explorer, yang mana datang dari feature yang sesuai dengan yang didapatkan dalam menggunakannya. \Click Next lagi untuk menunjukkna pilihan default .

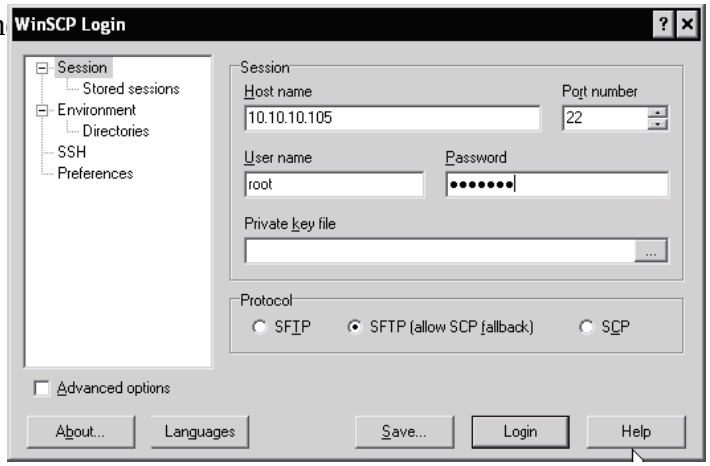


Dialog ini memilih untuk melihat WinSCP default.jika kita memilih interface pilihan Norton, anda akan mempresentasikan dengan window file manager memisahkan kedalam dua bagian.,local dan directory remote. Ini adalah pilihan default dan mungkin menjadi penggunaan salah satunya. Bagaimanapun juga, jika kita lebih suka style window explorer,kemudian memilih tombol Explorer-like interface, yang mana akan menunjukkan directory remote pada window single.

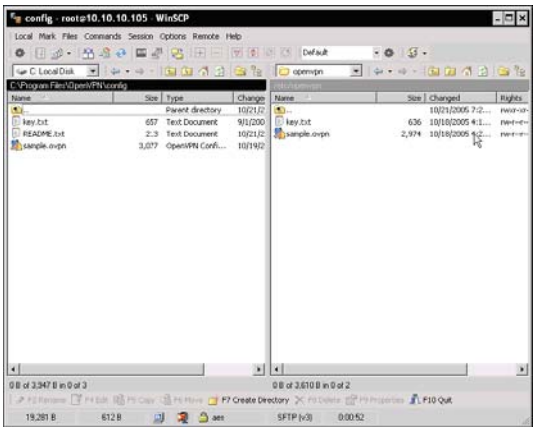
Selesai menginstal klik next dan kemudian install pada dialog dibawah ini. Set up program kemudian extract dan sets up WinSCP. Setelah itu klick Finish, WinSCP akan start.

Mentransfer file key dari windows ke linux dengan WinSCP

Setelah WinSCP dimulai,kita telah menunjukkan dimana kita akan mengkoneksikannya. Masuki alamat IP dan nama DNS pada system linux pada host name,nama pada pengguna linux (administrator "root") pada User name, dan password pada kotak Password. Semua pilihan memerlukan pada point ini. Klik on Login untuk memulai koneksi. Jika kita mengkoneksikan pada waktu pertama kali, WinSCP akan menanyakan autentifikasi pada host yang ingin kita koneksikan.jika kita click OK , WinSCP akan m



WinSCP menunjukkan dengan cara yang untuk mengikuti screenshot. Pada sisi kiri pada windows harusnya disana menjasi daftar directory local, yang mana gambaran sisi kanan directory pada server remote. Menu small drop-down diatas daftar mengikuti pilihan dan merubah pilihan tercepat dan rubah direktori kerjanya.



Sekarang copy file key dan konfigurasikan file dari windows ke system linux. Pada mesin windows merubah directory C:\Program Files\OpenVPN\config; pada linux merubah ke /etc/openvpn. Drag dan drop file key.txt dan konfigurasikan file sample.ovpn pada pada sistem Linux .

.ovpn adalah extension standard untuk konfigurasi file OpenVPN's Windows .conf adalah extension standard OpenVPN pada Linux

Pitfall kedua –membawa kembali/ tujuan akir pada baris

Merubah file text diantara Linux dan Windows selalu memproduksi masalah lainnya. Pada system UNIX, karakter line baru disignifikasikan akir pada baris pada DOS/Windows, karakter kembali dan baris baru selalu digunakan bersama-sama untuk menandakannya.

Text file dicopi dari system DOS ke system UNIX selalu mempunyai kelebihan-kelebihan karakter pada akir barisnya. Karena masalah ini umum, komunitas linux

tergantung pada **dos2unix** dan **unix2dos** . dos2unix mengkonvert text dari format DOS/Windows dengan benar kedalam format UNIX, dan unix2dos cara lainnya.

Pada contoh lainnya, kita telah mengkonvert kedua-duanya file key dan konfigurasi file ke dalam format UNIX. Jika kita sample.ovpn kelihatan sepeti menunjukkan vi :

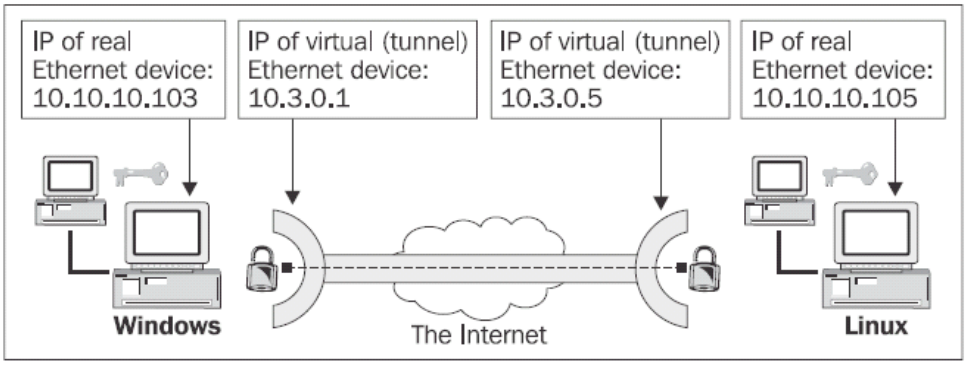
```
(...)
# Change 'myremote' to be your remote host,^M
# or comment out to enter a listening^M
# server mode.^M
remote 10.10.10.104^M
^M
# Uncomment this line to use a different^M
# port number than the default of 1194.^M
; port 1194^M
^M
# Choose one of three protocols supported by^M
# OpenVPN. If left commented out, defaults^M
# to udp.^M
(...)
```

Kemudian copy file dari Windows ke UNIX untuk mengconvert itu ke format UNIX simply type:

```
debian01:~# dos2unix sample.ovpn
```

Konfigurasi sistem linux

Pada step selanjutnya kita telah mengadapsikan konfigurasi linux, hanya kita tidak pada sistem windows sebelumnya. Kita akan menggunakan dengan sesungguhnya konfigurasi yang sama pada contoh pertama ; hanya tiga baris yang telah diubah. Dibawah ini figure yang memberikan pilihan bagaimana interface yang akan di set up :



Pada konfigurasi openVPn adalah windows sebagai rekan. Hanya memdifikasikan baris di bawah ini pada sample.ovpn:

1. remote 10.10.10.103
2. ifconfig 10.3.0.5 255.255.255.0
3. secret key.txt

Dan adapt dari yang anda inginkan. IP menspecifiikasikan pada baris remote 10.10.10.103 harus ditempatkan de ngan pada server windows. IP dispecifikasikan pada baris ifconfig 10.3.0.5 255.255.255.0 mendefinisikan IP pada interface jaringan tunnel virtual. Anda mungkin telah memberitahukan bahwa IP dapat dipilih dengan bebas pada segment jaringan ini.

Setelah anda melakukannya, up tunnel dengan perintah di bawah ini :

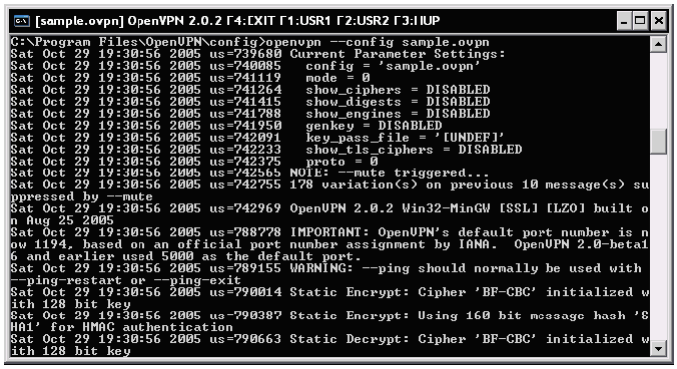
```
openvpn –-config sample.ovpn
```

Output yang akan diterima adalah :

```
Wed Oct 19 00:23:01 2005 us=318267 TUN/TAP device tap0 opened
Wed Oct 19 00:23:01 2005 us=318335 TUN/TAP TX queue length set to 100
Wed Oct 19 00:23:01 2005 us=318372 /sbin/ifconfig tap0 10.3.0.5 netmask
255.255.255.0 mtu 1500 broadcast 10.3.0.255
Wed Oct 19 00:23:01 2005 us=334639 Data Channel MTU parms [ L:1577 D:1450
EF:45 EB:135 ET:32 EL:0 AF:3/1 ]
Wed Oct 19 00:23:01 2005 us=334726 Local Options String: 'V4,dev-type
tap,link-mtu 1577,tun-mtu 1532,proto UDPv4,ifconfig 10.3.0.0
255.255.255.0,comp-lzo,cipher BF-CBC,auth SHA1,keysize 128,secret'
```

```
Wed Oct 19 00:23:01 2005 us=334740 Expected Remote Options String: 'V4,dev-
type tap,link-mtu 1577,tun-mtu 1532,proto UDPv4,ifconfig 10.3.0.0
255.255.255.0,comp-lzo,cipher BF-CBC,auth SHA1,keysize 128,secret'
Wed Oct 19 00:23:01 2005 us=334806 Local Options hash (VER=V4): 'e08453d7'
Wed Oct 19 00:23:01 2005 us=334831 Expected Remote Options hash (VER=V4):
'e08453d7'
Wed Oct 19 00:23:01 2005 us=334886 Socket Buffers: R=[109568->131072]
S=[109568->131072]
Wed Oct 19 00:23:01 2005 us=334961 UDPv4 link local (bound): [undef]:1194
Wed Oct 19 00:23:01 2005 us=334975 UDPv4 link remote: 10.10.10.103:1194
Wed Oct 19 00:23:03 2005 us=513994 Peer Connection Initiated with
10.10.10.103:1194
Wed Oct 19 00:23:03 2005 us=514046 Initialization Sequence Completed
```

Jika memulai tunnel secara manual seperti ini, openVPN GUI tidak mencatat :



Mengetest Tunnel

Untuk mengetest tunnel, gunakan pimg lagi untuk mencapai pada endpoint tunnel lainnya. Pada sistem linux :

```
debian01:~# ping 10.3.0.1
   PING 10.3.0.1 (10.3.0.1) 56(84) bytes of data.
   64 bytes from 10.3.0.1: icmp_seq=1 ttl=128 time=2.77 ms
   64 bytes from 10.3.0.1: icmp_seq=2 ttl=128 time=0.982 ms
   64 bytes from 10.3.0.1: icmp_seq=3 ttl=128 time=0.872 ms
   64 bytes from 10.3.0.1: icmp_seq=4 ttl=128 time=0.836 ms
   --- 10.3.0.1 ping statistics ---
   4 packets transmitted, 4 received, 0% packet loss, time 3020ms
   rtt min/avg/max/mdev = 0.836/1.366/2.774/0.814 ms
```

Melihat pada interface Linux

Telah kita ketahui pada windows, kita telah mempunyai pada interface linux sekarang. Type ifconfig menggambarkan linux yang interfacenya :

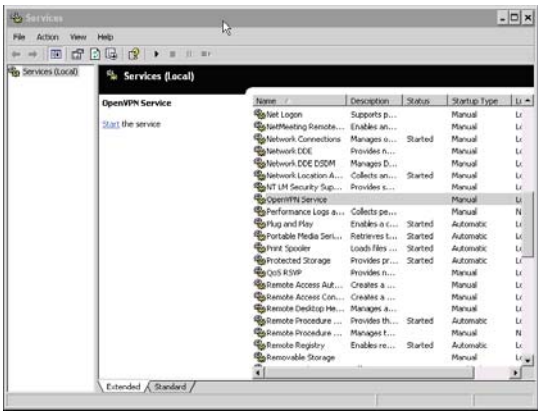
```
debian01:~# ifconfig
eth0 Link encap:Ethernet HWaddr 00:0C:29:4B:46:B3
inet addr:10.10.10.105 Bcast:10.10.10.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:11346 errors:0 dropped:0 overruns:0 frame:0
TX packets:8687 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1593787 (1.5 MiB) TX bytes:1458734 (1.3 MiB)
Interrupt:18 Base address:0x1080
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:644 errors:0 dropped:0 overruns:0 frame:0

TX packets:644 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:73352 (71.6 KiB) TX bytes:73352 (71.6 KiB)
tap0 Link encap:Ethernet HWaddr 00:FF:0E:87:FA:DD
inet addr:10.3.0.5 Bcast:10.3.0.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:10 errors:0 dropped:0 overruns:0 frame:0
TX packets:9 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:921 (921.0 b) TX bytes:666 (666.0 b)
```

Menjalankan secara otomatis OpenVPN

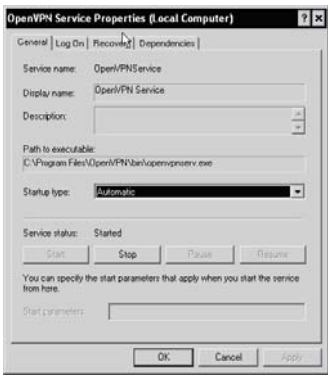
Jika ingin menjalankan mesin untuk melengkapi remote acces seperti server VPN, anda akan memulai proces openVPN (task) dan menjalankan secara permanent. Klien seperti yang kita konfigurasikan sebelum dikoneksikan, tunnel adalah up. Pada windows, task ini melakukan service module pada control panel.

OpenVPN sebagai server Windows

Dari main menu, pilih masukan Control Panel | Administrative Tools | Services untuk start service manager.



Scroll down daftar ini sampai memasuki OpenVPN Service. Kolom ke empat menggambarkan startup tipe untuk OpenVPN dan itu di set secara manual oleh default. Double-click masukan dan anda akan melihat properties window:



OpenVPN sebagai Server pada Linux

Selama instalasi linux pada system Debian-based systems, anda telah mempunyai apa yang diinginkan OpenVPN untuk memulai secara otomatis.Ini adalah standard jika memasuki pada semua waktu. Pada windows kita telah menservice dialog dan linux disana ada directory /etc/init.d yang memulai secara berlebihan pada process server. Secara tipical pada directory ini dapat disebut dengan pilihan start and stop .Proses server digambarkan pada code itu. Setelah anda menginstall

openVPN/etc/init.d/openvpn pada system anda dapat menggunakan untuk stop dan start server.

Beberapa contoh pada OpenVPN di Linux :

Program	Kegunaan
Init<runlevel>	Mengubah nomor runlevel<runlevel>
Runlevel	Daftar runlevel yang aktif
Update-rc.d<option>	Membantu untuk menyusun proses secara otomatis

Menggunakan runlevel dan init untuk merubah dan mengecek Runlevel

Antara run level dan init sangat mudah menggunakan program. Switch init 1 pada system untuk runlevel 1—dikonfigurasikan sebagai single user mode untuk perbaikan switch . init 5 ke runlevel 5, yang mana digunakan pada menu desktop.

Pada contoh di bawah ini, kita akan memulai menemukan yang maa runlevel pada system dan sebagai langkah selanjutnya, switch ke runlevel 5. Mulai lagi, kita akan mengecheck jika runlevel akan diubah dengan berhasil dan merubah itu ke runlevel 3, Dimana kita sebelumnya :

```
debian01:~# runlevel
N 2
debian01:~#init 5
INIT: Switching to runlevel: 5
(...)
debian01:~# runlevel
2 5
debian01:~#init 3
INIT: Switching to runlevel: 3
(...)
debian01:~# runlevel
5 3
debian01:~#
```

Kontrol system untuk Runlevel

File konfigurasi /etc/inittab berisikan informasi tentang program init untuk menentukan:

1. Standard runlevel (setelah booting)
2. Direktori yang akan digunakan

3. Banyak pilihan (contoh, apa yang terjadi setalah anda tekan Ctrl+Alt+Delete)

Berikut ini adalh ekstrak dari file inittab pada sistem Debian:

```
# /etc/inittab: init(8) configuration.
# $Id: inittab,v 1.91 2002/01/25 13:35:21 miquels Exp $
# The default runlevel.
id:2:initdefault:
(...)
```

Baris terakhir menunjukkan standard runlevel setelah reboot – pada system ini, runlevel 2 dan berikut comment nya mengindikasikan dimana init menunjukkan bagaimana runlevel bekeraha pada system Debian:

```
(...)
# /etc/init.d executes the S and K scripts upon change
# of runlevel.
#
# Runlevel 0 is halt.
# Runlevel 1 is single-user.
# Runlevels 2-5 are multi-user.
# Runlevel 6 is reboot.
(...)
```

Mengatur Script init

Peralatan penting yang ketiga untuk mengatur server pada Debian Linux adalah update-rc.d. Perl Script ini dapat mengecek, membuat, dan menghapus init script untuk system konfigurasi anda.

Pilihan untuk update-rc.d	**Keterangan**
update-rc.d <service> <options> <action>	Menkonfigurasi link pada init direktori anda sesuai kebutuhan
update-rc.d -n <options>	Dry-run Mode;hanya menunjukkan apa yang akan dilakukan
update-rc.d <options> remove	Mengganti start/stop daftar script pada

	option
update-rc.d -f <options>	Peringatan yang diabaikan

Mari kita lakukan beberapa contoh: perintah update-rc.d - n openvpn remove memindahkan semua link ke Openvpn, tetapi tidak benar-benar, hanya saat mengulangi untuk menguji jika akan ada permasalahan. Setelah perintah ini , Openvpn tidak akan dimulai lagi di manapun runlevel. Contoh, kita menghadapi suatu masalah kecil, yang dengan mudah ditetapkan oleh "force" tombol - f, update-rc.d - n - f openvpn remove memberi kita daftar file yang akan dihapus.

```
debian01:/etc/rc3.d# update-rc.d -n openvpn remove
update-rc.d: /etc/init.d/openvpn exists during rc.d purge (use -f to
force)
debian01:/etc/rc3.d# update-rc.d -n -f openvpn remove
update-rc.d: /etc/init.d/openvpn exists during rc.d purge (continuing)
Removing any system startup links for /etc/init.d/openvpn ...
/etc/rc0.d/K20openvpn
/etc/rc1.d/K20openvpn
/etc/rc2.d/S16openvpn
/etc/rc3.d/S16openvpn
/etc/rc4.d/S16openvpn
/etc/rc5.d/S16openvpn
/etc/rc6.d/K20openvpn
debian01:/etc/rc3.d# ls -l /etc/rc2.d/S16openvpn
lrwxrwxrwx 1 root root 17 2005-09-04 16:23 /etc/rc2.d/S16openvpn ->
../init.d/openvpn
debian01:/etc/rc3.d#
```

seperti yang anda lihat pada baris terakhir, file-file masid disana. Ulangi langkah-langkah ini tanpa option-n, and link-link akan dihapus secara permanent.
Update-rc dapat juga membuat link untuk anda. Syntaks nya mudah:
update-rc.d <options> <service name><start/stop><service number><runlevel>
Berikut ini adalah command untuk memulai OpenVPN menggunakan service nomor 16 runlevel 3:

```
debian01:/etc/rc3.d# update-rc.d -f openvpn start 16 3 .
```

```
Adding system startup for /etc/init.d/openvpn ...
/etc/rc3.d/S16openvpn -> ../init.d/openvpn
debian01:/etc/rc3.d# ls -l /etc/rc3.d/S16openvpn
lrwxrwxrwx 1 root root 17 2005-10-21 12:37 /etc/rc3.d/S16openvpn ->
../init.d/openvpn
debian01:/etc/rc3.d#
```

Sekarang cobalah anda buat link yang telah anda hapus diatas.

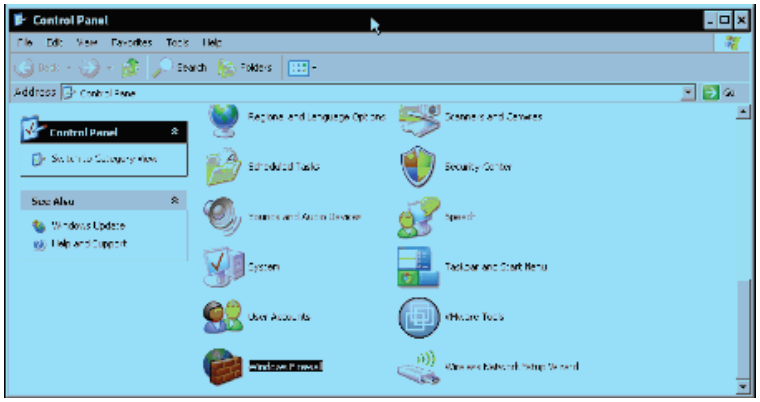
Jika anda ingin berbalik ke default konfigurasi OpenVPN— seperti setelah instalasi — maka hanya dengan masuk dpkg-reconfigure openvpn. Program ini memulai post-install dialog konfigurasi dan proses lagi, dan menginstal default yang menghubungkan ke runlevel direktori anda.

Troubleshooting Firewall Issues

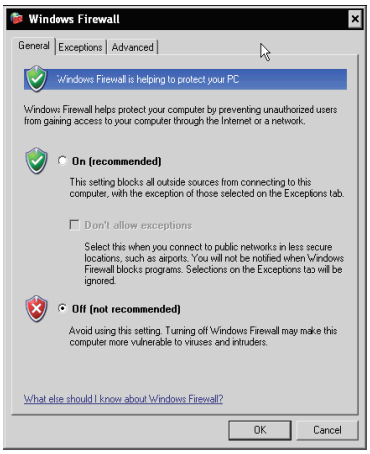
Windows XP dan Linux SuSE mempunyai sistem menginstall firewall yang diaktifkan secara otomatis setelah instalasi. Seperti kebanyakan firewall (personal atau desktop) dikonfigurasi untuk mengizinkan traffic dari sistim lokal dan ditujukan untuk Internet atau jaringan lokal. Konfigurasi ini cukup untuk OpenVPN pada hampir setiap kasus. Bagaimanapun, jika tunnel anda tidak akan mulai dan anda menerima pesan mengumumkan permasalahan koneksi, mungkin itu merupakan kesalahan dari mis-configured desktop firewall. Hanya Linux SuSE dan Windows XP datang dengan pre-installed firewall, kita akan belajar bagaimana caranya menonaktifkan firewall-firewall ini dengan cepat.

Menonaktifkan Firewall

Di Windows XP dengan layanan pack 2, anda akan menemukan konfigurasi firewall dengan memasuki Control Panel. Jika anda mempunyai service pack installed, anda akan menemukan icon Windows Firewall di dalam daftar yang tersedia pada modul-modul control panel.



Double-click pada icon Windows Firewall untuk memulai konfigurasi dialog dari firewall. Window akan ditampilkan seperti berikut :



Aktifkan tombol Off (tidak direkomendasikan) untuk menonaktifkan Windows Firewall. Klik OK untuk mengakhiri setup. sistim Windows anda tak dilindungi sekarang.

Itu harus dipertimbangkan ketidak bijaksanaan untuk menjalankan sistem Windows tanpa suatu firewall, tetapi bagi OpenVPN test-bed kita, ini dapat diterima. Tolong jangan menggunakan hal ini di dalam lingkungan produksi. Pada Bab 8, kita akan berhubungan dengan setup firewall yang tepat untuk OpenVPN host.

Jika anda tidak ingin menonaktifkan firewall Windows anda, anda dapat dengan tegas mengizinkan akses OpenVPN ke Internet. Jika anda memulai suatu koneksi OpenVPN, anda mungkin ditanya oleh software firewall anda:

Windows Security Alert dialog ini menginformasikan kepada anda bahwa sebuah local program disebut openvpn (asing, bukan?) menginginkan untuk menerima koneksi dari Internet. Klik Unblock di sini, dan OpenVPN akan bekerja bagus dengan firewall Windows.

Ringkasan

Pada bab ini, kita telah mengkonfigurasi tunnel pertama kita. Kita telah menghubungkan system windows dan linux dan mengirim dengan aman enkripsi key menggunakan WinSCP. Kita harus mengguanakan peralatan dos2unix untuk membenarkan plaintext files exchanged. Setelah kita menguji tunnel dan mengaktifkan pada boot time di kedua sistem, termasuk perkenalan singkat ke Linux init sistem dan runlevel. Topik terakhir kita telah mendiskusikan tentang Windows dan SuSE Linux firewall issues, termasuk menghentikan dan mengaktifkan firewall ini.

BAB 6
Troubleshooting dan Monitoring

Uji konektivitas jaringan

Pada setup openVpn typical, kita mempunyai koneksi dua jaringan (192.168.250.0/24 dan 172.16.76.0/24) via dua linux server yang dikoneksikan ke internet via gateway default. Diantara dua linux server adalah tunnel yang digunakan IP virtual 10.179.10.1 and 10.179.10.2. Pada koneksi jaringan local disana ada dua mesin linux yang akan kita gunakan untuk mengetest semua tunnel (mungkin dengan mengaksesnya akan menjamin keamananya). Kita sekarang akan menggunakan tool ifconfig, route dan ping untuk menggambarkan dan mengetest settingan jaringan.

Pada langkah awal, kita akan mengecek local sistem alamat jaringan, route default dan jika router default adalah pingable. Perintah ifconfig akan menunjukkan statistic pada semua interface jaringan aktif :

```
root@sydney:~ #ifconfig
eth0       Link encap:Ethernet HWaddr 00:0C:29:AE:8C:D7
           inet           addr:192.168.250.128          Bcast:192.168.250.255
           Mask:255.255.255.0
           UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
           RX packets:2640 errors:0 dropped:0 overruns:0 frame:0
           TX packets:2290 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:1000
           RX bytes:250738 (244.8 KiB) TX bytes:273328 (266.9 KiB)
           Interrupt:10 Base address:0x1080
lo         Link encap:Local Loopback
           inet addr:127.0.0.1 Mask:255.0.0.0
           UP LOOPBACK RUNNING MTU:16436 Metric:1
           RX packets:57 errors:0 dropped:0 overruns:0 frame:0
           TX packets:57 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:0
           RX bytes:7907 (7.7 KiB) TX bytes:7907 (7.7 KiB)
```

Sistem ini mempunyai alamat IP 192.168.250.128 dan interface jaringannya adalah up dan running. Sekarang lihat pada isi routing. Perintah route menunjukkan semua isi routing, meliputirouter ke internet. Gateway default adalah router yang mendukung untuk menghandle semua traffic yang tidak spesific oleh isi routing lainnya. Pada jaringan kita, server OpenVpn adalah router dari jaringan internal dan itu dikonfigurasikan sebagai gateway default untuk jaringan local.

Tipe route –n untuk menerima numeric output pada tabel routing pada sistemmu. Tipe route yang simple akan bekerja pada banyak kasus, tetapi perintah akan berusaha untuk meleawtkan IP via DNS yang mana mungkin akan mengambil waktu yang sebentar.

```
root@sydney:~ #route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
192.168.250.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
0.0.0.0 192.168.250.251 0.0.0.0 UG 0 0 0 eth0
```

Kita melihat dimana tabel tujuannya,gateway,netmask dan interface yang didengar.setiap baris adalah isi routing yang dapat dibaca seperti kalimat yang nyata. Isi dari matches simply 0.0.0.0 setiap alamat (source dan destination,tergantung dari isi) dan digunakan untuk gateway default. Baris ketiga maksudnya bahwa semua trafik ke jeringan 192.168.250.0 dikirim secara langsung ke interface jaringan eth0, tidak ada perihal yang mana gateway yang digunakan.baris keempat mengindikasikan bahwa semua traffic ke tiap destination akan dikirim lebih ke gateway default 192.168.250.25 via interface eth0. Setup ini hádala sempurna untuk client jeringan typical. Mari sekarang kita testgateway default yang dicapai dari ping dari client.

```
root@sydney:~ #ping 192.168.250.251
PING 192.168.250.251 (192.168.250.251): 56 data bytes
64 bytes from 192.168.250.251: icmp_seq=0 ttl=64 time=1.3 ms
64 bytes from 192.168.250.251: icmp_seq=1 ttl=64 time=0.6 ms
64 bytes from 192.168.250.251: icmp_seq=2 ttl=64 time=0.4 ms
--- 192.168.250.251 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.4/0.7/1.3 ms
```

Kemudian bekerja. Gateway default (semua server openvpn) menjawab ping request dari client. Jika itu tidak pada setupmu, chek rule firewall pada server apakah mengikuti traffic dari jaringan internal ke firewall itu sendiri. Jika kamu tidak yakin, itu mungkin akan menjadi ide yang bagus untuk sementara menstop pelayanan firewall.

```
root@munich:~ #ifconfig
    eth0   Link encap:Ethernet HWaddr 00:0C:29:21:07:FC
       inet addr:172.16.76.128 Bcast:172.16.76.255 Mask:255.255.255.0
       UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
       RX packets:2399 errors:0 dropped:0 overruns:0 frame:0
       TX packets:2715 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:345146 (337.0 KiB) TX bytes:271839 (265.4 KiB)
       Interrupt:10 Base address:0x1080
    lo       Link encap:Local Loopback
       inet addr:127.0.0.1 Mask:255.0.0.0
       UP LOOPBACK RUNNING MTU:16436 Metric:1
       RX packets:8 errors:0 dropped:0 overruns:0 frame:0
       TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:0
       RX bytes:772 (772.0 B) TX bytes:772 (772.0 B)
root@munich:~ #route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
172.16.76.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
0.0.0.0 172.16.76.251 0.0.0.0 UG 0 0 0 eth0
root@munich:~ #ping 172.16.76.251
PING 172.16.76.251 (172.16.76.251): 56 data bytes
64 bytes from 172.16.76.251: icmp_seq=0 ttl=64 time=2.0 ms
64 bytes from 172.16.76.251: icmp_seq=1 ttl=64 time=0.5 ms
64 bytes from 172.16.76.251: icmp_seq=2 ttl=64 time=0.5 ms
--- 172.16.76.251 ping statistics ---
3 packets transmitted, 3 packets received
```

Konfigurasi jaringan dan routing benar, dan ping ke server VPN bekerja.

Pada operasi system Microsoft kamu akan mempunyai tipe ping /t untuk pin persintent,ifconfig untuk jaringan data, dan /all route untuk menerima table routing.

Mengecek interface, routing dan koneksi pada server VPN

Pada langkah selanjutnya kita akan mempunyai close look pada settingan jaringan pada server VPN. Kita akan menggunakan tool yang sama tetapi outputnya akan menjadi complex yang lebih kecil :

```
opensuse01:~ # ifconfig
eth0 Protokoll:Ethernet Hardware Adresse 00:0C:29:13:EC:48
inet Adresse:172.16.103.2 Bcast:172.16.103.255 Maske:255.255.255.0
inet6 Adresse: fe80::20c:29ff:fe13:ec48/64
Gültigkeitsbereich:Verbindung
UP BROADCAST NOTRAILERS RUNNING MULTICAST MTU:1500 Metric:1
RX packets:2900 errors:0 dropped:0 overruns:0 frame:0
TX packets:4790 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 Sendewarteschlangenlänge:1000
RX bytes:759578 (741.7 Kb) TX bytes:666545 (650.9 Kb)
Interrupt:10 Basisadresse:0x1080
eth1 Protokoll:Ethernet Hardware Adresse 00:0C:29:13:EC:52
inet Adresse:172.16.76.251 Bcast:172.16.76.255 Maske:255.255.255.0
inet6 Adresse: fe80::20c:29ff:fe13:ec52/64
Gültigkeitsbereich:Verbindung
UP BROADCAST NOTRAILERS RUNNING MULTICAST MTU:1500 Metric:1
RX packets:797 errors:0 dropped:0 overruns:0 frame:0
TX packets:421 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 Sendewarteschlangenlänge:1000
RX bytes:77682 (75.8 Kb) TX bytes:42404 (41.4 Kb)
Interrupt:9 Basisadresse:0x1400
lo Protokoll:Lokale Schleife
inet Adresse:127.0.0.1 Maske:255.0.0.0
inet6 Adresse: ::1/128 Gültigkeitsbereich:Maschine
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:109 errors:0 dropped:0 overruns:0 frame:0
TX packets:109 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 Sendewarteschlangenlänge:0
   RX bytes:8380 (8.1 Kb) TX bytes:8380 (8.1 Kb)
tunVPN0 Protokoll:UNSPEC Hardware Adresse 00-00-00-00-00-00-00-00-00-00-00-
00-00-00-00-00
inet Adresse:10.179.10.2 P-z-P:10.179.10.1 Maske:255.255.255.255
UP PUNKTZUPUNKT RUNNING NOARP MULTICAST MTU:1500 Metric:1
RX packets:1337 errors:0 dropped:0 overruns:0 frame:0
TX packets:1547 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 Sendewarteschlangenlänge:100
```

```
RX bytes:470725 (459.6 Kb) TX bytes:181397 (177.1 Kb)
```

Ok, server ini mempunyai jaringan interface card eth0 dan eth1 (dengan dua jaringan 172.16.103.0/24 dan 172.16.76.0/24) pada penambahan ke tunnel jaringan openVpn tunVPN0 dengan alamat jaringan 10.179.10.2 dan partner point-to-point IP 10.179.10.2. bagaimana dengan routing?

```
opensuse01:~ # route -n
Kernel IP Routentabelle
Ziel Router Genmask Flags Metric Ref Use Iface
10.179.10.1 0.0.0.0 255.255.255.255 UH 0 0 0
tunVPN0
172.16.103.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
172.16.76.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1
192.168.250.0 10.179.10.1 255.255.255.0 UG 0 0 0
tunVPN0
127.0.0.0 0.0.0.0 255.0.0.0 U 0 0 0 lo
0.0.0.0 172.16.103.1 0.0.0.0 UG 0 0 0 eth0
```

Routing adalah bagian terkecil yang terumit disini. Kita mempunyai dua koneksi subnet eth0 dan eth1 dan dua isi untuk semua túnel. Semuanya ke alamat IP virtual 10.179.10 adalah route via interface tunVPN0 seperti traffic ke subnet 192.168.250.0/24 tetapi router via gateway 10.179.10.1. yang terakir tapi tidak terlalu penting adalah gateway default pada router ini yang mempunyai IP 172.16.103.1. Dengan benar jeringan lain diantara firewall dan internet. Mari sekarang kita ping partner point to point pada mesin ini.kita tidak dapat melihat dari maksud interface. Daftar bahwa mesin ini mempunyai IP virtual 10.179.10.2 dan partner VPN mempunyai IP 10.179.10.1. Jika semua tunnel bekerja.itu seharusnya mungkin untung ping tunnel :

```
opensuse01:~ # ping 10.179.10.1
PING 10.179.10.1 (10.179.10.1) 56(84) bytes of data.
64 bytes from 10.179.10.1: icmp_seq=1 ttl=64 time=1.77 ms
64 bytes from 10.179.10.1: icmp_seq=2 ttl=64 time=1.50 ms
64 bytes from 10.179.10.1: icmp_seq=3 ttl=64 time=1.42 ms
64 bytes from 10.179.10.1: icmp_seq=4 ttl=64 time=1.44 ms
--- 10.179.10.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3013ms
rtt min/avg/max/mdev = 1.425/1.535/1.770/0.141 ms
```

Itu bekerja. Tolong catat bahwa waktu mengambil untuk menjawab ping yang akan disignificant lebih tinggi melewati tunnel daripada untuk local atau ping langsung. Mari sekarang melakukan test yang sama dengan jalan lain. Kita akan menganalisa jaringan dan routing pada server sydney dan berusaha ping ke tunnel munich :

```
debian01:~# ifconfig
eth0 Link encap:Ethernet HWaddr 00:0C:29:99:7B:CA
inet addr:172.16.247.2 Bcast:172.16.247.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:7735 errors:0 dropped:0 overruns:0 frame:0
TX packets:11012 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:924335 (902.6 KiB) TX bytes:1714169 (1.6 MiB)
Interrupt:18 Base address:0x1080
eth1 Link encap:Ethernet HWaddr 00:0C:29:99:7B:D4
inet addr:192.168.250.251 Bcast:192.168.250.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:490 errors:0 dropped:0 overruns:0 frame:0
TX packets:468 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:47652 (46.5 KiB) TX bytes:43728 (42.7 KiB)
Interrupt:19 Base address:0x1400
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
tunVPN0 Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-
00-00
inet addr:10.179.10.1 P-t-P:10.179.10.2 Mask:255.255.255.255
UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
RX packets:1849 errors:0 dropped:0 overruns:0 frame:0
TX packets:1489 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:206765 (201.9 KiB) TX bytes:483493 (472.1 KiB)
debian01:~# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
10.179.10.2 0.0.0.0 255.255.255.255 UH 0 0 0 tunVPN0
172.16.247.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
```

```
172.16.76.0 10.179.10.2 255.255.255.0 UG 0 0 0 tunVPN0
192.168.250.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1
0.0.0.0 172.16.247.1 0.0.0.0 UG 0 0 0 eth0
debian01:~# ping 10.179.10.1
PING 10.179.10.1 (10.179.10.1) 56(84) bytes of data.
64 bytes from 10.179.10.1: icmp_seq=1 ttl=64 time=0.221 ms
64 bytes from 10.179.10.1: icmp_seq=2 ttl=64 time=0.069 ms
64 bytes from 10.179.10.1: icmp_seq=3 ttl=64 time=0.059 ms
--- 10.179.10.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 0.059/0.116/0.221/0.074 ms
```

Itu bekerja. Kita sekarang yakin mempunyai bahwa :

1. Server VPN mencapai jaringan localnya.
2. Tunnel openVPN adalah up dan running
3. Tunnel openVPN bekerja antara aturan.

Mari sekarang masuki level lainnya pada pengetestan. Kita akan tahu mengetest jika jaringan sidney tercapai dari server VPN di munich—masih menggunakan paket ICMP. Program traceroute akan menolong kita mengikuti route paket mengambil :

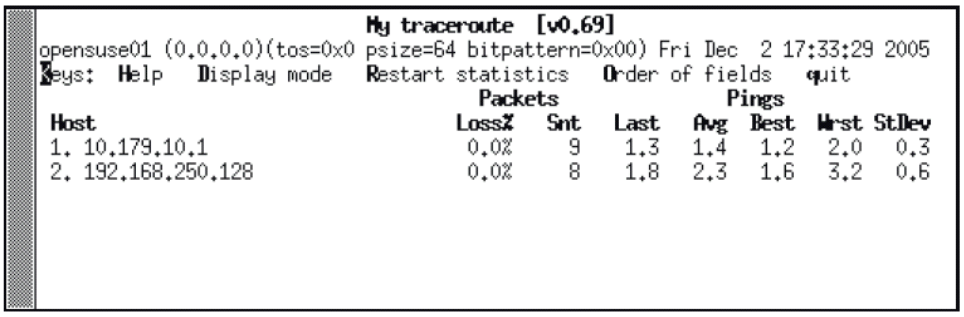
```
opensuse01:~ # ping 192.168.250.128
PING 192.168.250.128 (192.168.250.128) 56(84) bytes of data.
64 bytes from 192.168.250.128: icmp_seq=1 ttl=63 time=1.90 ms
64 bytes from 192.168.250.128: icmp_seq=2 ttl=63 time=1.26 ms
64 bytes from 192.168.250.128: icmp_seq=3 ttl=63 time=1.57 ms
--- 192.168.250.128 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2009ms
rtt min/avg/max/mdev = 1.261/1.577/1.900/0.264 ms
opensuse01:~ # traceroute -n 192.168.250.128
traceroute to 192.168.250.128 (192.168.250.128), 30 hops max, 40 byte
packets
1 10.179.10.1 1.874 ms 8.949 ms 20.241 ms
2 192.168.250.128 24.911 ms 35.618 ms 40.988 ms
```

Ping berjalan dengan baik. Ini mengindikasikan routing benar pada sisi sydney dan server VPN munich. Output pada program traceroute mendaftar semua server paket melalui jalan lain ke siney. Mereka akan masuk kedalam tunnel rata-rata dan datang pada server VPN di sidney 10.179.10.1, yang mana mengikuti pada mesin lokal yang

mana mengambil 10ms. Tentu saja kita dapat juga ”traceroute” semua paket yang pergi ke yang lain, menyedikan bahwa administrator pada server debian menginstall tracerote (232 apt-get install traceroute).

> Pada operasi system Microsoft perintah traceroute menawarkan fungsi yang sama sebagai tarceroute pada Linux.

Tool lainnya adalah ”My traceroute” atau mtr disebut mtr –n 192.168.250.128, mtr menjalankan perintah mtr –n 192.168.250.128, sampai tipe q atau ctrl+c. Output akan digambarkan pada table clear. Dengan perintah ini, kita dapat dengan mudah switch isi routing dan mengontrol effect secara interactive.



Debugging dengan tcpdump dan IPTraf

Tool lainnya adalah untuk mengontrol traffic tcpdump. Sebagai jaringan sniffer, tcpdump sering digunakan oleh administrator atau hacker untuk mengoleksi perubahan data pada jaringan. Gambarkan tcpdump semua traffic yang melewati. Interface yang memberikan parameter. Contoh dibawah ini menggambarkan penggunaan tcpdump. Pada saat kita memanggil pilihan -n dan -i eth1, tcpdump akan didengarkan pada interface eth1 dan memberikan jumlah output (dengan keputusan DNS).

```
debian01:~# tcpdump -n -i eth1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 96 bytes
21:00:16.640142 IP 192.168.250.128 > 172.16.76.128: ICMP echo request, id
55298, seq 0, length 64
```

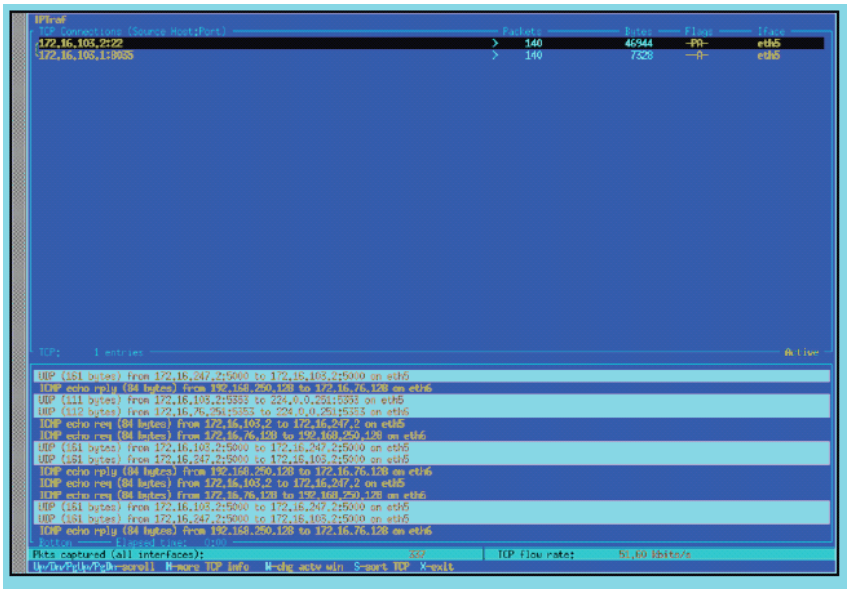
```
21:00:16.648116 IP 172.16.76.128 > 192.168.250.128: ICMP echo reply, id
55298, seq 0, length 64
21:00:17.678429 IP 192.168.250.128 > 172.16.76.128: ICMP echo request, id
55298, seq 256, length 64
21:00:17.680701 IP 172.16.76.128 > 192.168.250.128: ICMP echo reply, id
55298, seq 256, length 64
21:00:18.668565 IP 192.168.250.128 > 172.16.76.128: ICMP echo request, id
55298, seq 512, length 64
21:00:18.670722 IP 172.16.76.128 > 192.168.250.128: ICMP echo reply, id
55298, seq 512, length 64
21:00:19.688618 IP 192.168.250.128 > 172.16.76.128: ICMP echo request, id
55298, seq 768, length 64
21:00:19.690836 IP 172.16.76.128 > 192.168.250.128: ICMP echo reply, id
55298, seq 768, length 64
```

Kita dapat melihat, tcpdump disana ada empat pesan ICMP echo request dikirim dari 192.168.250.128 ke 172.16.76.128. semuanya dari mereka akan dijawab oleh mesin 172.16.76.128. dengan pesan “echo reply”. Sekarang kita dapat menggunakna pada setiap mesin di chain pada router antara dua klien pada track paket ICMP. Sebagai contoh, jika firewall dibloking oleh pesan ICMP kemudian no PC disembunyikan firewall ini akan menerima tiap permintaan dan jawaban, dimanapun mesin sebelum firewall akan melakukan.

```
debian01:~# tcpdump -ni tunVPN0
tcpdump: WARNING: arptype 65534 not supported by libpcap - falling back to
cooked socket
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tunVPN0, link-type LINUX_SLL (Linux cooked), capture size 96
bytes
21:07:53.800707 IP 172.16.76.128 > 192.168.250.128: ICMP echo request, id
19971, seq 9472, length 64
21:07:53.801608 IP 192.168.250.128 > 172.16.76.128: ICMP echo reply, id
19971, seq 9472, length 64
21:07:54.799266 IP 172.16.76.128 > 192.168.250.128: ICMP echo request, id
19971, seq 9728, length 64
21:07:54.800531 IP 192.168.250.128 > 172.16.76.128: ICMP echo reply, id
19971, seq 9728, length 64
21:07:55.800302 IP 172.16.76.128 > 192.168.250.128: ICMP echo request, id
19971, seq 9984, length 64
```

```
21:07:55.801296 IP 192.168.250.128 > 172.16.76.128: ICMP echo reply, id
19971, seq 9984, length 64
21:07:56.752248 IP 172.16.76.128 > 192.168.250.128: ICMP echo request, id
19971, seq 10240, length 64
21:07:56.752876 IP 192.168.250.128 > 172.16.76.128: ICMP echo reply, id
19971, seq 10240, length 64
8 packets captured
16 packets received by filter
0 packets dropped by kernel
```

Kita juga dapat tcpdump pada interface tunnel tetapi beberapa feature tidak ingin bekerja dengan interface TUN atau TAP. Juga karena pada interface tunnel akan menjalankan mode pengacau, tcpdump akan memburuhkan root. Informasi kembali akan di menjadi jarang pada switch jaringan, dimana hanya paket local yang akan digambarkan.tool lainnya yang menolong IPTraf (pada installed debian dengan apt-get install iptraf) IPTrafdatang dengan banyak pilihan, tetapi kita hanya mengetahui focus pada daftar pilihan masuk dan sembunyikan kembali empat waktu. Kamu akan mendapatkan jendela screenshot seperti di bawah ini :



Pada setengah window, koneksi TCP 234 akan didisplaykan. UDP, ICMP dan koneksi lainnya dapat ditemukan setengahnya. Pada contoh diatas kita dapat menyatakan sesion SSH (dari IPTraf kita memulai), paket ICMP diantara client PC sydney dan munich, dan

paket UDP encapsulating paket ICMP. Sembunyikan Xtwice dan masuk sekali lagi untuk menghentikan IPTraf.

Menggunakan Protokol OpenVPN dan File Status untuk Debugging

Metode yang mudah dicapai untuk melihat tunnel traffic adalah mensetting veborsity pada openVPN untuk 5 level. Secara sederhana digambarkan dengan memasuki verb 5 pada konfigurasi file. Di bawah ini output digambarkan pada protocol file openVPN (sebagai spesifikasi di konfigurasi file OpenVPN):

```
Fri Dec 9 21:05:15 2005 us=51912 Data Channel Encrypt: Cipher 'AES-256-
CBC' initialized with 256 bit key
Fri Dec 9 21:05:15 2005 us=51944 Data Channel Encrypt: Using 160 bit
message hash 'SHA1' for HMAC authentication
Fri Dec 9 21:05:15 2005 us=51962 Data Channel Decrypt: Cipher 'AES-256-
CBC' initialized with 256 bit key
Fri Dec 9 21:05:15 2005 us=52033 Data Channel Decrypt: Using 160 bit
message hash 'SHA1' for HMAC authentication
Fri Dec 9 21:05:15 2005 us=131924 Control Channel: TLSv1, cipher
TLSv1/SSLv3 DHE-RSA-AES256-SHA, 2048 bit RSA
WRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwr
WRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwrWR
wrWRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwrWRwr
wrWRwrWRwrWRwrWRwrWRwrWRwrWRwrW (...)
```

Pada baris terakir kita menemukan statistic pada semua traffic tunnel. Upper disebabkan oleh datagram TCP atau UDP pada pembacaan interface, encapsulating traffic openVPN dan sebab indikasi traffic pada interface TUN/TAP. R adalah untuk membaca dan w untuk menulis. Perintah ping yang berhasil melewati tunnel yang akan selalu menyebabkan masukan seperti WRwr atau vice versa. File lainnya yang ditulis contoh informasi ke status file. Tergantung dari periode waktu yang diberikan parameter, OpenVPN akan mengupdate informasi pada file pada basic regular. Pada contoh file /var/log/openvpn/feilner-it.status; perintah cat dapat menggambarkan isi dari file :

```
debian01:~# cat /var/log/openvpn/feilner-it.status
OpenVPN STATISTICS
Updated,Fri Dec 9 21:26:53 2005
```

```
TUN/TAP read bytes,1102504
TUN/TAP write bytes,806453
TCP/UDP read bytes,1302857
TCP/UDP write bytes,1588558
Auth read bytes,808809
pre-compress bytes,55193
post-compress bytes,53110
pre-decompress bytes,1449
post-decompress bytes,2076
END
```

Kita menemukan statistic data dengan detail. Jika kamu menjalankan kedalam masalah dengan OpenVPN itu akan menjadi ide yang bagus untuk mengecek file ini untuk ditemukan jika nilai membuat perbedaan, atau jika disana tidak terlalu lebih atau melupakan traffic pada sisi lain sebagai contohnya, jika mendapatkan kehilangan atau routing salah. Tergantung pada system dan logging setup, disana mungkin juga memasuki isi pada protocol system seperti system SuSE dibawah ini :

```
opensuse01:~ # tail /var/log/messages
Dec 2 17:50:09 opensuse01 openvpn[11661]: Local Options String: 'V4,dev-type tun,link-mtu 1545,tun-mtu 1500,proto UDPv4,ifconfig 10.179.11.1 10.179.11.2,comp-lzo,cipher BF-CBC,auth SHA1,keysize 128,secret'
Dec 2 17:50:09 opensuse01 openvpn[11661]: Expected Remote Options String: 'V4,dev-type tun,link-mtu 1545,tun-mtu 1500,proto UDPv4,ifconfig 10.179.11.2 10.179.11.1,comp-lzo,cipher BF-CBC,auth SHA1,keysize 128,secret'
Dec 2 17:50:09 opensuse01 openvpn[11661]: Local Options hash (VER=V4): '59c313f6'
Dec 2 17:50:09 opensuse01 openvpn[11661]: Expected Remote Options hash (VER=V4): '36b1f115'
Dec 2 17:50:09 opensuse01 openvpn[11661]: Output Traffic Shaping initialized at 20000 bytes per second
Dec 2 17:50:09 opensuse01 openvpn[11674]: Socket Buffers: R=[113664->131072] S=[113664->131072]
Dec 2 17:50:09 opensuse01 openvpn[11674]: UDPv4 link local (bound): [undef]:5001
Dec 2 17:50:09 opensuse01 openvpn[11674]: UDPv4 link remote: 172.16.247.2:5001
```

Ini menunjukkan bahwa tunnel VPN lainnya membuat : OpenVPN pada port UDP 5001.

Scanning server dengan Nmap

Nmap adalah port scanner yang dapat digunakan untuk memetapkan apakah port UDP dan TCP pada mesin dibuka dan apakah proses koneksi server diterima. Nmap dapat juga ditemukan jika firewall melindungi scan mesin dan Nmap dapat menscan jaringan. Mari kita scan PC local client (yang mana dengan jelas tidak dilindungi oleh firewall):

```
opensuse01:~ # nmap 172.16.76.128
Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-12-02 18:02
CET
Interesting ports on localhost (172.16.76.128):
(The 1661 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE
22/tcp open ssh
68/tcp open dhcpclient
MAC Address: 00:0C:29:21:07:FC
Nmap finished: 1 IP address (1 host up) scanned in 1.773 seconds
```

Disana ada dua port yang membuka system ; port 1661 dan port scan lainnya ditutup. Jika disana firewall pada system kemudian scanning tidak dengan mudah, karena lebih dari firewall mendeteksi IP dan banyak lagi.halaman manual sangat bagus. Kita dapat mengetahui scan salah satu pada semua server openVPN untuk menemukan jika port VPN (5000) dapat dicapai. nmap -sU <IP> -p <Port> akan mengambil Nmap menscan hanya jika port UDP pada mesin memberikan alamat IP membuka :

```
opensuse01:~ # nmap -sU 172.16.247.2 -p 5000
Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-12-02 18:06
CET
Note: Host seems down. If it is really up, but blocking our ping probes,
try -P0
Nmap finished: 1 IP address (0 hosts up) scanned in 2.067 seconds
opensuse01:~ # nmap -P0 -sU 172.16.247.2 -p 5000
Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-12-02 18:06
CET
Interesting ports on debian01.feilner-it.home (172.16.247.2):
```

```
PORT STATE SERVICE
5000/udp open|filtered UPnP
Nmap finished: 1 IP address (1 host up) scanned in 2.039 seconds
```

Kamu dapat melihat bagaimana shorewall firewall tidak memperlihatkan informasi tentang port pada saat kita menscan itu pada pertama kali. Bagaimanapun juga , Nmap siap untuk menyembunyikan : isi parameter PO untuk melakukan secara diam-diam. Dengan pilihan ini, Nmap tidak melakukan host ping, itu menscan sebelum benar-benar scanning mereka dulu. Beberapa firewall menunjukkan ini sebagai reaksi pada port scanner dan memblok itu. Usaha kedua adalah bagaimana port UDP 5000 difilter (oleh firewall). Ini berarti : rule firewall mungkin dilindungi dan acces limited ke port ini tetapi membuka.

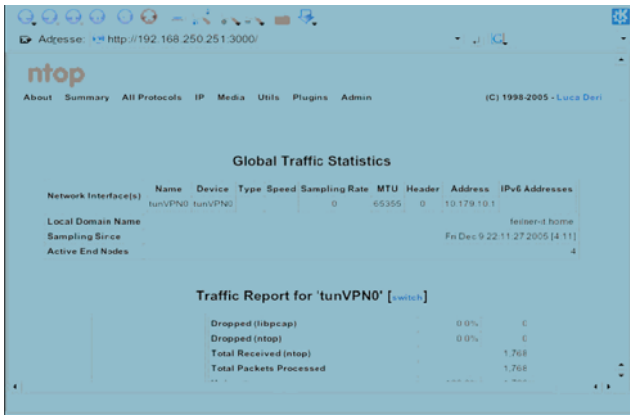
> Pada program windows “Angry IP scanner” akan mungkin menjadi pilihan utama kamu untuk scanning.

Tool monitoring

Banyak tool yang melengkapi statistic pada interface jaringan. Sangat mudah menginstall tool monitoring dengan fungsi great yaitu **ntop** dan **Munin**.

a) Ntop

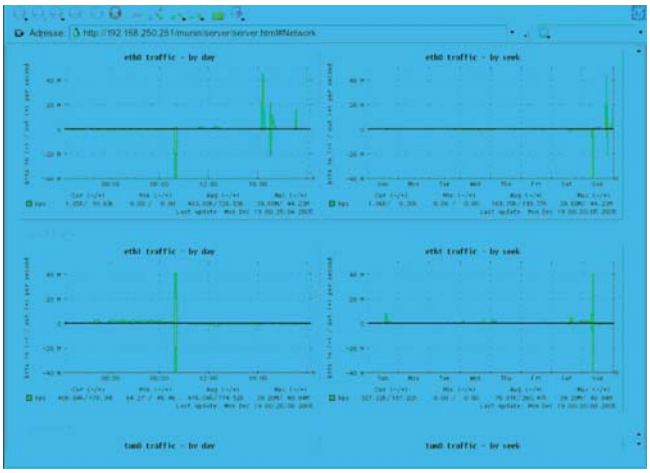
Monitor jaringan ntop dan mungkin di beberapa Negara menjadi illegal karena itu dibuat dengan detail merekam oada koneksi diantara alamat IP. Itu menerima browser GUI dan tidak membutuhkan menjalankan web server. Ntop diinstall dengan mudah pada debian. Masuk apt-get install ntop dan pilih interface yang diinginkan ke monitor. Setelah menginstalasi software , type ntop -A, dan masuki password administrator untuk account admin ntop'. Sekarang /etc/init.d/ntop start dan point browser ke http://IP:3000 pada sistem (ntop menjalankan pada port 3000). Kamu akan mendapatkan feature-rich window dengan growing amount pada informasi, sepesialnya jika ntop mempunyai waktu untuk menjalankan :



Ntop menerima banyak kemungkinan. Kita dapat menyimpan data ke database dapat terjamin dan dimonitor,interface dapat di onlinekan dan banyak kemungkinan lainnya

b) Munin

Tool statistic lainnya yang dapat menolong adalah munun. Munin terdiri dari proses server yang dikoleksikan datanya yang ditemukan berdasarkan source pada sistem linux (atau windows).Contoh dibawah ini menggambarkan standard interface munin setelah instalasi sebagai document pada http://munin.sf.net. Munin membutuhkan web server seperti apache, instalansinya sangat mudah. Munin dikonfigurasikan dari file di /etc/munin/, dan menggunakan pada jumlah yang dapat di download.



Monitoring open VPN plug-in. Plug-in harus membuat dan mengembalikan data pada format :

```
router:/usr/share/munin/plugins # /etc/munin/plugins/if_eth0
down.value 1777836059
up.value 94615124
router:/usr/share/munin/plugins #
```

Sejak permintaan untuk munin plug-in, kita dapat dengan mudah membuat monitoring Open VPN plug-in sendiri sebagai contoh pada http://rodolphe.quiedeville.org/hack/openvpn disana ada plug-in yang sederhana yang memberi laporan jumlah user yang terhubung ke server OpenVPN. Tinggalkan itu untuk menggambarkan kemungkinan plug-in pada saat menkombinasikan dengan samba, iptables, OpenVPN, dan lainnya. Hanya pikirkan pada status file OpenVPN dan informasi yang ditemukan.

Petunjuk untuk Tool lainnya

Kelebihan pada tools monitoring jaringan, , sniffing, dan scanning. Dua yang paling favorite adalah Cacti dan Nagios. Cacti is a tool monitoring yang familiar ke Munin, tetapi kelihatannya lebih kuat. Nagios adalah tool yang didisain untuk mesin monitoring dan service.

Dengan Nagios kita tidak hanya dapat menujukkan jika server dapat menunjukkan ping tetapi dapat juga mengecek untuk pelayanan oleh acces (menggunakan e.g samba atau protocol HTTP) dan trigger reaksi pada saat server tidak bisa. Kita dapat mempunyai mesin Nagios mengirimkan SMS jika kita membuka tunnel Open VPN turun, atau jika management interface tidak reaksi.

Ringkasan

Pada bab ini kita telah belajar bagaimana mengecek semua Open VPN dan mensetup jaringan step by step menggunakan standard tool linux dan mengevaluasi outputnya. Dengan tool seperti ifconfig, ping, traceroute, and mtr, Kita dapat menganalisa mengikuti datagram antara server VPN dan koneksi jaringan. Program seperti tcpdump, IPTraf, ntop,dan Munin akan memberikan kita informasi secara detail tentang traffic atau statistic breakdowns. Tempat pertama kali untuk mencari troubleshooting harus selalu menjadi log file dari OpenVPN itu sendiri—khususnya pada level lebih tinggi atau verbosity.