BAB 3
PELAKSANAAN KERJA MAGANG

3.1 Kedudukan dan Koordinasi

Pelaksanaan magang di PT. Exeed Indo Jaya dilakukan pada posisi Network Security Intern. Posisi ini berada dalam naungan tim Network Security yang dipimpin secara bersama oleh Bapak Duha Abdul Rahman dan Bapak Hamzah Mohamad Alpariji. Keduanya berperan sebagai pembimbing sekaligus penanggung jawab tim yang bertugas melakukan asesmen terhadap proyek baru untuk disesuaikan dengan Scope of Work (SOW) serta memastikan keberhasilan proyek yang sedang berjalan.

Alur kerja dan koordinasi terkait tugas diatur sebagai berikut. Proses umumnya dimulai ketika tim sales menerima permintaan atau proyek baru dari client. Informasi tersebut kemudian diteruskan kepada pimpinan tim Network Security untuk dianalisis dan dinilai kelayakannya. Setelah asesmen dan perencanaan, tugas-tugas spesifik yang berkaitan dengan implementasi, konfigurasi, atau dokumentasi teknis diberikan kepada anggota Network Security.

Proses koordinasi untuk membahas tugas atau progres dilakukan melalui dua cara. Untuk komunikasi cepat, koordinasi dilakukan secara daring menggunakan WhatsApp. Namun, untuk pembahasan yang memerlukan detail teknis, perencanaan strategis, atau diskusi mendalam dengan tim lain, pembahasan dilanjutkan secara tatap muka di ruang meeting.

3.2 Tugas yang Dilakukan

Selama periode kerja magang, tugas-tugas yang dilaksanakan berpusat pada bidang keamanan jaringan. Kegiatan utama dapat dikelompokkan ke dalam empat kategori utama, yaitu praktik laboratorium dan konfigurasi jaringan, dokumentasi teknis, kolaborasi tim, serta implementasi di lapangan.

A. Praktik Laboratorium dan Konfigurasi Jaringan

Kegiatan utama berfokus pada praktik langsung di lingkungan laboratorium yang diawali dengan perancangan dan pembangunan topologi jaringan untuk berbagai skenario uji coba. Praktik ini dilanjutkan dengan instalasi, konfigurasi,

hingga upgrade firmware pada perangkat FortiGate, serta implementasi dan troubleshooting konektivitas IPsec VPN Tunnel dan SSL VPN untuk akses jarak jauh. Selain itu, dilakukan pula penerapan kebijakan keamanan (security policies), integrasi otentikasi SAML menggunakan SimpleSAMLphp, dan pengenalan dasar LDAP (Lightweight Directory Access Protocol).

B. Dokumentasi Teknis dan Pelaporan

Pekerjaan teknis diimbangi dengan tugas pembuatan berbagai dokumen pendukung proyek yang terstruktur. Tugas ini mencakup penyusunan dokumen teknis perencanaan seperti Low Level Design (LLD) dan Staging Report sebelum implementasi, serta pembuatan Minute of Meeting (MoM) sebagai catatan hasil diskusi teknis. Tanggung jawab dokumentasi juga meliputi penyusunan laporan operasional rutin seperti Preventive Maintenance (PM) dan Corrective Maintenance (CM) untuk berbagai client, pembuatan panduan instalasi step-by-step, hingga finalisasi dokumen User Acceptance Test (UAT).

C. Manajemen Proyek dan Kolaborasi Tim

Keterlibatan aktif dalam alur kerja tim dilakukan melalui partisipasi dalam assessment meeting untuk memahami ruang lingkup proyek, mengikuti diskusi teknis dengan client, dan melakukan pendampingan (shadowing) pada proses instalasi, migrasi, maupun implementasi perangkat di lapangan. Selain itu, partisipasi dalam kolaborasi juga mencakup kegiatan probing (pendekatan proaktif) untuk mengidentifikasi kebutuhan spesifik client. Hasil analisis ini kemudian digunakan untuk memberikan rekomendasi produk dan konfigurasi yang paling sesuai. Keterlibatan dengan pihak eksternal juga dilakukan dengan mempresentasikan hasil kerja, seperti dokumen Preventive Maintenance, kepada pimpinan tim serta kepada client.

D. Instalasi dan Implementasi di Lapangan

Pengalaman praktis juga diperoleh melalui kegiatan implementasi langsung di lokasi client (on-site). Kegiatan ini mencakup dukungan teknis selama proses User Acceptance Test (UAT), melakukan injeksi lisensi (inject license) pada perangkat, pengujian konektivitas untuk memastikan fungsionalitas sistem, serta memberikan dukungan teknis langsung sesuai kebutuhan di lokasi.

3.3 Uraian Pelaksanaan Magang

Tabel 3.1 menunjukkan ringkasan kegiatan selama kerja magang di PT Exeed Indo Jaya

Tabel 3.1. Pekerjaan yang dilaksanakan setiap minggu selama periode magang

Minggu Ke -	Pekerjaan yang dilakukan
1	Melakukan orientasi yang mencakup pengenalan tim dan mengikuti assessment proyek. Tugas yang dikerjakan meliputi pembuatan makalah keamanan jaringan, partisipasi dalam assessment meeting beserta pembuatan rangkumannya, serta pengerjaan lab 1 FortiGate. Selain itu, dilakukan juga bantuan persiapan dokumen seperti staging report dan LLD (Low Level Design), partisipasi dalam rapat bersama client, dan instalasi Kaspersky End point.
2	Melanjutkan pengisian dokumen LLD, mengerjakan lab 2 FortiGate, dan menyusun dokumen instalasi untuk client. Dilakukan juga pembelajaran mengenai prosedur respons Fortinet L1 Support, mendalami pengetahuan mengenai proxy dan reverse proxy, serta pengerjaan lab. Selain itu, dikerjakan dokumen untuk client, melakukan shadowing (pendampingan) implementasi dan mounting perangkat di lokasi (on site), dan membuat MoM.
3	Mengerjakan dokumen instalasi untuk salah satu proyek client dan memulai pembelajaran serta implementasi teknis SAML (Security Assertion Markup Language). Proses ini meliputi konfigurasi SAML pada virtual machine (VM), instalasi VM FortiGate, serta melakukan serangkaian tindakan teknis seperti pengaturan, upgrade, reset, dan update pada VM tersebut.
4	Melanjutkan implementasi SAML dengan platform Apache dan NGINX, serta melakukan reset pada FortiManager dan pengecekan FortiSwitch. Tugas pada minggu ini diselesaikan dengan keberhasilan integrasi simplesamlphp dengan FortiGate, yang kemudian hasilnya didokumentasikan dengan membuat instruksi instalasi lengkap.
Lanjut pada halaman berikutnya	

Lanjutan Tabel 3.1

Minggu Ke -	Pekerjaan yang dilakukan
5	Mengerjakan Lab 5 yang berfokus pada konfigurasi IPsec Tunnel dan penerapan berbagai jenis aturan pemblokiran. Dilakukan juga pembelajaran mengenai VPN Forti, SSL VPN, dan setup SAML, serta memulai penyusunan maintenance report dan dokumen untuk proyek lainnya.
6	Berpartisipasi dalam kegiatan on-site untuk User Acceptance Test (UAT), yang mencakup tugas inject license, pengujian konektivitas, dan pembacaan log firewall Huawei. Pekerjaan dilanjutkan dengan penyusunan dokumentasi PM (Preventive Maintenance) untuk berbagai perangkat seperti FortiGate, Huawei, dan FortiManager.
7	Melakukan sesi berbagi pengetahuan (sharing knowledge) mengenai manajemen proyek, finalisasi dokumen proyek, dan instalasi Kaspersky dari jarak jauh (remote). Dilakukan juga pembelajaran teknologi baru seperti LDAP dan FortiToken sambil melanjutkan pengerjaan dokumen PM berdasarkan catatan record troubleshooting.
8	Mengerjakan seluruh siklus Preventive Maintenance (PM), mulai dari analisis dokumentasi, finalisasi dokumen implementasi untuk salah satu client, hingga presentasi hasil dan proses revisi. Pembelajaran mengenai record troubleshooting dari berbagai kasus instalasi juga terus dilanjutkan.
9	Merancang desain topologi lab beserta tujuan dan konstrain, diikuti dengan pengerjaan lab IPsec Tunnel yang meliputi troubleshooting dan uji coba upgrade firmware. Kegiatan ini diselingi dengan diskusi dan pengerjaan tugas PM.
10	Menyusun laporan Preventive Maintenance (PM) untuk berbagai client. Dilakukan juga pembuatan dokumen teknis instalasi dan analisis intrusi pada FortiAnalyzer yang hasilnya didokumentasikan.

Lanjut pada halaman berikutnya

Lanjutan Tabel 3.1

Minggu Ke -	Pekerjaan yang dilakukan
11	Mengerjakan tugas Corrective Maintenance (CM) untuk perangkat FortiGate seri enterprise, bersamaan dengan tugas PM dan pengerjaan lab FortiGate. Diadakan juga sesi berbagi pengetahuan dan pembuatan soal tes.
12	Berpartisipasi dalam proses seleksi kandidat baru melalui assessment, tes teori, dan praktik. Dilakukan juga kunjungan on-site ke sebuah institusi pendidikan, sambil melanjutkan pekerjaan PM dan CM untuk beberapa client.
13	Melaksanakan tugas operasional pemeliharaan secara intensif, mencakup Preventive Maintenance (PM) dan Corrective Maintenance (CM) untuk berbagai client dan perangkat, dengan volume pekerjaan mencakup beberapa site per hari.
14	Melanjutkan pekerjaan rutin Preventive Maintenance (PM) dan Corrective Maintenance (CM). Diadakan juga meeting dengan salah satu client eksternal untuk membahas kebutuhan proyek.
15	Memulai pengerjaan proyek migrasi SonicWall yang meliputi kegiatan lab dan pelaksanaan migrasi di luar jam kerja normal. Tugas rutin seperti PM, CM, dan meeting dengan client tetap berjalan.
16	Menyelesaikan proyek migrasi SonicWall dengan membuat dokumentasi migrasi. Kegiatan rutin seperti PM, CM, dan pengerjaan lab tetap dilaksanakan, serta diadakan sebuah meeting internal untuk koordinasi tim.

3.3.1 Studi Kasus: Implementasi Keamanan Jaringan Dasar untuk Kantor Cabang

Sub-bab ini merinci studi kasus implementasi dan konfigurasi perangkat FortiGate yang telah dilakukan untuk membangun jaringan yang aman dan terhubung antara kantor pusat (HO) dan kantor cabang (SITE). Skenario ini didasarkan pada kebutuhan umum yang ditemukan di lingkungan perusahaan.

Sebagai bagian dari perencanaan implementasi, dilakukan pemilihan

perangkat yang sesuai dengan kebutuhan dan skala masing-masing lokasi. Dalam studi kasus ini, kantor cabang (SITE) menggunakan FortiGate 40F, sementara kantor pusat (HO) yang memerlukan kapasitas lebih besar menggunakan FortiGate 60F. Rincian perangkat, estimasi biaya investasi awal, serta biaya perpanjangan lisensi tahunan dapat dilihat pada Tabel 3.2.

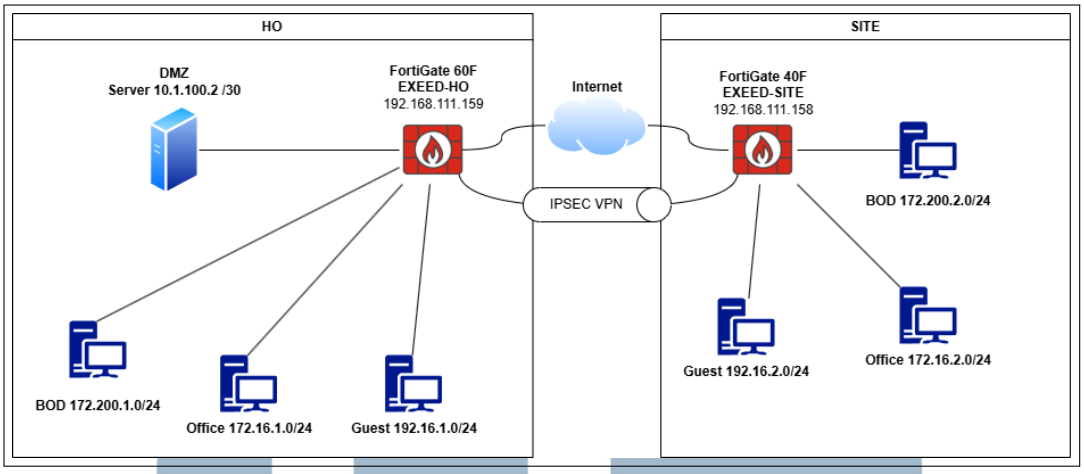
Tabel 3.2. Device Specification and Cost

Hardware	Software	Cost
FortiGate 40F	FortiOS v7.4.6 build2726 (Mature)	Rp. 15,9 juta – Rp. 17,2 juta (per bundle dengan lisensi UTM 1 tahun) Lisensi UTM Sekitar Rp. 6,2 juta per tahun
FortiGate 60F	FortiOS v7.4.6 build2726 (Mature)	Rp. 20,0 juta - Rp. 25,0 juta (per bundle dengan lisensi UTM 1 tahun) Lisensi UTM Sekitar Rp. 9,1 juta – Rp. 10,4 juta per tahun

A Topologi Jaringan

Topologi jaringan yang diimplementasikan dalam studi kasus ini terdiri dari dua lokasi: Kantor Pusat (HO) dan Kantor Cabang (SITE), seperti yang diilustrasikan pada Gambar 3.1. Masing-masing kantor menggunakan perangkat FortiGate, yaitu model 60F untuk HO (hostname: EXEED-HO) dan model 40F untuk SITE (hostname: EXEED-SITE).

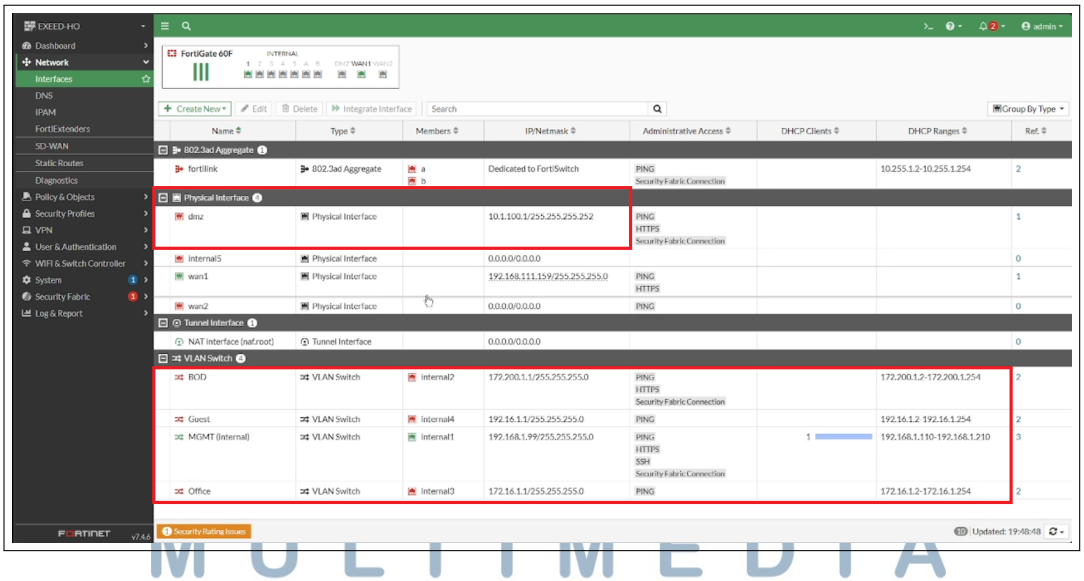
Pada sisi HO, sebuah server ditempatkan di zona DMZ dengan alamat IP 10.1.100.2/30. Untuk segmentasi jaringan, kedua lokasi menerapkan tiga VLAN yang identik secara fungsional: VLAN untuk Board of Directors (BOD), VLAN Office, dan VLAN Guest. Skema pengalamatan IP untuk setiap segmen dibuat unik di setiap lokasi untuk mencegah konflik, misalnya VLAN BOD di HO menggunakan subnet 172.200.1.0/24, sedangkan di SITE menggunakan 172.200.2.0/24.



Gambar 3.1. Topologi Lab Kantor Pusat (HO) dan Kantor Cabang (SITE)

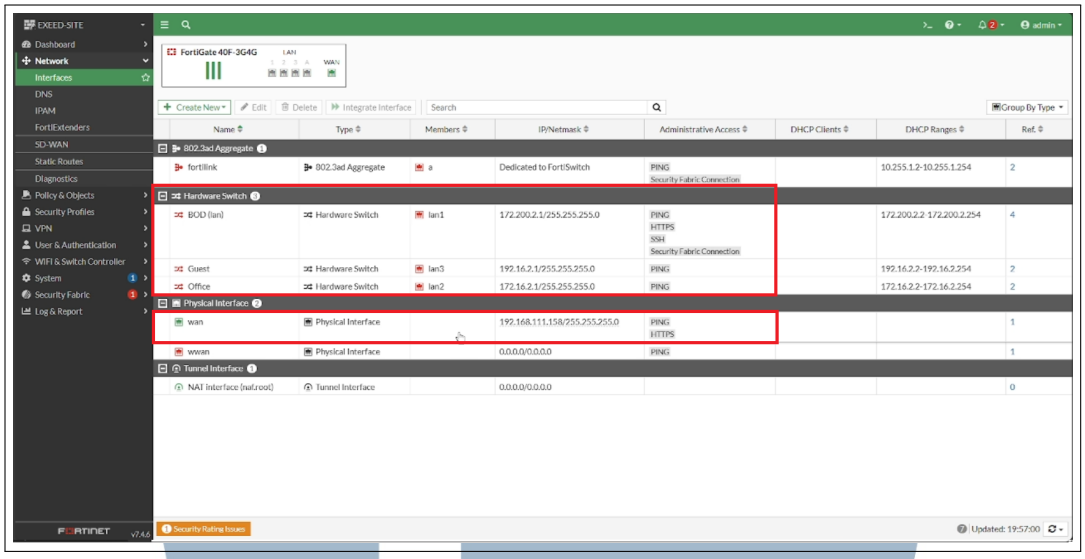
B Konfigurasi Interface dan Objek Jaringan

Konfigurasi dasar pada kedua perangkat FortiGate mencakup pembuatan interface VLAN dan objek alamat. Interface VLAN dibuat untuk setiap segmen jaringan (Gambar 3.2 dan Gambar 3.3). Perbedaan utama antara konfigurasi di HO dan SITE adalah skema pengalamatan IP yang diterapkan pada setiap interface sesuai dengan topologi.



Gambar 3.2. Konfigurasi Interface pada FortiGate-HO

Selanjutnya, objek alamat dibuat untuk merepresentasikan setiap entitas jaringan pada FortiGate-HO seperti yang diilustrasikan pada Gambar 3.4 dan juga pada FortiGate-SITE yang diilustrasikan pada Gambar 3.5. Implementasi ini merupakan fondasi untuk membangun kebijakan keamanan yang spesifik dan



Gambar 3.3. Konfigurasi Interface pada FortiGate-SITE

terkontrol, sejalan dengan prinsip least privilege.

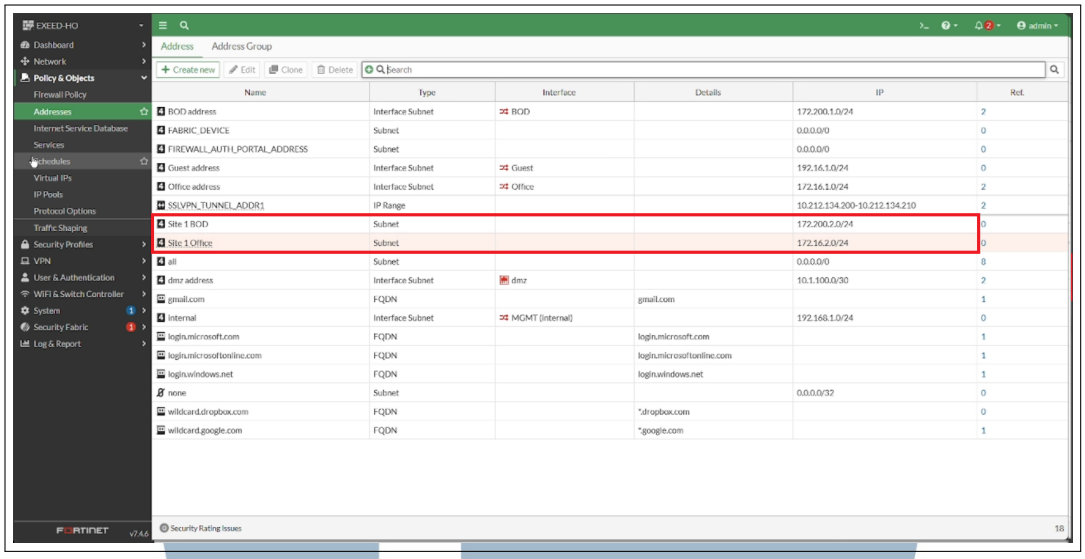
Tujuan utamanya adalah untuk memastikan bahwa hanya alamat yang telah terdefinisi secara eksplisit yang dapat dimasukkan ke dalam peraturan keamanan. Dengan mendefinisikan setiap server, subnet pengguna, atau perangkat yang sah sebagai sebuah objek, firewall policy dapat dirancang untuk hanya mengizinkan traffic dari dan ke entitas-entitas yang sudah disetujui tersebut.

Pada FortiGate-HO, objek dibuat untuk mendefinisikan jaringan lokal HO dan juga jaringan remote SITE. Sebaliknya, pada FortiGate-SITE, objek dibuat untuk jaringan lokal SITE dan jaringan remote HO. Pendekatan ini krusial agar kedua perangkat dapat saling mengenali sumber dan tujuan traffic saat membuat kebijakan untuk koneksi VPN.

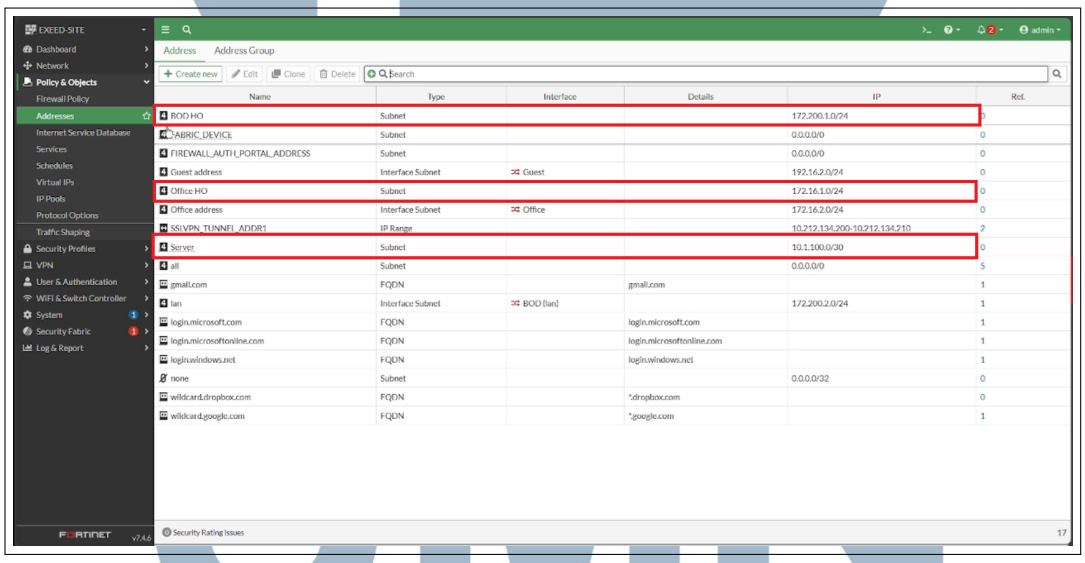
C Implementasi IPsec VPN

Untuk menjawab tantangan keamanan jaringan dan risiko kebocoran data saat berkomunikasi antar kantor, seperti yang telah diuraikan pada Latar Belakang Masalah, maka diimplementasikan koneksi site-to-site IPsec VPN. Teknologi ini dipilih untuk membangun jalur komunikasi yang aman melalui jaringan internet publik yang pada dasarnya tidak aman.

Secara teknis, IPsec bekerja dengan menciptakan sebuah ”terowongan” (tunnel) virtual yang aman antara kantor HO dan kantor SITE. Seluruh paket data yang dikirim melalui jalur ini akan melalui tiga proses keamanan utama:



Gambar 3.4. Addresses SITE pada HO



Gambar 3.5. Addresses HO pada SITE

- **Enkapsulasi:** Paket data asli (misalnya, dari PC di SITE ke server di HO) ”dibungkus” dengan sebuah header IPsec baru, menyembunyikan alamat IP internal yang sesungguhnya.
- **Enkripsi:** Isi dari paket yang telah dibungkus kemudian dienkripsi menggunakan algoritma kriptografi yang kuat. Proses ini memastikan kerahasiaan (confidentiality) data. Jika ada pihak yang berhasil menyadap lalu lintas di tengah jalan, mereka hanya akan melihat data acak yang tidak dapat dibaca.

- **Otentikasi dan Integritas:** IPsec memastikan bahwa data tidak diubah selama transmisi melalui mekanisme pengecekan integritas (integrity). Selain itu, kedua ujung tunnel (FortiGate HO dan SITE) saling melakukan otentikasi menggunakan Preshared Key untuk memastikan bahwa keduanya adalah perangkat yang sah dan terpercaya, bukan penyamar.

Dengan mekanisme ini, implementasi IPsec VPN secara langsung memberikan perlindungan terhadap risiko ”pencurian data” dan ”peretasan”.

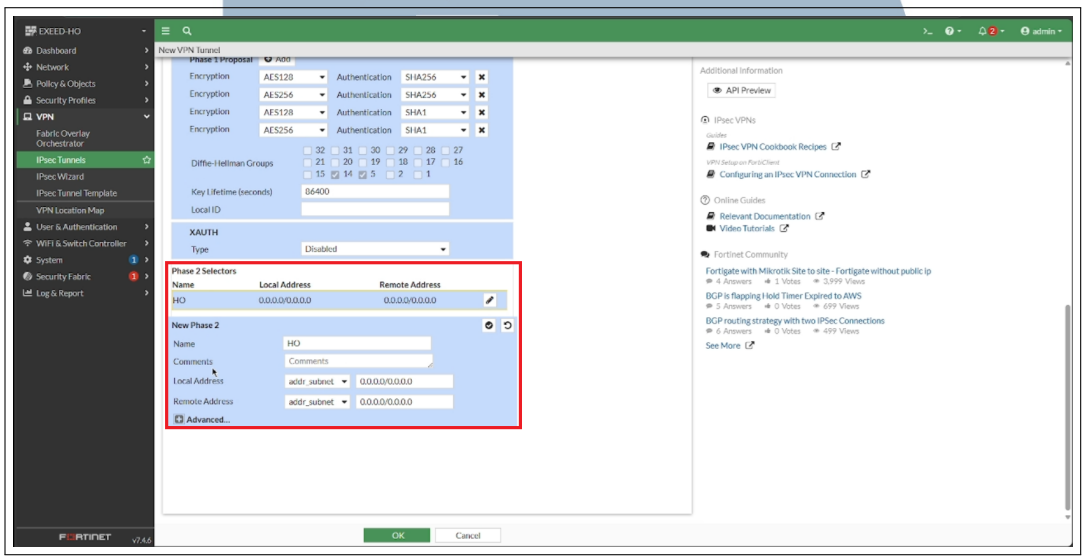
Dalam studi kasus ini, model implementasi yang dipilih adalah Dial-up VPN. Model ini memberikan skalabilitas, di mana FortiGate-HO berperan sebagai server yang siap menerima koneksi dari berbagai cabang, tanpa perlu mengetahui alamat IP publik setiap cabang yang mungkin bersifat dinamis. FortiGate-HO dikonfigurasikan sebagai server, dan FortiGate-SITE sebagai client. Rincian konfigurasi yang telah diterapkan adalah sebagai berikut:

- **Konfigurasi Phase 1 (Otentikasi tunnel):** Untuk memungkinkan HO menerima koneksi dari cabang manapun, Remote Gateway pada FortiGate-HO diatur ke mode Dialup User. Sebaliknya, FortiGate-SITE dikonfigurasi dengan alamat IP publik statis dari HO sebagai Remote Gateway-nya. Proses otentikasi diamankan menggunakan Preshared Key yang identik di kedua sisi. Fitur NAT Traversal (NAT-T) juga diaktifkan untuk memastikan koneksi tetap stabil meskipun SITE berada di belakang perangkat NAT.

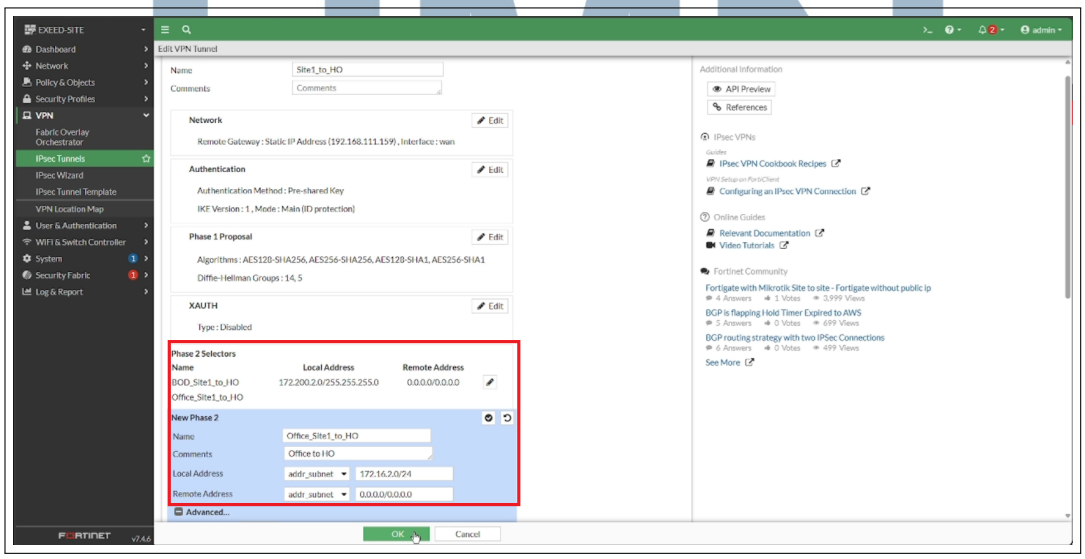
- **Konfigurasi Phase 2 (Seleksi Traffic):** Setelah secure tunnel terbentuk, Phase 2 Selectors mendefinisikan traffic dari mana yang diizinkan untuk dienkripsi. Seperti yang diilustrasikan pada Gambar 3.6 yang menunjukkan konfigurasi selector di FortiGate-HO dan pada Gambar 3.7 yang menunjukkan konfigurasi selector di FortiGate-SITE. Dalam konfigurasi Dial-up ini, pendekatan yang berbeda diterapkan pada HO dan SITE untuk mencapai fleksibilitas dan keamanan.

  Di sisi FortiGate-HO, selector dikonfigurasi dengan 0.0.0.0/0 untuk sumber dan tujuan seperti pada Gambar 3.6. Tujuan dari konfigurasi ini adalah agar HO dapat menerima proposal selector spesifik dari cabang manapun yang terhubung. Nantinya, FortiGate-HO akan secara otomatis menyetujui proposal tersebut dan membangun jalur koneksi (network route) dua arah yang sesuai dengan alamat jaringan yang diajukan oleh SITE.

Di sisi lain, FortiGate-SITE harus dikonfigurasi dengan selector yang spesifik seperti pada Gambar 3.7. Local Address didefinisikan sebagai subnet yang diizinkan dari sisi SITE (yaitu VLAN BOD dan Office), dan Remote Address didefinisikan sebagai subnet tujuan di HO yang perlu diakses. Konfigurasi spesifik pada SITE ini memastikan bahwa hanya traffic yang sah yang akan dinegosiasikan dan dikirim melalui tunnel.



Gambar 3.6. Konfigurasi Phase 2 Selector pada FortiGate-HO

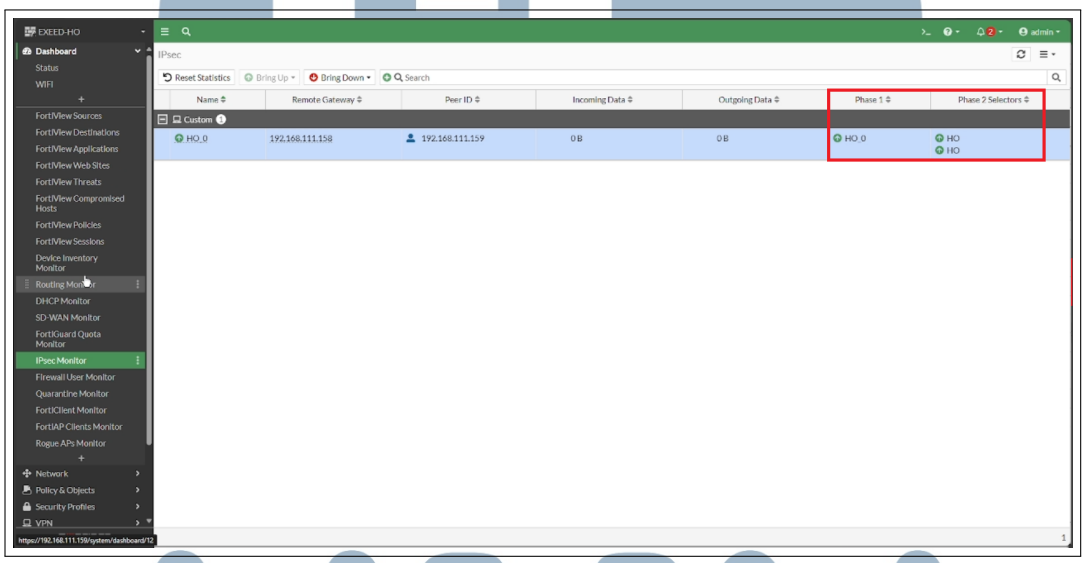


Gambar 3.7. Konfigurasi Phase 2 Selector pada FortiGate-SITE

D Verifikasi Konektivitas Tunnel dan Jalur Routing

Sebelum menerapkan kebijakan keamanan, langkah pertama adalah melakukan verifikasi untuk memastikan koneksi tunnel IPsec telah berhasil dibangun dan jalur perutean (routing path) antar kedua lokasi telah terbentuk dengan benar.

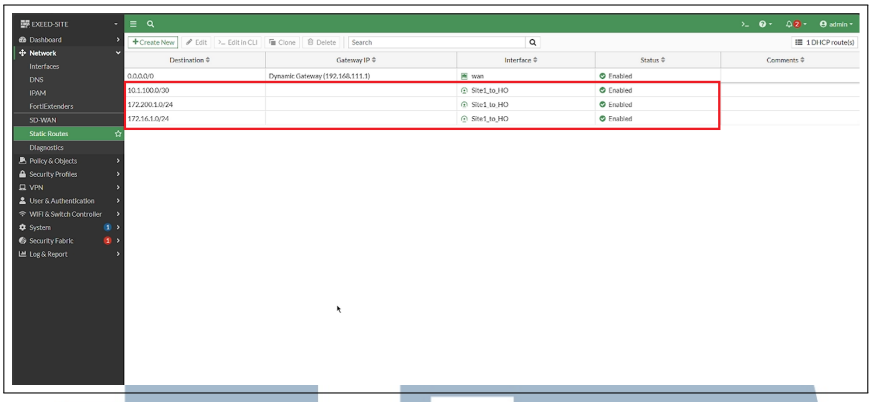
Hasil verifikasi menunjukkan bahwa tunnel IPsec berhasil berada dalam status ”Up”, seperti yang terlihat pada IPsec Monitor di FortiGate-HO pada Gambar 3.8.



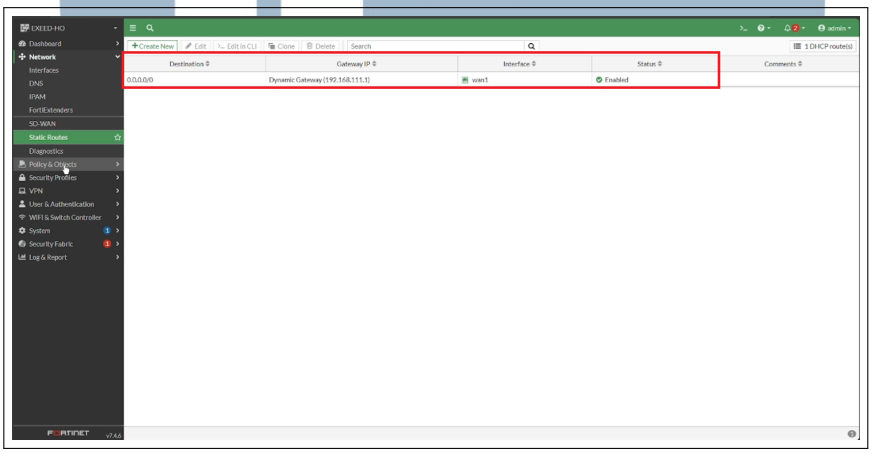
Gambar 3.8. Status Tunnel IPsec dalam Kondisi ”Up” pada Monitor HO

Selanjutnya, verifikasi routing dilakukan. Di sisi FortiGate-SITE, sebuah static route secara eksplisit dikonfigurasikan seperti yang ditunjukkan pada Gambar 3.9. Pada rute ini, kolom destination diisi dengan alamat-alamat subnet yang berada di HO, dan interface keluar yang digunakan adalah interface tunnel IPsec. Hal ini memastikan semua traffic dari SITE yang ditujukan ke HO akan diarahkan melalui jalur VPN.

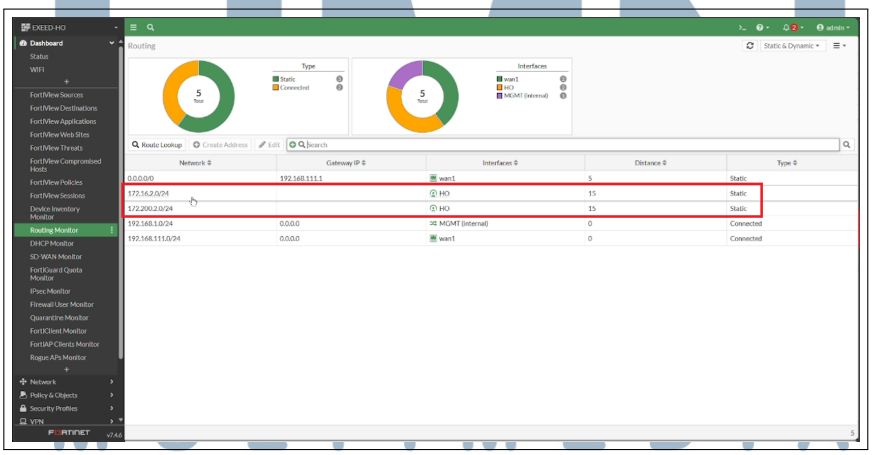
Seperti yang ditunjukkan pada Gambar 3.10 yang memperlihatkan static route di FortiGate-HO, tidak ada rute statis yang dibuat secara manual untuk menuju jaringan SITE. Namun, pada Routing Monitor di Gambar 3.11 membuktikan bahwa rute menuju berbagai subnet di SITE telah terpasang secara otomatis. Hal ini menunjukkan fitur add-route pada konfigurasi Dial-up VPN berfungsi sesuai harapan, di mana HO secara dinamis menerima dan membangun rute dari cabang yang terhubung.



Gambar 3.9. Konfigurasi Static Route pada FortiGate-SITE



Gambar 3.10. Tabel Konfigurasi Static Route pada FortiGate-HO



Gambar 3.11. Routing Monitor di HO yang Menunjukkan Rute Terpasang Otomatis

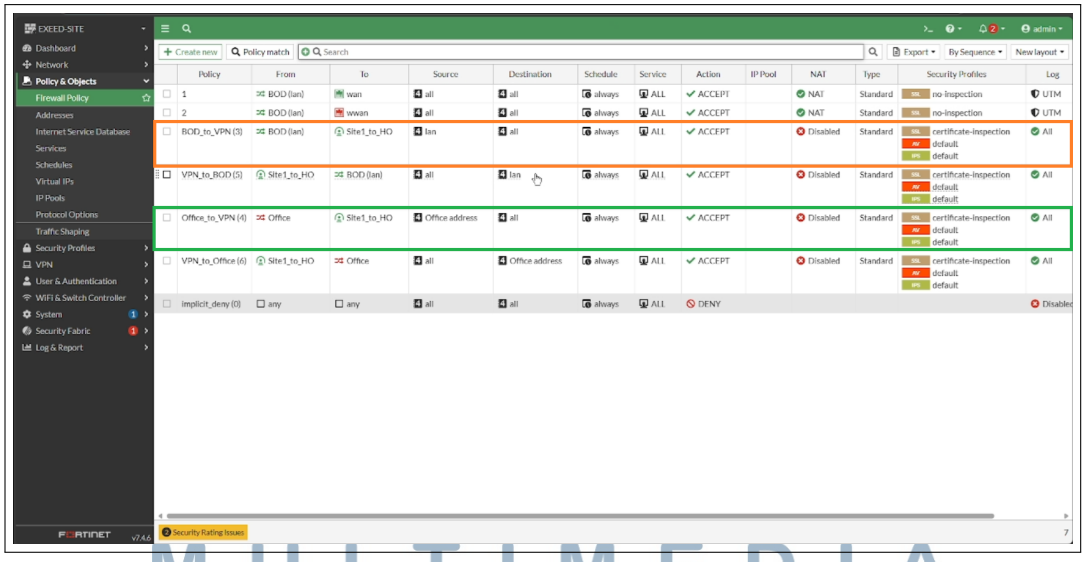
E Implementasi Kebijakan Keamanan dan Kontrol Akses

Berikutnya adalah konfigurasi Firewall Policy yang berfungsi sebagai gerbang kontrol akses. Tanpa adanya kebijakan yang mengizinkan secara eksplisit, semua traffic akan ditolak oleh FortiGate sesuai dengan prinsip implicit deny. Tujuan dari tahap ini adalah untuk mendefinisikan secara eksplisit traffic dari mana saja yang sah dan diizinkan berdasarkan kebutuhan antarjaringan.

E.1 Firewall policy VPN

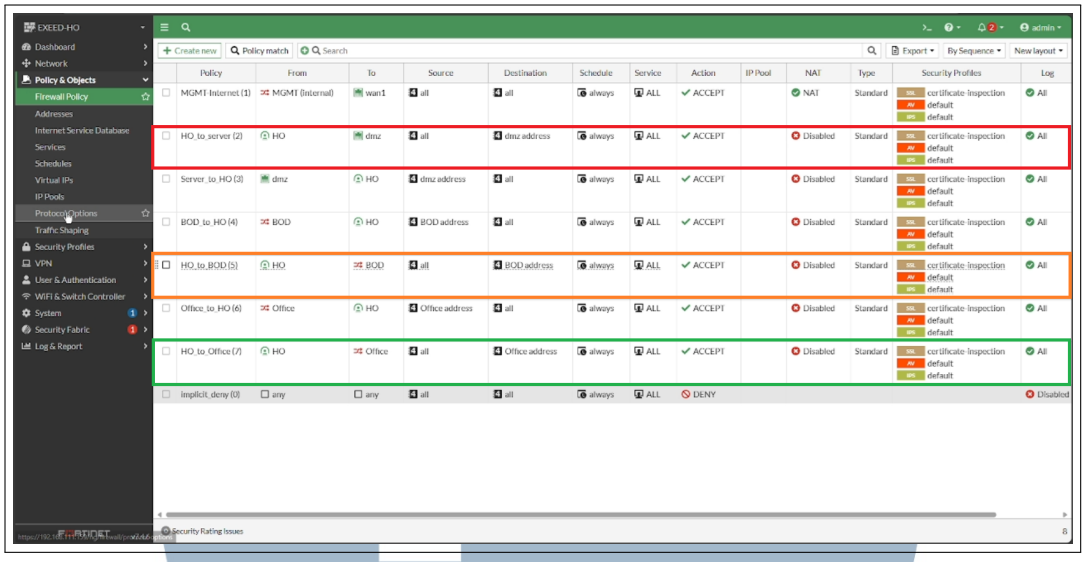
Untuk mengamankan komunikasi dua arah melalui tunnel IPsec, beberapa kebijakan spesifik telah diterapkan. Agar komunikasi berjalan dengan lancar, setiap sisi HO dan SITE memerlukan konfigurasi kebijakan masing-masing yang saling melengkapi.

- **Di FortiGate SITE:** Kebijakan dibuat untuk mengizinkan traffic dari jaringan internal SITE menuju interface IPsec tunnel. Gambar 3.12 menunjukkan konfigurasi firewall policy ini. Sebagai contoh, bagian yang dibatasi dengan warna oranye merupakan aturan yang berasal dari VLAN BOD.



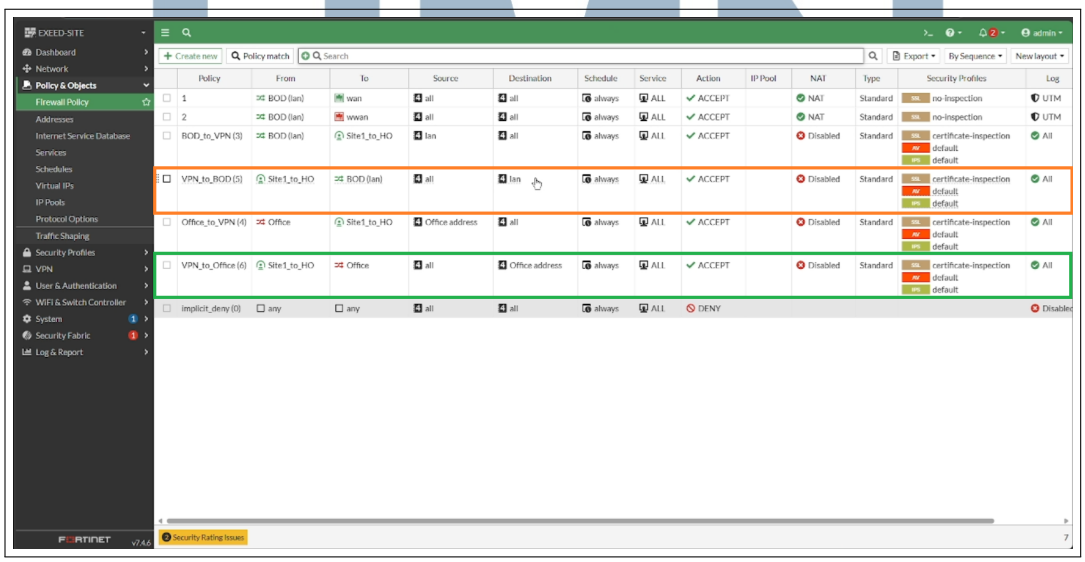
Gambar 3.12. Kebijakan Outgoing di SITE: Mengizinkan traffic ke Tunnel VPN

- **Di FortiGate HO:** Kebijakan incoming dikonfigurasi untuk mengizinkan traffic yang datang dari tunnel masuk ke jaringan internal HO. Seperti ditampilkan pada Gambar 3.13, bagian yang dibatasi dengan warna oranye juga menunjukkan aturan yang mengatur akses menuju VLAN BOD.

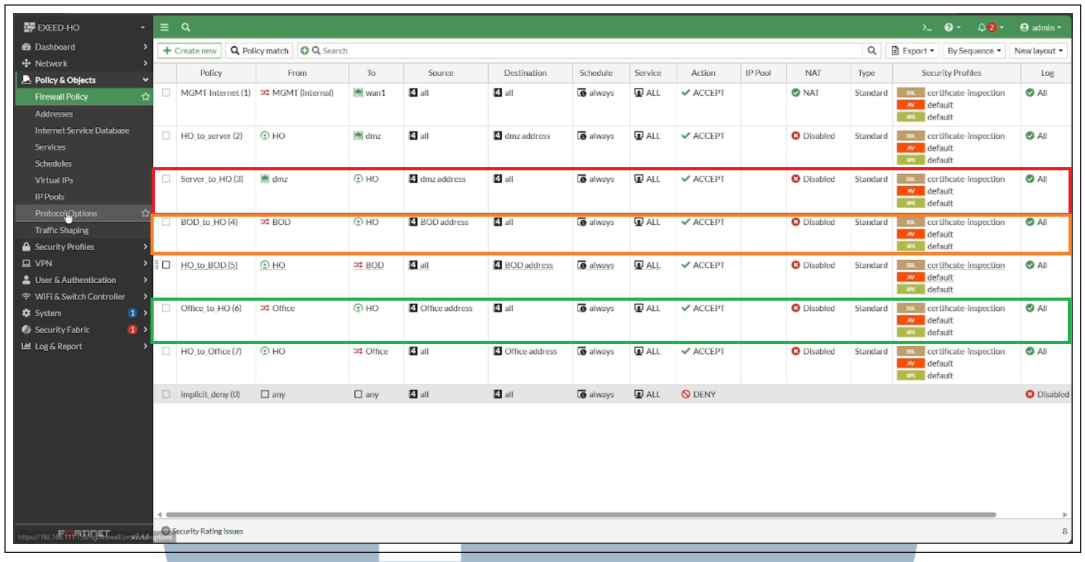


Gambar 3.13. Kebijakan Incoming di HO: Menerima traffic dari Tunnel VPN

Konfigurasi serupa juga diterapkan untuk return traffic (lalu lintas balasan) dari HO ke SITE, sehingga komunikasi dua arah dapat berjalan tanpa hambatan. Gambar 3.14 menunjukkan kebijakan incoming di SITE yang mengizinkan traffic masuk dari tunnel VPN ke jaringan internal, sedangkan Gambar 3.15 memperlihatkan kebijakan outgoing di HO untuk mengizinkan traffic balasan dikirim dari jaringan internal HO ke arah tunnel. Keduanya melengkapi jalur komunikasi dengan arah berlawanan dari dua gambar sebelumnya.



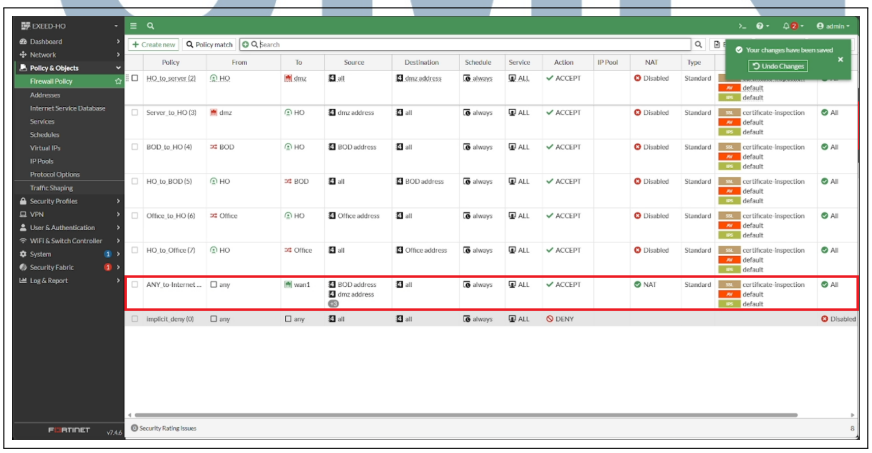
Gambar 3.14. Kebijakan Incoming di SITE: Menerima Traffic Balasan dari Tunnel VPN



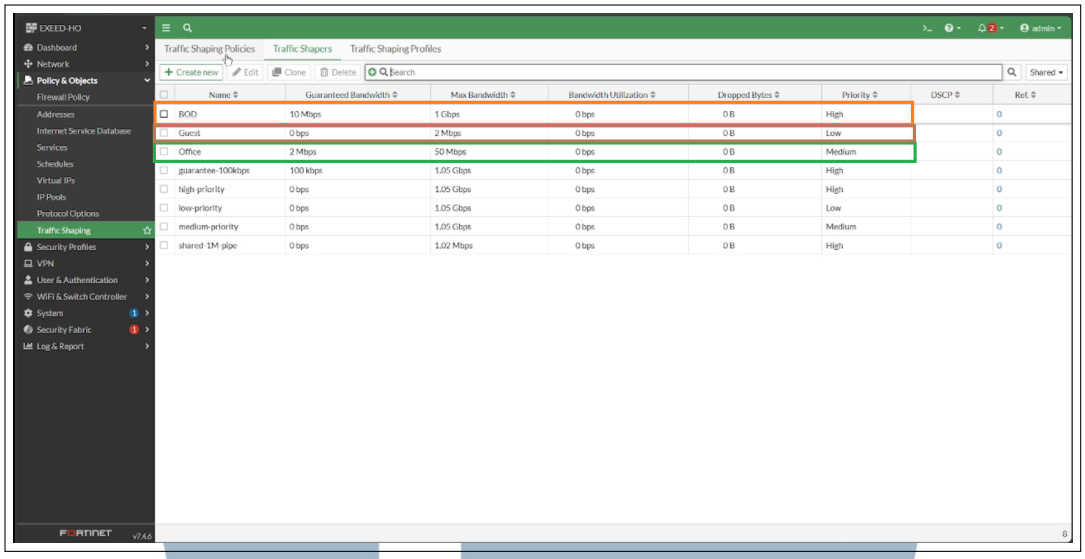
Gambar 3.15. Kebijakan Outgoing di HO: Mengizinkan Traffic Balasan ke Tunnel VPN

E.2 Kebijakan Akses Internet dan Kontrol Bandwidth

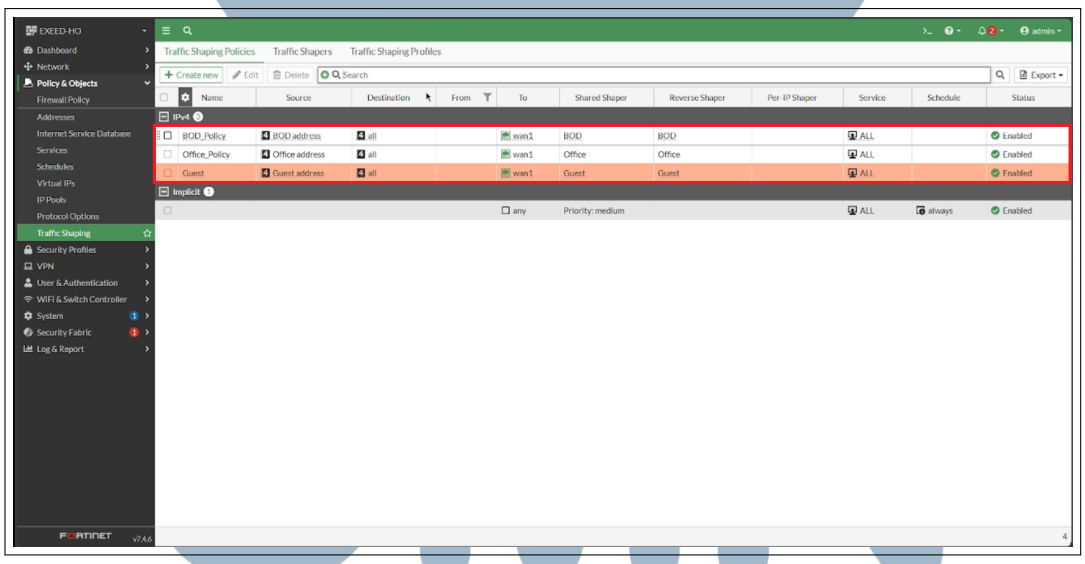
Kebijakan terpisah dibuat untuk mengatur akses pengguna ke internet, yang mengizinkan traffic dari jaringan internal menuju internet seperti yang diilustrasikan pada Gambar 3.16. Untuk membatasi penggunaan bandwidth internet perusahaan dan memastikan alokasi yang sesuai berdasarkan prioritas bisnis, konfigurasi traffic shaping diterapkan. Profil Traffic Shaper yang ditunjukkan pada Gambar 3.17 juga harus dibuat dan diatur untuk menetapkan batas kecepatan minimal dan maksimal koneksi internet (dalam satuan Mbps) bagi masing-masing grup pengguna, yang kemudian diterapkan melalui traffic shaping policies seperti yang ditunjukkan pada Gambar 3.18.



Gambar 3.16. Kebijakan Akses Internet untuk Pengguna



Gambar 3.17. Profil Traffic Shapers untuk Kontrol Bandwidth



Gambar 3.18. Penerapan Traffic Shapers pada Traffic Shaping Policy (Contoh di HO)

F Implementasi dan Verifikasi Fitur Keamanan NGFW

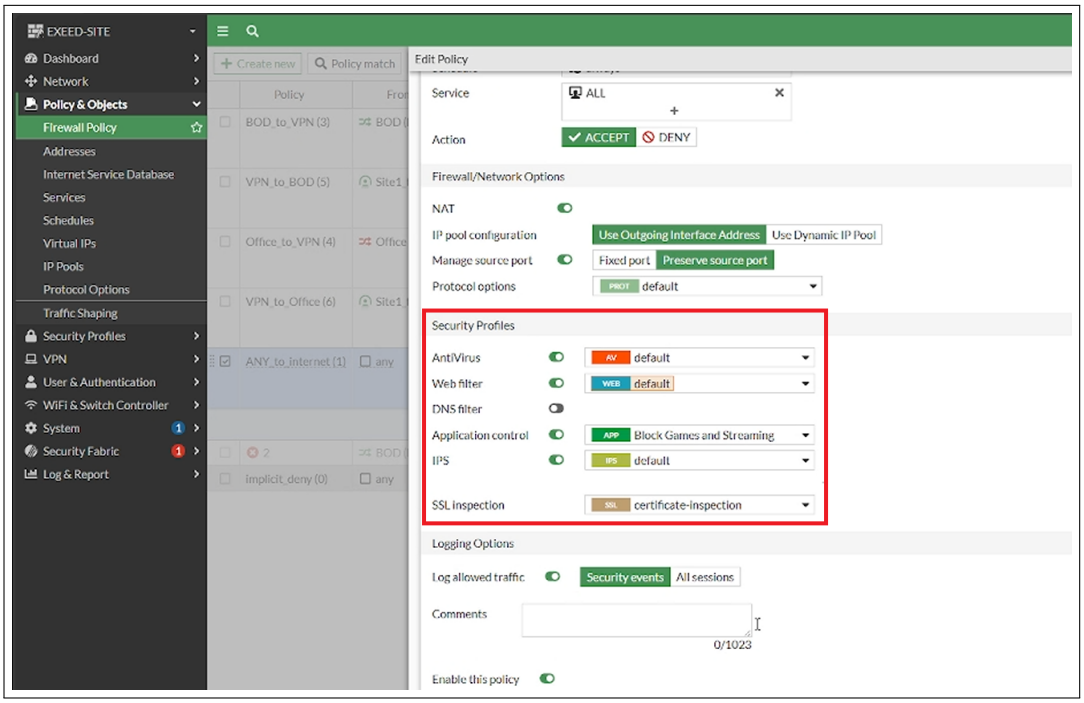
Untuk memberikan perlindungan berlapis terhadap ancaman modern, fitur-fitur Next-Generation Firewall (NGFW) telah diimplementasikan. Mengingat adanya keterbatasan lisensi FortiGuard pada perangkat lab, laporan ini berfokus pada hasil akhir konfigurasi dan verifikasi fungsionalitas dasar dari fitur-fitur yang dapat diuji.

F.1 Aktivasi Security Profiles pada Firewall Policy

Langkah implementasi utama adalah dengan mengaktifkan Security Profiles yang relevan pada Firewall Policy yang mengatur traffic ke internet. Tujuannya adalah untuk mengubah kebijakan dari sekadar mengizinkan atau menolak lalu lintas berdasarkan alamat, menjadi inspeksi keamanan yang mendalam (deep packet inspection).

Setelah profil-profil ini diaktifkan, seperti yang ditunjukkan pada Gambar 3.19, semua paket data yang cocok dengan kebijakan tersebut akan diarahkan ke alamat tujuan. Lalu lintas akan dianalisis berdasarkan aturan pada profil Antivirus, WebFilter, Application Control, dan IPS. Berdasarkan hasil inspeksi, FortiGate akan mengambil tindakan seperti memblokir, mengizinkan, atau hanya memonitor sesuai dengan konfigurasi pada setiap profil.

Untuk memastikan inspeksi ini efektif pada mayoritas lalu lintas web modern yang terenkripsi, fitur SSL/TLS Inspection juga diaktifkan. Langkah ini krusial karena memungkinkan FortiGate untuk melakukan pengecekan lebih ke dalam lalu lintas HTTPS, sehingga fitur keamanan lain dapat bekerja secara maksimal. Penerapan lengkap dari semua profil ini pada satu kebijakan menciptakan sebuah sistem pertahanan berlapis yang sangat komprehensif.



Gambar 3.19. Penerapan Lengkap Security Profiles pada Firewall Policy

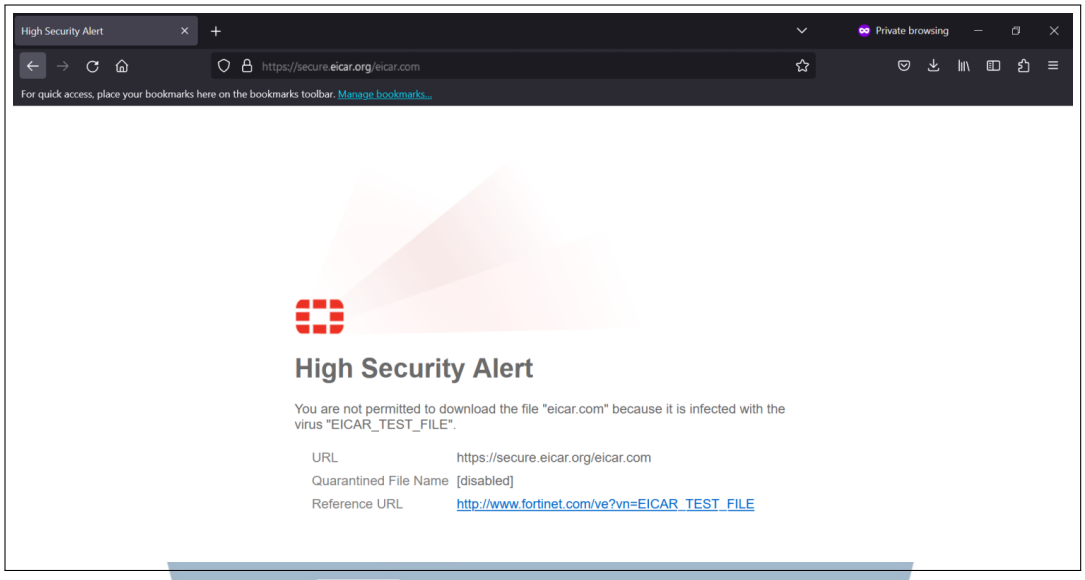
F.2 Hasil Pengujian dan Verifikasi Security Profiles

Verifikasi dilakukan untuk menguji fungsionalitas dari beberapa profil keamanan yang telah diaktifkan.

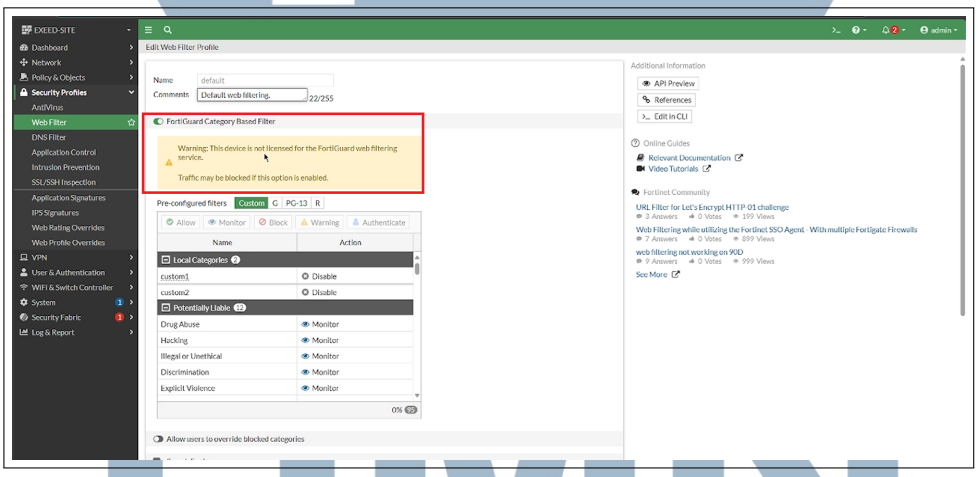
- **Antivirus:** Profil Antivirus telah diaktifkan pada firewall policy. Untuk melakukan verifikasi fungsi AntiVirus, laporan ini merujuk pada pengujian standar yang didokumentasikan secara teknis oleh Fortinet. Pengujian dilakukan dengan mengunduh berkas tes antivirus EICAR. Seperti yang ditunjukkan pada Gambar 3.20 dari dokumentasi teknis, FortiGate berhasil mendeteksi dan memblokir berkas tersebut, yang mengkonfirmasi bahwa modul Antivirus berfungsi sesuai rancangan [6].

- **Web Filter:** Profil Web Filter dikonfigurasi untuk memblokir kategori website tertentu. Gambar 3.21 menunjukkan antarmuka konfigurasi beserta peringatan lisensi yang ada. Oleh karena itu, untuk menunjukkan hasil fungsionalitasnya, laporan ini mengutip dari simulasi yang dilakukan oleh NSE. Hasil pengujian dengan mengakses website yang diblokir ditunjukkan pada Gambar 3.22 yang memperlihatkan bahwa halaman blokir berhasil ditampilkan ketika membuka shopee.co.id [7].

- **Application Control:** Serupa dengan Web Filter, profil Application Control juga telah dikonfigurasi di perangkat lab untuk memblokir signature aplikasi tertentu. Karena kendala yang sama, bukti pemblokiran dikutip dari sumber eksternal. Hasilnya, seperti yang terlihat pada Gambar 3.23, menunjukkan bahwa FortiGate berhasil mengidentifikasi dan memblokir aplikasi whatsapp [7].



Gambar 3.20. Bukti Pemblokiran Berkas Tes Antivirus EICAR

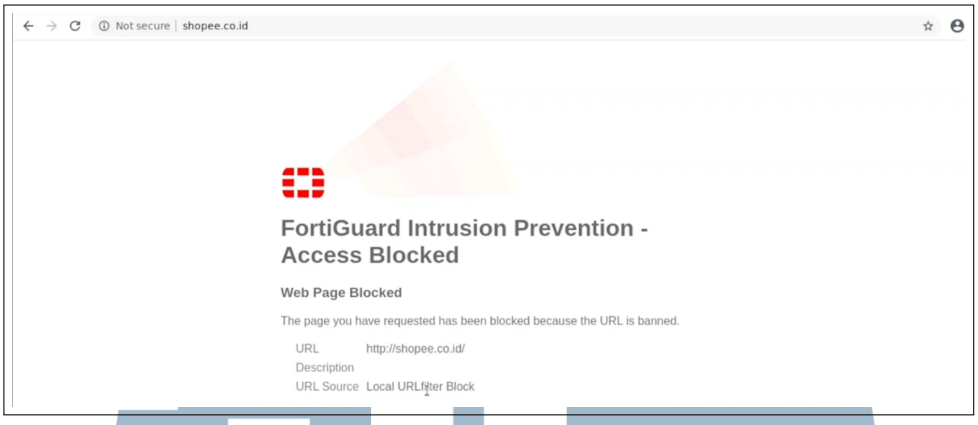


Gambar 3.21. Konfigurasi Profil Web Filter dengan Peringatan Lisensi

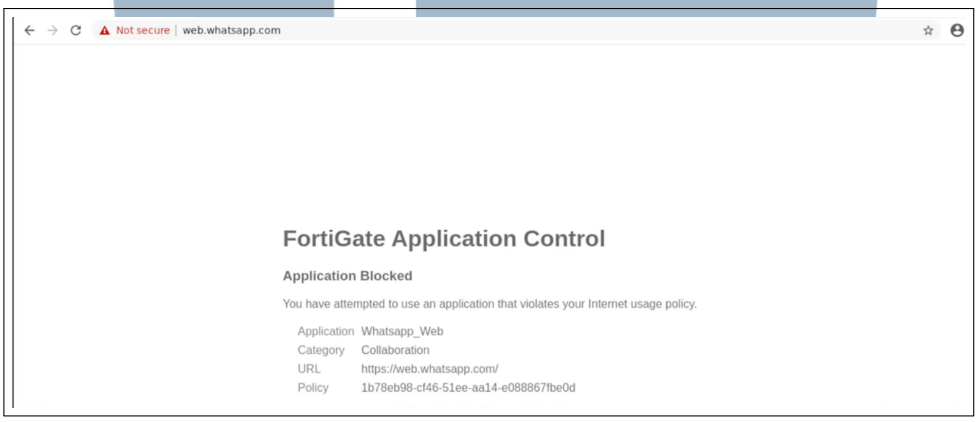
G Verifikasi Fungsionalitas Sistem dan Kebijakan

Sebagai tahap final dari studi kasus, serangkaian pengujian akhir dilakukan untuk memverifikasi bahwa keseluruhan konfigurasi sistem, mulai dari konektivitas dasar hingga penerapan kebijakan, berfungsi sesuai dengan yang diharapkan.

- **Verifikasi Konektivitas End-to-End:** Pengujian konektivitas dasar dilakukan menggunakan utilitas ping dari PC client di SITE subnet Office menuju server dan client di HO. Seperti yang ditunjukkan pada Gambar 3.24 dimana PC pada SITE berhasil melakukan koneksi terhadap server dan pada Gambar 3.25, mencapai client BOD di HO. Hal ini membuktikan bahwa



Gambar 3.22. Hasil Pemblokiran Website oleh Web Filter



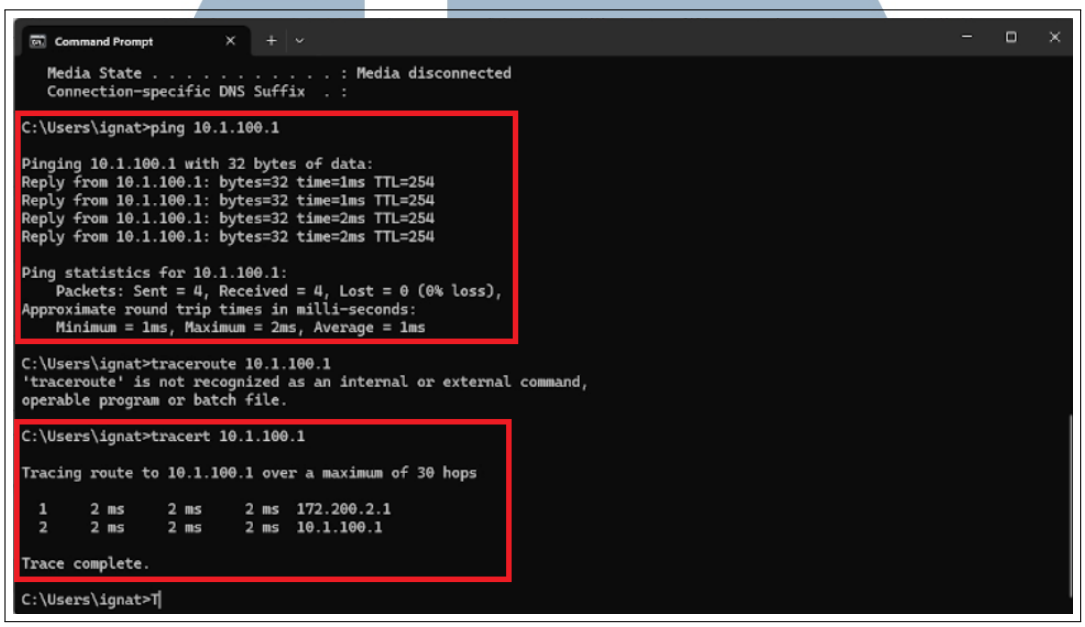
Gambar 3.23. Pemblokiran Web-Application oleh Application Control

konektivitas melalui tunnel IPsec telah berjalan lancar untuk berbagai segmen jaringan.

- **Verifikasi Kontrol Bandwidth:** Pengujian fungsionalitas Traffic Shaping dilakukan dengan menerapkan kebijakan pembatasan bandwidth sebesar 5 Mbps untuk BOD di SITE, disesuaikan dengan keterbatasan bandwidth yang tersedia untuk lingkungan lab. Hasil pengujian kecepatan internet, seperti yang ditunjukkan pada Gambar 3.26, mengkonfirmasi bahwa kecepatan unduh dan unggah berhasil dibatasi mendekati angka 5 Mbps, membuktikan kebijakan shaping berjalan efektif.
- **Verifikasi Traffic pada Log:** Untuk memastikan traffic diproses oleh kebijakan yang benar, pemantauan dilakukan pada Forward Traffic Log di FortiGate. Gambar 3.27 menunjukkan sesi-sesi traffic yang aktif, lengkap dengan informasi sumber, tujuan, dan yang terpenting, ID Kebijakan (Policy

ID) yang menanganinya. Ini memvalidasi bahwa firewall policy yang telah dibuat benar-benar diterapkan pada traffic yang relevan.

Dengan selesainya semua tahap pengujian dan verifikasi ini, implementasi keamanan jaringan dasar untuk menghubungkan kantor cabang dinyatakan berhasil dan berfungsi sesuai dengan rancangan.



Gambar 3.24. Hasil Uji Konektivitas Ping dari SITE ke Server di DMZ HO

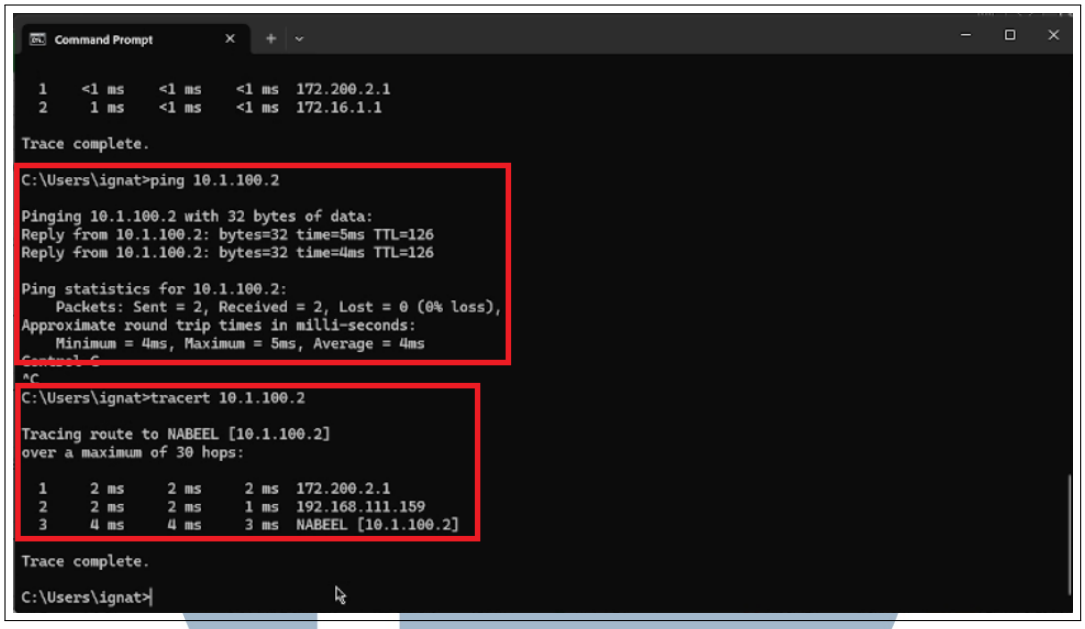
3.4 Kendala dan Solusi yang Ditemukan

3.4.1 Kendala yang Ditemukan

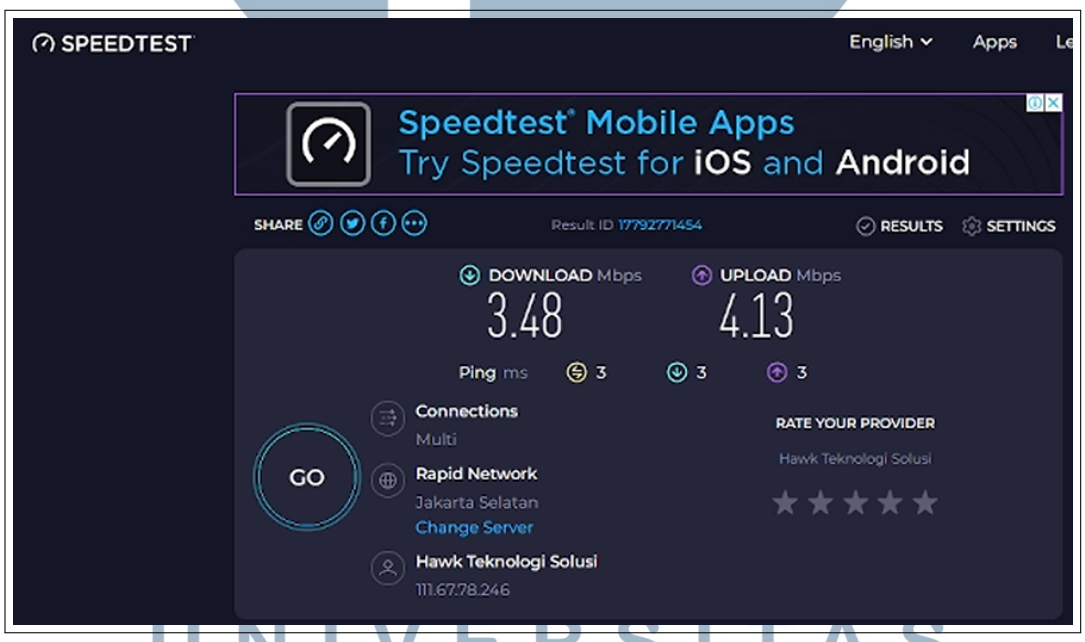
Berdasarkan kegiatan kerja magang pada PT. Exeed Indo Jaya, terdapat beberapa kendala yang ditemukan selama bekerja maupun saat pekerjaan studi kasus (lab). Untuk kendala yang ditemukan selama kerja magang adalah sebagai berikut:

1. Kurangnya pemahanan mendalam mengenai industri network security, pengetahuan jaringan, dan dasar networking.

2. Banyak dokumen laporan yang hanya tersimpan di penyimpanan pribadi masing-masing karyawan dan tidak tersimpan di repositori terpusat seperti Google Drive perusahaan. Hal ini berpotensi tinggi akan terjadinya



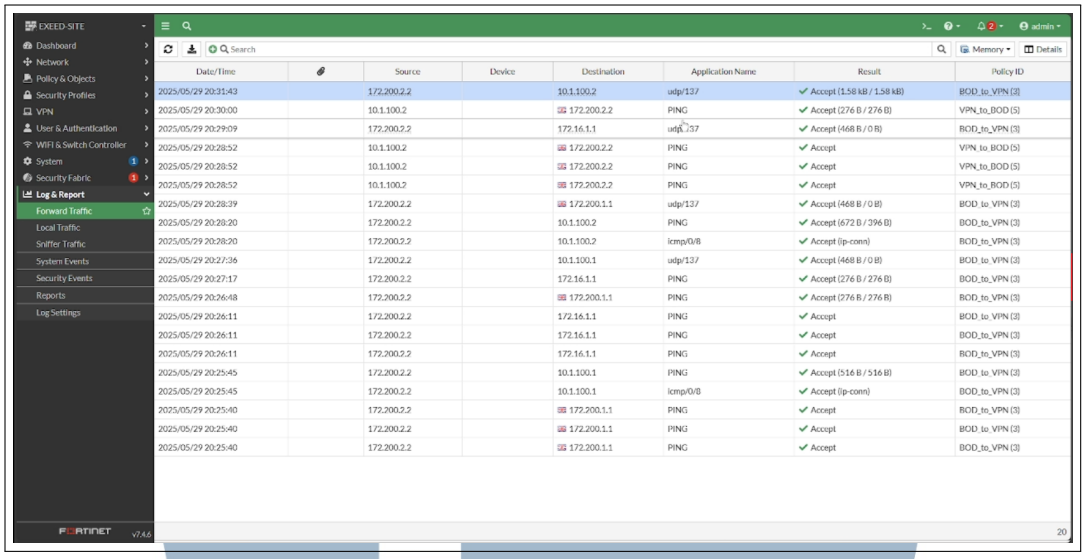
Gambar 3.25. Hasil Uji Konektivitas Ping dari SITE ke Subnet BOD di HO



Gambar 3.26. Hasil Uji Kecepatan dengan Traffic Shaping 5 Mbps

dokumentasi penting hilang dan menghambat proses pencarian referensi dan standardisasi format laporan.

3. Keterbatasan dokumentasi teknis internal yang komprehensif menjadi tantangan dalam proses adaptasi karyawan baru. Hal ini menyebabkan ketergantungan yang tinggi pada pembekalan secara lisan dari staf senior,



Gambar 3.27. Pemantauan Sesi Aktif pada Forward Traffic Log

sehingga berpotensi menyita waktu produktif staf senior dalam penyelesaian tugas utama.

4. Perangkat FortiGate yang digunakan di lingkungan lab memiliki lisensi layanan FortiGuard (seperti Antivirus, Web Filter, dan IPS) yang telah expired. Hal ini menyebabkan fitur-fitur tersebut tidak dapat digunakan dalam studi kasus(lab).

5. Ketersediaan bandwidth internet yang terbatas pada 2 Mbps untuk lingkungan lab menjadi tantangan dalam menunjukkan dampak dari kebijakan traffic shaping secara representatif. Keterbatasan ini membuat perbedaan antara berbagai tingkatan kebijakan (misalnya, antara 1 Mbps dan 1.5 Mbps) sulit untuk diukur dan divalidasi secara akurat.

3.4.2 Solusi yang Ditemukan

Berdasarkan kendala yang telah ditemukan selama kegiatan kerja magang, terdapat beberapa solusi yang telah dilakukan untuk mengatasi kendala yang ada, yaitu:

1. Untuk mengatasi keterbatasan dalam pengetahuan seputar network security dan networking, melakukan pembuatan makalah mengenai perbedaan firewall dan Next-Generation Firewall beserta dengan penjelasan fitur dan coverage fungsi.

2. Melakukan pembelajaran mandiri dan diskusi mengenai ilmu teknis dan juga ikut serta membuat dokumentasi yang lengkap dan komprehensif untuk pembekalan karyawan baru.
3. Melakukan pengusulan untuk pengumpulan dokumen dalam google drive, mengusulkan pembuatan template laporan yang akan disampaikan kepada client dan ikut serta membagikan ilmu untuk pelaporan yang baik terhadap tim.
4. Keterbatasan lisensi untuk fitur keamanan NGFW diatasi dengan menggunakan bukti fungsionalitas dan hasil pengujiannya merujuk pada contoh representatif dari dokumentasi teknis eksternal dengan sitasi yang sesuai.
5. Melakukan adaptasi untuk membatasi traffic shaping sehingga perbedaan bandwidth yang diuji dapat terlihat walaupun tidak signifikan.