

# Implementasi vpn berbasis ipsec menggunakan fortigate pada rumah sakit atma jaya

Nurul Arifin<sup>1</sup>; Jordy Lasmana Putra<sup>2</sup>

<sup>1</sup>*Fakultas Teknologi Informasi, Universitas Nusa Mandiri, Jl. Raya Jatiwaringin, Cipinang melayu, Makasar, Jakarta Timur*

<sup>2</sup>*Fakultas Teknologi Informasi, Universitas Nusa Mandiri, Jl. Raya Jatiwaringin, Cipinang melayu, Makasar, Jakarta Timur*

<sup>1</sup> [nurfin.kamura@gmail.com](mailto:nurfin.kamura@gmail.com), <sup>2</sup> [jordy.jlp@nusamandiri.ac.id](mailto:jordy.jlp@nusamandiri.ac.id),

Kata kunci:  
SIMRS, Computer Network, VPN, IPSec, Fortigate.

## Abstract

As a hospital that implements the SIMRS system and technology (Hospital Management Information System) that supports hospital management so as to create optimal service. For this reason, all support will certainly require a secure information and communication technology and has become a major requirement, including in terms of processing information and exchanging information. Atma Jaya Hospital already has computer network technology that supports employees' needs for data access through computer networks. However, the computer network technology currently owned cannot be utilized optimally by the hospital, so that the safety of accessing data from outside the hospital is not guaranteed by both doctors and employees. The current condition is that access to data from outside the hospital uses third-party applications, whose history cannot be known and is not deactivated. By maximizing the existing Fortigate in the hospital network infrastructure, we implemented a VPN with the IPSec method to access hospital data for doctors and employees, so that it can be more calm and guaranteed security from both the hospital and doctor or employee sides.

## Pendahuluan

### A. Latar Belakang

Kehidupan masyarakat banyak berubah karena kemajuan teknologi yang semakin mudah diakses, terutama dalam bidang teknologi informasi, komunikasi dan *transfer data*. Dengan adanya jaringan komputer dapat menghubungkan satu komputer beserta perangkat pendukung lainnya, yang dapat memudahkan *user* untuk terhubung satu sama lain[1].

Rumah Sakit sebagai sarana pelayanan medis turut serta terpengaruh dengan kemajuan perkembangan teknologi saat ini. Sebagai pusat lembaga kesehatan Rumah Sakit memiliki peran penting untuk masyarakat, sehingga Rumah Sakit harus mampu memberikan pelayanan yang mudah, cepat, dan nyaman[2]. Sistem layanan berbasis informasi dan jaringan bisa memudahkan untuk kordinasi pelayanan[3]. Dalam menunjang pelayanannya yang dituntut untuk cepat, semua urusan Rumah Sakit mulai dari pendaftaran, pembayaran hingga pemulangan pasien menggunakan Sistem Manajemen Rumah Sakit (SIMRS) yang membutuhkan jaringan lokal dan internet[4].

Keuntungan dari penggunaan teknologi komputerisasi adalah pengguna dapat saling mengakses dokumen atau perangkat lunak yang terhubung ke jaringan yang sama melalui jaringan lokal atau internet[5]. Dengan adanya teknologi tersebut sangat membantu para dokter ataupun karyawan yang dituntut untuk memberikan pelayanan cepat dalam melayani administrasi atau pengecekan rekam medis pasien pada SIMRS.

Pada saat ini untuk menunjang pelayanan cepat di RS Atma Jaya beberapa dokter dan karyawan yang kebetulan tidak berada di lingkungan Rumah Sakit untuk dapat

mengakses SIMRS rumah sakit atau sharing folder menggunakan aplikasi remote pihak ketiga, seperti Teamviewer dan Anydesk. Dibalik kemudahan yang ditawarkan aplikasi tersebut ada beberapa kekurangan yang ditemui dilapangan, seperti *user* diharuskan menghidupkan komputernya yang ada di rumah sakit dengan bantuan dari *cleaning service* yang sedang berdinis. Kemudian dari sisi keamanan jaringan sangatlah kurang karena setiap orang bisa mengakses komputer hanya dengan mengetahui *user id* dan *password* pada komputer tersebut[6].

Salah satu solusi untuk menangani hal tersebut adalah dengan menggunakan teknologi *remote acces VPN (Virtual Private Network)* sayangnya RS Atma Jaya belum menerapkan *remote acces VPN* dalam jaringan komputernya. *Virtual Private Network (VPN)* merupakan sistem keamanan jaringan yang dapat membuat dua jaringan yang lokasinya berbeda bisa saling terhubung dan seakan-akan berada didalam jaringan yang sama[7].

Dalam penerapan *remote acces VPN* metode kemananan yang digunakan dalam desain VPN ini adalah *Internet Protocol Security (IPSec)*. *IPSec* adalah tunneling VPN yang beroperasi pada lapis jaringan ke-3, sehingga dapat mengamankan data pada lapisan yang berada diatasnya[8]. Paket IP (*IP Package*) sendiri tidak memiliki keamanan yang membuat isi dan alamat paket mudah diketahui, oleh sebab itu *IPSec* bertugas menjaga keamanan *IP Package* ketika paket ditransmisikan[9].

RS Atma Jaya sendiri sebenarnya sudah memiliki perangkat kemananan jaringan yaitu Fortigate, akan tetapi belum dimaksimalkan secara baik karena faktor tenaga ahli yang belum menguasai Fortigate. Fortigate adalah perangkat keamanan jaringan sekaligus dapat berfungsi sebagai *gateway* dan router[10]. Fortigate yang digunakan saat ini merupakan *Firewall* dari Perusahaan Fortinet[11]. Metode VPN berbasis *IPSec* menggunakan Fortigate, yang dapat mengatasi masalah keamanan jaringan di RS Atma Jaya sebab Fortigate dapat mendeteksi dan mengeliminir secara *real time* ancaman yang terintegrasi, tanpa menurunkan kinerja jaringan[12].

## METODE PENELITIAN

Mendiskusikan metode yang digunakan dalam pengumpulan dan analisis data.Observasi.

### A. Metode Pengumpulan Data

- 1) Observasi  
Yaitu pengumpulan data yang diperoleh dengan cara melakukan Riset serta analisa problem di RS Atma Jaya.
- 2) Wawancara  
Penulis melaksanakan wawancara dengan tim IT di RS Atma Jaya saat melakukan riset secara langsung untuk memperoleh informasi yang jelas.
- 3) Studi Kepustakaan  
Untuk mengetahui masalah secara mendalam yang berkaitan dengan Skripsi ini, oleh sebab itu penulis juga melakukan studi kepustakaan salah satunya dengan mengumpulkan data-data teoritis dan mempelajari dan memahami buku - buku atau literature yang bertujuan untuk mendapatkan teori - teori dan bahan - bahan yang berkaitan dengan masalah tersebut.

### B. Analisa Penelitian

Analisis penelitian ini dilakukan sebagai alat proses pengambilan keputusan, analisis penelitian ini sangat membantu dalam mengurangi ketidakpastian dengan memberikan informasi yang akurat untuk meningkatkan proses pengambilan keputusan. Metode penelitian yang penulis buat antara lain :

- Analisa Kebutuhan  
Disini penulis sangat memerlukan akses ke perangkat Fortigate untuk menganalisa konfigurasi awal sebelum menggunakan VPN berbasis IPSec dan kita Analisa kemampuan fitur yang ada di Fortigate RS Atma Jaya, kemudian untuk jaringan penulis menggunakan jaringan yang sudah berjalan di RS Atma Jaya.
- Desain  
Penulis menggunakan desain jaringan yang saat ini sudah berjalan di RS Atma Jaya.
- Testing

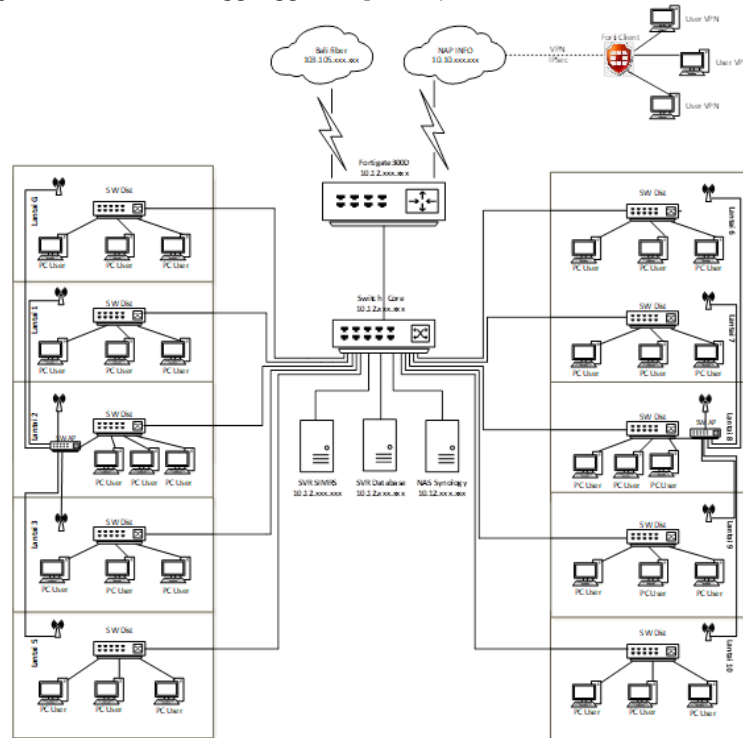
Penulis melakukan testing dengan cara menginstal aplikasi Forticlient di Laptop user yang memiliki kebutuhan untuk akses data dari luar rumah sakit, memastikan VPN berbasis IPsec yang kita implementasikan tersambung dan termonitor dengan baik di Fortigate.

- Implementasi  
Setelah melakukan testing berkali-kali sampai konfigurasi di Fortigate sesuai dengan kebutuhan User, penulis baru bisa melakukan implementasi ke semua user yang membutuhkan VPN, agar pada saat sudah dijalankan tidak berkendala

## HASIL dan DISKUSI

### A. Skema Jaringan

Pada skema jaringan usulan penulis menambahkan sebuah konfigurasi VPN dengan metode *IPSec*, yang berfungsi sebagai jalur akses user user yang aman dari rumah ke jaringan rumah sakit. *Tuneling* yang di bangun melalui ISP secondary yaitu NAP Info, sehingga jalur VPN tidak mengganggu ISP *primary* rumah sakit



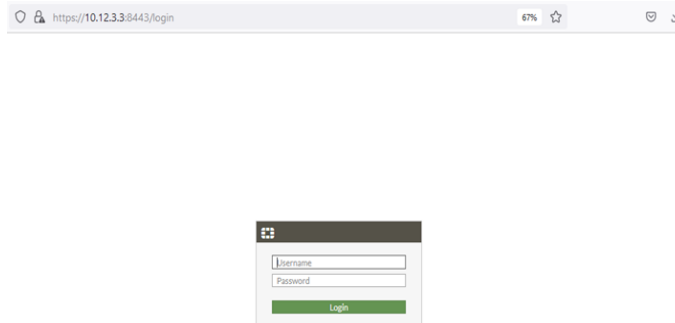
Gambar 1. Skema Jaringan

### B. Perancangan Jaringan

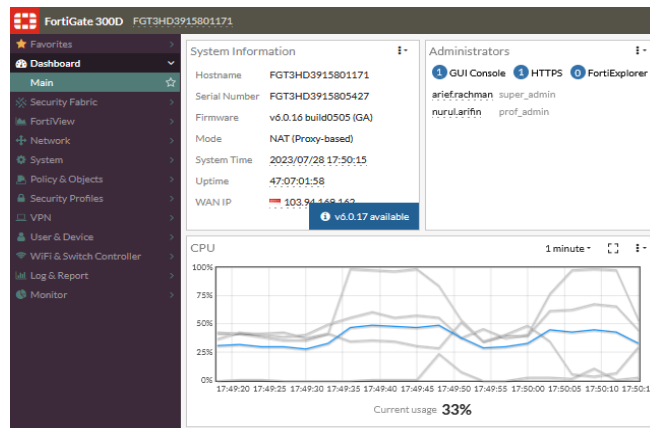
Dalam rancangan VPN dengan metode *IPSec* penulis tidak menggunakan simulator, akan tetapi penulis mendapat kesempatan langsung untuk mengimplementasikan di Fortigate pada rumah sakit. Untuk hasil implementasi VPN dengan metode *IPSec* sudah diserahkan terimakan kepada rumah sakit, sehingga implementasi VPN dengan metode *IPSec* bisa langsung bisa dimanfaatkan oleh RS. Atma Jaya.

Ada beberapa tahapan proses konfigurasi VPN *IPSec* di Fortigate adalah sebagai berikut :

- Akses dan login di Fortigate langkah pertama kita panggil IP Fortigate via browser, akan tampil seperti Gambar dibawah ini :

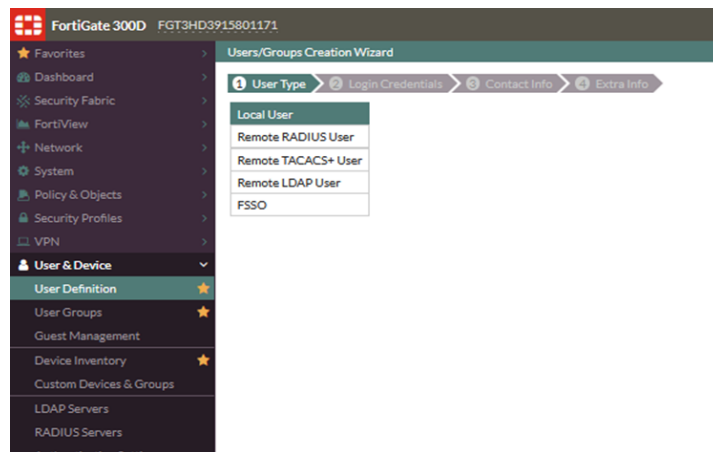


**Gambar 2.** Halaman Login



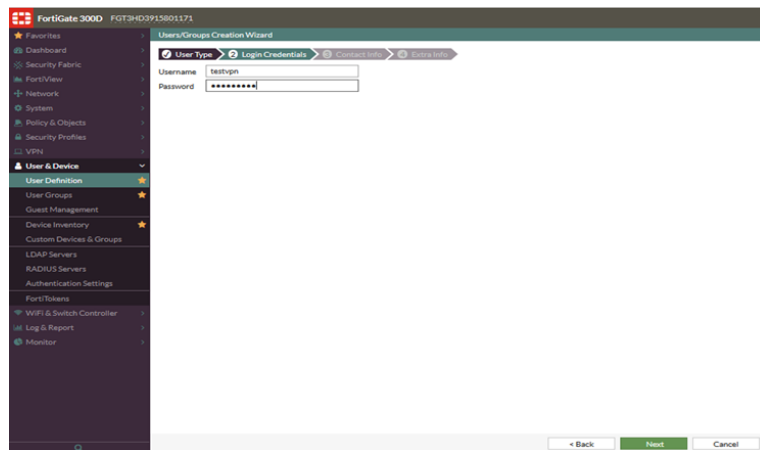
**Gambar 3.** Dashboard Fortigate

- Pembuatan User VPN dan Grup VPN sebelum membuat konfigurasi VPN adalah mempersiapkan user dan grup usernya terlebih dahulu karena diperlukan untuk login pada Forticlient jika ada kebutuhan akses ke jaringan rumah sakit. masuk ke *menu User Definition* pilih *Local User* lalu *next* seperti Pada Gambar dibawah ini :



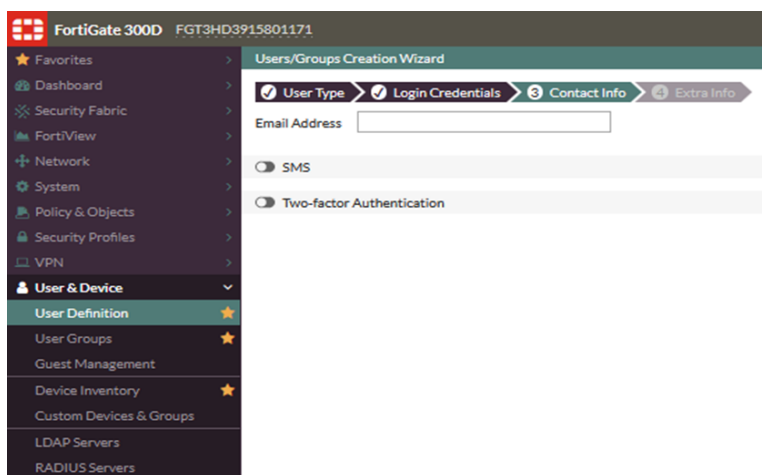
**Gambar 4.** Tampilan *User Definition*

Selanjutnya akan muncul tampilan seperti pada Gambar 5. Untuk dikolom *username* bisa kita isi nama testvpn dengan *password* 12345678910 lalu klik *next*.



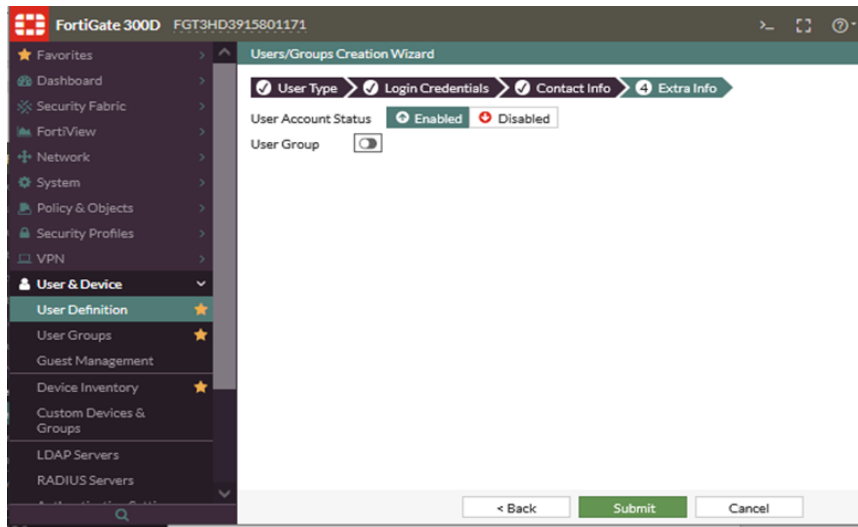
**Gambar 5.** Tampilan *Login Credentials*

Selanjutnya akan muncul tampilan seperti pada Gambar 6. *menu Contact Info* di sini kita bisa *skip* saja, lalu klik *next*.



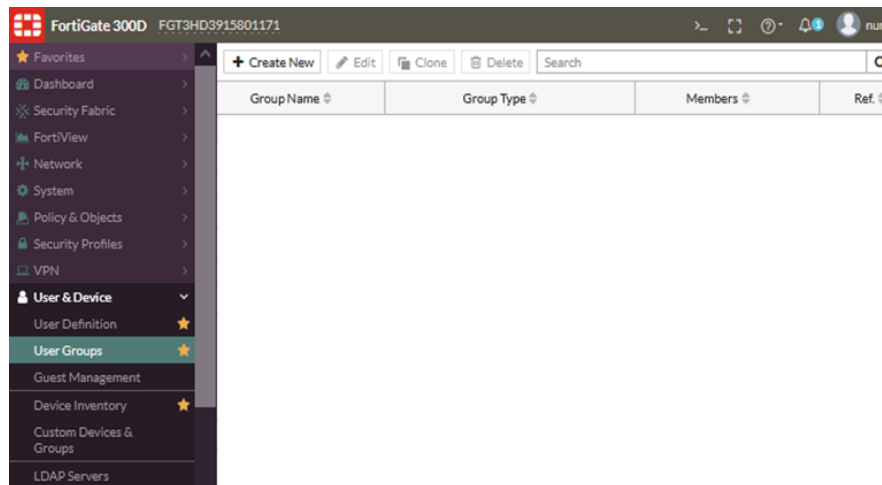
**Gambar 6.** Tampilan *Contact Info*

Selanjutnya akan muncul tampilan seperti pada Gambar IV.8 dimana akan muncul menu Extra Info lalu kita bisa klik *Submit*, maka sudah selsesai proses pembuatan *user* untuk *login* di VPN kita nanti.



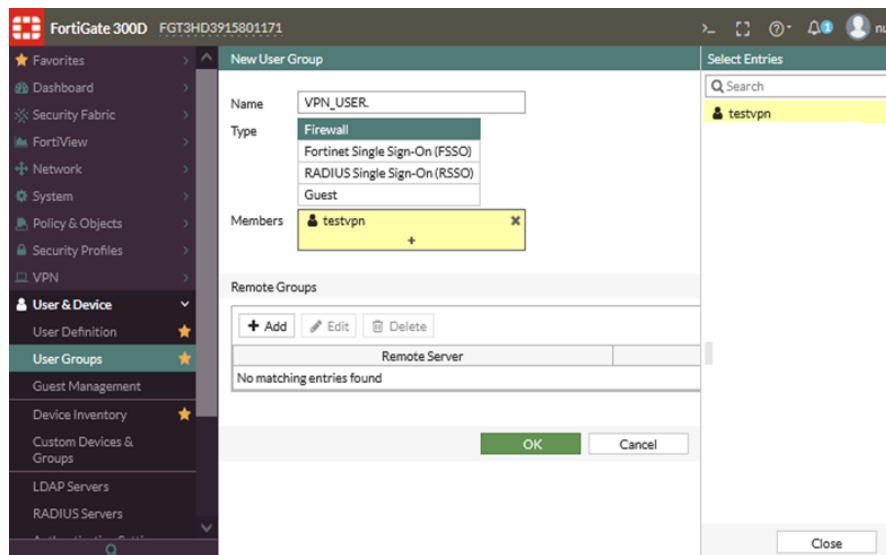
**Gambar 7.** Tampilan *Extra Info*

Selanjutnya kita mesti buat grup *user* VPN, grup *user* difungsikan untuk membatasi akses *user* hanya sebatas *policy* grup VPN saja. Untuk langkahnya kita pilih menu *User Group* lalu akan muncul tampilan seperti pada Gambar 8. disana kita pilih *Create New*.



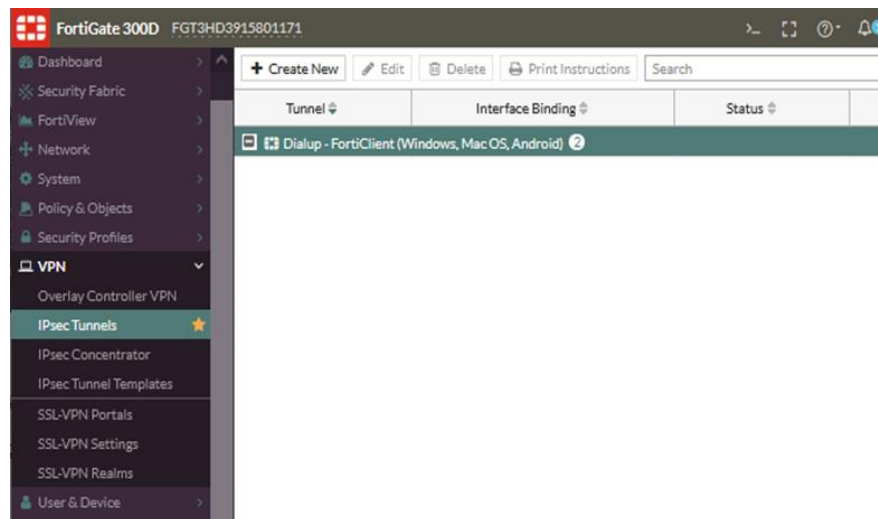
**Gambar 8.** Tampilan *User Groups*

Setelah kita pilih *Create New* akan muncul tampilan pada Gambar 9. Dimana penulis bisa buat nama grup VPN. Untuk kolom nama penulis mengisi dengan *VPN\_USER*, kolom *Type* pilih *Firewall*, lalu di kolom *members* kita klik tanda plus nanti akan muncul nama user yang kita buat sebelumnya disebelah kanan, pilih user nya dari sebelah kanan akan masuk ke kolom *members*, lalu klik ok. Sampai disini untuk grup VPN sudah terbentuk termasuk dengan membernya, yaitu user yang kita buat sebelumnya.



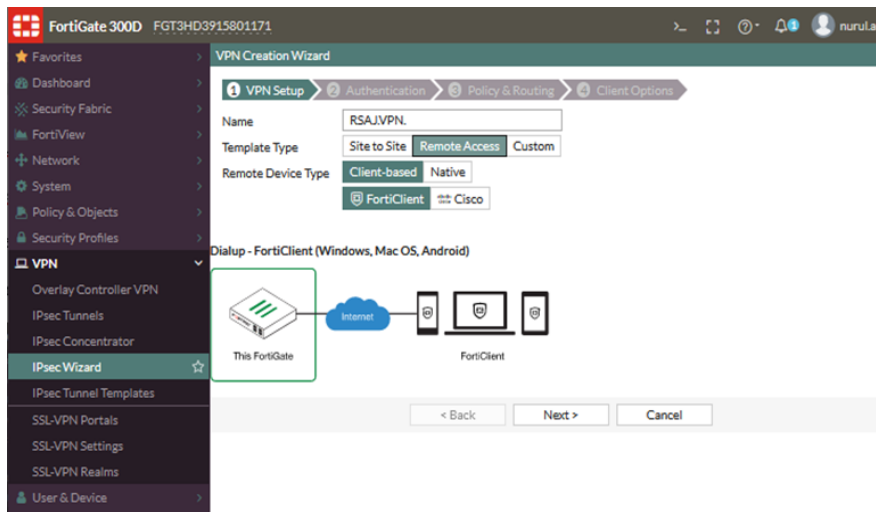
**Gambar 9.** Tampilan Menu Create New pada User Group

- Pembuatan Koneksi VPN  
Untuk membuat konfigurasi VPN kita bisa masuk ke menu VPN lalu pilih IPsec Tunnels seperti pada Gambar 10. lalu pilih Create New.



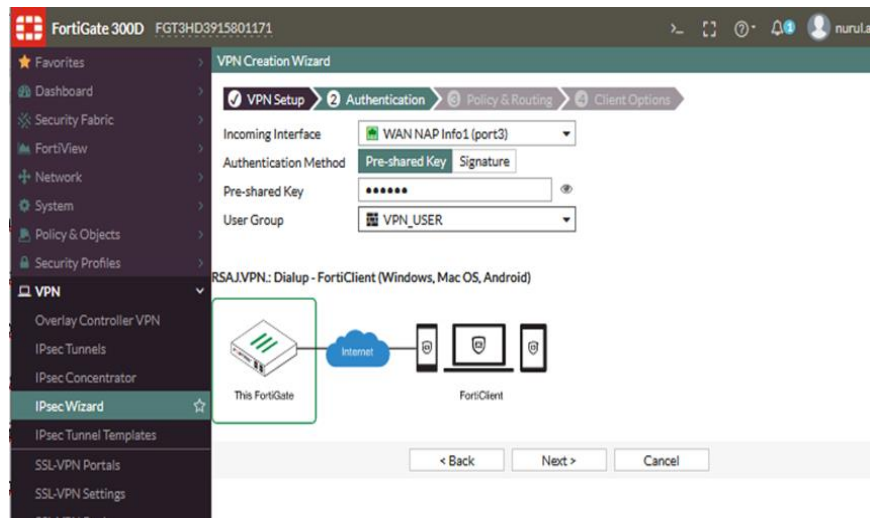
**Gambar 10.** Tampilan Menu IPsec Tunnels

Setelah kita pilih *Create New* akan muncul tampilan seperti Gambar IV.12 penulis memberi nama RSAJ.VPN untuk *template type* bisa bilih *Remote Acces*, untuk *Remote Device Type* penulis memilih Fortigate, lalu *Next*.



**Gambar 11.** Tampilan Menu Setup VPN

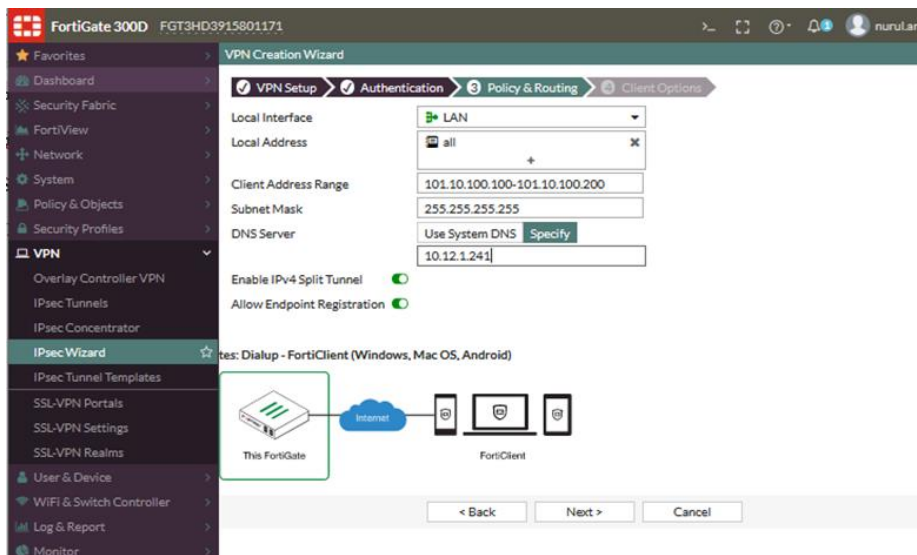
Selanjutnya setelah *next* kita masuk pada tampilan Authentication seperti pada gambar 12. penulis memilih *Incoming Interface* ke jalur ISP NAP Info, selanjutnya untuk *Authentication Method* pilih *Pre-Shared Key* kemudian isi *passwordnya*, setelah itu di kolom *User Group* Kita pilih *User Group* yang sebelumnya kita buat *VPN\_USER*, lalu *Next*.



**Gambar 12.** Tampilan Menu Authentication

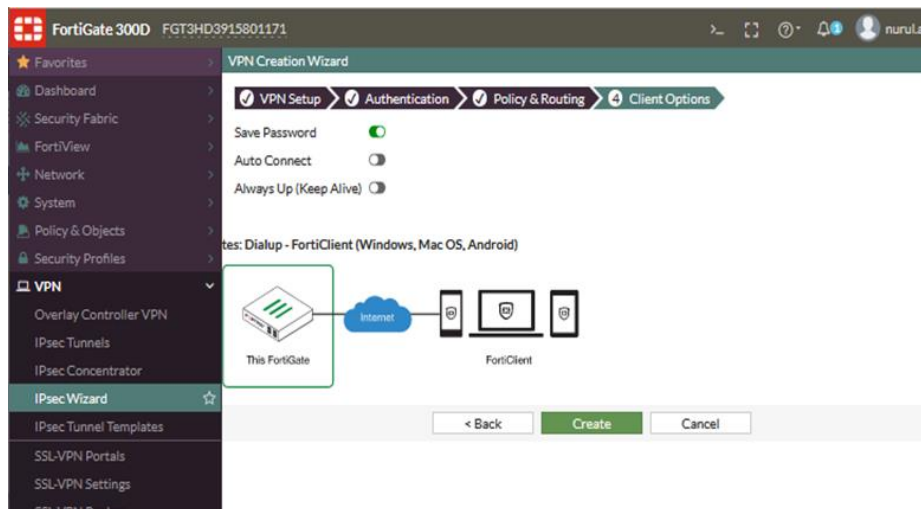
Kemudian setelah *Next* masuk ke *menu Policy dan Routing* seperti pada Gambar 13. untuk *local interface* penulis pilih jalur LAN (*Destinasion Interface*), kemudian *Local Address* pilih *ALL* (*Address* yang sudah ada sebelumnya untuk kesemua jalur), lalu di kolom *Client Address Range* penulis mengisi 101.10.100.100-101.10.100.200 ( IP ini yang nantinya akan didapatkan oleh user yang sudah berhasil tersambung dengan jaringan VPN), kolom Subnetmask penulis isi 255.255.255.255, selanjutnya untuk *DNS Server* penulis memilih *Specify* menggunakan *DNS existing* rumah sakit 10.12.1.241 (*Use System DNS* dapat DNS dari Fortigate) kemudian *Next*.



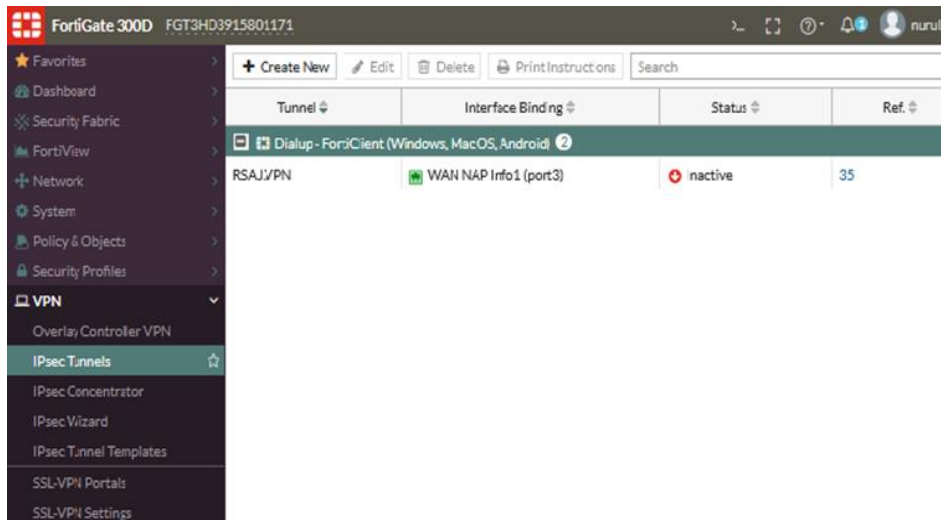


**Gambar 13.** Tampilan Menu Policy & routing

Setelah *Next* akan muncul tampilan *Client Option* seperti pada Gambar 14. disini penulis pilih *default* dan klik *Create*. Sampai disini untuk Pembuatan VPN IPsec untuk *Remote Acces* sudah selesai bisa di cek pada menu VPN pilih *IPsec Tunnels* serperti pada Gambar 15.

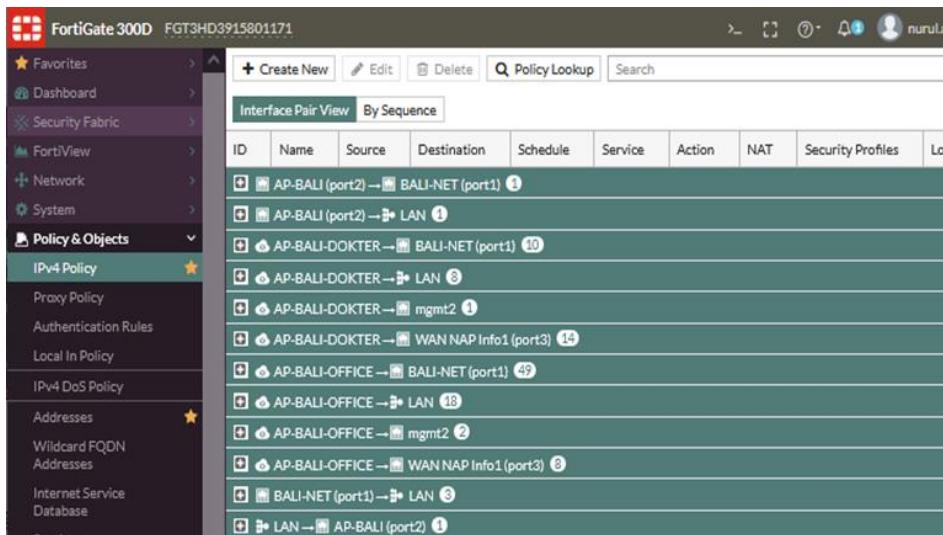


**Gambar 14.** Tampilan *Client Option*



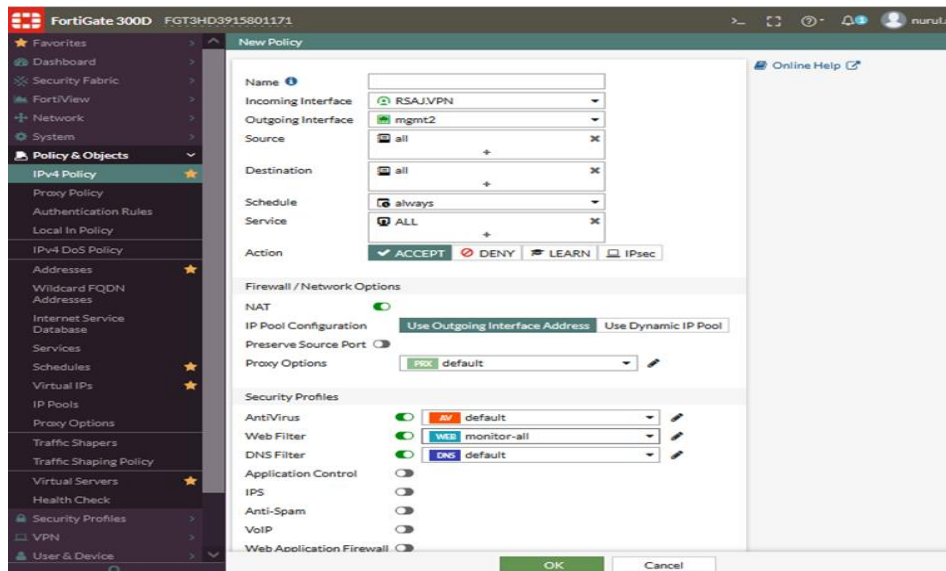
Gambar 15. Tampilan IPsec Tunnels

- Membuat *Policy Local* dan Internet Untuk VPN  
Langkah selanjutnya adalah membuat policy untuk VPN yang sudah kita buat, supaya akses VPN yang masuk dapat policy bisa akses ke jaringan mana saja. Langkahnya adalah masuk ke menu IPv4 Policy maka akan muncul tampilan seperti pada Gambar 16. lalu kita pilih Create New.



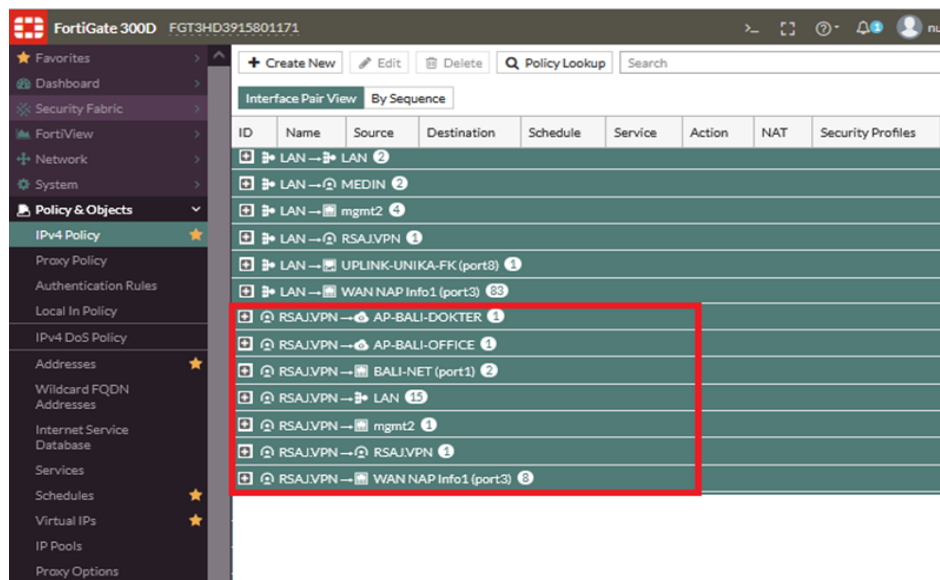
Gambar 16. Tampilan Menu IPv4 Policy

Selanjutnya akan muncul tampilan setelah kita *Create new* Seperti Pada Gambar 17. untuk nama *Policy* yang kita buat di dalamnya nanti, kemudian *incoming Interface* pilih *Profile* VPN yang sebelumnya kita buat penulis memasukkan *Profile* RSAJ.VPN, untuk *Outgoing Interfacenya* penulis pilih ke *mgmt2* yaitu jalur ke *server storage* (sebelumnya kita sudah buat ke LAN di saat buat VPN di Langkah sebelumnya), kemudian *source* kita pilih *all* (bisa juga untuk spesifik user), lalu di kolom *destination* penulis mengisi *all* (bisa juga untuk spesifik ), selanjutnya untuk kolom *Schedule* penulis pilih *always*, kemudian di kolom *service* penulis *all* (bisa pili spesifik seperti *http*, *RDP*, dll), lalu *Security* Profilnya penulis untuk *AntiVirus* diaktifkan pilih *default*, kemudian *WebFilter* diaktifkan pilih *default* (membatasi akses internet sesuai rule yang berlaku), untuk *DNS Filter* penulis aktifkan dan pilih *default* (membatasi *website* tertentu dari DNS), untuk selanjut pilih *default* dan klik OK. Maka *Policy* untuk jalur VPN kita kearah *mgmt2* (jalur NAS server) sudah selesai dibuat.



Gambar 17. Tampilan Menu IPv4 Policy

Kita bisa lihat *policy* yang sudah kita buat sebelumnya seperti pada Gambar 18 kita juga bisa menambahkan VPN kita bisa akses kemana saja dengan cara seperti sebelumnya.



Gambar 18. Tampilan Policy Yang Dibuat Pada Menu IPv4 Policy

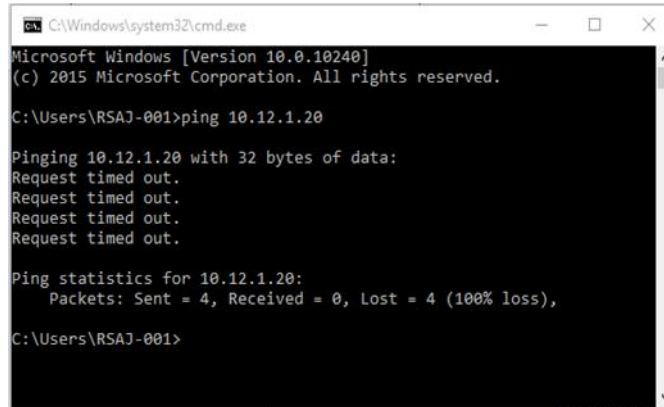
### C. Pengujian Jaringan

Dalam hal membangun jaringan komputer perlu dilakukan sebuah pengujian terhadap jaringan yang telah dibangun sebelumnya, hal ini berguna untuk memastikan bahwa semua sistem yang telah dibuat berjalan dengan baik dan sesuai dengan yang direncanakan. Pengujian disini menggunakan *device* dari *user* yang sudah terdaftar sebagai user VPN, dan *device* yang digunakan sudah ada aplikasi Forticlient, setelah koneksi dari Forticlient tersambung bisa menggunakan *command prompt* untuk *test ping ke SIMRS* atau server NAS.

### D. Pengujian Jaringan Awal

Pada sub bab ini akan dilakukan beberapa pengujian awal diantaranya penulis mengisntal aplikasi Forticlient pada *device* yang akan mencoba koneksi VPN ke rumah sakit menggunakan *user* VPN yang sebelumnya kita buat. Langkah awalnya kita lakukan uji koneksi dengan *Ping* ke SIMRS dan server NAS, seperti pada Gambar 19. dan Gambar 20. Kemudian dilanjutkan membuka aplikasi Forticlient seperti pada Gambar 21. dan

sebelumnya kita diminta untuk *Configure* VPN.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

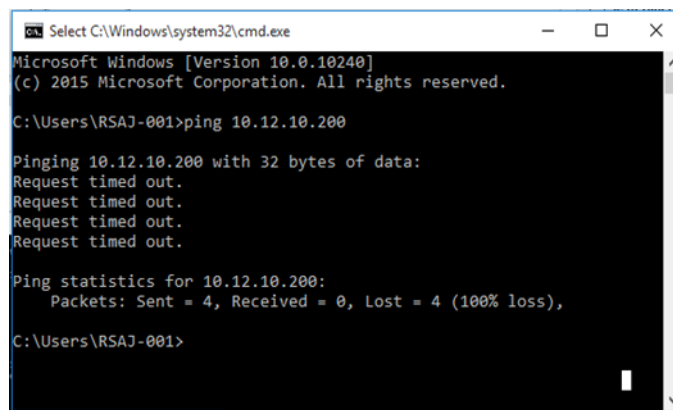
C:\Users\RSAJ-001>ping 10.12.1.20

Pinging 10.12.1.20 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.12.1.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\RSAJ-001>
```

**Gambar 19.** Test Ping ke Server SIMRS



```
Select C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\RSAJ-001>ping 10.12.10.200

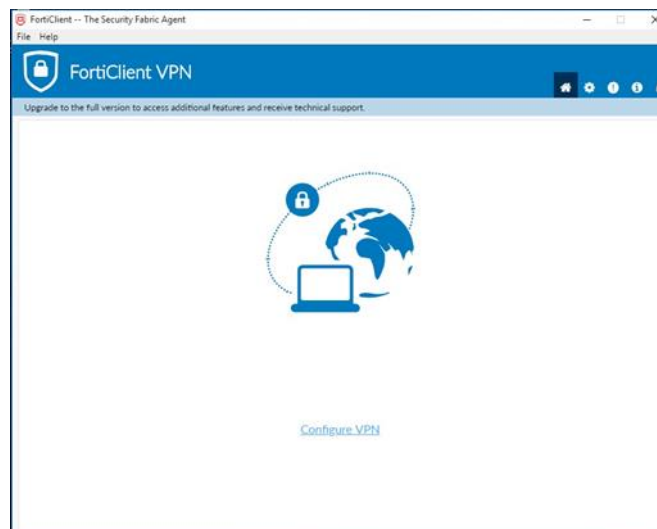
Pinging 10.12.10.200 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.12.10.200:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\RSAJ-001>
```

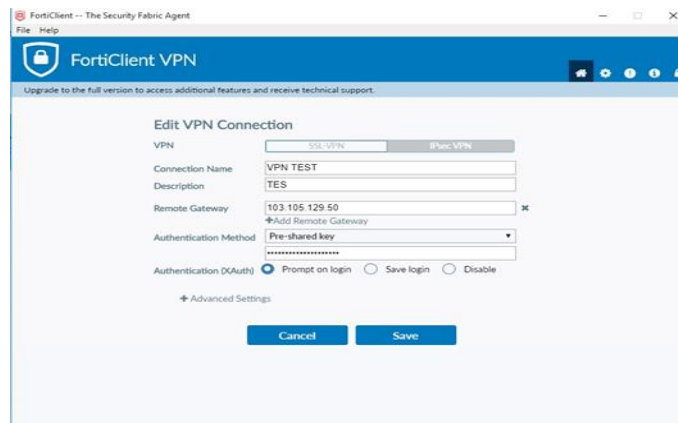
**Gambar 20.** Test Ping ke Server NAS

Dari hasil tes ping ke *server* SIMRS dan *server* NAS menunjukkan *time out* dimana belum ada nya koneksi yang terhubung ke server tersebut.



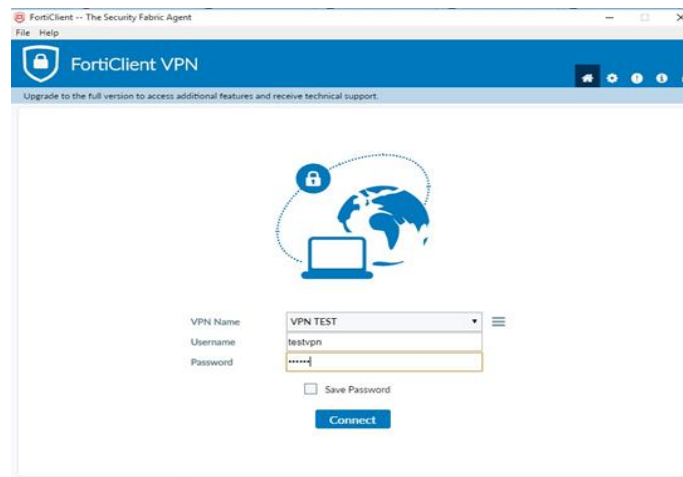
**Gambar 21.** Aplikasi Forticlient Ver. 6.2.6

Selanjutnya kita masuk ke menu *Configure* VPN kita pilih *IPsec* VPN kemudian *Connection Name* diisi *VPN TEST*, kolom *Description* penulis isi TES, untuk *Remote Gateway* penulis masukan IP public Fortigate yaitu 103.105.129.50, untuk *Presharedkey* penulis masukan *Preshared key* yang sebelumnya dibuat di Fortigate yaitu 4tmavpnIT, lalu pilih *Save*.



**Gambar 22.** Tampilan *Configure Forticlient*

Selanjutnya diminta untuk *login* seperti pada Gambar 22. untuk *user name* penulis menggunakan *user* yang sebelumnya dibuat yaitu *testvpn* dan *password* 123456, lalu Ok.



**Gambar 23.** Halaman *Login Forticlient*

Jika koneksi sudah berhasil akan tampil seperti pada Gambar IV.29, Kita bisa lihat *Ip Address* yang kita dapat, sesuai dengan *IP Address* range yang kita buat di Fortigate, *username* testvpn dan durasi koneksi juga dapat di lihat pada tampilan Forticlient. Selanjutnya dimana bisa dilihat kita telah keterangan *VPN Connected* menandakan kita berhasil terhubung ke jaringan rumah sakit.



**Gambar 23.** Halaman *Login* Forticlient

**E. Pengujian Jaringan Akhir**

Pada sub bab ini akan dilakukan beberapa pengujian akhir diantaranya mencoba ping ke server SIMRS dan server NAS seperti pada Gambar 24 dan Gambar 25.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\RSAJ-001>ping 10.12.1.20

Pinging 10.12.1.20 with 32 bytes of data:
Reply from 10.12.1.20: bytes=32 time=5ms TTL=126
Reply from 10.12.1.20: bytes=32 time=2ms TTL=126
Reply from 10.12.1.20: bytes=32 time=4ms TTL=126
Reply from 10.12.1.20: bytes=32 time=1ms TTL=126

Ping statistics for 10.12.1.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 3ms

C:\Users\RSAJ-001>
```

**Gambar 24.** Tes Ping ke Server SIMRS

```
Select C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\RSAJ-001>ping 10.12.10.200

Pinging 10.12.10.200 with 32 bytes of data:
Reply from 10.12.10.200: bytes=32 time=3ms TTL=62
Reply from 10.12.10.200: bytes=32 time=3ms TTL=62
Reply from 10.12.10.200: bytes=32 time=5ms TTL=62
Reply from 10.12.10.200: bytes=32 time=3ms TTL=62

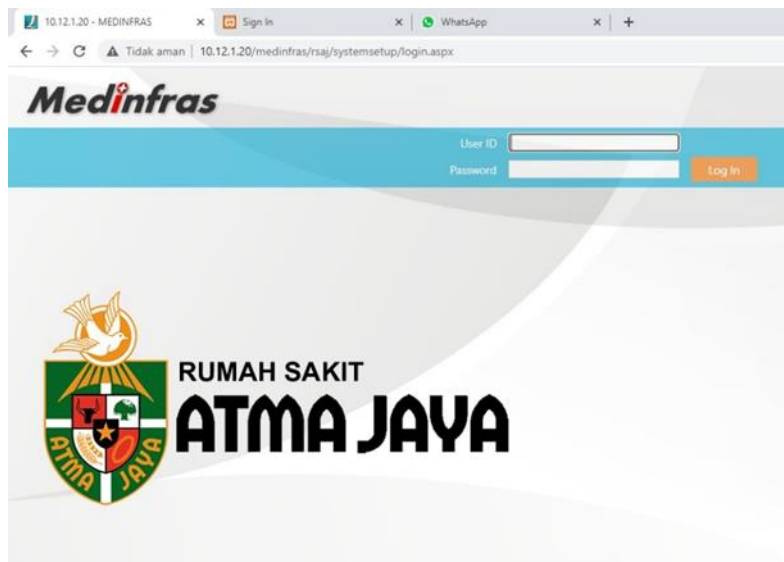
Ping statistics for 10.12.10.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 5ms, Average = 3ms

C:\Users\RSAJ-001>
```

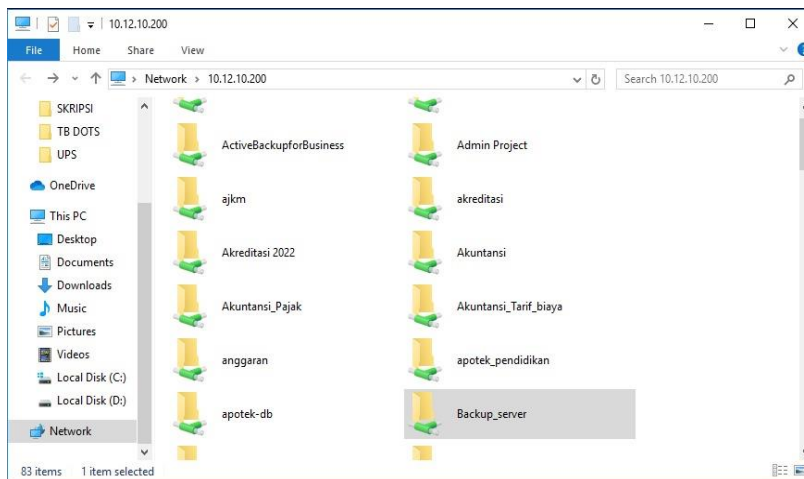
**Gambar 25.** Tes Ping ke Server NAS

Selanjutnya penulis mencoba akses SIMRS dari *browser* seperti pada Gambar 26, dan berhasil akses SIMRS dari *device* yang sudah terkoneksi VPN. Dan penulis mencoba akses *folder sharing* rumah sakit dan berhasil masuk ke *folder sharing* seperti pada Gambar 27.



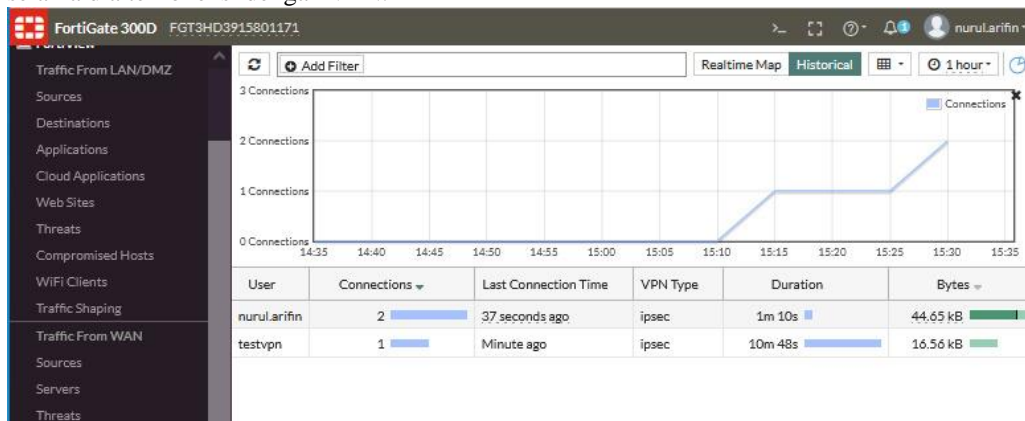


Gambar 26. Tes Ping ke Server NAS

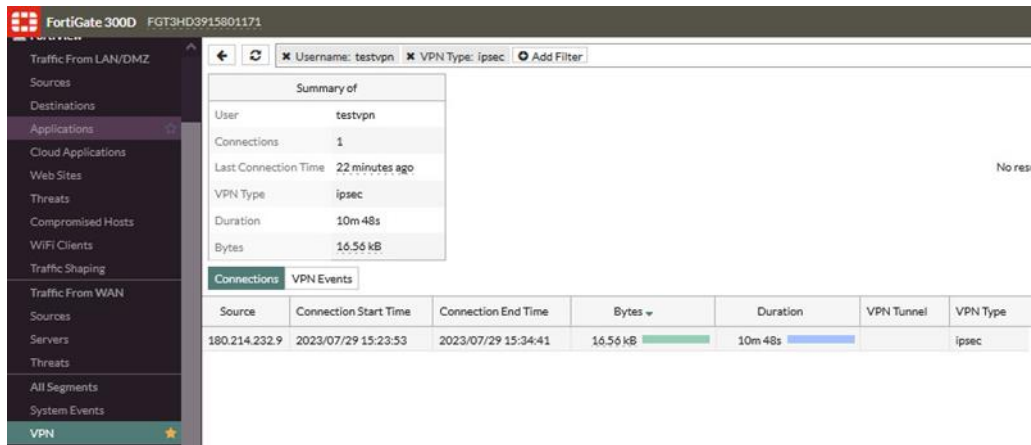


Gambar 27. Tes Ping ke Server NAS

Selanjutnya penulis mengecek dari Fortigate di menu Fortiview dimana di dalam menu ini kita bisa monitoring *user* yang sedang tersambung dengan VPN rumah sakit seperti pada Gambar 28, Gambar 29 dan Gambar 30. Dengan Fortiview sangat membantu untuk *memonitoring real time user VPN* siapa saja yang masuk ke jaringan rumah sakit, seperti *user* yang penulis buat (*testvpn*) bisa dilihat akses kemana saja, trafik *bandwith* dan durasi selama dia terkoneksi dengan VPN.



Gambar 27. Tes Ping ke Server NAS



Gambar 28. Tes Ping ke Server NAS

### Kesimpulan

Berdasarkan implementasi VPN *IPSec* yang telah dilakukan, maka dapat diambil kesimpulan sebagai berikut:

- 1) Pada jaringan sebelumnya tidak ada keamanan jaringan dalam pertukaran data, setelah dilakukan penerapan VPN *IPSec* menjadi lebih aman dan terkontrol, karena tidak lagi menggunakan aplikasi remote pihak ketiga.
- 2) Sebelumnya user dan dokter mengalami kesulitan akses SIMRS dan data pasien saat mereka sedang tidak berada di rumah sakit sekarang sudah tidak lagi, karena tidak perlu meminta bantuan rekan kerja yang berada di rumah sakit untuk memastikan komputer yang mau di remote harus aktif.
- 3) Tim IT bisa mengetahui siapa saja user yang membutuhkan akses VPN dan dapat mengontrolnya saat user tersebut sudah resign, sekaligus dapat memantau user yang menggunakan akses VPN pada Fortigate.

### Ucapan terima kasih

Penulis mengucapkan terima kasih kepada tim IT RS Atma Jaya dan pihak-pihak yang telah memberi dukungan terhadap penelitian ini.

### Referensi

- [1] M. G. A. Ars, S. Samsugi, and M. Paradisiaca, "PELATIHAN JARINGAN KOMPUTER ( MICROTIK ) UNTUK MENAMBAH KEAHLIAN BAGI SISWA SMAN 8 BANDAR LAMPUNG," *Univ. Teknokr. Indones.*, vol. 3, no. 2, pp. 209–212, 2022, doi: doi.org/10.33365/jsstcs.v3i2.2105.
- [2] F. C. Hanoum, F. G. Kosasih, and R. T. H. Safariningsih, "Penerapan Total Quality Management (TQM) dalam Meningkatkan Kualitas Pelayanan Rumah Sakit," *Reslaj Relig. Educ. Soc. Laa Roiba J.*, vol. 4, no. 3, pp. 804–815, 2022, doi: 10.47467/reslaj.v4i3.950.
- [3] M. I. Triwahyudi and I. Veritawati, "Sistem Informasi Pelayanan Jaringan Komputer," *Format J. Ilm. Tek. Inform.*, vol. 11, no. 1, p. 55, 2022, doi: 10.22441/10.22441/format.2022.v11.i1.006.



- [4] D. Sitompul, Hamonangan, Ryan, O. J. Harmaja, and E. Indra, "Perancangan Pengembangan Desain Arsitektur Jaringan Menggunakan Metode Ppdioo," *Jusikom Prima*, vol. 4, no. 2, pp. 1–5, 2021, [Online]. Available: <http://jurnal.unprimdn.ac.id/index.php/JUSIKOM/article/view/2306>
- [5] S. Sumarna and A. Maulana, "Implementasi Virtual Private Network Menggunakan L2TP/IPsec pada BBPK Jakarta," *Expert J. Manaj. Sist. Inf. dan Teknol.*, vol. 11, no. 2, p. 90, Dec. 2021, doi: [dx.doi.org/10.36448/expert.v11i2.1829](https://doi.org/10.36448/expert.v11i2.1829).
- [6] Yuswardi A. Suud, "Ketika Peretas Bajak TeamViewer untuk Racuni Suplai Air ke Rumah Warga, Pernah Gegerkan Jakarta," *cyberthread.id*, 2021. <https://cyberthreat.id/read/10304/Ketika-Peretas-Bajak-TeamViewer-untuk-Racuni-Supai-Air-ke-Rumah-Warga-Pernah-Gegerkan-Jakarta> (accessed Jun. 10, 2023).
- [7] J. L. Putra, L. Indriyani, and Y. Angraini, "Penerapan Sistem Keamanan Jaringan Menggunakan VPN Dengan Metode PPTP Pada PT. Asri Pancawarna," *IJCIT (Indonesian J. Comput. Inf. Technol.)*, vol. 3, no. 2, pp. 260–267, 2018, doi: [doi.org/10.31294/instk.v2i1.424](https://doi.org/10.31294/instk.v2i1.424).
- [8] M. Arif and A. Surya Budiman, "Interkoneksi Site-to-Site dan Remote Access Menggunakan Virtual Private Network dan IP Security," *JSI J. Sist. Inf.*, vol. 12, no. 1, 2020, doi: [doi.org/10.36706/jsi.v12i1.9413](https://doi.org/10.36706/jsi.v12i1.9413).
- [9] W. O. Zamalia, L. M. F. Aksara, and M. Yamin, "Analisis Perbandingan Performa Qos, Pptp, L2Tp, Sstp Dan Ipvsec Pada Jaringan Vpn Menggunakan Mikrotik," *semantik*, vol. 4, no. 2, pp. 29–36, 2018, doi: [dx.doi.org/10.55679/semantik.v4i2.4338](https://doi.org/10.55679/semantik.v4i2.4338).
- [10] S. Dewi and A. Iqbal Islami, "Implementasi Web Filtering Menggunakan Router Fortigate FG300D," 2021. doi: [doi.org/10.31294/instk.v2i1.424](https://doi.org/10.31294/instk.v2i1.424).
- [11] M. A. Novianto and S. Munir, "PERANCANGAN KEAMANAN JARINGAN NEXT-GENERATION FIREWALLMENGUNAKAN ROUTER FORTINETPADA PT. ALODOKTER TEKNOLOGI SOLUSI," *J. Inform. Terpadu*, vol. 8, no. 2, pp. 47–61, 2022, doi: [doi.org/10.54914/jit.v9i1.649](https://doi.org/10.54914/jit.v9i1.649).
- [12] W. Agustina and M. Rifqi, "Implementasi Dual Link IPVPN dan GSM Berbasis IPsec pada Fortigate 50 E," *LPPM Univ. BINA SARANA Inform.*, vol. 4, pp. 228–236, 2020, doi: [doi.org/10.29207/resti.v4i2.1465](https://doi.org/10.29207/resti.v4i2.1465).



**Nurul Arifin S.Kom**

Fakultas Teknologi Informasi

Universitas Nusa Mandiri

Jl.Raya Jatiwaringin, Cipinang melayu, Makasar, Jakarta Timur

**Jordy Lasmana Putra**

Fakultas Teknologi Informasi

Universitas Nusa Mandiri

Jl.Raya Jatiwaringin, Cipinang melayu, Makasar, Jakarta Timur