JOURNAL SYNTAX IDEA
p–ISSN: 2723-4339 e-ISSN: 2548-1398
Vol. 6, No. 06, Juni 2024

IMPLEMENTASI SSL VPN (SECURE SOCKET LAYER VIRTUAL PRIVATE NETWORK) PADA BADAN BANK TANAH

Farid Setiawan, Fajar Siddik Chaniago, Arief Wibowo
Universitas Budi Luhur, Indonesia
Email: 2231600095@student.budiluhur.ac.id, 2231600186@student.budiluhur.ac.id, arief.wibowo@budiluhur.ac.id

Abstrak

Badan Bank Tanah adalah badan khusus yang dibentuk oleh Pemerintah Pusat pada Desember 2021, merupakan Badan Hukum Indonesia yang memiliki kewenangan khusus untuk mengelola tanah Negara. Tujuan dari penelitian ini yaitu guna melihat rancangan skema yang berkaitan dengan perancangan jaringan VPN pada Badan Bank Tanah untuk dikembangkan menuju skema jaringan yang lebih efisien, efektif dan aman menggunakan metode SSL-VPN yang terdapat pada perangkat Firewall yang terdapat pada jaringan IT infrasturktur Badan Bank Tanah. Metode penelitian yang digunakan dalam penelitian ini adalah metode kualitatif dengan cara mengumpulkan data. Selanjtnya diperoleh hasil bahwa setelah melakukan pengujian dengan menghubungkan user dengan menggunakan SSL VPN ke jaringan IT infrastruktur Badan Bank Tanah melalui perangakat Firewall (Remote Gateway) dapat dilakukan dimanapun lokasi user berada menggunakan VPN Client.
.

Kata kunci: Virtual Private Network; Secure Socket Layer; enkripsi; Firewall

Abstract

The Land Bank Agency is a special body formed by the Central Government in December 2021, is an Indonesian Legal Entity that has special authority to manage State land. The purpose of this study is to see the design of the scheme related to the design of the VPN network at the Land Bank Agency to be developed towards a more efficient, effective and secure network scheme using the SSL-VPN method found in the Firewall device found in the IT infrastructure network of the Land Bank Agency. The research method used in this study is a qualitative method by collecting data. Subsequently, the results were obtained that after testing by connecting the user using SSL VPN to the IT network of the Land Bank Agency infrastructure through the Firewall (Remote Gateway) system, it can be done wherever the user is located using the VPN Client.

Keywords: *Virtual Private Network; Secure Socket Layer; enkripsi; Firewall*

PENDAHULUAN

Virtual Private Network (VPN) adalah layanan yang memungkinkan pengguna membuat koneksi terenkripsi yang aman antara internet publik dan jaringan perusahaan atau institusional (Subekti, 2020). Karena semakin banyak orang menggunakan internet publik

How to cite:	Farid Setiawan, Fajar Siddik Chaniago, Arief Wibowo (2024) Implementasi SSL VPN (Secure Socket Layer Virtual Private Network) Pada Badan Bank Tanah, *(06) 05*, https://doi.org/10.36418/syntax-idea.v3i6.1227
E-ISSN:	2684-883X
Published by:	Ridwan Institute

untuk bekerja, insiden penipuan semakin meningkat. Satu studi yang dilaporkan oleh Reuters, menemukan bahwa kerugian terkait COVID-19 mencapai hampir $100 juta. Jelas, penjahat dunia maya menyadari bahwa semakin (ISTN, 2020). Banyak orang terhubung ke internet melalui koneksi yang berpotensi lemah dan tidak aman. Dengan demikian, mereka menggunakan berbagai strategi jahat untuk mengganggu pekerjaan rutin. Karena kebutuhan kerja-dari-rumah membutuhkan puluhan juta untuk mengubah rumah mereka menjadi tempat kerja, karyawan menggunakan koneksi internet rumah mereka untuk mengakses jaringan perusahaan, setiap hari dan sepanjang hari (Sudarma, 2021).

Organisasi harus menawarkan pengalaman internet yang aman dan terjamin bagi karyawan, yang berarti solusi VPN harus mudah digunakan dan dapat diskalakan (Farizy & Eriana, 2022). Dengan VPN, bisnis dapat memiliki ketenangan pikiran dan terus mengizinkan karyawan untuk bekerja dari rumah sambil tetap terlindungi dari serangan dunia maya. Lebih lanjut, karena internet dan VPN bersifat agnostik lokasi, tidak masalah di mana individu memilih untuk terhubung ke internet. Dengan demikian, karyawan dapat bekerja dari mana saja dengan aman dan nyaman. Virtual Private Network (VPN) memberikan solusi keamanan dan konektifitas untuk melakukan pekerjaan kantor, walaupun berada di luar kantor aplikasi dan datacenter yang berada dikantor dapat diakses dan data dapat diproses layaknya kita berada dilingkungan kantor (Jariono & Subekti, 2020)

SSL VPN adalah jenis jaringan pribadi virtual (VPN) yang menggunakan protokol Secure Sockets Layer (SSL). Koneksi SSL VPN menggunakan enkripsi ujung-ke-ujung (E2EE) untuk melindungi data yang dikirimkan antara perangkat lunak klien perangkat titik akhir dan server SSL VPN tempat klien terhubung dengan aman ke internet. Dalam penelitian yang dilakukan scenario test pengamanan video conference menggunakan VPN SSL, hasil pengujian untuk faktor keamanan menunjukkan bahwa video conference yang dilakukan dengan pengamanan VPN SSL tidak dapat dilihat informasi protocol seperti IP address, user ID, RTP dan SIP karena semua data telah dienkripsi dan dikapsulisasi (ISTN, 2020; Kolopaking, Wahyono, Irmayani, Habibullah, & Erwinsyah, 2022). SSL VPN dapat digunakan oleh individu dengan sedikit atau tanpa pengalaman komputasi perusahaan, dapat diakses dari perangkat apa pun, dan dapat dikonfigurasi agar sama aman dan pribadinya dengan protokol VPN IPsec yang mendahuluinya.

Badan Bank Tanah adalah badan khusus yang dibentuk oleh Pemerintah Pusat pada Desember 2021, merupakan Badan Hukum Indonesia yang memiliki kewenangan khusus untuk mengelola tanah Negara (WATMAH, 2020). Pada Desember 2022, Divisi Informasi Teknologi Operasional Badan Bank Tanah membangun lingkungan IT infrastruktur baru meliputi pusat pengelola jaringan pusat (Core Network) dan Hyperconverged Infrastructure atau HCI sebagai pendukung dari Sistem Informasi yang digunakan untuk operasional kegiatan usaha pada Badan Bank Tanah. Maksud dan tujuan dari penelitian ini yaitu guna melihat rancangan skema yang berkaitan dengan perancangan jaringan VPN pada Badan Bank Tanah untuk dikembangkan menuju skema jaringan yang lebih efisien, efektif dan aman menggunakan metode SSL-VPN yang terdapat pada perangkat Firewall yang terdapat pada jaringan IT infrasturktur Badan Bank Tanah.

METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah metode kualitatif dengan cara mengumpulkan data (Noor, 2020). Hasil dari pengumpulan data kemudian dianalisa sehingga menjadi beberapa tahapan-tahapan analisa penelitian.

Pada tahapan ini penulis melakukan metode pengumpulan data dan informasi yang diperlukan untuk mengetahui sebuah sampel untuk penelitian dengan melakukan beberapa metode pengumpulan data antara lain yaitu :

Observasi, Metode penelitian dengan cara melihat objek penelitian IT infrastruktur di Badan Bank Tanah secara langsung di lapangan. Wawancara, Melakukan tanya jawab dengan pegawai bagian Divisi Informasi Teknologi Operasional Badan Bank Tanah. Studi Pustaka, Pengumpulan data dilakukan dengan membaca dan mempelajari materi-materi referensi dari jurnal, literatur di internet dan dokumentasi IT infrastruktur Badan Bank Tanah.

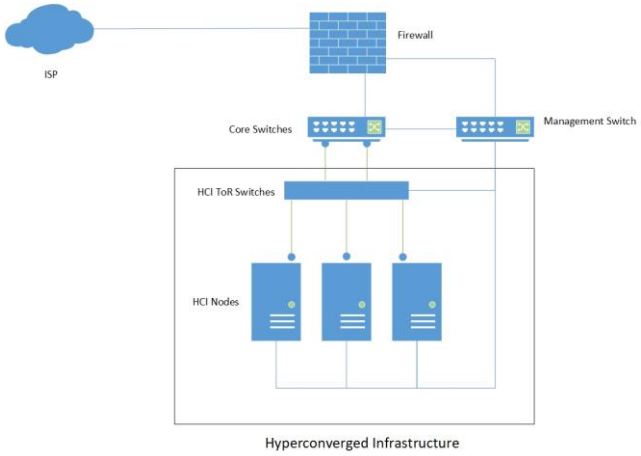
Analisa Penelitian yang dilakukan ialah Analisa Kebutuhan, Tahap ini merupakan tahap awal untuk dilakukan analisa kebutuhan, analisa keinginan user akan keamanan dan kestabilan jaringan dan cepat, dan analisa topologi infrastruktur pada Badan Bank Tanah (Bertarina & Arianto, 2021).

Desain, Pada tahap ini gambar desain topologi jaringan VPN yang akan dibangun dibuat dari data-data yang telah dianalisa sebelumnya, dan dengan gambar ini diharapkan dapat memberikan gambaran seutuhnya dari kebutuhan (Makbul, 2021). Testing, Untuk mengetahui bahwa jaringan tersebut dapat berjalan penulis melakukan test koneksi menggunakan aplikasi VPN client, kemudian ping dari client ke server agar mengetahui jaringan tersebut berjalan dengan baik. Implementasi, Pada IT infrastruktur yang dibuat perancangan jaringannya. Masing-masing user karyawan Divisi Informasi Teknologi Operasional, dan mitra penyedia perangkat diberikan user VPN untuk terhubung dari jarak jauh ke jaringan IT infrastruktur Badan Bank Tanah.

HASIL DAN PEMBAHASAN

Rancangan IT Infrastruktur

Topologi jaringan yang digunakan di Badan Bank Tanah adalah sebagai berikut :



Gambar 1. Topologi Jaringan

Perangkat Firewall yang digunakan untuk mendukung jaringan VPN pada Badan Bank Tanah adalah berfungsi sebagai **:**

1. Next Generation Firewall (NGFW)

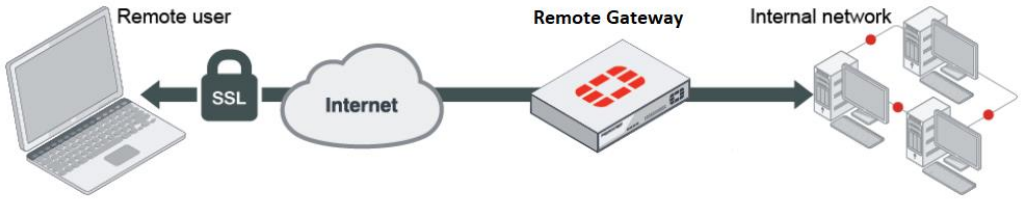
Mengamankan web, konten, dan perangkat serta melindungi jaringan dari ransomware dan serangan siber yang canggih (Liang & Kim, 2022).

2. Secure SD-WAN

Menghadirkan kualitas pengalaman yang unggul dan postur keamanan yang efektif untuk model kerja-dari-mana saja, SD-Branch, dan kasus penggunaan cloud-first WAN (Wood, 2017).

Skema Jaringan

Skema yang diusulkan dengan fitur SSL VPN *Tunnel mode* (Bayu & Susila, 2023), skemanya sebagai berikut. Dalam *tunnel mode*, klien SSL VPN mengenkripsi semua lalu lintas dari komputer klien jarak jauh dan mengirimkannya ke Remote Gateway melalui *tunnel* SSL VPN melalui tautan HTTPS antara pengguna dan Remote Gateway.



Gambar 2. Skema Jaringan

Remote Gateway membuat *tunnel* dengan klien, dan menetapkan alamat IP virtual (VIP) ke klien dari rentang alamat yang dicadangkan (Lojka, Bundzel, & Zolotova, 2015). Meskipun protokol yang mendasarinya berbeda, hasilnya sangat mirip dengan terowongan VPN IPsec. Semua lalu lintas klien dienkripsi, memungkinkan pengguna dan jaringan untuk bertukar berbagai lalu lintas, terlepas dari aplikasi atau protokolnya.

Keamanan Jaringan

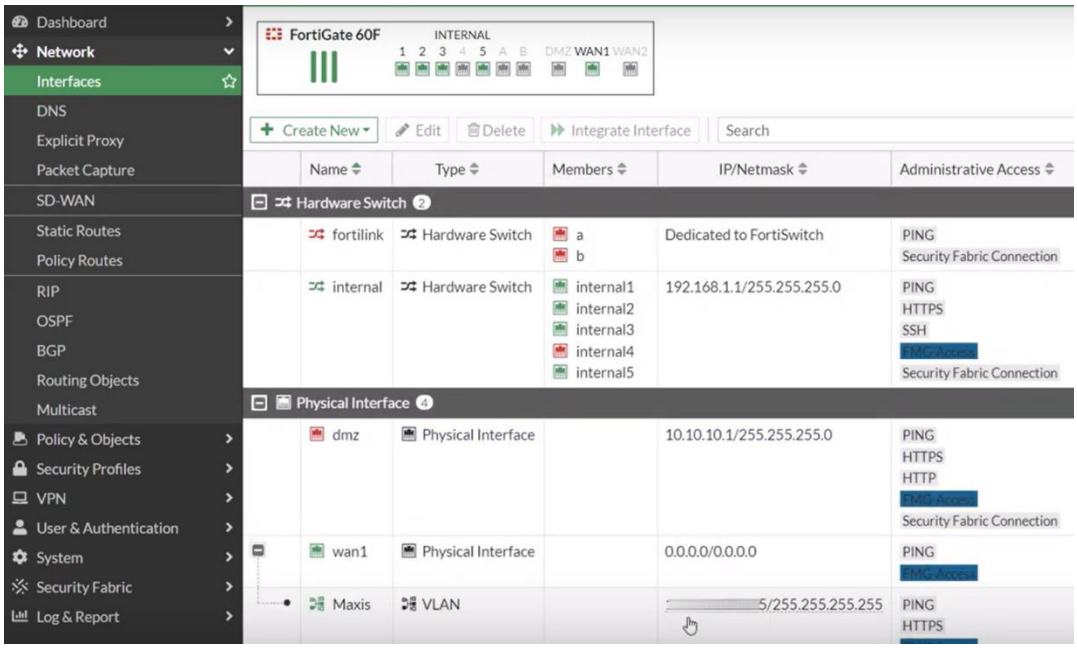
Selain melalui jaringan VPN Tunnel yang terenkripsi dengan SSL, setiap user juga harus memverifikasi *user* dan *password* yang diminta oleh perangkat yang diakses pada jaringan lokal yang ada pada Badan Bank Tanah (Badrul, 2016).

Rancangan Aplikasi

Selain melalui jaringan VPN Tunnel yang terenkripsi dengan SSL (Siregar & Melani, 2019), setiap user juga harus memverifikasi *user* dan *password* yang diminta oleh perangkat yang diakses pada jaringan lokal yang ada pada Badan Bank Tanah.

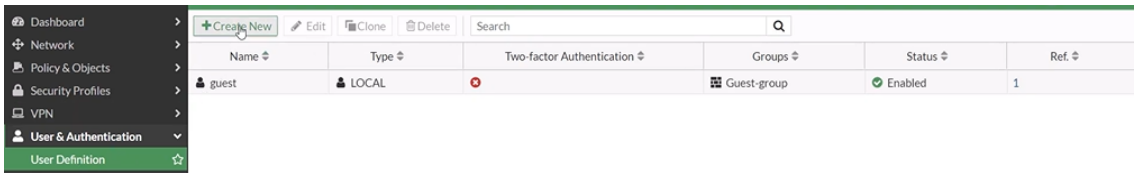
Berikut langkah-langkah konfigurasi pada perangkat *Remote Gateway* pada Badan Bank Tanah.

Langkah pertama konfigurasi *interface* dan *firewall addresses* dari menu *Network* > *Interface* seperti pada gambar 3.



Gambar 3. Remote Gateway Network Interfaces

Berikutnya konfigurasi *user* dan *user group* seperti pada gambar 4.

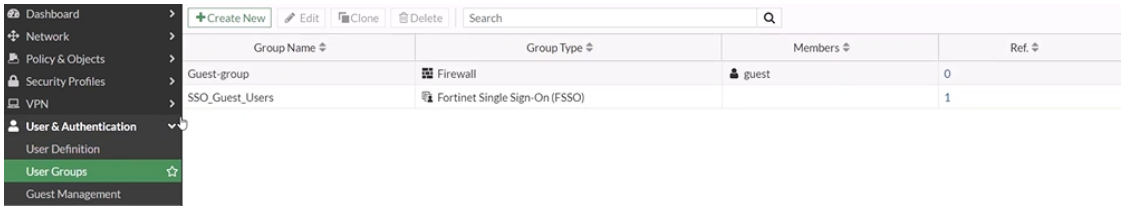


Gambar 4. Remote Gateway User Definition

Tahap selanjutnya buat user baru dengan tipe *Local User* seperti pada gambar 4.

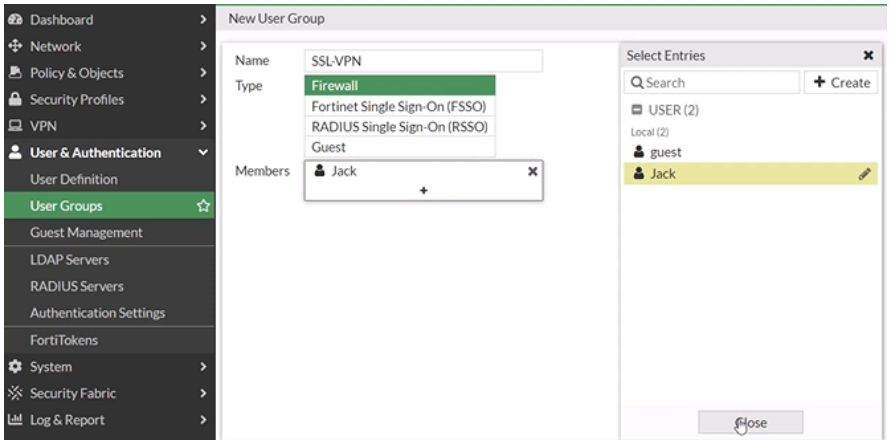
Gambar 5. Remote Gateway User/Groups Creation Wizard

Berikutnya buat group user baru seperti pada gambar 6.



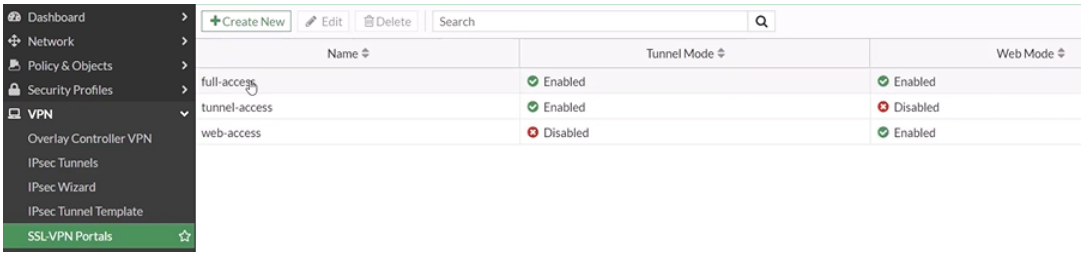
Gambar 6. Remote Gateway User Groups

Tahap selanjutnya buat group user baru dengan anggota user yang sebelumnya sudah dibuat seperti pada gambar 7.



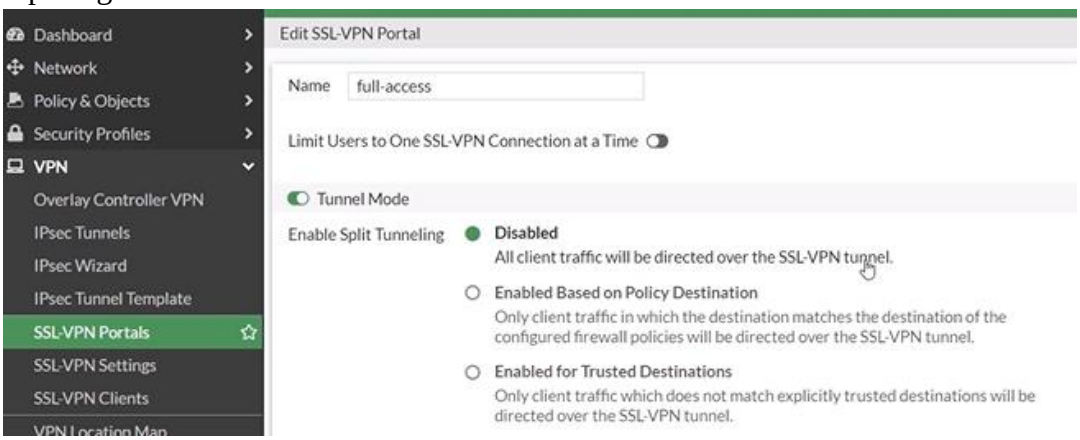
Gambar 7. Remote Gateway New User Group

Berikutnya konfigurasi SSL web portal seperti pada gambar 8.



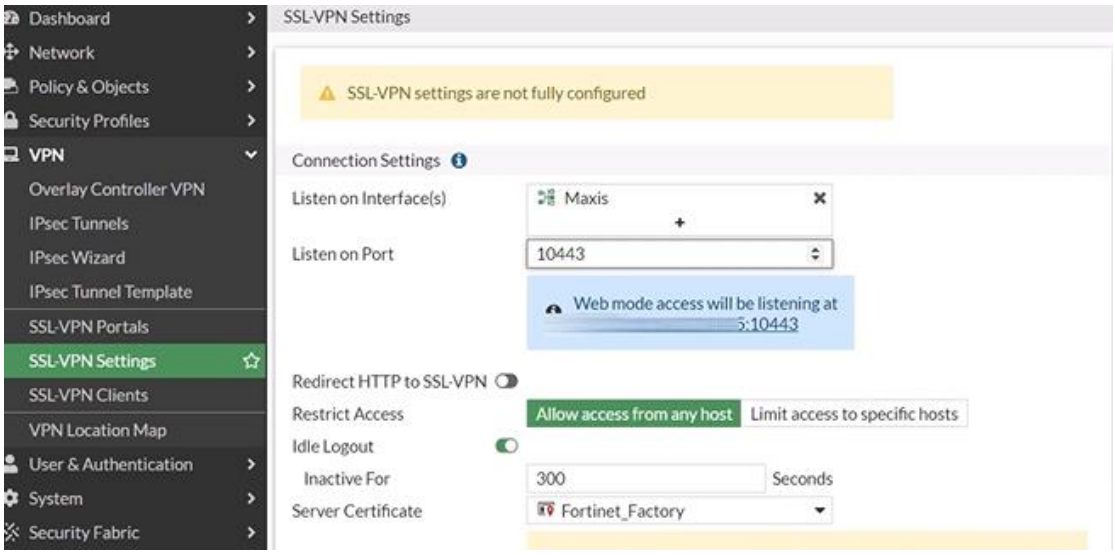
Gambar 8. Remote Gateway SSL-VPN Portals

Tahap selanjutnya Edit SSL-VPN portal, pilih *Disabled* untuk *Enable Split Tunneling* seperti pada gambar 9.



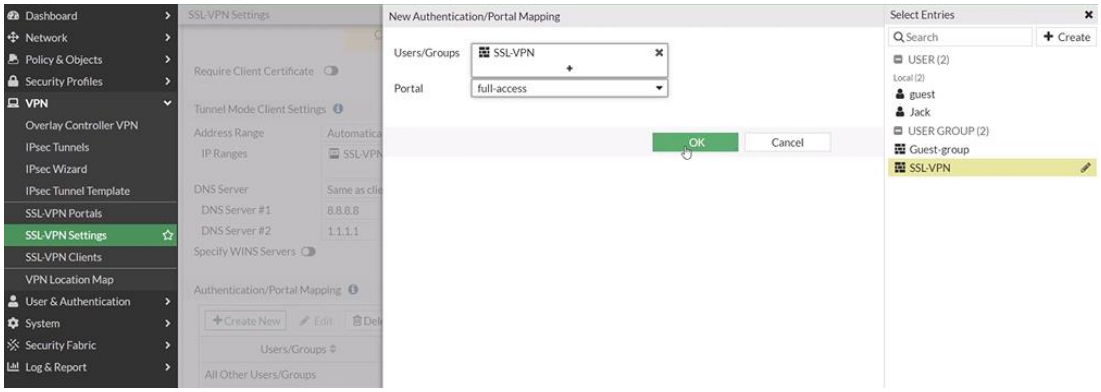
Gambar 9. Remote Gateway Edit SSL-VPN Portals

Berikutnya SSL-VPN settings, untuk *Listen on Interface(s)*, pilih wan1, atur *Listen on port* menjadi 10443, pilih *Server Certifiate*. Standarnya adalah Fortinet_Factory seperti gambar 10.



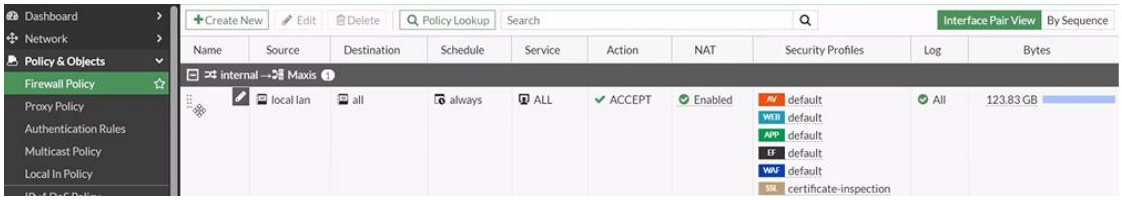
Gambar 10. Remote Gateway SSL-VPN Settings

Tahap selanjutnya SSL-VPN settings, pada *Authentication/Portal All other Users/Groups*, atur *Portal* ke *tunnel-access.* Klik *Create New*, *New Authentication/Portal Mapping* untuk *User/Groups* dan mapping portal seperti gambar 11.



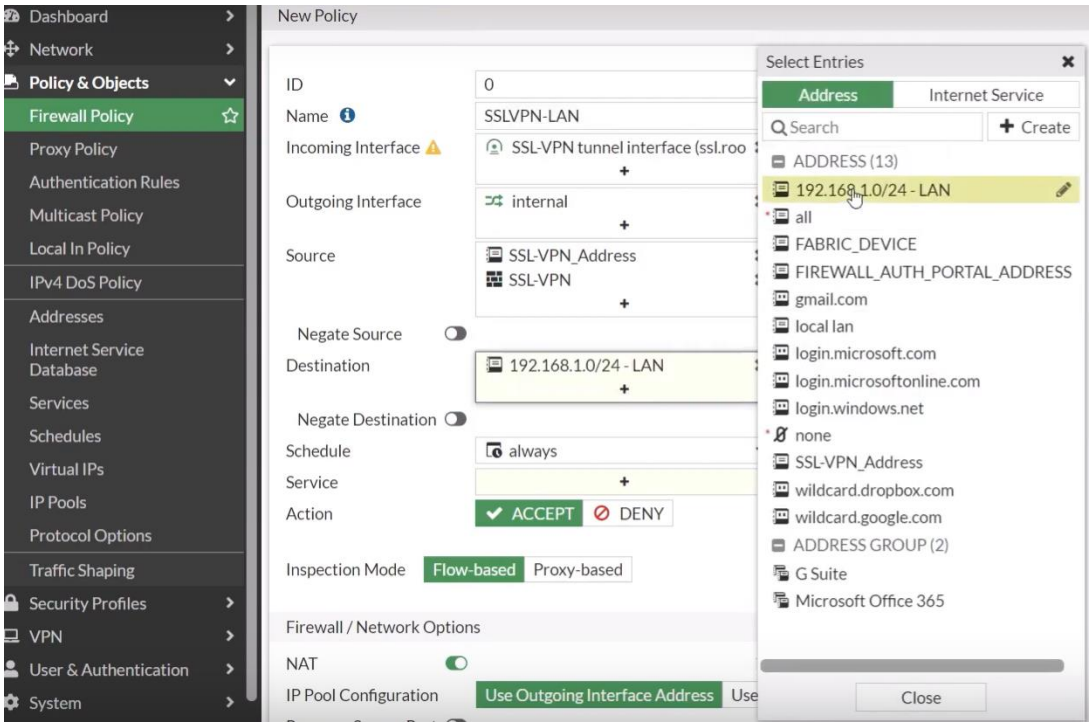
Gambar 11. Remote Gateway New/Authentication/Portal Mapping

Berikutnya konfigurasi SSL VPN Firewall Policy untuk mengizinkan pengguna jarak jauh untuk mengakses jaringan internal seperti gambar 12.



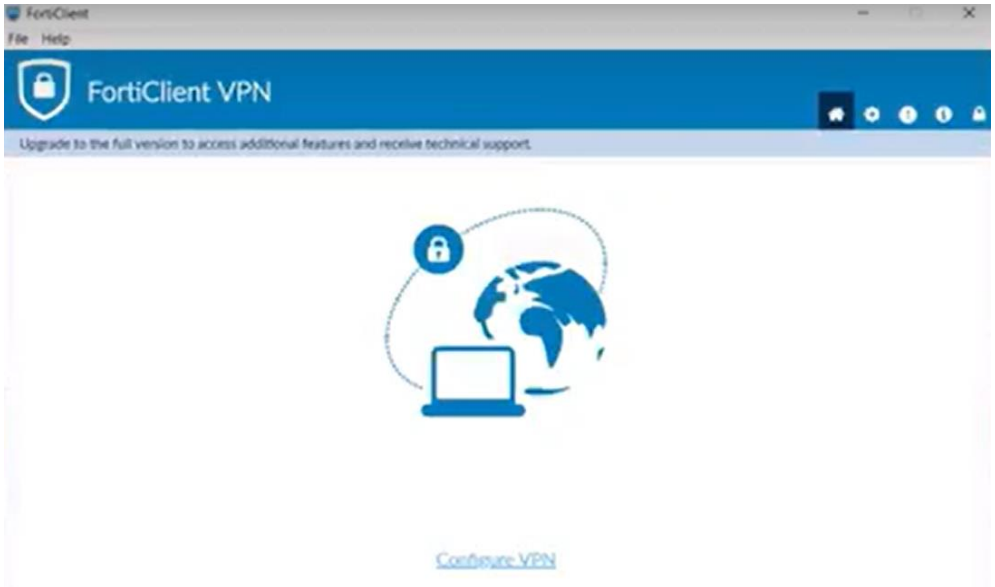
Gambar 12. Remote Gateway FireWall Policy

Tahap berikutnya klik Create New untuk konfigurasi SSL VPN Firewall Policy. Atur *Name*, atur *Incoming Interface* ke *SSL-VPN tunnel interface(ssl.root)* seperti gambar 13.



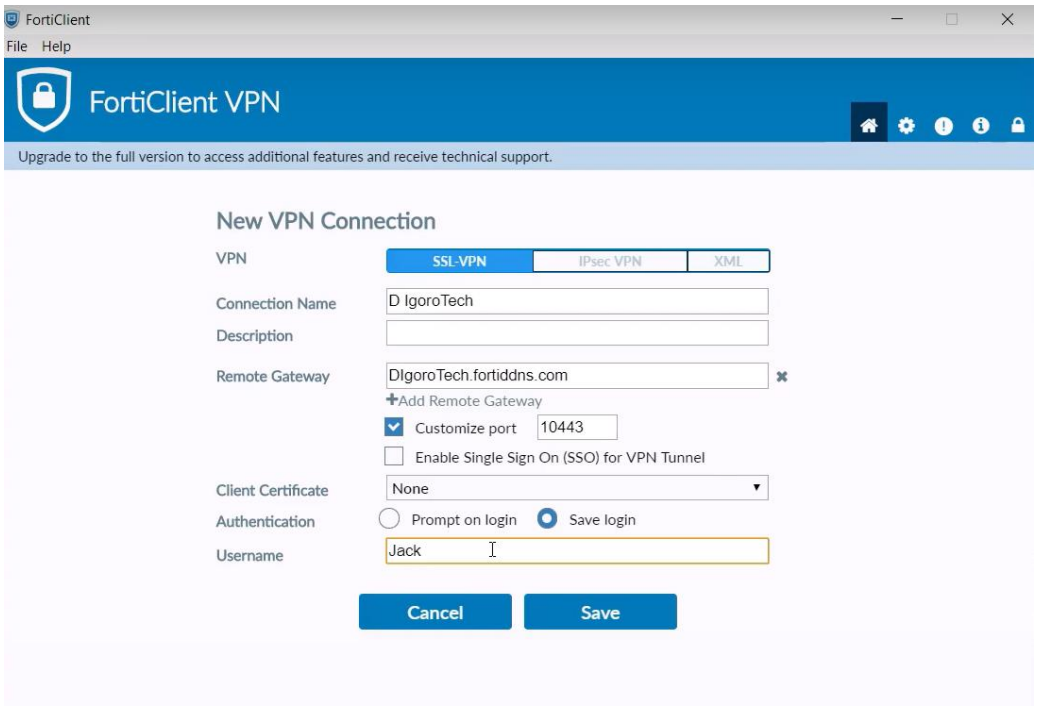
Gambar 13. Remote Gateway New FireWall Policy

Tahap selanjutnya konfigurasi VPN Client pada *user*, klik *Configure VPN*.



Gambar 14. VPN Client

Berikutnya pada *New VPN Connection*, pilih SSL-VPN, atur *Connection Name*, *Remote Gateway* dan centang *Customize port*, atur nomor port seperti pada gambar 15.



Gambar 15. VPN Client – New VPN Connection

Manajemen Jaringan

Pada penerapan metode SSL VPN memungkinkan pengguna jarak jauh mengakses sumber daya organisasi dengan aman, serta untuk mengamankan sesi *internet* pengguna yang mengakses *internet* dari luar perusahaan. *Administrator* jaringan jadi sangat terbantu untuk lebih mudah melakukan pekerjaan, memonitoring jaringan dan mengakses sumber daya tanpa harus melakukan kunjungan ke lokasi perangkat.

Pengujian Jaringan

a. Pengujian Jaringan Awal

Pada tahap pengujian ini dilakukan sebelum adanya penggunaan VPN Client *SSL-VPN*, dapat dilihat bahwa setiap *user* yang terhubung ke koneksi *internet* tidak dapat terhubung langsung dengan jaringan IT infrastruktur Badan Bank Tanah.

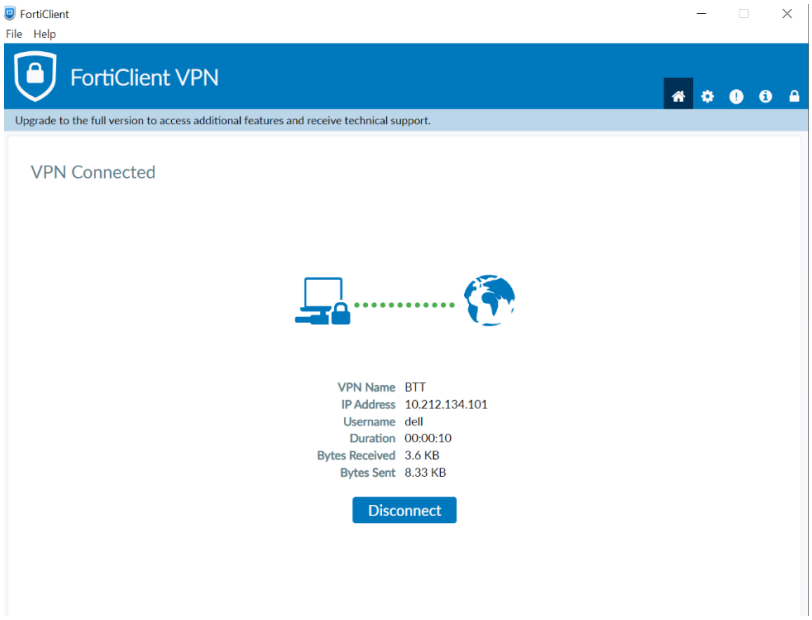
```
C:\Users\setiaf>ping jktdcvc-bt.banktanah.id
Ping request could not find host jktdcvc-bt.banktanah.id. Please check the name and try again.

C:\Users\setiaf>ping 10.254.43.99

Pinging 10.254.43.99 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.254.43.99:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\setiaf>
```

Gambar 16. Test Ping vCenter Server (Pengujian Jaringan Awal)

Pada Gambar 16, penulis melakukan pengujian dengan melakukan *Test Ping* ke komponen vCenter *Server* dari *workstation* yang terkoneksi dengan jaringan *internet*, dapat dilihat bahwa hasilnya *request timed out* atau dikarenakan jaringan tidak terhubung.

b. Pengujian Jaringan Akhir

Pada tahap pengujian jaringan ini penulis sudah menggunakan VPN Client SSL-VPN yang terhubung ke *internet* seperti pada gambar 17.



Gambar 17. VPN Client VPN – VPN Connected

```
C:\Users\setiaf>ping jktdcvc-bt.banktanah.id

Pinging jktdcvc-bt.banktanah.id [10.254.43.99] with 32 bytes of data:
Reply from 10.254.43.99: bytes=32 time=3ms TTL=63
Reply from 10.254.43.99: bytes=32 time=2ms TTL=63
Reply from 10.254.43.99: bytes=32 time=4ms TTL=63
Reply from 10.254.43.99: bytes=32 time=11ms TTL=63

Ping statistics for 10.254.43.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 11ms, Average = 5ms

C:\Users\setiaf>ping 10.254.43.99

Pinging 10.254.43.99 with 32 bytes of data:
Reply from 10.254.43.99: bytes=32 time=3ms TTL=63
Reply from 10.254.43.99: bytes=32 time=5ms TTL=63
Reply from 10.254.43.99: bytes=32 time=3ms TTL=63
Reply from 10.254.43.99: bytes=32 time=5ms TTL=63

Ping statistics for 10.254.43.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 5ms, Average = 4ms

C:\Users\setiaf>
```

Gambar 18. Test Ping vCenter Server (kondisi akhir)

Pada Gambar 18 hasil yang didapat setelah Penulis melakukan *Test Ping* disimpulkan bahwa jaringan IT infrastruktur Bank Tanah sudah terhubung ke workstation *user* melalui jaringan *internet* dengan baik dengan menggunakan VPN metode SSL-VPN

KESIMPULAN

Berdasarkan hasil penelitian maka disimpulkan bahwa setelah melakukan pengujian dengan menghubungkan user dengan menggunakan SSL VPN ke jaringan IT infrastruktur Badan Bank Tanah melalui perangakat Firewall (Remote Gateway) dapat dilakukan dimanapun lokasi user berada menggunakan VPN Client.

Prospek untuk penelitian selanjutnya yang dapat dikembangkan antara lain yaitu, meneliti anomali jaringan, pemantauan pola lalu lintas yang mencurigakan pada jaringan guna mengurangi ancaman keamanan atau sebelum pelanggaran akses yang bisa terjadi melalui jaringan VPN. Meneliti performa jaringan, melakukan optimalisasi jaringan serta melakukan benchmarking jaringan VPN.

BIBLIOGRAFI

Badrul, Mohammad. (2016). Open Vpn-Access Server Dengan Enskripsi Ssl/Ti Open Ssl. *Informatics For Educators And Professional: Journal Of Informatics*, *1*(1), 1–12.

Bayu, Nur, & Susila, Atang. (2023). Penerapan Teknologi Fortigate Dalam Pembangunan Jaringan Vpn Berbasis Ssl-Vpn (Studi Kasus: Kementerian Panrb). *Logic: Jurnal Ilmu Komputer Dan Pendidikan*, *2*(1), 153–159.

Bertarina, Bertarina, & Arianto, Waras. (2021). Analisis Kebutuhan Ruang Parkir (Studi Kasus: Area Parkir Ict Universitas Teknokrat Indonesia). *Jurnal Teknik Sipil*, *2*(02), 67–77.

Farizy, Salman, & Eriana, Emi Sita. (2022). *Cloud Computing= Komputasi Awan*. Unpampress.

Istn, Irmayani. (2020). Implementasi Secure Socket Layer Pada Virtual Private Network Untuk Pengamanan Komunikasi Video Conference. *Sinusoida*, *22*(2), 45–57.

Jariono, Gatot, & Subekti, Nur. (2020). Sports Motivation Survey And Physical Activity Students Of Sport Education Teacher Training And Education Faculty Fkip Muhammadiyah University Surakarta. *Kinestetik: Jurnal Ilmiah Pendidikan Jasmani*, *4*(2), 86–95.

Kolopaking, Lala M., Wahyono, Eko, Irmayani, Nyi R., Habibullah, Habibullah, & Erwinsyah, Rudy G. (2022). Re-Adaptation Of Covid-19 Impact For Sustainable Improvement Of Indonesian Villages' Social Resilience In The Digital Era. *International Journal Of Sustainable Development & Planning*, *17*(7).

Liang, Junyan, & Kim, Yoohwan. (2022). Evolution Of Firewalls: Toward Securer Network Using Next Generation Firewall. *2022 Ieee 12th Annual Computing And Communication Workshop And Conference (Ccwc)*, 752–759. Ieee.

Lojka, Tomáš, Bundzel, Marek, & Zolotova, Iveta. (2015). Industrial Gateway For Data Acquisition And Remote Control. *Acta Electrotechnica Et Informatica*, *15*(2), 43–48.

Makbul, M. (2021). *Metode Pengumpulan Data Dan Instrumen Penelitian*.

Noor, H. R. Zulki Zulkifli. (2020). *Metodologi Penelitian Kualitatif Dan Kuantitatif: Petunjuk Praktis Untuk Penyusunan Skripsi, Tesis, Dan Disertasi: Tahun 2015*. Deepublish.

Siregar, Helmi Fauzi, & Melani, Melani. (2019). Perancangan Aplikasi Komik Hadist Berbasis Multimedia. *Jurnal Teknologi Informasi*, *2*(2), 113–121.

Subekti, Rino. (2020). Implementasi Virtual Private Network (Vpn) Sebagai Solusi Security Selama Work From Home. *Jurnal Nasional Informatika (Junif)*, *1*(1), 57–65.

Sudarma, Momon. (2021). *Daring Duraring Belajar Dari Rumah: Strategi Jitu Guru, Orang Tua, Dan Siswa Di Masa Pandemi*. Elex Media Komputindo.

Watmah, S. R. I. Watmah. (2020). Implementasi Vpn Menggunakan Point-To-Point Tunneling Protocol (Pptp) Mikrotik Router Pada Bprs Bumi Artha Sampang. *Insantek-Jurnal Inovasi Dan Sains Teknik Elektro*, *1*(1), 6–12.

Wood, Michael. (2017). How To Make Sd-Wan Secure. *Network Security*, *2017*(1), 12–14.