JDSP
Jurnal Data Science Penusa

Perancangan Dan Implementasi Jaringan Pribadi Virtual (Vpn) Dengan Cisco Packet Tracer

Gunung juanda Tampubolon[1)*], Baringin Sianipar[2)]
[1,2]Teknologi Rekayasa Komputer Jaringan, STMIK Pelita Nusantara,
[1,2] juandatampubolon16@gmail.com
aniparbaringin87@gmail.com

Received: 25 Januari 2025 Accepted: 13 Maret 2025 Published: 22 Juli 2025
Pg. 654-667

OPEN ACCESS

***Penulis Koresponden**
Kata Kunci:perancangan, implementasi, vpn, jaringan, dengan cisco packet tracer.
JDSP: Jurnal Data Science Penusais licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).

Abstrak Dalam era digital yang terus berkembang, keamanan komunikasi dan pertukaran data menjadi aspek yang sangat penting bagi organisasi dan individu. teknologi yang berhubungan dengan komunikasi jarak jauh. membuat jarak seperti tidak ada ratusan atau bahkan ribuan kilometer menggunkan teknologi telekomunikasi. Jaringan pribadi secara virtual juga menjadi solusi populer untuk mengamankan komunikasi dan mengakses sumber daya jaringan secara aman melalui internet. Analisa yang di lakukan untuk menganalisa sebuah rancangan yang akan di bangun pada pembuatan suatu design jaringan , mulai dari tahap rancangan bangun design jaringan hingga pengujian jaringan terserbut pengumpulan data yang di dilakukan dalam penelitian ini dengan melalui observasi langsung menuju ke lokasi untuk menganalisa permasalahan yang ada. Menganalisa jaringan lama yang sudah di bangun,menganalisa skema jaringan yang akan di bangun untuk perancangan vpn, dan menganalisa kendala yang akan terjadi pada proses penelitianHasil penelitian menunjukan bahawa perancangan dan implementasi aman jaringan pribadi virtual vpn dengan cisco packet tracer sangat baik di terapkan dalam melakukan pengirim data dan serta menggamankan data dari berbagai serangan dan pencurian melalui jaringan public atau jaringa pribadi.Untuk penelitian selanjutnya, disarankan untuk mengembangkan fitur keamanan tambahan dalam jaringan VPN, seperti implementasi firewall atau deteksi intrusi untuk meningkatkan tingkat keamanan Menyertakan pengembangan system pemantauan dan manajemen jaringan untuk memudahkan pengelolaan dan pemantauan konrksi vpn secara efisien. Simulasi dengan cisco packet tracer sangat berguna , namun pengujian dalam lingkungan nyata dengan perangkat keras dan jaringan yang sebenarnya dapat memberikan wawasan tambahan mengenai kinerja dan masalah yang akan timbul. Meningkatkan pemahaman dan keterampilan pengguna melalui pelathian mengenai manajemen dan pengolahan VPN . hal ini dapat membantu dalam memaksimalkan manfaat teknologi dan mengurangi resiko kesalahan konfigurasi

PENDAHULUAN

Dalam era digital yang terus berkembang, keamanan komunikasi dan pertukaran data menjadi aspek yang sangat penting bagi organisasi dan individu. Teknologi yang berhubungan dengan komunikasi jarak jauh. membuat jarak seperti tidak ada ratusan atau bahkan ribuan kilometer menggunkan teknologi telekomunikasi. Jaringan pribadi secara virtual juga menjadi solusi populer untuk mengamankan komunikasi dan mengakses sumber daya jaringan secara aman melalui internet. Jaringan virtual memungkinkan seseorang dapat mengirimkan informasi atau menerima informasi ke atau dari pihak lain yang letakberjauhan.

VPN atau Jaringan Pribadi Virtual (Virtual Private Network)membuat koneksi jaringan privat diantara beberapa perangkat melalui internet. VPN digunakan untuk mentransmisikan data secara aman dan anonim melalui jaringan public (Mujiastuti & Prasetyo, 2021). VPN bekerja dengan cara menyembunyikan alamat IP pengguna dan mengenkripsi data sehingga tidak dapat dibaca oleh siapa pun yang tidak berwenang untuk menerima. VPN memungkinkan pengguna untuk membentuk koneksi aman melalui jaringan publik yang tidak aman, seperti Internet, dengan mengenkripsi data yang dikirimkan antara titik-titik akhir.Seiring dengan meningkat ancaman keamanan cyber, organisasi dan individu semakin sadar akan penting menerapkan solusi VPN yang aman untuk melindungi informasi sensitive. Penggunaan internet yang kurang baik dapat menimbilkan pencurian data pribadi dari internet (phising). VPN membutuhkan jaringan yang stabil dan andal untuk menyiapkan koneksi yang aman, jadi koneksi yang tidak stabil bisa jadi penyebab. Masalah koneksi VPN dapat bervariasi tergantung pada keadaan tertentu. Salah satu alasan umum untuk koneksi VPN yang gagal adalah kredensial login yang salah.

Cisco systems, sebagai salah satu penyedia utama perangkat jaringan, telah menyediakan berbagai solusi VPN yang handal dan terpercaya. Salah satu perangkat lunak yang populer untuk merancang, mengonfigurasi, dan menguji jaringan, termasuk jaringan pribadi virtual, adalah Cisco Packet Tracer (Kus Heryadi & Surya Budiman, 2021). VPN (Virtual Private Network) bekerja dengan memungkinkan pengguna untuk membuat koneksi internet pribadi yang terenkripsi dari perangkat mereka ke server VPN di tempat lain di dunia. Ini dilakukan dengan menggunakan protokol koneksi internet yang aman untuk mengirim dan menerima data melalui jaringan publik, seperti internet. Cisco Packet tracer adalah perangkat lunak simulasi jaringan yang memungkinkan pengguna untuk membangun topologi jaringan virtual dan melakukan konfigurasi perangkat jaringan yang sesuai (Drajana & Bode, 2021). Topologi jaringan komputer berfungsi untuk mengetahui bagaimana masing-masing komputer atau host dalam jaringan komputer dapat saling berkomunikasi satu sama lain.

Penelitian PenggunaanAplikasi Simulasi Jaringan Cisco Packet Tracer Dalam Design Network, menjelaskan Aplikasi cisco packet tracer dapat digunakan sebagai simulasi data jaringan yang dapat dimanfaatkan menjadi informasi tentang keadaan koneksi suatu komputer dalam suatu jaringan, apabila terjadi masalah dalam akses jaringan (Samsumar & Subli, 2019). Koneksi VPN mengalihkan paket data dari mesin ke server jarak jauh lain sebelum mengirimkannkepihak ketiga melalui internet. Packet Tracer memungkinkan pengguna untuk menyimulasikan jaringan yang terdiri dari perangkat Cisco, termasuk router, switch, perangkat wireless, dan perangkat jaringan lain.Penelitian ini bertujuan untuk merancang dan mengimplementasikan jaringan pribadi virtual (VPN) yang aman dengan menggunakan Cisco Packet Tracer untuk mengintegrasikan fitur keamanan yang kuat ke dalam desain jaringan VPN dan memastikan keamanan data selama proses komunikasi melalui jaringan yang tidak aman juga akan mempertimbangkan faktor performa dan skalabilitas untuk memastikan VPN yang diimplementasikan dapat beroperasi secara efisien dan efektif.

TINJAUAN LITERATUR

Dalam era digital yang terusberkembang, keamanankomunikasi dan pertukaran data menjadiaspek yang sangatpentingbagiorganisasi dan individu. Teknologi yang berhubungan dengan komunikasi jarak jauh. Membuat jarak seperti tidak adaratusan atau bahkanribuan kilometer menggunkanteknologitelekomunikasi. Jaringan pribadi secara virtual juga menjadi solusipopuler untuk mengamankan komunikasi dan mengakses sumberdaya jaringan secara aman melalui internet. Jaringan virtual memungkinkan seseorang dapat mengirimkaninformasi atau menerima informasi ke atau dari pihak lain yang letak berjauhan.

VPN atau JaringanPribadi Virtual *(Virtual Private Network)*membuat koneksi jaringan privat diantara beberapa perangkat melalui internet. VPN digunakan untuk mentransmisikan data secaraaman dan anonimmelaluijaringan public[1].VPN bekerja dengan cara menyembunyikan alamat IP pengguna dan mengenkripsi data sehingga tidak dapat dibaca oleh siapa pun yang tidak berwenang untuk menerima.VPN memungkinkanpengguna untuk membentuk koneksi aman melalui jaringan publik yang tidak aman, seperti Internet, dengan mengenkripsi data yang dikirimkanantaratitik-titikakhir.Seiring dengan meningkatancamankeamanan cyber, organisasi dan individusemakinsadarakanpentingmenerapkansolusi VPN yang aman untuk melindungiinformasi sensitive. Penggunaan internet yang kurang baik dapat menimbilkanpencurian data pribadidari internet *(phising)*.VPN membutuhkan jaringan yang stabil dan andal

untuk menyiapkan koneksi yang aman, jadi koneksi yang tidak stabil bisa jadi penyebab. Masalah koneksi VPN dapat bervariasi tergantung pada keadaan tertentu. Salah satu alasan umum untuk koneksi VPN yang gagal adalah kredensial login yang salah.

*Cisco systems,*sebagai salah satupenyediautamaperangkatjaringan, telahmenyediakanberbagaisolusi VPN yang handal dan terpercaya. Salah satuperangkatlunak yang populer untuk merancang, mengonfigurasi, dan mengujijaringan, termasukjaringanpribadi virtual, adalah Cisco Packet Tracer[2]. VPN *(Virtual Private Network)*bekerja dengan memungkinkanpengguna untuk membuatkoneksi internet pribadi yang terenkripsidariperangkatmerekake server VPN di tempat lain di dunia. Ini dilakukan dengan menggunakanprotokolkoneksi internet yang aman untuk mengirim dan menerima data melaluijaringanpublik, seperti internet. *Cisco Packet tracer*adalahperangkatlunaksimulasijaringan yang memungkinkanpengguna untuk membanguntopologijaringan virtual dan melakukankonfigurasiperangkatjaringan yang sesuai[3]. Topologijaringankomputerberfungsi untuk mengetahuibagaimana masing-masing komputer atau host dalamjaringankomputer dapat salingberkomunikasisatusama lain.

METODE PENELITIAN

Analisa yang di lakukan untuk menganalisasebuahrancangan yang akan di bangun padapembuatansuatu design jaringan , mulaidaritahaprancanganbangun design jaringanhinggapengujianjaringanterserbut apakah hasil yang di dapat darirancangan yang telah di implementasikanakanmendapatkanhasil yang baik

AnalisaData

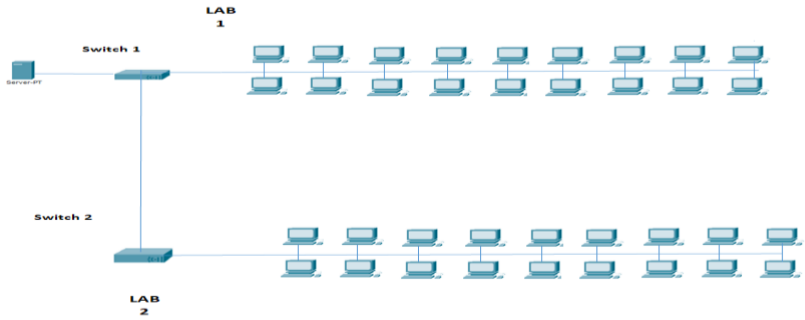
pengumpulan data yang di dilakukandalam penelitian ini dengan melaluiobservasilangsungmenujukelokasi untuk menganalisapermasalahan yang ada. Menganalisajaringan lama yang sudah di bangun,menganalisaskemajaringan yang akan di bangun untuk perancanganvpn, dan menganalisakendala yang akanterjadi pada proses penelitian.

Perancangan system

Perancangan system di lakulan dengan beberapatahapyaituperancangan design jaringan dan design konfigurasijaringan ,perancanganjaringanmeliputidesaintopologijaringan, design konfigurasi router meliputi setting ip address dan routing pada router,Adapuntahapantahapansebagai berikut:

PerancanganJaringan

Pada penerapanjaringan ini mengunakanjaringan local yang terdiridari 20 pc client dengan cisco packet tracer yang digunakansebagaimendesaigntopologijaringan.



Gambar 3.1 TopologiJaringan

pada gambar di atasterdapat 1 buah server dan 2 buah switch. Pada dua switch tersebut itukitaubahnamamenjadi Lab1 dan Lab 2. Switch pertama atau Lab 1 terdapat 20 komputer dan switch kedua atau Lab 2 juga terdapat 20 komputer. Perangkat switch yang di gunakansebagaimenghubungkansejumlah computer client agar bisamelakukanpertukaranpaket dan meneruskan data yang dikirimmelaluimelalui switch ke computer client yang akandituju.

DesainKonfigurasiRouter

Pada desaign ini akanmenggambarkanpengalamatan router pada jalurip address yang sudah di tentukan agar lebihmempermudahdalammelakukanpengaturankonfigurasijaringan.

Tabel 3.1 Desain konfigurasi router

Router	Interface	IPAddress	Subnet mask	Gateway

Pc server	-	192.168.1.2	255.255.255.0	192.168.1.1
R1	Eth1/g0/1	192.168.1.1	255.255.255.0	-
	se0/0/0	10.10.10.1	255.255.255.0	-
R2	Eth1/g0/1	192.168.2.1	255.255.255.0	-
	se0/0/0	20.20.20.1	255.255.255.0	-
R3	Se2/0	10.10.10.2	255.255.255.0	-
	Se3/0	20.20.20.2	255.255.255.0	-
Pc client	-	192.168.2.2	255.255.255.0	192.168.2.1

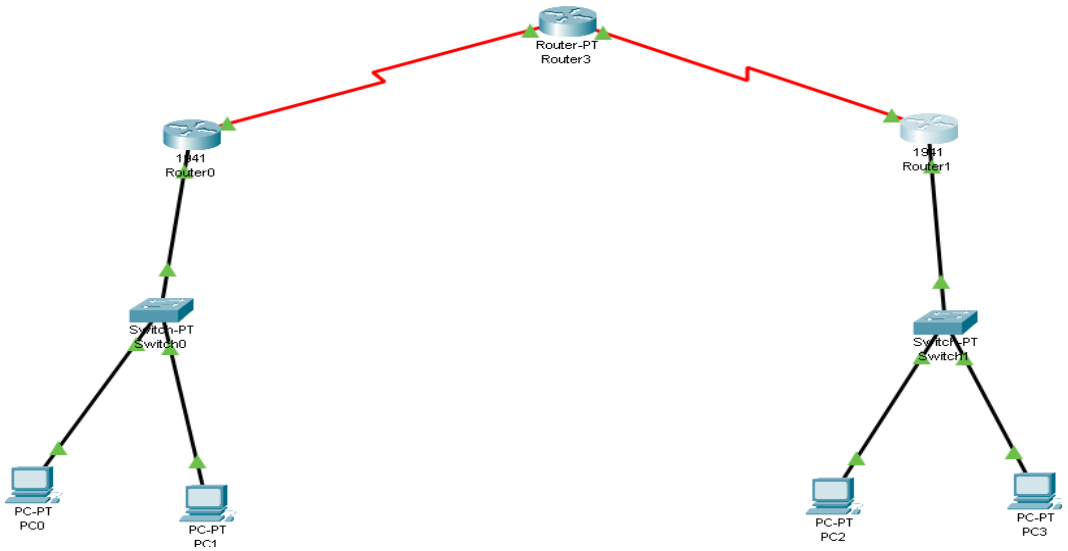
Gambar 1 Analisis Usia dan Pendapatan Pelanggan

HASIL PENELITIAN

Hasil Desain Topologi

Hasil penelitian

Hasil penelitian menunjukan bahawa perancangan dan implementasi aman jaringan pribadi virtual vpn dengan cisco packet tracer sangat baik di terapkan dalam melakukan pengirim data dan serta menggamankan data dari berbagai serangan dan pencurian melalui jaringan public atau jaringa pribadi.



Gambar 1 hasil desain topologi

Berikut hasil desain topologi yang dilakukan

Pada gambar di atas terdapat komponen komponen sebagai berikut

1. Router 1

   Berfungsi sebagai vpn server

2. Router 2

   Berfungsi sebagai clinet vpn

3. Router 3

   Berfungsi sebagai portal antara router 1 dan router 2

4. Switch

   Berfungsi sebagai penghubung antara pc dengan switch

5. PC/Client

   Berfungsi sebagai user client / Pengguna

Kode Konfigurasi pada Router 1

Pada konfigurasi router 1 ini kitaakanmenghubungantara router 1 dengan switch melalui cli yang ada di router 1.

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname labl
labl(config)#int gig0/0
labl(config-if)#ip add 192.168.1.1 255.255.255.0
labl(config-if)#no sh

labl(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

labl(config-if)#ex
labl(config)#int se0/0/0
labl(config-if)#ip add 10.10.10.1 255.255.255.0
labl(config-if)#no sh

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
labl(config-if)#ex
```

Gambar 2 Hasil Konfigurasi Router

Setelah kitaberhasilmenghubungkan router 1 dengan switch melaluikonfigurasi yang ada pada router .Selanjutkitaakanmemasukanipdhcp pool pada router 1 atau lab1.

```
labl(config)#ip dhcp pool labl
labl(dhcp-config)#network 192.168.1.0 255.255.255.0
labl(dhcp-config)#default-router 192.168.1.1
labl(dhcp-config)#dns-server 192.168.1.1
labl(dhcp-config)#ex
```

Gambar 3 Hasil Konfigurasi IP dhcp pool pada Router 1

Setelah kitamemasukankodekonfigurasiipdhcp pool dan router rip pada router atau lab 1 . selanjutkitaakanmemasukanipdhcp excluded-address pada router 1

```
labl(config)#ip dhcp excluded-address 192.168.1.1
labl(config)#router rip
labl(config-router)#version 2
labl(config-router)#network 192.168.1.0
labl(config-router)#router rip
labl(config-router)#version 2
labl(config-router)#network 10.10.10.0
labl(config-router)#no au
labl(config-router)#ex
labl(config)#do sh run
Building configuration...

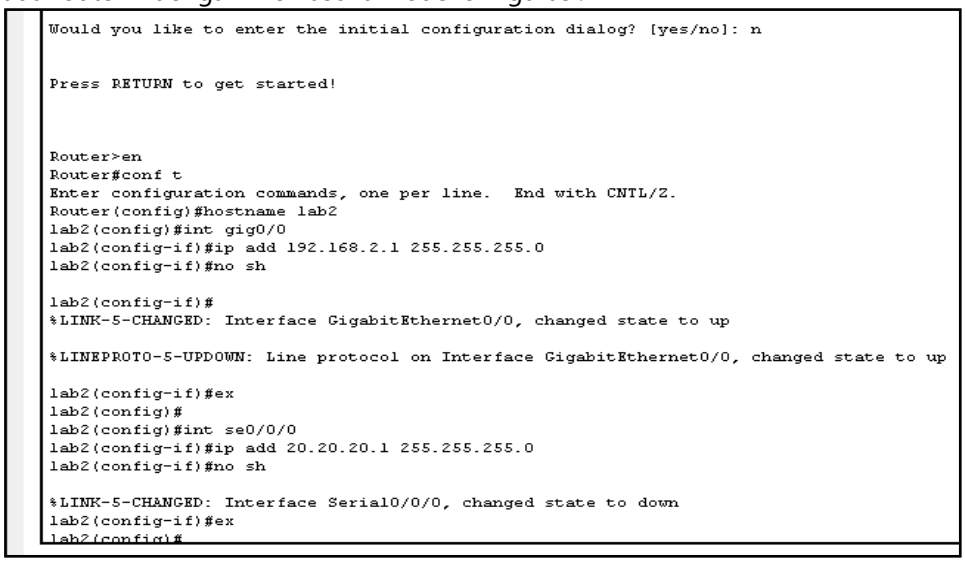
Current configuration : 994 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
```

Gambar 4 Hasil Konfigurasi IP dhcp excluded pada Router 1

Berikut adalahkodekonfigurasiipdhcp excluded-address pada router 1Selanjutkitaakanmelakukanhal yang sama pada router 2 .

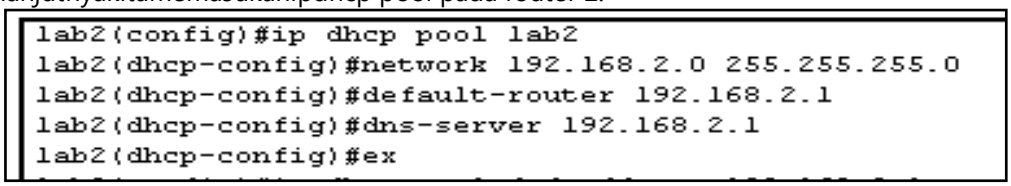
Hasil Konfigurasi pada Router 2

Pada router 2 ini kitaakanmenghubungantara router 2 dengan switch 2 dimanakitaakanmenghubungmelalui cli yang ada pada router 2 dengan memasukankodekonfigurasi.



Gambar 5 Hasil Konfigurasi pada Router 2

Setelah kitamemasukankodekonfigurasi pada router 2 dan berhasilmenghubungantara router 2 dengan switch 2. Selanjutnyakitamemasukanipdhcp pool pada router 2.



Gambar 6 Hasil Konfiguras IP dhcp pool pada Router 2

Setelah kitamemasukankodekonfigurasiipdhcp pool pada router 2. Selanjutkitamemasukanipdhcp excluded pada router 2 serta router rip pada router 2.

```
lab2(dhcp-config)#ex
lab2(config)#ip dhcp excluded-address 192.168.2.1
lab2(config)#router rip
lab2(config-router)#version 2
lab2(config-router)#network 192.168.2.0
lab2(config-router)#network 20.20.20.0
lab2(config-router)#no au
lab2(config-router)#ex
lab2(config)#do sh run
Building configuration...

Current configuration : 974 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname lab2
!
!
!
!
ip dhcp excluded-address 192.168.2.1
!
ip dhcp pool lab2
 network 192.168.2.0 255.255.255.0
 default-router 192.168.2.1
 dns-server 192.168.2.1
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO1941/K9 sn FTX1524B40D-
!
!
!
!
!
!
!
```

Gambar 7 Hasil Konfigurasi IP dhcp excluded dan Router rip router 2

Setelah kitamemasukankodekonfigurasi pada ipdhcp pool excluded dan router rip pada router 2 selanjutkitaakanmelakukankodekonfigurasi pada router 3

Hasil Konfigurasi pada Router 3

Pada router 3 ini kitaakanmenghubungantara router 1 dan router 2 dimana router 3 sebagai portal antara router 1 dan 2.

```
Would you like to enter the initial configuration dialog? [yes/no]: n

Press RETURN to get started!


Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname isp
isp(config)#int se2/0
isp(config-if)#ip add 10.10.10.2 255.255.255.0
isp(config-if)#no sh

isp(config-if)#
%LINK-5-CHANGED: Interface Serial2/0, changed state to up

isp(config-if)#ex
isp(config)#
isp(config)#int se3
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
                ^
% Invalid input detected at '^' marker.

isp(config)#int se3/0
isp(config-if)#ip add 20.20.20.2 255.255.255.0
isp(config-if)#no sh

isp(config-if)#
%LINK-5-CHANGED: Interface Serial3/0, changed state to up

isp(config-if)#ex
isp(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state to up
```

Gambar 8 Hasil Konfigurasi pada Router 3

Berikut adalahhasilkonfigurasu pada router 3. Setelah kitamenghubungkan router 1 dan router 2 selanjutkitaakanmemasukan router rip pada router 3

```
isp(config)#router rip
isp(config-router)#version 2
isp(config-router)#network 10.10.10.0
isp(config-router)#network 20.20.20.0
isp(config-router)#no au
isp(config-router)#ex
isp(config)#
isp(config)#
```

Gambar 9 Hasil Konfigurasi Router rip pada Router 3

Berikut adalahhasilkonfigurasi router rip pada router 3. Setelah kitamemasukan router rip pada router 3 selanjutkitaakanmemasukkonfigurasivpn pada router 1.

Hasil Konfigurasi VPN

Pada konfigurasivpn ini kita pertama kitaakanmemasukankodekonfigurasivpn pada router 1.

setelah kitamemasukankodekonfigurasivpn license boot module c1900 technology-package securtyk9 pada router 1 disituterdapatpilihanantarakitapilih yes/no .

```
labl>en
labl#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
labl(config)#lincense boot module c1900 technology-package securityk9
             ^
% Invalid input detected at '^' marker.

labl(config)#license boot module c1900 technology-package securityk9
PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR
LICENSE  KEY  PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING SUCH
PRODUCT  FEATURE  CONSTITUTES  YOUR  FULL ACCEPTANCE  OF  THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO  BE BOUND
BY ALL THE TERMS SET FORTH HEREIN.

Use of this product feature requires  an additional license from Cisco,
together with an additional  payment.  You may use this product feature
on an evaluation basis, without payment to Cisco, for 60 days. Your use
of the  product,  including  during the 60 day  evaluation  period,  is
subject to the Cisco end user license agreement
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html
If you use the product feature beyond the 60 day evaluation period, you
must submit the appropriate payment to Cisco for the license. After the
60 day  evaluation  period,  your  use of the  product  feature will be
governed  solely by the Cisco  end user license agreement (link above),
together  with any supplements  relating to such product  feature.  The
above  applies  even if the evaluation  license  is  not  automatically
terminated  and you do  not receive any notice of the expiration of the
evaluation  period.  It is your  responsibility  to  determine when the
evaluation  period is complete and you are required to make  payment to
Cisco for your use of the product feature beyond the evaluation period.

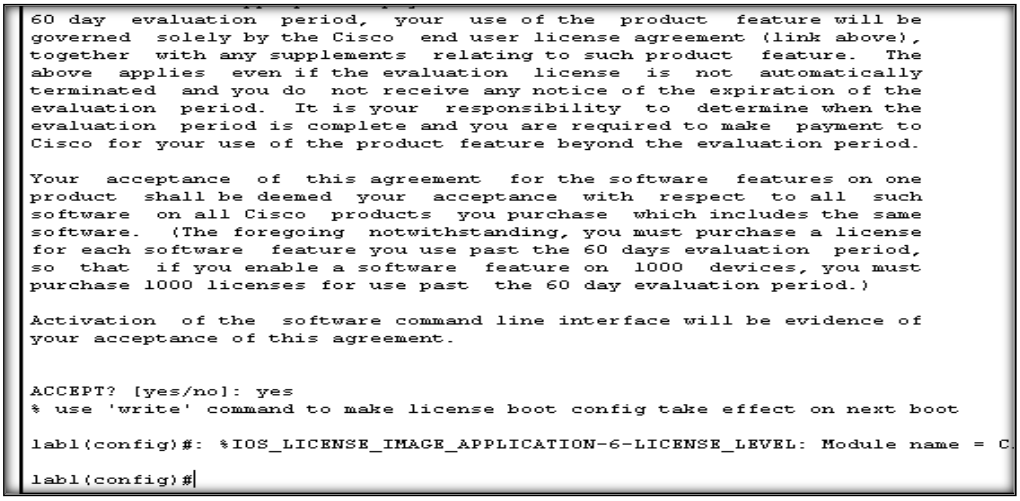
Your  acceptance  of  this agreement  for the software  features on one
product  shall be deemed  your  acceptance  with  respect  to all  such
software  on all Cisco  products  you purchase  which includes the same
software.  (The foregoing  notwithstanding, you must purchase a license
for each software  feature you use past the 60 days evaluation  period,
so  that  if you enable a software  feature on  1000  devices, you must
purchase 1000 licenses for use past  the 60 day evaluation period.)

Activation  of the  software command line interface will be evidence of
your acceptance of this agreement.


ACCEPT? [yes/no]:
```

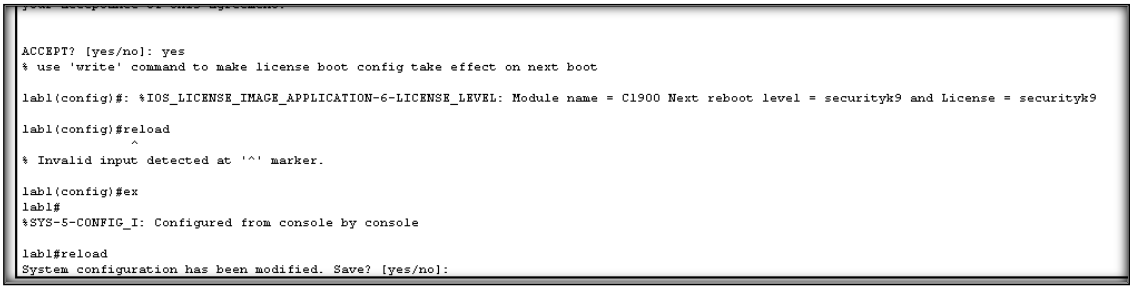
Gambar 10 Hasil KonfigurasiVPN pada Router 1

setelah kita memasukan kode konfigurasi vpn license boot module c1900 technology-package securtyk9 pada router 1 disitu terdapat pilihan antara kita pilih yes/no .



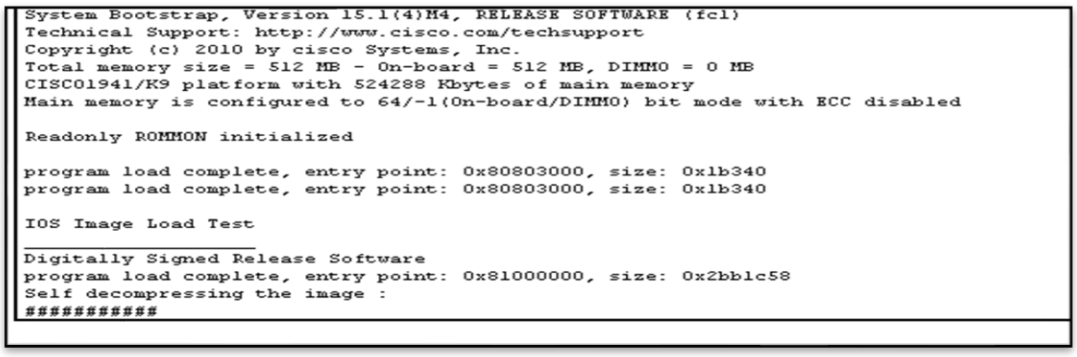
Gambar 11 Hasil Konfigurasi VPNRouter 1

Berikut adalah hasil setelah kita memilih yes pada pilihan kode konfiguras license boot module c1900 technology-package securityk9. selanjut kita akan mereload router 1



Gambar 12 Hasil Konfigurasi VPN Router 1

Setelah kita memasukan kode konfigurasi reload. Pada gambar di atas terdapat pilihan antara pilih yes/no kita akan memilih yes pada pilih tersebut.

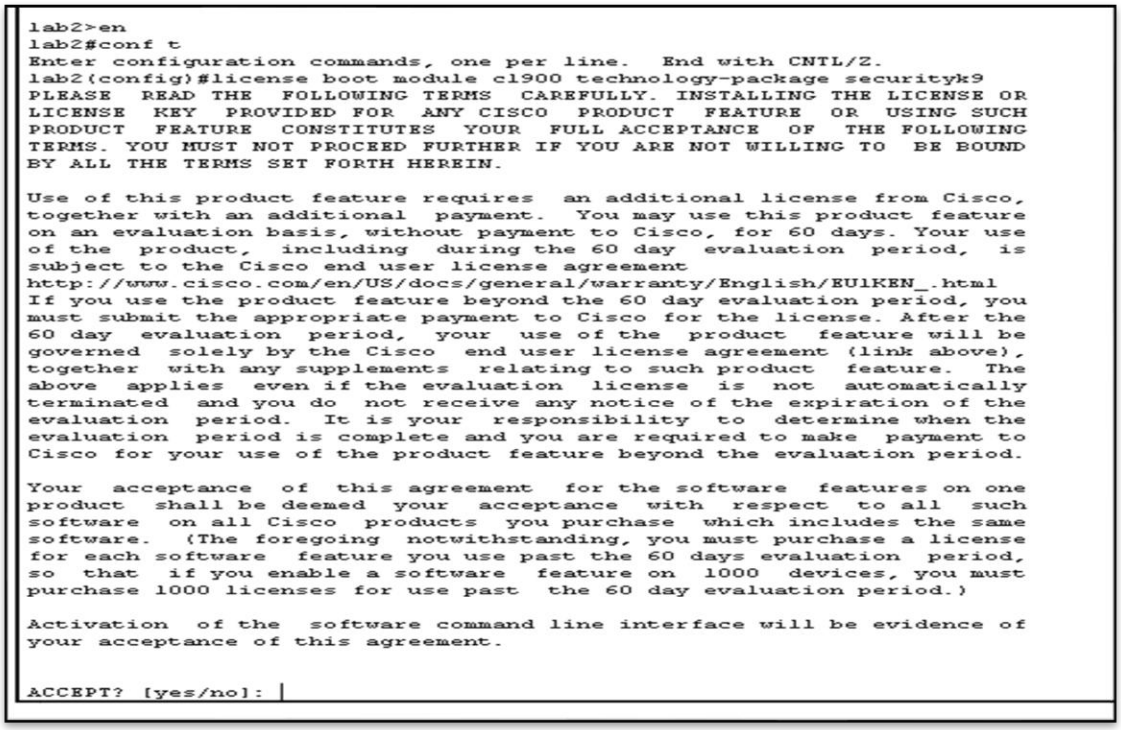


Gambar 13 Konfigurasi VPN Router 1

Berikut adalah hasil Setelah kita memilih yes Selanjut kita melakukan hasil yang sama pada router 2.

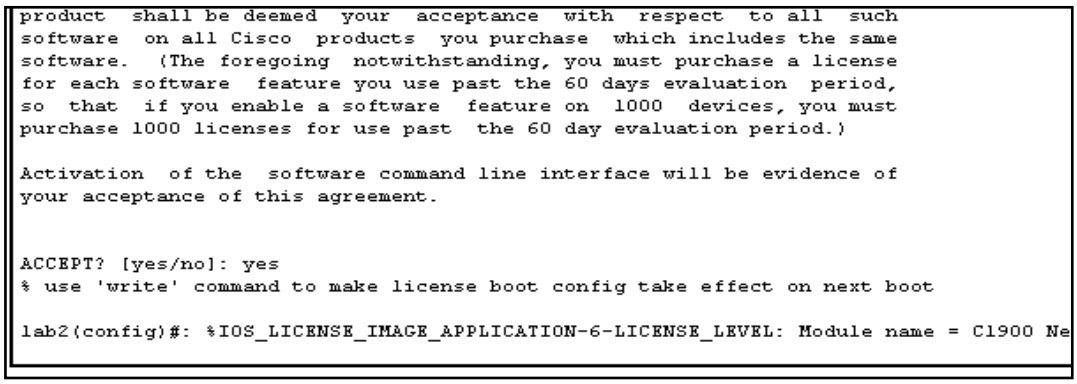
Pada router ke 2 ini kita akan melaku kan hal yang sama dengan router 1 yaitu memasukan kode konfigurasi licensen

boot module c1900 technology-package securityk9



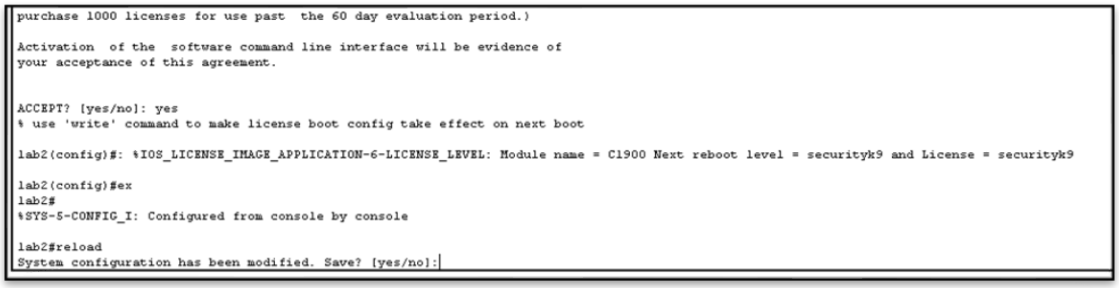
Gambar 14 Hasil Konfigurasi VPN Router 2

Berikut adalah hasil konfigurasi license boot module c1900 technology-package securityk9 pada router 1.pada gambar diatas tersebut terdapat pilihan antara pilih yes/no. disene kita akan memilih yes



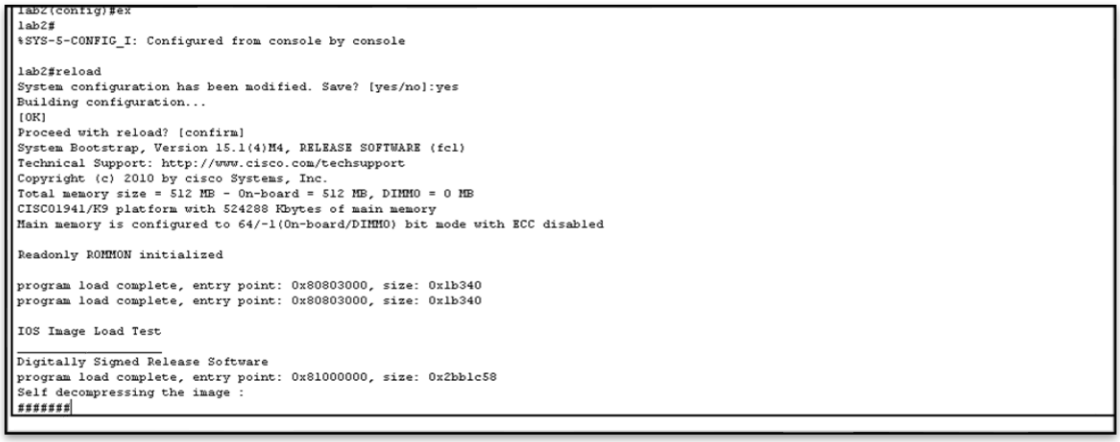
Gambar 15 Hasil Konfigurasi Router 2

Berikut adalah hasil setelah kita memilih yes. Selanjut kita akan mereload router 2 tersebut.



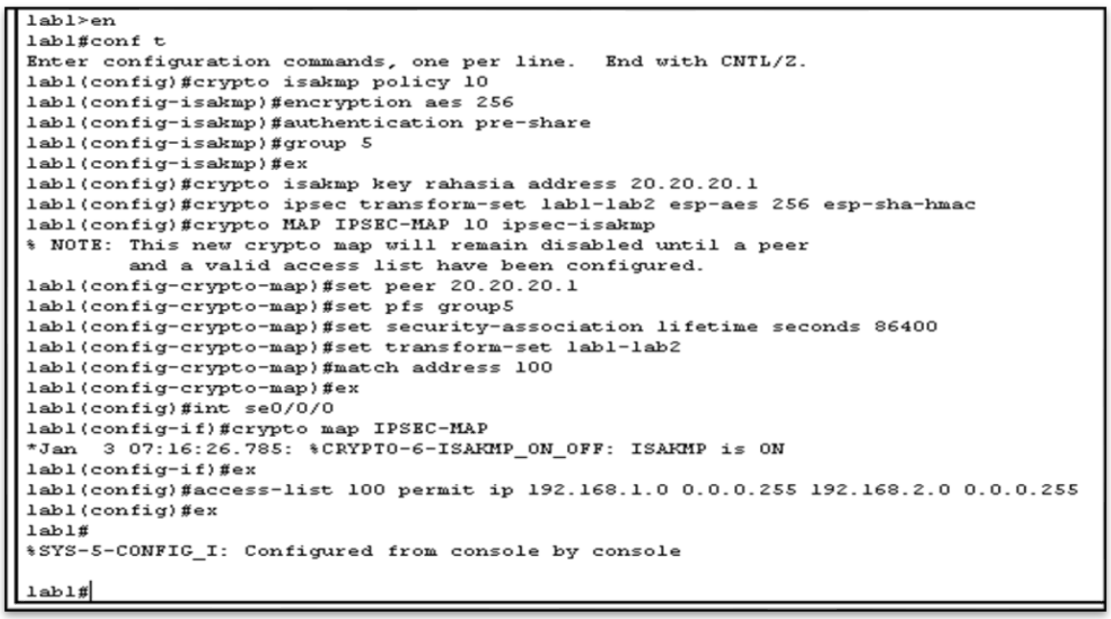
Gambar 16 Hasil Konfigurasi VPN Router 2

Setelah kita mengetikan atau memasukan kode konfigurasi reload pada router 2. Pada gambar tersebut terdapat pilihan dimna kita akan memilih salah satu di antara pilihan tersebut yaitu antara pilih yes/no.



Gambar 17 Hasil Konfigurasi VPN Router 2

Berikut adalah tampilan hasil konfigurasi reload setelah kita memilih yes.selanjut kita akan memasukan kode konfigurasi vpn pada router 1



Gambar 18 Hasil Konfigurasi VPN Router 1

Berikut adalah kode konfigurasi vpn pada router 1

Selanjut kita akan melihat hasil dari kode konfigurasi tersebut dengan mengetik show int brief

```
lab1#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.1.1     YES NVRAM  up                    up
GigabitEthernet0/1     unassigned      YES NVRAM  administratively down down
Serial0/0/0            10.10.10.1      YES NVRAM  up                    up
Serial0/0/1            unassigned      YES NVRAM  administratively down down
Vlan1                  unassigned      YES NVRAM  administratively down down
lab1#
```

Gambar 19 Hasil Konfigurasi VPN Router 1

Selanjut kita akan melihat hasil konfigurasi vpn crypto dengan mengetikan show crypto policy

```
lab1#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:    AES - Advanced Encryption Standard (256 bit keys).
        hash algorithm:          Secure Hash Standard
        authentication method:   Pre-Shared Key
        Diffie-Hellman group:    #5 (1536 bit)
        lifetime:                86400 seconds, no volume limit
lab1#
lab1#
```

Gambar 20 Hasil Konfigurasi VPN Router 1

Berikut adalah hasil dari konfigura show crypto isakmp policy

Selanjut kita akan melihat show crypto isakmp sa

```
        lifetime:                86400 seconds, no volume limit
lab1#
lab1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status

IPv6 Crypto ISAKMP SA


lab1#
```

Gambar 21 Hasil Konfigurasi VPN pada Router 1

Berikut adalah hasil show crypto isakmp sa. Setelah melihat hasil vpn pada router 1 selanjut kita akan melakukan kode konfigurasi pada router 2

```
lab2>en
lab2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
lab2(config)#crypto isakmp policy 10
lab2(config-isakmp)#encryption aes 256
lab2(config-isakmp)#authentication pre-share
lab2(config-isakmp)#group 5
lab2(config-isakmp)#ex
lab2(config)#crypto isakmp key rahasia address 10.10.10.1
lab2(config)#crypto ipsec transform-set lab2-lab1 esp-aes 256 esp-sha-hmac
lab2(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
lab2(config-crypto-map)#set peer 10.10.10.1
lab2(config-crypto-map)#set pfs group5
lab2(config-crypto-map)#set security-association lifetime seconds86400
                                                                ^
% Invalid input detected at '^' marker.

lab2(config-crypto-map)#set security-association lifetime seconds 86400
lab2(config-crypto-map)#set trasnform-set lab2-lab1
                           ^
% Invalid input detected at '^' marker.

lab2(config-crypto-map)#set transform-set lab2-lab1
lab2(config-crypto-map)#match address 100
lab2(config-crypto-map)#ex
lab2(config)#int se0/0/0
lab2(config-if)#crypto map IPSEC-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
lab2(config-if)#ex
lab2(config)#accesslist 100 permit ip 192.168.2.0
                    ^
% Invalid input detected at '^' marker.

lab2(config)#accesslist 100 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
                    ^
% Invalid input detected at '^' marker.

lab2(config)#access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
lab2(config)#
```

Gambar 22 Hasil Konfigurasi VPN Router 2

Berikut adalah hasil konfigurasi vpn pada router 2. Setelah kita memasukan kode konfigurasi vpn pada router selanjut kita akan melihat konfigurasi tersebut.

Dengan memasukan kode show ip int brief.

```
%SYS-5-CONFIG_I: Configured from console by console

lab2#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.2.1     YES NVRAM  up                    up
GigabitEthernet0/1     unassigned      YES NVRAM  administratively down down
Serial0/0/0            20.20.20.1      YES NVRAM  up                    up
Serial0/0/1            unassigned      YES NVRAM  administratively down down
Vlan1                  unassigned      YES NVRAM  administratively down down
lab2#
```

Gambar 23 Hasil Konfigurasi VPN Router 2

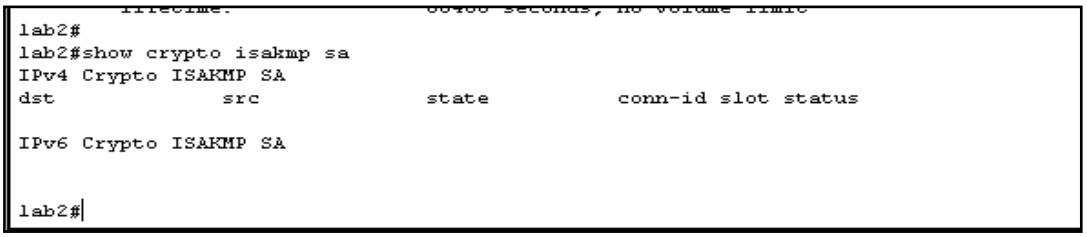
Berikut adalah tampilan hasil konfiguras vpn dengan setelah kita memasukan kode show ip int brief. Selanjut kita akan melihat hasil konfigurasi vpn dengan memasukan kode konfigurasi show crypto isakmp policy

```
Vlan1                  unassigned      YES NVRAM  administratively down down
lab2#
lab2#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:    AES - Advanced Encryption Standard (256 bit keys).
        hash algorithm:          Secure Hash Standard
        authentication method:   Pre-Shared Key
        Diffie-Hellman group:    #5 (1536 bit)
        lifetime:                86400 seconds, no volume limit
lab2#
```

Gambar 24 Hasil KonfigurasiVPN Router 2

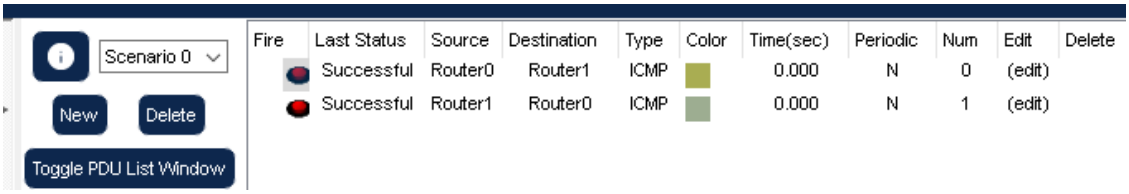
Berikut adalah hasil konfigurasi vpn dengan memasukan kode konfigurasi show crypto isakmp policy.selanjut kita akan melihat hasil vpn dengan memasukan kode show crypto isakmp sa



Gambar 25 Hasil Konfigurasi VPN pada Router 2

Berikut adalah hasil konfigurasi vpn pada router 2 dengan memasukan kode konfigurasi show crypto isakmp sa

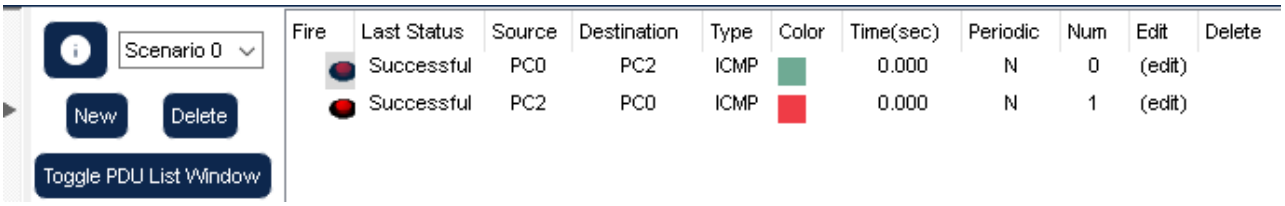
Selanjut kita akan mencoba mengirim pesan pada router 1 ke router dan sebalik nya



Gambar 26 Hasil Transfer pesan pada Router 1 ke Router 2

Berikut adalah hasil setelah kita mengirimkan pesan pada router 1 dan router 2

Selanjut kita akan mencoba mengirimkan pesan pada pc 1 yang ada pada router 2 ke pc 2 yang ada pada router 2 dan begitu juga sebalik nya .



Gambar 27 Hasil Transfer pesan pada PC 1 ke PC 2

Berikut adalah hasil setelah kita melalukan pengirimakan pesan pada pc 1 yang ada pada router 1 ke pc 2 yang ada pada router 2 dan sebalik nya .

KESIMPULAN

Ada pun kesimpulandari proses penelitian mengunakan protocol VPN yang dapat dari penelitian ini adalah:

1. Perancanganvpnmengunakan cisco packet tracer berhasilmencapaitujuanutamayaitumembangunjaringan virtual pribadi yang aman dan dapat menghubungkanbeberapalokasisecaraaktif. Dengan mengunakan protocol vpn yang sesuai ,seperti PPTP,L2TP dan IPsec, desain VPN yang di usulkan dapat memenuhikebutuhankomunikasi yang amanantarlokasi yang berbeda

2. Dengan mengunakanvpnmaka data yang di kirim ataupun di terima dalamkondisiaman dan sudah dienkripsi dengan baik dan akandikirimmelaluiisp. Sehinggapihak-pihak yang tidak berhak tidak dapat mengakses data tersebut.
3. Implementasi VPN ini memilikisignifikansidalamkontekskeamananinformasi dan privasi data. Dapat di gunakansebagaisolusi untuk mengamankankomunikasidalamlingkupperusahaanmaupunoraganisasi
4. Evaluasikinerjajaringan VPN menunjukanstabilitas dan kehandalandalammenstramisikan data secaraamanmelaluienkripsi

REFERENCES

[1] R. Mujiastuti and I. Prasetyo, "Membangun Sistem Keamanan Jaringan Berbasis VPN yang Terintegrasi dengan DNS Filtering PIHOLE," *J. Tek. Inform.*, no. November 2021, pp. 1–10, 2021, [Online]. Available: www.google.com

[2] D. Kus Heryadi and A. Surya Budiman, "Optimasi Keamanan Pada Jaringan Multi-Endpoint Access Menggunakan Network Access Control Berbasis Cisco ISE," *JIKA (Jurnal Inform. Univ. Muhammadiyah Tangerang* , pp. 313–324, 2021.

[3] I. C. R. Drajana and A. Bode, "Simulasi Jaringan Menggunakan Cisco Packet Tracer," *Simtek J. Sist. Inf. dan Tek. Komput.*, vol. 6, no. 1, pp. 24–27, 2021, doi: 10.51876/simtek.v6i1.91.

[4] L. D. Samsumar and M. Subli, "Penggunaan Aplikasi Simulasi Jaringan Cisco Packet Tracer Dalam Design Network," *Explore*, vol. 9, no. 1, p. 24, 2019, doi: 10.35200/explore.v9i1.23.

[5] M. N. Afdhol. P. Y., A. Anggraini Samudra, and R. Trisetyowati Untari, "Perancangan Jaringan Komputer Menggunakan Metode Failover," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 7, no. 3, pp. 1474–1481, 2023, doi: 10.36040/jati.v7i3.7313.

[6] Randy Ikhsan Ramadhan and Siti Madinah Ladjamuddin, "Perancangan Sistem Web Filtering Dengan Metode Dns Forwarding Pada Jaringan Komputer Berbasis Mikrotik Routeros," *J. Inform. Dan Tekonologi Komput.*, vol. 2, no. 2, pp. 146–157, 2022, doi: 10.55606/jitek.v2i2.231.

[7] O. D. Putra, D. Destiarini, A. Rahman, A. Azhari, and S. Safaruddin, "Penggunaan Virtual Private Network (Vpn) Pada Pt Semen Baturaja (Persero) Tbk.," *Intech*, vol. 3, no. 1, pp. 17–21, 2022, doi: 10.54895/intech.v3i1.1267.

[8] B. W. Aulia, M. Rizki, P. Prindiyana, and surgana, "Peran Krusial Jaringan Komputer dan Basis Data dalam Era Digital," *JUSTINFO (Jurnal Sist. Inf. dan Teknol. Informasi)*, vol. 1, no. 1, pp. 9–20, 2023, doi: 10.33197/justinfo.vol1.iss1.2023.1253.

[9] A. Y. P. Adena Susita, Heri Mulyono, "PENGARUH PENGGUNAAN SIMULASI JARINGAN KOMPUTER CISCO PACKETTRACER TERHADAP KREATIVITAS BELAJAR SISWA DI SMK N 1 LEMBAH MELINTANG," *Semin. Nas. Jambore Konseling 3*, vol. 00, no. 00, pp. XX–XX, 2022, doi: 10.1007/XXXXXX-XX-0000-00.