Jurnal Ekselenta
e- ISSN: xxxx-xxxx
Vol. 1 No. 1. Des 2024

JURNAL EKSELENTA
JURNAL ILMIAH FAKULTAS TEKNIK
UNIVERSITAS SAINS INDONESIA

PERANCANGAN INTERKONEKSI JARINGAN MENGGUNAKAN VPN BERBASIS INTERNET DENGAN IMPLEMENTASI IPV6

Ade Frihadi[1], Widianto[2]
[1]Prodi Teknik Elektro, Universitas Sains Indonesia, Bekasi
[2]Prodi Teknik Elektro, Universitas Sains Indonesia, Bekasi

Email : ade.frihadi@lecturer.sains.ac.id

Kebutuhan akan konektivitas jaringan yang aman, andal, dan skalabel mendorong penggunaan teknologi Virtual Private Network (VPN) dan protokol Internet Protocol version 6 (IPv6). Penelitian ini membahas perancangan dan implementasi interkoneksi jaringan menggunakan VPN berbasis internet yang terintegrasi dengan teknologi IPv6. Metode perancangan dilakukan dengan simulasi topologi jaringan yang mendukung pengalamatan IPv6 serta konfigurasi VPN untuk mengamankan komunikasi antar jaringan. Hasil pengujian menunjukkan bahwa integrasi VPN dan IPv6 mampu meningkatkan efisiensi dalam pengalamatan serta memberikan tingkat keamanan yang memadai untuk transmisi data lintas jaringan. Penelitian ini menjadi referensi strategis bagi perusahaan atau institusi yang sedang melakukan transisi dari IPv4 ke IPv6, sekaligus mengadopsi solusi keamanan jaringan berbasis VPN.

Kata Kunci: VPN, IPv6, Interkoneksi Jaringan, Keamanan Jaringan, Desain Jaringan

Abstract

The need for secure, reliable, and scalable network connectivity has driven the adoption of Virtual Private Network (VPN) technology and Internet Protocol version 6 (IPv6). This study discusses the design and implementation of network interconnection using internet-based VPN integrated with IPv6 technology. The design method was carried out through network topology simulations that support IPv6 addressing and VPN configurations to secure inter-network communications. Testing results indicate that the integration of VPN and IPv6 enhances addressing efficiency and cabangides an adequate level of security for cross-network data transmission. This study serves as a strategic reference for organizations or institutions undergoing the transition from IPv4 to IPv6 while adopting VPN-based network security solutions.

Keywords: VPN, IPv6, Network Interconnection, Network Security, Network Design

1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi yang pesat telah mendorong meningkatnya kebutuhan akan pertukaran data yang efisien dan aman, baik di sektor swasta maupun pemerintahan. Dalam mendukung operasional harian, entitas organisasi seperti perusahaan dan instansi pemerintah memerlukan sistem jaringan yang mampu menghubungkan berbagai lokasi secara andal. Salah satu tantangan utama dalam implementasi jaringan tertutup (private network) adalah tingginya biaya pembangunan dan pemeliharaan infrastruktur,

khususnya dalam menghubungkan kantor pusat dengan kantor cabang atau instansi pemerintah pusat dengan instansi di daerah. Sebagai solusi, pemanfaatan jaringan publik seperti internet menjadi alternatif yang menarik karena lebih ekonomis dan fleksibel dalam pelaksanaannya. Namun, penggunaan jaringan publik menimbulkan tantangan terkait keamanan dan integritas data yang ditransmisikan. Oleh karena itu, dibutuhkan teknologi yang mampu mengamankan komunikasi melalui jaringan publik, seperti Virtual Private Network (VPN), yang dikombinasikan dengan protokol Internet Protocol version 6 (IPv6) guna mendukung kebutuhan pengalamatan yang lebih luas dan sistem yang lebih modern. Penelitian ini mengkaji perancangan dan implementasi solusi interkoneksi jaringan berbasis VPN VTun dan IPv6 over IPv4 untuk mendukung kebutuhan komunikasi antar kantor pusat dan cabang secara aman, efisien, dan terintegrasi.

2. Landasan Teori

a) Jaringan Komputer

Jaringan komputer merupakan penggabungan teknologi komputer dan komunikasi yang merupakan sekumpulan komputer berjumlah banyak yang terpisah-pisah akan tetapi saling berhubungan dalam melaksanakan tugasnya.

b) Topologi jaringan

Topologi jaringan terdiri dari berbagai macam topologi yaitu, topologi bus, ring, star, extended star, hirarkikal/Tree, dan mesh. Jenis-jenis Jaringan Komputer Berdasarkan ruang lingkup geografisnya terdapat tiga jenis jaringan computer yaitu, Local Area Network, Metropolitan Area Network, Wide Area Network.

c) Routing Protokol

Routing protokol adalah suatu aturan yang mempertukarkan informasi routing yang akan membentuk sebuah tabel routing sehingga pengalamatan pada paket data yang akan dikirim menjadi lebih jelas dan mencari rute tersingkat.

Routing protocol dibagi menjadi 2, yaitu:

i. Interior Routing Protocol

Interior Routing Protocol digunakan pada jaringan yang bernama Autonomous System, yaitu sebuah jaringan yang berada hanya dalam satu kendali teknik yang terdiri dari beberapa subnetwork dan gateway yang saling berhubungan satu sama lain. Interior routing diimplementasikan melalui:

- Routing Information Protocol (RIP), biasanya terdapat pada sistem operasi UNIX dan Novell yang menggunakan metode distance vector algoritma yang bekerja dengan menambahkan satu angka matrik jika melewati 1 gateway, sehingga jika melewati beberapa gateway maka metriknya juga akan bertambah.
- Open Shortest Path First (OSPF), routing ini memakan banyak resource komputer dibanding Routing Information Protocol (RIP), akan tetapi pada routing ini rute dapat dibagi menjadi beberapa jalan sehinggga data dapat melewati dua atau lebih rute secara pararel.

ii. Exterior Routing Protocol

Pada dasarnya internet terdiri dari beberapa Autonomous System yang saling berhubungan satu sama lain dan untuk menghubungkan Autonomous System dengan Autonomous System yang lainnya maka Autonomous System menggunakan exterior routing protocol sebagai pertukaran informasi routingnya.

- Exterior Gateway Protocol (EGP) merupakan protokol yang mengumumkan kepada Autonomous System yang lain tentang jaringan yang berada dibawahnya maka jika sebuah Autonomous System ingin berhubungan dengan jaringan yang ada dibawahnya maka harus melaluinya sebagai router utama. akan tetapi kelemahan

protokol ini tidak bisa memberikan rute terbaik untuk pengiriman paket data.

- Border Gateway Protocol (BGP). Protocol ini sudah dapat memilih rute terbaik yang digunakan pada ISP besar yang akan dipilih.

d) TCP/IP

Internet Protokol dikembangkan pertama kali oleh Defense Advanced Research Projects Agency (DARPA) pada tahun 1970 sebagai awal dari usaha untuk mengembangkan protokol yang dapat melakukan interkoneksi berbagai jaringan komputer yang terpisah, yang masing-masing jaringan tersebut menggunakan teknologi yang berbeda. Protokol utama yang dihasilkan proyek ini adalah Internet Protokol (IP)

e) IPv6

IP Versi ini merupakan generasi penerus IPv4, disebut juga sebagai IPng (= IP Next Generation){Formatting Citation}, Kelebihan dari IPv6 antara lain :

- IPv6 memiliki kapasitas 128 bit, dibandingkan dengan IPv4 yang hanya 32 bit – membuat kapasitas IPv6 jauh lebih besar (2^96 kali lipat dibandingkan dengan IPv4).
- IPv6 memiliki scope (jangkauan) IP address yang terdefinisi dengan baik, spt node-local, link-local, site-local, organization-local, global-scope. Scope ini mirip dengan pemakaian private atau global ip address pada IPv4, tetapi jauh lebih fleksibel.
- Header IPv6 lebih simple dibanding dengan IPv4, ada beberapa field yang dihapuskan, sehingga dengan kemampuan yang sangat luar biasa besar, header IPv6 hanya 2x lebih besar daripada IPv4.
- IPv6 memiliki kemampuan builtin untuk otentikasi & privasi. Jika pada IPv4 harus menambahkan tunnel IPsec.

Format IPv6 Address:

- 128 Bit dan di bagi menjadi 16 bit segment.
- Setiap segment mewakilkan 4 digit hexadecimal
- X:X:X:X:X:X:X:X (X = 16 bit, cth = A2FE)
  Contoh:
  2001:0DB8:124C:C1A2:BA03:6735:EF1C:683D Di sebut sebagai colon-hexdecimal
- Penulisan IPv6 bisa di perpendek dengan menghilangkan awalan 0
- Setiap blok setidaknya harus memiliki 1 digit Sebelum di pendekan
  Contoh:
  2001:0DB8:0023:0000:0000:036E:1250:2B00 atau 2001:DB8:23:0:0:36E:1250:2B00

Mekanisme Transisi dari IPv4 ke IPv6:

- Dual-Stack, yaitu IPv4 dan IPv6 berjalan secara bersamaan di dalam host atau router
- Tunneling:
  – Melewatkan traffic IPv6 diatas jaringan IPv4
  – Melewatkan traffic IPv4 diatas jaringan IPv6

f) VPN

VPN adalah sebuah teknologi komunikasi yang memungkinkan seorang pegawai yang berada didalam kantor terkoneksi ke jaringan publik dan menggunakannya untuk bergabung dalam jaringan lokal. VPN dapat terjadi antara dua end-system atau dua PC atau bisa juga antara dua atau lebih jaringan yang berbeda. VPN dapat dibentuk dengan menggunakan teknologi tunneling dan encryption, Data dienkapsulasi (dibungkus) dengan header yang berisi informasi routing untuk mendapatkan koneksi point to point sehingga data dapat melewati jaringan publik dan dapat mencapai akhir tujuan.

Teknologi VPN menyediakan tiga fungsi utama untuk penggunanya. Fungsi utama tersebut adalah sebagai berikut:

i. Confidentiality (Kerahasiaan)

Teknologi VPN memiliki sistem kerja mengenkripsi semua data yang lewat melaluinya. Dengan adanya teknologi enkripsi ini, maka kerahasiaan data menjadi lebih terjaga.

ii. Data Integrity (Keutuhan Data)

Ketika melewati jaringan Internet, data sebenarnya sudah berjalan sangat jauh melintasi berbagai negara. Di tengah perjalanannya, apapun bisa terjadi terhadap isinya. Baik itu hilang, rusak, bahkan dimanipulasi isinya.VPN memiliki teknologi yang dapat menjaga keutuhan data yang dikirim agar sampai ke tujuannya

iii. Origin Authentication (Autentikasi Sumber)

Teknologi VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumber-sumber pengirim data yang akan diterimanya. VPN akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi source datanya. Kemudian alamat source data ini akan disetujui jika proses autentikasinya berhasil.

Jenis implementasi VPN

i. Remote Access VPN

Remote access yang biasa juga disebut virtual private dialup network (VPDN), menghubungkan antara pengguna yang mobile dengan local area network (LAN). Jenis VPN ini digunakan oleh pegawai perusahaan yang ingin terhubung kejaringan khusus perusahaannya dari berbagai lokasi yang jauh(remote) dari perusahaannya.

ii. Site to site VPN

Jenis implementasi VPN yang kedua adalah site-to-site VPN. Implementasi jenis ini menghubungkan antara 2 kantor atau lebih yang letaknya berjauhan, baik kantor yang dimiliki perusahaan itu sendiri maupun kantor perusahaan mitra kerjanya.

g) Kriptografi

Kriptografi adalah ilmu pengetahuan dan seni menjaga pesan atau informasi agar tetap aman atau secure. Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi.

Enkripsi merupakan teknik untuk mengamankan data yang dikirim dengan mengubah data tersebut ke dalam bentuk sandi-sandi yang hanya dimengerti oleh pihak pengirim dan pihak penerima data. Enkripsi yang banyak digunakan saat ini adalah enkripsi kunci simetris dan enkripsi kunci publik.

i. Kunci simetris

Pada enkripsi menggunakan kunci simetris, setiap komputer memiliki kunci rahasia (kode) yang dapat digunakan untuk mengenkripsi informasi sebelum informasi tersebut dikirim ke komputer lain melalui jaringan. Kunci yang digunakan untuk mengenkripsi data sama dengan kunci yang digunakan untk mendekripsi data. Oleh karena itu, kunci tersebut harus dimiliki kedua komputer. Kunci harus dipastikan ada pada komputer penerima. Artinya pengirim harus memberitahu kunci yang digunakan pada penerima melalui orang yang dipercaya. Selanjutnya informasi yang akan dikirim, dienkripsi imenggunakan kunci tersebut. Sehingga penerima bisa mendekripsi, dan mendapatkan informasi yang diinginkan.

ii. Kunci publik

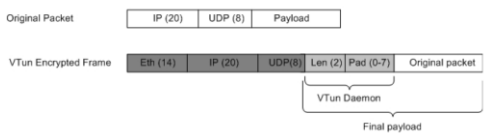
Enkripsi kunci publik menggunakan kombinasi kunci privat dan kunci publik. Kunci privat hanya diketahui oleh pihak pengirim informasi. Sedangkan kunci publik dikirim ke pihak penerima. Untuk mendekripsi informasi, pihak penerima harus menggunakan kunci public dan kunci privat miliknya. Kunci privat penerima berbeda dengan kunci privat pengirim, dan hanya penerima saja yang mengetahuinya.

Dekripsi adalah kebalikan dari enkripsi yaitu teknik untuk mengubah data yang tersamar kembali menjadi data yang bisa dibaca atau dimengerti oleh pihak penerima data.

h) VTun

Vtun adalah aplikasi jaringan yang dapat membuat virtual tunnel diatas jaringan TCP/IP. Seperti aplikasi VPN lainnya VTun membuat single koneksi diantara 2 mesin. Vtun Server menginisialisasi koneksi dengan UDP Protokol. Vtun menggunakan Private Share Key untuk melakukan negoisasi dan autentikasi. VTun adalah aplikasi VPN yang sangat mudah sekali

diimplementasikan. Untuk enkripsi Vtun menggunakan Algoritma MD5, 3DES dan Blowfish. VTun terdiri dari tiga komponen yaitu: Paket VTun, TUN/TAP Driver dan ethernet bridge driver. untuk menghasilkan pengiriman data yang cepat pada Aplikasi VTun dimasukkan teknologi kompresi yaitu zlib.



Gambar 2.1 Format Paket VTun

Tipe enkripsi pada VTun

Untuk tipe enkripsi pada aplikasi VPN Vtun menggunakan tipe enkripsi DES, 3 DES dan BlowFish.

a. DES (Data Encryption Standart)

Data Encryption Standart (DES) adalah chiper yang digunakan oleh Federal Information Processing Standart(FIPS) untuk Amerika Serikat pada tahun 1976, dan secara bertahap tersebar luas digunakan oleh seluruh dunia. Algoritma ini pada permulaan munculnya sangat kontroversi karena mempuyai key length yang sangat pendek. Selain itu ditengarai mempuyai backdoor oleh National Security Agency (NSA). Saat ini DES diketahui menjadi tidak aman untuk beberapa aplikasi. Hal ini dikarenakan ukuran dari key nya hanya 56 bit. Berikut gambaran singkat tentang perhitungan algoritma DES:

i. DES merupakan algoritma yang terdiri dari 64 block ciper dengan besar key 56 bit. Sebenarnya besarnya key untuk DES adalah 64 bit tetapi dengan pertimbangan tertentu, 8 bit key untuk proses checking parity.

ii. Separuh untuk setiap blocknya, dalam hal ini terdiri dari 28 bit (1 block = 56 bit) dengan pengertian 8 bit untuk proses checking parity, dipermutasikan menjadi 48 bit subkey untuk setiap putarannya. Dengan menggunakan fungsi Feitsel, DES 64 bit cipher block dibagi menjadi 16 putaran.

iii. Setelah terbentuk 16 subkey yang masing-masing terdiri dari 48 bits, key tersebut akan dicampur (mix) dengan 32 bit (separuh block) dengan operasi XOR, yaitu:

- Output dari XOR yang berupa 48 bit dibagi menjadi 8 bagian dan setiap bagiannnya terdiri dari 6 bit sebelum melalui proses S-box. Setiap S-box terdiri dari 6 bit input dan 4 bit output.
- Step terakhir dengan permutasi tertentu 32 bit output (4x8) diatur kembali dan ditempatkan ke P-box.

b. 3DES (Triple DES)

Triple DES (3DES) adalah sekumpulan chipper (block chipper) dari Data Encryption Standart (DES) yang digunakan 3 kali. Triple DES juga dikenal dengan nama TDES atau TDEA (Triple Data EncryptionAlgorithm). Semenjak ditemukan DES pertama kali yang menggunakan 56 bit, key length. DES sangat rentan terhadap brute force. Sudah dapat ditebak block chiper pada 3DES sama dengan DES yaitu 64 bitsedangkan key size untuk 3DES adalah 168 bit dengan pengulangan DES (56 bit) sebanyak 3 kali.

c. Blowfish

Ini adalah salah satu dari enkripsi publik yang paling umum algoritma enkripsinya yang disediakan oleh Bruce Schneier satu dari kriptologi terkemuka di dunia, dan presiden Sprei Systems, sebuah perusahaan konsultan yang mengkhususkan diri dalam kriptografi dan keamanan komputer. Key size yang digunakanmulai dari 32 bit ke 448 bit, dengan default key size yang biasa digunakan adalah 128bit. Blowfish tidak dipatentkan dan bebas lisensi, dan tersedia gratis untuk semua penggunaan.

Blowfish memiliki keunggulan yang lebih baik dibandingkan dengan AES karena kinerja yang dilakukan oleh algoritma Blowfish tidak

memerlukan kekuatan pemrosesan yang lebih [5], sehingga penulis dalam perancangan model interkoneksi ini memilih enkripsi blowfish selain performanya juga lisensinya yang opensource.

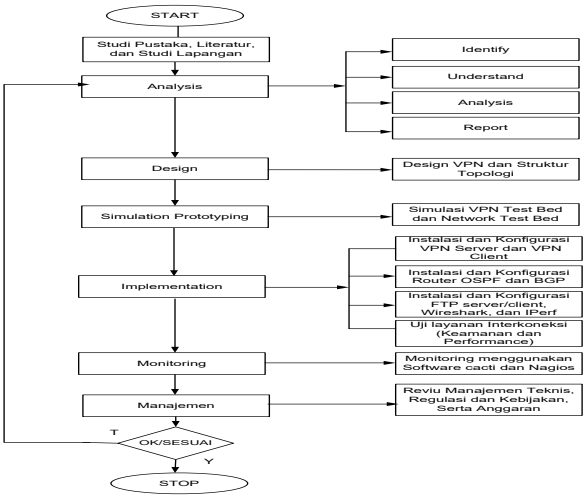
PerbandinganVPN VTun, IPSec dan Aplikasi VPN Lainnya. Pada perbandingan kali ini penulis memperbandingkan aplikasi VPN antara Vtun, IPSec, dan Openvpn, yang dijelaskan pada tabel dibawah ini:

Security Scheme	Application Name and Version	Security Provided	Network Layer
IPSec	FreeS/WAN	• Authentication/encryption with 3DES • Integrity with MD5	Network (Layer 3)
SSL/TLS	OpenVPN 2.0-beta15	• Authentication/encryption with 3DES • Integrity with MD5	Network (Layer 3)
Miscellaneous	VTun 2.9.90	• Authentication/encryption with Blowfish • Integrity with MD5	Network (Layer 3)
	Zebedee 2.4.1	• Authentication/encryption: with Blowfish • Does not provide integrity checking	Network (Layer 3)

Tabel 2.2 Perbandingan beberapa skema keamanan software VPN.

3. Metode Penelitian

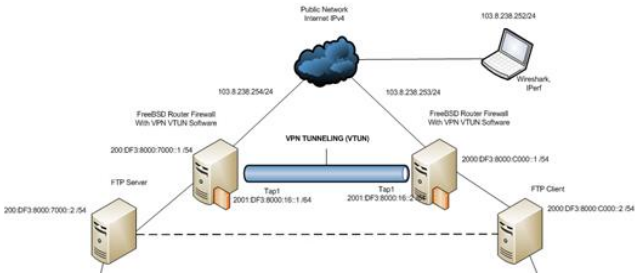
Metode penelitian yang penulis gunakan yaitu melalui studi pustaka untuk mencari landasan teori tentang VPN, IPv6, Jaringan dan Routing Protokol, literatur review penelitian yang sama seperti jurnal, dan buku yang berkaitan dengan masalah interkoneksi jaringan, dan juga berdasarkan langkah-langkah penelitian dalam model Network Development Life Cycle (NDLC). Berikut flowchart proses penelitian yang dilakukan:



Gambar 3. Flowchart Proses Penelitian

3.1. Simulasi

Dalam perancangan sistem jaringan VPN ini penulis membuat sebuah simulasi dalam bentuk network Test Bed dengan merepresentasika desain topologi jaringan.



Gambar. 3.1 Simulasi VPN Test Bed

Dalam menjalankan simulasi prototype ini, penulis menggunakan aplikasi virtual box , OS FreeBSD, FTP server dan FTP Client. IPerf software untuk menguji throughput pengiriman data, dan wireshark untuk melihat keamanan data.

3.2. Eksperimen

Setelah melakukan proses simulasi prototype penyusun langsung melakukan percobaan pada desain simulasi jaringan Testbed.

a) Instalasi dan konfigurasi server VPN dan Router BGP/OSPF

Untuk Instalasi dan konfigurasi komputer server menggunakan operating sistem FreeBSD 8.3. Pada instalasi freeBSD ini dilakukan konfigurasi alamat IPv4 Publik pada Interface WAN FreeBSD yang menghadap ke Internet dan konfigurasi alamat IPv6 pada Interface VPN yaitu Interface tap1 dan Interface LAN. Sebelum melakukan konfigurasi IP address pada semua server yang akan disimulasikan maka sebagai acuan adalah daftar tabel IPv6 addres yang sudah dipetakan agar proses pengalamatan IP address bisa langsung dilakukan di server. Konfigurasi pemasangan IP di server freeBSD sebagai Berikut :

1. Konfigurasi jaringan pada OS FreeBSD (Kantor Pusat)

a. file /etc/rc.conf

- ipv6_enable="YES"
- network_interfaces="auto"
- ifconfig_lo0="inet 127.0.0.1 netmask 255.255.255.255 mtu 8232"
- ifconfig_em0_name="wan0"
- ifconfig_em1_name="lan0"
- ipv4_addrs_wan0="192.168.43.10/24"
- ipv4_addrs_lan0="172.25.1.1/30"
- ipv6_ifconfig_lan0="2001:DF3:8000:7400::1/64"

2. Konfigurasi jaringan pada OS FreeBSD (Kantor Cabang)

a) file /etc/rc.conf

- ipv6_enable="YES"
- network_interfaces="auto"
- ifconfig_lo0="inet 127.0.0.1 netmask 255.255.255.255 mtu 8232"
- ifconfig_em0_name="wan0"
- ifconfig_em1_name="lan0"
- ipv4_addrs_wan0="192.168.43.15/24"
- ipv4_addrs_lan0="172.26.28.1/30"
- ipv6_ifconfig_lan0="2001:DF3:8000:C000::1/64"

b) Instalasi VPN server menggunakan VTun Pada OS FreeBSD

Untuk menginstall VTun di server FreeBSD dapat melakukan hal berikut. Perintah ini untuk menginstal Vtun.

a. VTUN installation

```
# cd /usr/ports/net/vtun
# make install clean && rehash
```

b. Konfigurasi VTUN server pada OS FreeBSD (Kantor Pusat)

```
#
# Server configuration options
#
options {
        type stand;
        port 21176;
        ifconfig /sbin/ifconfig;
    route/sbin/route;
    firewall/etc/rc.d/pf;
    syslog auth;
}
default {
        stat yes;
        compress no;
        encrypt no;
        persist yes;
        keepalive yes;
}

##########Cabang P-T-P############
idc_3d {
passwd 123@#*;
type ether;
device tap1;
proto tcp;
compress lzo:9;
encrypt yes;
up {
ifconfig "%% inet6 2001:df3:8000:16::1/64 up";
firewall "reload";
};
 down { ifconfig "%% delete"; firewall "reload"; };
multi killold;
}
```

c. Konfigurasi VTUN Server dan VTun Client pada OS FreeBSD (Client Site)

```
#
# Server configuration options
#
options {
        type stand;
        port 21176;
        ifconfig /sbin/ifconfig;
         route /sbin/route;
          firewall /etc/rc.d/pf;
          syslog auth;
```

JURNAL EKSELENTA
JURNAL ILMIAH FAKULTAS TEKNIK
UNIVERSITAS SAINS INDONESIA

```
}
default {
        stat yes;
    compress no;
        encrypt no;
        persist yes;
        keepalive yes;
}
##########Pusat  P-T-P###########
idc_3d {
 passwd 123@#*;
 type ether;
 device tap1;
 proto tcp;
 compress lzo:9;
 encrypt yes;
 up {
 ifconfig "%% inet6 2001:df3:8000:16::2/64 up";
      firewall "reload";
 };
 down { ifconfig "%% delete"; firewall "reload"; };
 multi killold;
}
```

d. Menjalankan VTUND server pada server site kantor pusat

```
# /usr/local/etc/rc.d/vtund start, atau
# vtund –s
```

Mengetahui VTUND telah siap untuk terima koneksi, lakukan perintah berikut

```
# netstat –tan | grep 21176
```

“tcp4 0 0 *.21176 *.* LISTEN”

e. Menjalankan VTUND client pada server site Kantor Cabang

```
# vtund -f /usr/local/etc/vtund.conf idc_3d 192.168.43.10 (Ip address VPN server tujuan)
```

cek status VPN VTun client sudah terkoneksi dengan VTUN Server dengan cara :

```
# netstat -tan | grep 21176
tcp4       0      0 *.21176
 *.*                    LISTEN
tcp4            0          0  192.168.43.15.1024
192.168.43.10.21176    ESTABLISHED
```

f. Konfigurasi Protokol OSPF dan BGP

a. Konfigurasi OSPF pada Site Kantor Pusat

Pusat-bgp(config)# router ospf6
Pusat-bgp(config-router)# router-id 255.1.1.1
Pusat-bgp(config-router)# area 0.0.0.0 range 2001:df3:8000:16::/64
Pusat-bgp(config-router)# interface tap1 area 0.0.0.0

b. Konfigurasi OSPF pada Site Kantor Cabang

cabang-bgp# config t
cabang-bgp(config)# Router ospf6
cabang-bgp(config-router)# router-id 255.1.1.2
cabang-bgp(config-router)# area 0.0.0.0 range 2001:df3:8000:16::/64
cabang-bgp(config-router)# area 0.0.0.16 range 2001:df3:8000:1a::/64
cabang-bgp(config-router)# interface tap1 area 0.0.0.0
cabang-bgp(config-router)# interface tap2 area 0.0.0.16

c. Konfigurasi BGP Jaringan Kantor Pusat

Pusat-bgp# config t
Pusat-bgp(config)# router bgp 64513
Pusat-bgp(config-router)# bgp log-neighbor-changes
Pusat-bgp(config-router)# network 2001:df3:8000:7400::/64
Pusat-bgp(config-router)# neighbor 2001:df3:8000:16::2remote-as 65531
Pusat-bgp(config-router)# neighbor 2001:df3:8000:16::2update-source tap1

JURNAL EKSELENTA
JURNAL ILMIAH FAKULTAS TEKNIK
UNIVERSITAS SAINS INDONESIA

Pusat-bgp(config)# ip route 2001:df3:8000:7400::/64 Null0

d. Konfigurasi BGP pada Kantor Cabang

cabang-bgp# config t
cabang-bgp(config)# router bgp 65531
cabang-bgp(config-router)# bgp log-neighbor-changes
cabang-bgp(config-router)# network 2001:df3:8000:C000::/64
cabang-bgp(config-router)# neighbor 2001:df3:8000:16::1 remote-as 64513
cabang-bgp(config-router)# neighbor 2001:df3:8000:16::1 update-source tap1
cabang-bgp(config-router)# neighbor 2001:DF3:8000:1a::2 remote-as 65531
cabang-bgp(config-router)# neighbor 2001:DF3:8000:1a::2 update-source tap2
cabang-bgp(config-router)# neighbor 2001:DF3:8000:1a::2 route-reflector-client
cabang-bgp(config)# ip route 2001:df3:8000:C000::/64 Null0

3.3. Pengujian

Pengujian keamanan dan throughput pada VPN VTun dilakukan melalui dua mekanisme, yaitu :

a. Pengujian Keamanan Authentikasi dan Enkapsulasi pada saat Aplikasi VPN VTun pertama kali dijalankan dan pengujian dilakukan menggunakan aplikasi Wireshark.

- Konfigurasi VPN VTun tanpa enkripsi :

```
root@gfw-vpn [/home/ade/www] $ tail -f /var/log/auth.log
Feb  5 17:14:19 gfw-vpn vtund[7071]: Broken pipe (32)
Feb  5 17:14:19 gfw-vpn vtund[7071]: Session diy_ade closed
Feb  5 19:12:53 gfw-vpn vtund[10935]: Session diy_ade[111.94.57.138:1106] opened
Feb  5 19:12:53 gfw-vpn vtund[10935]: LZO compression[level 9] initialized
Feb  5 19:22:03 gfw-vpn sudo:      ade : TTY=pts/0 ; PWD=/home/ade ; USER=root ;
 COMMAND=/usr/bin/su -
Feb  5 19:34:43 gfw-vpn vtund[11546]: VTUN server ver 3.X 10/04/2014 (stand)
Feb  5 19:34:54 gfw-vpn vtund[11546]: Terminated
Feb  5 19:34:54 gfw-vpn vtund[11568]: VTUN server ver 3.X 10/04/2014 (stand)
Feb  5 19:35:16 gfw-vpn vtund[11587]: Session diy_ade[111.94.57.138:1121] opened
Feb  5 19:35:16 gfw-vpn vtund[11587]: LZO compression[level 9] initialized
```

Gambar 3.3 VPN VTun tanpa enkripsi

- Konfigurasi VPN VTun dengan enkripsi:

```
#############################################
Uji Coba IPv6 ke Daerah Pakai Quagga#
#############################################3

# Kominfo e-Gov DC-2
#

diy_ade {
  passwd diy_dc2;
  type ether;
  device tap2;
  proto tcp;
  compress lzo:9;
  encrypt yes;
  up {
        ifconfig "%% inet 192.168.1.1 netmask 255.255.255.252 up";
        ifconfig "%% inet6 2001:DF3:8000:16::1/64 up";
        firewall "reload";
  };
  down { ifconfig "%% delete"; firewall "reload"; };
  multi killold;
}
```

Gambar 3.3a. Konfigurasi VPN VTun dengan enkripsi

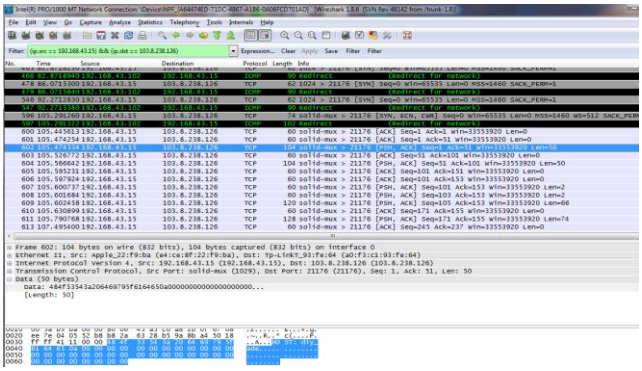
- Status pada saat aplikasi VTun pertama kali dijalankan

```
Feb  5 19:43:43 gfw-vpn vtund[11895]: Session diy_ade[111.94.57.138:1028] opened
Feb  5 19:43:43 gfw-vpn vtund[11895]: LZO compression[level 9] initialized
Feb  5 19:43:43 gfw-vpn vtund[11895]: Blowfish-128-ECB encryption initialized
```

Gambar 3.3b. VPN VTun saat terkoneksi

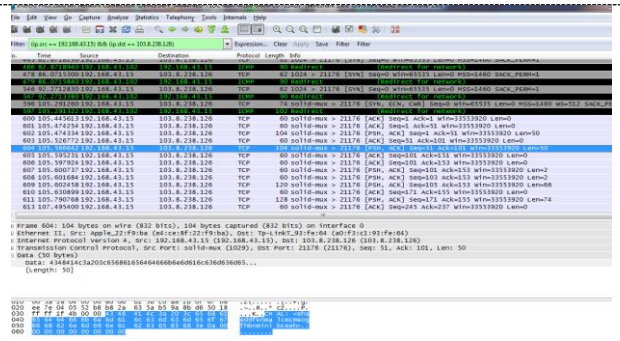
Pengujian ini dilakukan dengan mengcapture pada interface wan OSFreeBSD dimana applikasi VTun client melakukan autentikasi dan enkapsulasi kepada VTun Server. Dalam autentikasi dilakukan validasi profile koneksi dan kunci autentikasi. Dalam pengujian ini didapatkan hasil pengiriman data kunci tidak dapat terbaca dan dalam keadaan terenkripsi sedangkan profile dari VPN tersebut terbaca dengan nama diy_ad.

Berikut hasil capture dengan wireshark :



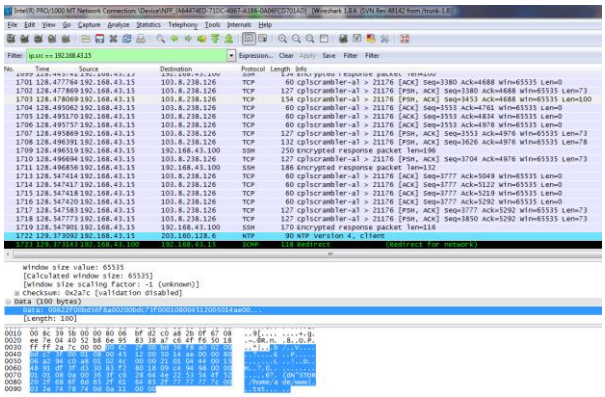
Gambar 3.3c Hasil Capture VPN VTun utk proses autentikasi keamanan

JURNAL EKSELENTA
JURNAL ILMIAH FAKULTAS TEKNIK
UNIVERSITAS SAINS INDONESIA

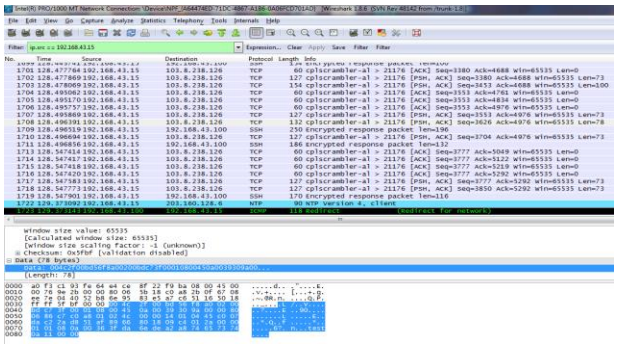


Gambar 3.3d Hasil Capture Profile VPN VTun

b. Pengujian Keamanan pada saat transaksi data melawati jalur VPN VTun menggunakan aplikasi Wireshark. Pengujian ini dilakukan pengiriman data dari FTP Client ke FTP server melalui tunnel VPN yang telah terbangun dan mengcapture data txt dalam pengiriman tersebut.

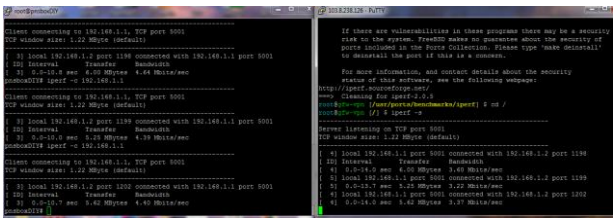


Gambar 3.3e Hasil Capture pengiriman data dengan FTP Pada jalur VPN tidak terenkripsi

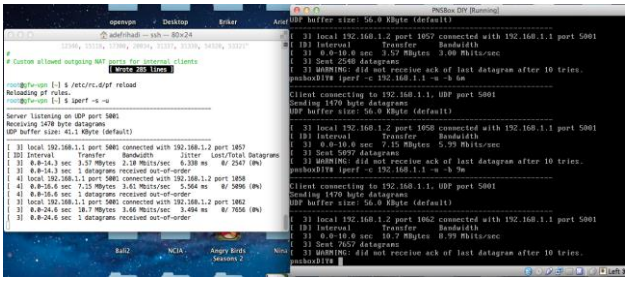


Gambar 3.3f Hasil Capture isi data txt pada saat pengiriman melalui jalur VPN yang tidak terenkripsi

c. Pengujian Throughput pada saat tidak ada transaksi data pada jalur VPN VTun dan VPN speed di set sebesar 3Mbps. Hasil Tes Throughput Up Down 3 Mbps saat trafik kosong tidak ada data yang lewat maka hasilnya sama yaitu kurang lebih sama dengan bandwidth 3 Mbps. Berikut capturenya :



Gambar 3.3g Hasil Capture Throughput dengan bandwidth yang ada sebesar 3Mbps



Gambar 3.3h Hasil Capture Throughput Up Down sebesar 3Mbps

Transfer Data (MBytes)	Available Bandwidth (Mbps)	Jitter (ms)	Jumlah Paket	Paket Loss (%)
3 MB	2,10 Mbps	6,338 ms	2547	0
6 MB	3,61 Mbps	5,564 ms	5096	0
9 MB	3,66 Mbps	3,494 ms	7656	0

Tabel 3.3 Hasil pengukuran throughput

Dari pengukuran diatas diperoleh nilai jitter antara 3,494 ms hingga 6,338 ms dengan rata-rata nilai jitter sebesar 5,132 ms. Berdasarkan standar ITU-T, nilai jitter yang masih ditoleransi adalah 30 ms. Dari hasil percobaan terlihat rata-rata jitter masih termasuk dalam rekomendasi, begitu juga untuk paket loss yang masih di toleransi oleh standar ITU-T adalah 5% sedangkan nilai pengukuran diatas adalah 0%. Sehingga Jitter dan Paket Loss diatas dapat diterima untuk melakukan

komunikasi suara pada Interkoneksi jaringan VPN VTun antar kantor pusat dan cabang.

4. Kesimpulan

a. Dengan menggunakan VPN VTun komunikasi jaringan *private* yang melewati jaringan *public* (Internet) akan lebih aman sehingga dapat merahasiakan transaksi pertukaran data antar kantor pusat dan cabang
b. Kualitas pertukaran data, gambar dan suara menggunakan VPN VTun untuk interkoneksi jaringan antar kantor pusat dan cabang cukup baik untuk dapat diimplementasikan dengan kondisi dan kualitas internet yang ada
c. Untuk interkoneksi jaringan dengan menggunakan IPv6 akan menjangkau banyak jumlah site yang akan diimplentasikan

5. Saran

a. Penggunaan Aplikasi VPN VTun untuk interkoneksi jaringan antar kantor pusat dan cabang sebaiknya lebih dioptimalkan dengan memanfaatkan fitur traffic shaping (bandwidth management) dan kompresi pada aplikasi tersebut.
b. Untuk menjaga kualitas pertukaran data, suara dan gambar melalui VPN VTun diharapkan dapat melakukan penelitian kepada beberapa ISP (Internet Service Provider) dengan SLA yang tinggi untuk layanan internet.

Daftar Pustaka

1. S. Pemikiran, I. Pengetahuan, and I. Development, "Fundamental Internetworking Development & Design Life Cycle "," no. April, pp. 1–13, 2009.
2. J. F. Kurose and K. W. Ross, *Computer Networking A Top-Down Approach Featuring the Internet*, vol. 1. 2005, p. 712.
3. S. Singh and R. Maini, "Comparison of data encryption algorithms," *Int. J. Comput. Sci. ...*, vol. 2, no. 1, pp. 125–127, 2011.
4. H. Olaf and R. Thomschutz, "Security in Packet-Switched Land Mobile Radio Backbone Networks Security in Packet-Switched Land Mobile Radio Backbone Networks," 2005.
5. R. K. Murugesan and S. Ramadass, "Fast CEH : an Algorithm to Enhance Performance of IPv6 Packets with CRC Extension Header," vol. 5, no. 1, pp. 137–144, 2012.
6. M. O. Buob, S. Uhlig, and M. Meulle, "Designing optimal iBGP route-reflection topologies," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2008, vol. 4982 LNCS, pp. 542–553.
7. Y. Rekhter, E. T. Li, and E. S. Hares, "A border gateway protocol 4 (BGP-4)," *RFC 4271*, pp. 1–105, 2006.
8. S. Convery and D. Miller, "Ipv6 and ipv4 threat comparison and best-practice evaluation (v1. 0)," *Cisco Syst.*, pp. 1–43, 2004.
9. R. B. Bahaweres, M. Alaydrus, and A. Wahab, "ANALISIS KINERJA VOIP CLIENT SIPDROID DENGAN MODUL ENKRIPSI," vol. 2012, no. Snati, pp. 15–16, 2012.
10. P. Dell, "Australian IPv6 readiness: Results of a national survey," *Journal of Research and Practice in Information Technology*, vol. 44. pp. 3–15, 2012.
11. B. Kang and M. Balintanas, "Vulnerabilities of VPN using IPSec and Defensive Measures," *International Journal of Advanced Science and Technology*, vol. 8. pp. 9–17, 2009.
12. D. Dobariya and J. Gajjar, "Threats In SIP Based VoIP Systems," vol. 2, no. 3, pp. 2666–2675, 2013.

13. Windasari, S. (2024). Designing An Omni Wheel Robot. Jurnal Ekselenta-Jurnal Ilmiah Fakultas Teknik, 1(1), 40-48.
14. Suwoyo, H., Abdurohman, A., Li, Y., Adriansyah, A., Tian, Y., & Hajar, M. H. I. (2022). The Role of Block Particles Swarm Optimization to Enhance The PID-WFR Algorithm. International Journal of Engineering Continuity, 1(1), 9-23.
15. Dama, M., & Alaydrus, M. (2019, October). Analysis of multi coils in misalignment conditions in the WPT system. In 2019 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET) (pp. 20-23). IEEE.
16. Baskoro, B. (2024). Pemanfaatan IoT Sebagai Teknologi Terkini di Kehidupan Masyarakat. Jurnal Ekselenta-Jurnal Ilmiah Fakultas Teknik, 1(1),
17. Frihadi,. A. (2024). Pemanfaatan IoT Sebagai Teknologi Terkini di Kehidupan Masyarakat. Jurnal Ekselenta-Jurnal Ilmiah Fakultas Teknik, 1(1),
18. Adi Affandi Rotib (2024). Pusat Data dan Layanan Cloud Center: Jaringan Protokol dan Manajement. Jurnal Ekselenta-Jurnal Ilmiah Fakultas Teknik, 1(1),