Penerapan Firewall Dan Protokol IpSec/L2TP Sebagai Solusi Keamanan Akses Jaringan Publik

Muhammad Ayub[1], Andry Maulana[2,] Ahmad Fauzi[3]

[1] Program Studi Teknologi Komputer, Fakultas Teknik dan Informatika, Universitas Bina Sarana Informatika
Jl. Kramat Raya No.98, Jakarta Pusat, DKI Jakarta 10450, Indonesia

[2,3] Program Studi Sistem Informasi, Universitas Nusa Mandiri
Jl. Jatiwaringin No. 2, Cipinang Melayu, Makasar, Jakarta Timur - 13620, Indonesia

e-mail: [1]ayub.mhmd25@gmail.com [2]andry.ayz@nusamandiri.ac.id, [3]ahmad.azy@nusamandiri.ac.id

Artikel Info : Diterima : 14-06-2021 | Direvisi : 22-06-2021 | Disetujui : 29-06-2021

Abstrak - Firewall merupakan sebuah algoritma yang memungkinkan terjadinya kegiatan filterisasi untuk menentukan pembatasan akses sebuah komputer yang dapat menggunakan akses jaringan Publik dan komputer mana saja yang tidak dapat melewati akses jaringan Publik , hal ini biasa disebut dengan filtering. Seiring berjalannya waktu, perkembangan teknologi jaman sekarang semakin bertambah pesat. bahwa kecangihan teknologi menjadi pengaruh besar dalam memudahkan kehidupan manusia. Berdasarkan hal tersebut maka penulis membuat *Firewall* Dan Protokol IpSec/L2TP Sebagai Solusi Keamanan PT.Neu Indonesia bertujuan untuk mencegah terjadinya serangan terhadap jenis Malware yang terdapat pada sebuah situs yang beredar pada jaringan Publik dengan memfilerisasi dengan penggunaan Firewall itu sendiri sehingga resiko kejahatan pada dunia *cyber* dapat meminimalisir terjadinya akses illegal yang dapat masuk kedalam jaringan PT.Neu Indonesia.

Kata Kunci : firewall, l2tp, vpn

Abstracts *- Firewall is an algorithm that allows filtering activities to determine access restrictions on a komputer that can use Publik network access and which komputer s cannot pass through Publik network access, this is commonly called filtering. As time goes by, the development of today's technology is increasing rapidly. that the sophistication of technology is a major influence in facilitating human life. Based on this, the authors create a Firewall and IpSec/L2TP Protocol as a Security Solution for PT.Neu Indonesia, which aims to prevent attacks on the types of malware found on a site circulating on Publik networks by filtering it with the use of the firewall itself so that the risk of crime in the cyber world can minimize the occurrence of illegal access that can enter the PT.Neu Indonesia network.*

Keywords : firewall, l2tp, vpn

PENDAHULUAN

Perkembangan teknologi informasi yang sangat pesat membuat kebutuhan masyarakat dunia akan akses internet semakin tinggi. Perkembangan tersebut mengharuskan sebuah perusahaan dapat memiliki hak akses pada jaringan Publik /layanan internet. Dengan internet perusahaan dapat saling terhubung satu dengan lainnya dengan jaringan komputer berbasi WAN (*Wide Area Network*) (Wahyudi & Firmansyah, 2021). Khususnya pada Perusahan PT. Neu Indonesia yang terletak di Jl. TB Simatupang Jakarta merupakan perusahaan yang beroprasi pada bidang industri yang mempunyai bidang kerja di dalam perusahaannya tersebut PT. Neu Indonesia Telah melakukan pengembangan terhadap sistem komputer dimana telah di impletasikan sistem kerja jaringan publik dimana tugas komputer ditangani oleh komputer yang terpisah tetapi dapat saling berkomunkasi.

Perusahaan menjalankan dan mengembangkan bisnisnya menggunakan sistem teknologi jaringan *Wide Area Network* (WAN) yang merupakan sebuah jaringan komputer yang mencakup area lokasi yang lebih luas, dengan melibatkan kesatuan komputer yang lebih banyak untuk melakukan proses pengiriman data maupun penerimaan data dari server solo atau pusat, baik itu data penjualan maupun *return* barang melalui program sinkronisasi yang berbasis Java. Setelah data masuk, cabang Indonesia baru bisa melakukan proses penerimaan barang untuk di bagikan ke cabang departemen *store* lainnya menggunakan program MRPRO.

Program MRPRO hanya terinstall di *server* pusat atau solo, jadi setiap ada proses penambahan atau pengurangan data harus dilakukan sinkronisasi agar antara *server* pusat dan *server* cabang datanya sama. Oleh karena itu dibutuhkan koneksi VPN (*Virtual Privat Network*) sebagai media transmisi untuk menghubungkan antara *server* cabang dan *server* pusat. *Virtual Private Network (VPN)* bertindak sebagai penghubung satu node jaringan ke node jaringan lainnya dengan mengguncakan jaringan publik (internet). Data yang diperbolehkan untuk lewat akan dibalut (encapsulation) dan dienkripsi agar kerahasiaannya dapat terjamin (Maulana & Fauzi, 2019)

Maka di dalam penelitian ini melakukan penelitian merancang jaringan WAN (*Wide Area Network*) dan membangun jaringan komputer untuk membantu komunikasi antar komputer seperti: sharing data dan melakukan pendataan, pemasangan kabel serta pengaturan topologi. bergeraknya infrastruktur dan kelancaran arus informasi. Jaringan komputer adalah sebuah konektifitas yang menghubungkan antar sebuah perangkat komputer agar dapat saling berkomunikasi antar satu sama lain. Data atau informasi yang diteruskan melalui kabel maupun *wireless* sehingga orang yang menggunakan komputer dapat saling bertukar dokumen dan data, mencetak pada printer yang sama dan bersama-sama menggunakan *hardware/software* yang terhubung dengan jaringan (Firmansyah et al., 2020).

METODE PENELITIAN

NDLC (*Network Development Life Cycle*) merupakan metode yang saling mendukung pada proses pembangunan seperti perancangan proses bisnis dan perancangan infrastruktur (Maulana, 2018). Adapun tahapannya adalah sebagai berikut :

1. Analysis

Tahapan ini adalah tahapan pertama yang digunakan dalam penelitian yang meliputi analisa kebutuhan, analisa keinginan pengguna dan analisa topologi jaringan yang digunakan. .Pada tahap ini juga dilakukan pengumpulan dokumen yang dibutuhkan untuk mengetahui perumusan masalah dan cara menyelesaikan masalah tersebut. Dari tahapan ini penulis mendapatkan analisa bahwa perusahaan tersebut belum menerapkan vpn yang baik dan filter keamanan *firewall* (Firmansyah & Wahyudi, 2021).

2. Design

Dari dokuemen yang didapatkan pada tahap analysis, Tahap desain ini akan membuat cerminan desain topologi jaringan, diharapkan dengan desain ini akan memberikan gambaran dari kebutuhan yang ada. Desain berupa desain struktur topologi yang akan diimplementasikan, desain kebutuhan perangkat, desain jalur pengkabelan yang digunakan. Dalam penelitian ini penulis menggunakan *Cisco Packet Tracer* untuk membuat desain jaringan yang sudah ada dan yang akan dibuat.

3. Simulation Prototyping

Sebelum menerapkan jaringan yang dirancang pada penelitian ini maka sebelumnya dibuat dalam bentuk simulasi dengan bantuan tools khusus di bidang network seperti *Boson, Packet Tracert, Netsim* dan sebagainya. Hal ini dimaksudkan untuk melihat kinerja awal dari network yang akan. Namun karena keterbatasan perangkat lunak simulasi ini, maka penulis hanya menggunakan alat bantu program *Packet Tracer*.

4. Implementation

Di tahapan ini penerapan jaringan akan dibuat dngan menggunakan perangkat cisco. Penerapan ini akan memakan waktu lebih lama dari tahapan sebelumnya. Dalam tahap implementasi, penulis menerapkan semua yang telah direncanakan dan dirancang sebelumnya. Pada posisi inilah akan tampak bagaimana penerapan ipsec/l2tp dan firewall yang akan diterapkan.

5. Monitoring

Pada tahap ini penulis melakukan pengujian langsung jaringan yang dibangun pada Perusahan PT. Neu Indonesia. Pengujian ini dilakukan dengan cara pengambilan data untuk melihat kinerja jaringan yang telah dirancang dan dikonfigurasi

6. Management

Di manajemen atau pengaturan, salah satu yang menjadi perhatian khusus adalah masalah kebijakan, yaitu dalam hal aktivitas, pemeliharaan dan pengolahan dikategorikan pada tahap ini.Kebijakan perlu di buat untuk membuat dan mengatur agar jaringan yang telah dibangun dapat berjalan dengan baik. Pada Teknik penelitian ini menggunakan vpn untuk menghubungkan lokasi yang berada di solo dan pusat.

HASIL DAN PEMBAHASAN

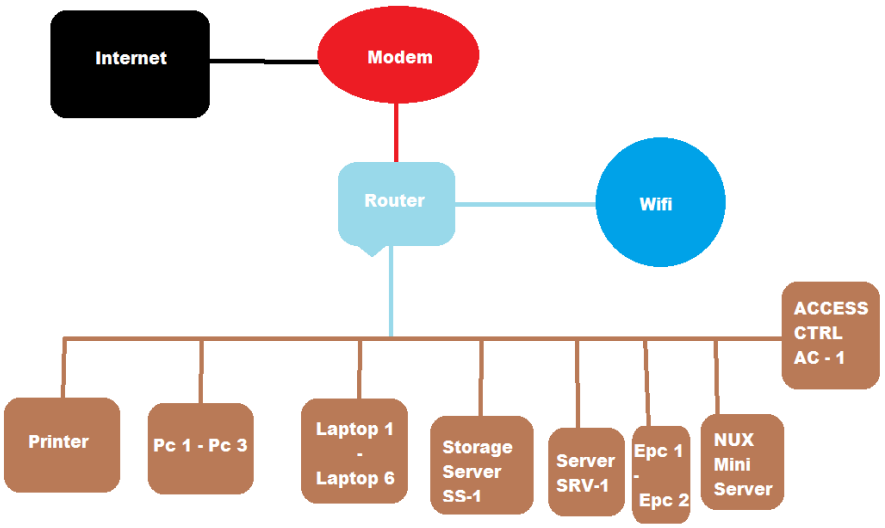
1. Skema Jaringan Pada Perusahaan

a. Topologi Jaringan

Topologi jaringan berperan dalam menentukan pembuatan jaringan berdasarkan asas kebutuhan (Maulana, 2018).Sistem jaringan komputer di kantor PT.Neu Indonesia secara umum menggunakan jaringan *client-server*

dengan koneksi kabel. Untuk lebih detailnya penulis akan menjelaskan perangkat apa saja yang digunakan di dalam kantor PT.Neu Indonesia. Berikut rinciannya :

1. Dalam kantor PT.Neu Indonesia menggunakan satu buah jenis server.
2. Untuk menghubungkan komputer satu dan lainnya jaringan komputer di kantor PT.Neu Indonesia.
3. Kabel yang digunakan dalam jaringan komputer digunakan dalam jaringan komputer di PT.Neu Indonesia menggunkan kabel jenis Fiber Optic.



Sumber : Dokumen Riset (2021)

Gambar 1. Blok Diagram Jaringan PT. Neu Indonesia

Penjelasan tentang blok diagram jaringan di atas terdapat sebuah modem yang di koneksikan dengan internet lalu terhubung dengan Router melalui port yang terdapat pada router tersebut, kemudian Router tersebut terhubung ke seluruh perangkat seperti Printer, PC 1 – PC 3, Laptop 1- Laptop 6, Storage Server SS-1, Server SRV-1, Epc 1- Epc 2, NUX Mini Server, dan Access CTRL AC-1, semua perangkat terhubung melalui media kabel Fiber Optic dengan type konektor RJ-45. Untuk menopang data pada semua jaringan komputer, penyimpan data menggunakan Server sebagai penyimpan data utama pada semua jaringan komputer pada gedung PT.Neu Indonesia.

b. Arsitektur Jaringan

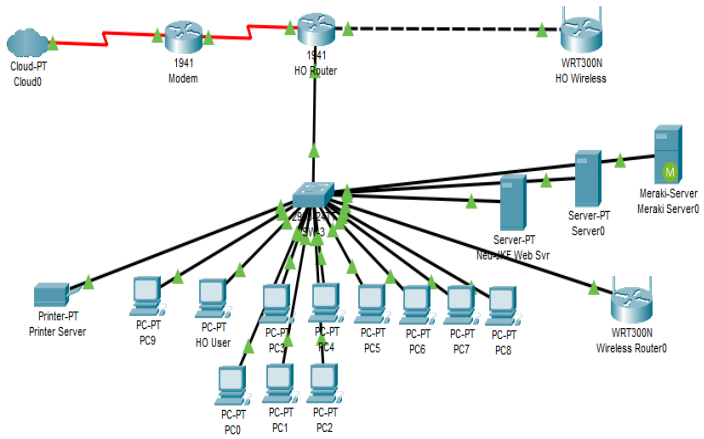
Secara umum arsitektur jaringan komputer perlu dilakukan untuk meminimalkan risiko(Pratama et al., 2018), penelitian ini membahas mulai dari aspek *Quality of Service* (QoC) yang akan diterapkan guna untuk menyeimbangkan troughput sehingga aktualisasi penggunaan bandwith dapat terukur dengan sesuai kebutuhan (Syawaludin et al., 2020). Selain kelancaran komunikasi dalam jaringan komputer hal yang krusial datang dari sisi firewall yang merupakan batas Local Area Network dengan internet (Pratama, 2019). Maka diperlukan juga untuk membuat sebuah Virtual Private Network dengan menggunakan Ipsec dengan perangkat Firewall Cisco ASA yang akan disimulasikan pada Packet Tracer.

Tabel 1. Ip Address PT. Neu Indonesia

Nama	IP Address	Subnet Mask	Default Gateway
Storage Server	192.168.1.7	255.255.255.0	
Main Server	192.168.1.1	255.255.255.0	
Mini Server	192.168.1.24	255.255.255.0	
MF Printer	192.168.1.9	255.255.255.0	
Laptop Dell	192.168.1.3	255.255.255.0	
Laptop Lenovo P50	192.168.100.202	255.255.255.0	

Sumber : Dokumen Riset (2021)

c. Skema Jaringan



Sumber : Dokumen Riset (2021)

Gambar 2. Skema Jaringan PT. Neu Indonesia

Skema jaringan adalah sebuah gambaran jaringan yang akan dibangun. Dengan adanya skrema yang baik maka akan lebih mudah memanajemen jaringan. Penjelasan tentang skema jaringan di atas dapat disimpulkan bahwa jenis yang digunakan jenis jaringan client-server, terdapat satu buah file server yang berfungsi memberikan lokas untuk akses disk arena, yaitu penyimpanan file komputer seperti dokumen, data, gambar dan lainnya yang dapat diakses oleh pc-*client*. Topologi yang digunakan adalah Topologi *Star* dimana setiap *client* dan printer terhubung ke *switch*, kemudian dari switch dihubungkan lagi ke modem. Kemudian baru dari modem dihubungkan ke spliter kabel telpon untuk bisa terhubung ke internet.Ip address yang digunakan pada jaringan pada perusahaan tersebut menggunakan IP kelas C dengan subnetmask 255.255.255.0/24 Manajemen IP yang digunakan pada jaringan komputer adalah IP *static* yang dikonfigurasikan secara manual.

d. Keamanan Jaringan

Seiring dengan semakin meningkatnya penggunaan internet pada jaringan komputer PT.Neu Indonesia celah keamanan pada jaringan pun menjadi sangat rentan untuk di serang virus maupun di bobol, proteksi keamanan yang digunakan dalam jaringan komputer tersebut adalah mengandalkan sistem keamanan firewall bawaan perangkat, baik berupa firewall bawaan pada perangkat keras maupun firewall yang terpasang pada perangkat lunak yang terpasang pada jaringan komputer PT.Neu Indonesia untuk menangkal serangan virus serta mencegah gangguan serangan pada jaringan komputer mengaplikasikan perangkat lunak seperti memasang Anti Virus (kapersky Ant Virus dan Norton Internet Security 2010) sebagai penjaga keamanan jaringan komputer dari serangan oleh pihak luar.

2. Spesifikasi Perangkat Jaringan

a. Perangkat Keras Jaringan

1) Komputer Server

Tabel 2. Spesifikasi Komputer Server

Komponen Hardware	Spesifikasi
Processor	Intel Core 15-4200M @2.4Ghz
RAM	V-GEN PC 1600MHz DDR3 4 Gb
HARDISK	Seagate arena da sata II. 1 TB
MOTHERBOARD	Asrock H110M-HDV
VGA CARD	Nvidia GeForce 720M 2 Gb
CD/DVD DRIVE	Samsung DVD RW 24X
MONITOR	Samsung LCD 14”
KEYBOARD	Komic Keyboard Standart
MOUSE	Optic Logitech B100

PC CASE	Power Logic Modena GTX2000

Sumber : Dokumen Riset (2021)

2) Storage Server Synology

Tabel 3. Spesifikasi Storage Server

Komponen Hardware	Spesifikasi
Processor	Realtek RTD1296 Quad Core 1.4GHz
Memori	512MB DDR4 (Non Upgradable)
Drive Bay	2x Bay 2.5"/3.5" SATA HDD/SSD (Hard Drive not included).
Port	1x Gigabit (RJ45), 2x USB 3.0
System Fan	92x92x25 mm x1
Wake on LAN/WAN	Yes
RAID support	Hybrid RAID (SHR), Basic, JBOD, RAID 0/1
Max IP Camera support	Total 12 Camera (include two free camera license).
Max VPN Server connection	10

Sumber : Dokumen Riset (2021)

3) Router 1941

Tabel 4. Spesifikasi Router Cisco

Product Code	CISCO1941/K9
Rack Units	2 RU
Interfaces	2 integrated 10/100/1000 Ethernet ports: GE0/0&GE0/1
Expansion Slot(s)	2 enhanced High-Speed WAN Interface Card slots 1 Internal Services Module slot
RAM	512 MB (installed) / 2 GB (max)
Flash Memory	256 MB (installed) / 8 GB (max)
Dimensions	34.3 cm x 29.2 cm x 8.9 cm
Package Weight	10.48 Kg

Sumber : Dokumen Riset (2021)

4) Switch 2960

Tabel 5. Spesifikasi Switch Cisco

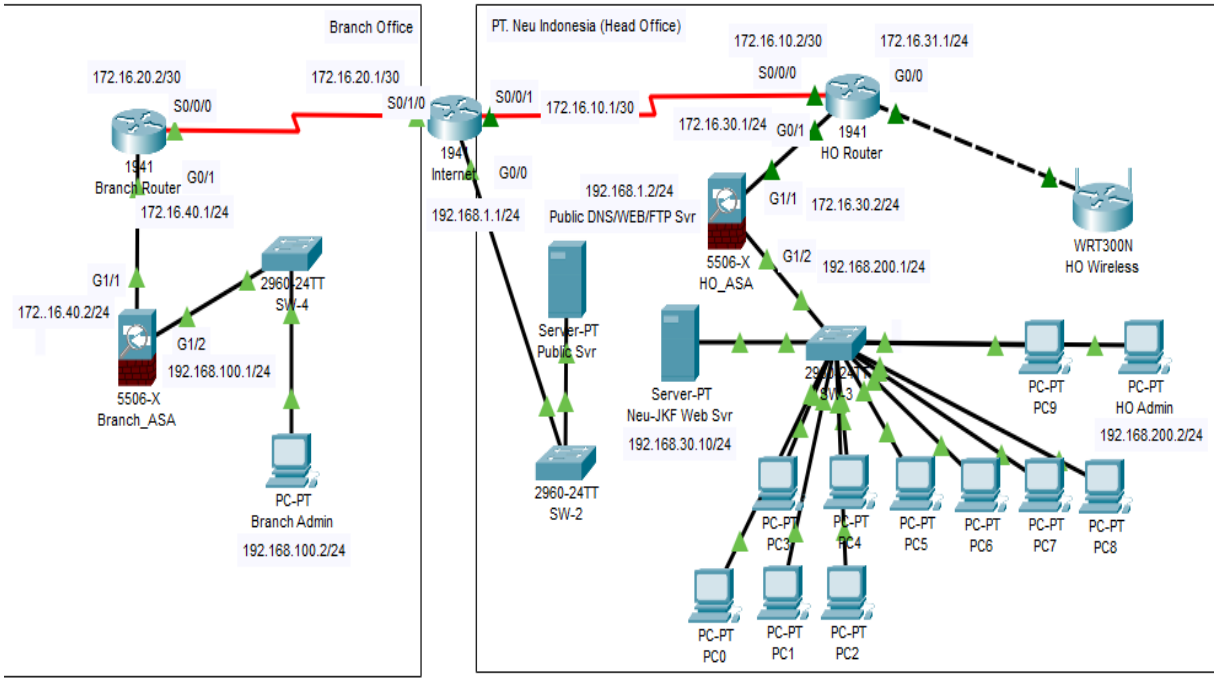
Product Code	WS-C2960X-24PS-L
Enclosure Type	Rack-mountable - 1U
Feature Set	LAN Base
Uplink Interfaces	4 x 1G SFP
Ports	24 x Ethernet 10/100/1000 Gigabit ports
Available PoE Power	370W
Maximum stacking number	8
Stack bandwidth	80G

Forwarding Bandwidth	108Gbps
Switching Bandwidth	216Gbps
RAM	512MB
Flash Memory	128MB
Dimensions	44.5 cm x 36.8 cm x 4.5 cm
Package Weight	10.65 Kg

Sumber : Dokumen Riset (2021)

3. Skema Jaringan Usulan

Setelah penulis mendeskripsikan topologi jaringan yang ada pada PT. Neu Indonesia. Maka penulis membuatkan sebuah topologi baru dimana topologi ini berfungsi merubah susuanan topologi yg sudah ada. Dalam topologi ini lah yang nantinya akan diterapkan *firewall* dan ipsec/l2tp.



Sumber : Dokumen Riset (2021)

Gambar 3. Skema Jaringan Usulan

Dalam topologi diatas penulis juga melakukan analisa penerapan ip address yang dapat dilihat pada tabel dibawah ini :

Tabel 6. Tabel Rancangan Ip Address

Nama	IP Address	Subnet Mask	Default Gateway
Router G0/1	172.16.40.1	255.255.255.0	N/A
Router S0/0/0	172.16.20.2	255.255.255.252	N/A
Branch_ASA G1/2	192.168.100.1	255.255.255.0	N/A
Branch_ASA G1/1	172.16.40.2	255.255.255.0	-
Internet S/0/1/0	172.16.20.1	255.255.255.2	N/A

Internet S/0/0/1	172.16.10.1	255.255.255.0	N/A
Internet G0/0	192.168.1.1	255.255.255.0	N/A
Ho Router S0/0	172.16.10.2	255.255.255.252	N/A
Ho Router G0/0	172.16.31.1	255.255.255.0	N/A
Ho Router G0/1	172.16.30.1	255.255.255.0	N/A
Ho_ASA G1/1	172.16.30.2	255.255.255.0	N/A
Ho Wireless Et0/0	172.16.31.2	255.255.255.0	172.16.31.2
Neu-JKF Web server G0/0	192.168.200.10	255.255.255.0	192.168.200.1
Publik DNS/Web server G0/0	192.168.1.2	255.255.255.0	192.168.1.1
PC Ho Admin Eth0	192.168.200.2	255.255.255.0	192.168.200.1
PC0-PC9 Eth0	DHCP	-	192.168.200.1
Branch Admin Eth0	192.168.100.2	255.255.255.0	192.168.100.1

Sumber : Dokumen Riset (2021)

4. Penerapan Jaringan

Pada tahap penelitian ini penulis mencoba menerapkan hasil analisa yang penulis buat berupa konfigurasi firewall dan tunneling dengan ipsec/l2tp.

```
branchasa(config)#crypto ikev1 enable outside

branchasa(config)#crypto ikev1 policy 2
branchasa(config-ikev1-policy)#encryption aes
branchasa(config-ikev1-policy)#hash sha
branchasa(config-ikev1-policy)#group 2
branchasa(config-ikev1-policy)#authentication pre-share
branchasa(config-ikev1-policy)#lifetime 86400
```

Sumber : Dokumen Riset (2021)

Gambar 7. Setup VPN Ipsec/l2tp

```
branchasa(config)#tunnel-group 172.16.30.2 type ipsec-l2l
WARNING: L2L tunnel-groups that have names which are not an IP
address may only be used if the tunnel authentication
method is Digital Certificates and/or The peer is configured to use
Aggressive Mode
branchasa(config)#tunnel-group 172.16.30.2 ipsec-attributes
branchasa(config-tunnel-ipsec)#ikev1 pre-shared-key yabuy
```

Sumber : Dokumen Riset (2021)

Gambar 8. Create Group Tunnel

```
branchasa(config)#access-list LAN1_LAN2 extended permit ip 192.168.100.0 255.255.255.0
192.168.200.0 255.255.255.0
branchasa(config)#crypto ipsec ikev1 transform-set yabuy_transform esp-aes-256 esp-sha-hmac
Membuat Crypto MAP untuk memetakan setelan konfigurasi IPsec
branchasa(config)#crypto ipsec ikev1 transform-set yabuy_transform esp-aes-256 esp-sha-hmac
branchasa(config)#crypto map yabuy_map 10 match address LAN1_LAN2
branchasa(config)#crypto map yabuy_map 10 set peer 172.16.30.2
branchasa(config)#crypto map yabuy_map 10 set ikev1 transform-set yabuy_transform
branchasa(config)#crypto map yabuy_map 10 set security-association lifetime seconds 3600
branchasa(config)#crypto map yabuy_map interface outside
branchasa(config)#do write memory
```

Sumber : Dokumen Riset (2021)

Gambar 9. Create Access List

```
hoasa(config)#crypto ikev1 policy 10
hoasa(config-ikev1-policy)#authentication pre-share
hoasa(config-ikev1-policy)#encryption aes
hoasa(config-ikev1-policy)#hash sha
hoasa(config-ikev1-policy)#group 2
hoasa(config-ikev1-policy)#lifetime 3600
```

Sumber : Dokumen Riset (2021)

Gambar 10. Enskripsi Algoritma Hash

```
hoasa(config)#tunnel-group 172.16.40.2 type ipsec-      l2l
WARNING: L2L tunnel-groups that have names which  are not an IP
address may only be used if the tunnel authentication method is
Digital Certificates and/or The peer is configured to use Aggressive
Mode
hoasa(config)#tunnel-group 172.16.40.2 ipsec-attributes
hoasa(config-tunnel-ipsec)#ikev1 pre-shared-key yabuy
hoasa(config)# do write memory
```

Sumber : Dokumen Riset (2021)

Gambar 11. tunnel group yang merupakan IP dari hoasa firewall

5. Manajemen Jaringan

Manajemen jaringan yang baik perlu dilakukan untuk mempermudah monitoring, Manajemen yang dilakukan pada penelitian kali ini adalah dengan menerapkan sebuah konsep firewall untuk memfilter paket data yang masuk dan keluar baik dari sisi lokal maupun Publik . Kemudian menerapkan pengiriman data dengan membuat jalur khusus yaitu virtual private network dengan menggunakan ipsec/l2tp. Dengan konsep ini maka pengguna dari luar jaringan lokal tetap dapat terhubung ke jaringan lokal dengan aman.dan dengan metode vpn ini dapat menghubungkan wilayah secara site to site.

6. Pengujian Jaringan

Berikut adalah pengujian terhadap sebuah konektifiktas sebelum menggunakan koneksi tunneling dengan VPN IPsec dari Branch_ASA ke HO_ASA dengan table kebenaran sebagai berikut:

Tabel 7. Uji ICMP dari Branch_ASA ke HO_ASA sebelum VPN

Sumber IP	Tujuan IP	Hasil
192.168.100.2	192.168.100.2	Terkoneksi
192.168.100.2	172.16.40.2	Terkoneksi
192.168.100.2	172.16.40.1	Terkoneksi
192.168.100.2	172.16.20.2	Terkoneksi
192.168.100.2	172.16.20.1	Terkoneksi
192.168.100.2	172.16.10.1	Tidak Terkoneksi
192.168.100.2	172.16.10.2	Tidak Terkoneksi
192.168.100.2	192.168.30.10	Tidak Terkoneksi

Sumber: Dokumen Riset(2021)

Sedangkan Berikut ini adalah pengujian terhadap sebuah konektifiktas sebelum menggunakan koneksi tunneling dengan VPN IPsec dari HO_ASA ke Branch_ASA dengan table kebenaran sebagai berikut:

Tabel 8. Uji ICMP HO_ASA ke dari Branch_ASA Sebelum

Sumber IP	Tujuan IP	Hasil
192.168.100.2	192.168.30.10	Terkoneksi
192.168.100.2	192.168.100.1	Terkoneksi
192.168.100.2	172.16.30.2	Terkoneksi
192.168.100.2	172.16.30.1	Terkoneksi
192.168.100.2	172.16.10.2	Terkoneksi

192.168.100.2	172.16.10.1	Terkoneksi
192.168.100.2	172.16.20.1	Tidak Terkoneksi
192.168.100.2	172.16.40.1	Tidak Terkoneksi
192.168.100.2	172.16.40.2	Tidak Terkoneksi

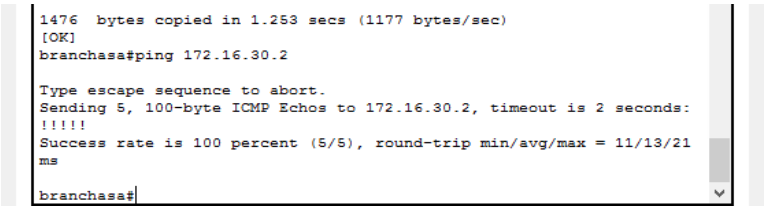
Sumber: Dokumen Riset(2021)

Tahap akhir dari penelitian ini adalah melakukan pengujian dari haril penerapan firewall dan ipsec/l2tp. Pengujian ini dilakukan dengan cara mengirim paket dan didapatkan pengiriman tersebut berhasil dengan paket ping yang sampai dengan sempurna 5/5. Hasil ping (Site-to-Site) koneksi tunneling dengan VPN IPsec dari Branch_ASA ke HO_ASA

Tabel 9. Uji ICMP dari Branch_ASA ke HO_ASA Setelah VPN

Sumber IP	Tujuan IP	Hasil
192.168.100.2	192.168.100.2	Terkoneksi
192.168.100.2	172.16.40.2	Terkoneksi
192.168.100.2	172.16.40.1	Terkoneksi
192.168.100.2	172.16.20.2	Terkoneksi
192.168.100.2	172.16.20.1	Terkoneksi
192.168.100.2	172.16.10.1	Terkoneksi
192.168.100.2	172.16.10.2	Terkoneksi
192.168.100.2	192.168.30.10	Terkoneksi

Sumber: Dokumen Riset(2021)



Sumber : Dokumen Riset (2021)

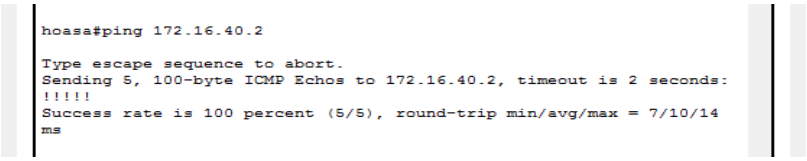
Gambar 12. Hasil ping (Site-to-Site)

Hal yang sebaliknya juga penulis lakukan dengan cara mengirim paket icmp ping terhadap HO_ASA ke Branch_ASA.

Tabel 10. Uji ICMP HO_ASA ke dari Branch_ASA Setelah VPN

Sumber IP	Tujuan IP	Hasil
192.168.100.2	192.168.30.10	Terkoneksi
192.168.100.2	192.168.100.1	Terkoneksi
192.168.100.2	172.16.30.2	Terkoneksi
192.168.100.2	172.16.30.1	Terkoneksi
192.168.100.2	172.16.10.2	Terkoneksi
192.168.100.2	172.16.10.1	Terkoneksi
192.168.100.2	172.16.20.1	Terkoneksi
192.168.100.2	172.16.40.1	Terkoneksi
192.168.100.2	172.16.40.2	Terkoneksi

Sumber: Dokumen Riset(2021)



Sumber : Dokumen Riset (2021)

Gambar 2. Hasil ping terhadap HO_ASA ke Branch_ASA

KESIMPULAN

Setelah melakukan tahapan demi tahapan dalam melakukan penelitian ini maka penulis mendapatan kesimpulan. Pada perusahaan PT Neu Indonesia yang memiliki wiliyah pusat dan solo dapat menerapkan keamanan jaringan komputer dengan menerapkan Jaringan *Wide Area Network* . Dengan memanfaatkan fitur internet maka perusahaan tersebut menerapkan firewall yang sebelumnya firewall hanya keamanan bawaan dari windows sehingga memudahkan sesorang dalam mencuri data baik secara internal maupun external jaringan sehingga diterapkan firewall pada sebuah router agar mendeteksi hadirnya malware ataupun bahaya . Oleh karena sebuah situs keunggulan terutama oleh karena penerapan firewall bagi komputer kita ialah bisa untuk mendeteksi hadirnya malware yang bahaya dari berbagai jenis situs yang kita kunjungi.Karena Firewall peka terhadap kesalahan konfigurasi dan kegagalan untuk menerapkan kebijakan, sehingga diperlukan tambahan atau peningkatan keamanan jaringan pada PT.Neu Indonesia. Kemudian dalam bertukar informasi dan data kini dapat dilakukan dalam sebuah metode yang aman dengan menerapkan protokol ipsec/l2tp. Vpn ini diterapkan seolah olah antara cabang pusat dan solo memiliki jaringan private yang aman dan terenskripsi dengan memanfaatkan internet yang sebelumnya data antar cabang tidak dapat dijadikan satu secara private.

REFERENSI

Firmansyah, Wahyudi, M & Rachmat, P. (2018). Analisis Perbandingan Kinerja Jaringan CISCO Virtual Router Redundancy Protocol (VRRP) Dan CISCO Hot Standby Router Protocol (HSRP). *Teknik Komputer AMIK BSI Tegal*, *1*(1), 764–769.

Firmansyah, Dewi, S., & Purnama, R. adi. (2020). Quality Of Service Gateway Load Balancing Protocol Message Digest Algorithm 5 Authentication Untuk Peningkatan Kualitas Jaringan. *Jurnal Teknik Informatika*, *5*(November), 45–50.

Firmansyah, & Wahyudi, M. (2021). *Analisis Performa Access Control List menggunakan Metode Firewall Policy Base Performance Analysis of the Access Control List Using the Firewall Policy- Based Method*. *20*(2), 283–292. https://doi.org/10.30812/matrik.v20i1.1068

Maulana, A.-. (2018). Penerapan Routing EIGRP, RIPv2 Dan OSPF Pada IPv6 Menggunakan Metode Redistribution. *Jurnal Pendidikan Teknologi Dan Kejuruan*, *15*(2), 234–243. https://doi.org/10.23887/jptk-undiksha.v15i2.14276

Maulana, A., & Fauzi, A. (2019). *Administrasi jaringan Komputer* (1st ed.). Graha Ilmu.

Mugi Raharjo, Frengki Pernando, A. F. (2019). Perancangan Performansi Quality Of Service Dengan Metode Virtual Routing Redudancy Protocol (VRRP). *Teknik Komputer*, *V*(1), 87–92. https://doi.org/10.31294/jtk.v5i1.4555

Pratama, E. K. (2019). IMPLEMENTASI HOT STANDBY ROUTER PROTOCOL CISCO PADA JARINGAN THIN CLIENT. *Jurnal AKRAB JUARA*, *4*(4), 160–168.

Pratama, E. K., Hasan, F. N., & Asteroid, K. M. (2018). PEMANFAATAN REDUDANCY ROUTER DENGAN FITUR VRRP MIKROTIK PADA JARINGAN THIN CLIENT. *AKRAB JUARA*, *3*(2), 21–28.

Syawaludin, H. A., Fauzi, A., & Rosyida, S. (2020). *PERANCANGAN DAN IMPLEMENTASI JARINGAN TUNNEL DENGAN METODE PPTP PADA YAYASAN PENDIDIKAN BINA PUTERA INDONESIA*. *7*(1), 133–142. https://doi.org/https://doi.org/10.22202/ei.2020.v7i1.4346

Wahyudi, M., & Firmansyah. (2021). Network Performance Optimization using Dynamic Enhanced Interior Routing Protocols Gateway Routing Protocol for IPv6 (EIGRPv6) and IPv6 Access Control List. *Journal of Physics: Conference Series*, *1830*(1). https://doi.org/10.1088/1742-6596/1830/1/012017