#### 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

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,
U	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
N	keberhasilan integrasi simplesamlphp dengan FortiGate, yang
	kemudian hasilnya didokumentasikan dengan membuat instruksi
	instalasi lengkap.
	Lanjut pada halaman berikutnya

Tabel 3.1. Pekerjaan yang dilaksanakan setiap minggu selama periode magang

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
M	berbagai client. Dilakukan juga pembuatan dokumen teknis
	instalasi dan analisis intrusi pada FortiAnalyzer yang hasilnya
N	didokumentasikan. TARA
	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.

		_	
Hardware	Software		Cost
FortiGate 40F	FortiOS v	7.4.6	Rp. 15,9 juta – Rp. 17,2 juta (per bundle
	build2726 (Mat	ure)	dengan lisensi UTM 1 tahun) Lisensi
			UTM Sekitar Rp. 6,2 juta per tahun
FortiGate 60F	FortiOS v	7.4.6	Rp. 20,0 juta - Rp. 25,0 juta (per bundle
	build2726 (Mat	ure)	dengan lisensi UTM 1 tahun) Lisensi
			UTM Sekitar Rp. 9,1 juta – Rp. 10,4 juta
			per tahun

Tabel 3.2. Device Specification and Cost

#### 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.

Dashboard >	[							
Network 🗸	FortiGate 60F INTE	RNAL 4 5 A 8 DMZ WAN1 WAN2						
interfaces 🎲	888							
DNS								
	+ Create New * P Edit	Delete     Marcelante     Integrate     Integrate	rface Search		Q		H	Group By
	Name 🗘	Type \$	Members \$	IP/Netmask 🕆	Administrative Access \$	DHCP Clients \$	DHCP Ranges \$	Re
	🖃 📴 802.3ad Aggregate 1							
tatic Routes Nagnostics	₽• fortilink	₽ 802.3ad Aggregate	🗎 a 🛅 b	Dedicated to FortiSwitch	PING Security Fabric Connection		10.255.1.2-10.255.1.254	2
olicy & Objects	📼 📰 Physical Interface 🕘							
ecurity Profiles > PN >	🖷 dmz	Physical Interface		10.1.100.1/255.255.255.252	PING HTTPS Security Fabric Connection			1
All Switch Controllar	internal5	Physical Interface		0.0.0.0/0.0.0.0				0
ystem 1	🖮 wan1	Physical Interface		192.168.111.159/255.255.255.0	PING HTTPS			1
ecurity Fabric U >	🖷 wan2	Physical Interface	ð	0.0.0.0/0.0.0.0	PING			0
ag or including and	Tunnel Interface 1							
	<ul> <li>NAT interface (naf.root)</li> </ul>	Tunnel Interface		0.0.0.0/0.0.0.0				0
	🖃 🎿 VLAN Switch 🎯							
	⊐⊄ BOD	at VLAN Switch	internal2	172.200.1.1/255.255.255.0	PING HTTPS Security Fabric Connection		172.200.1.2-172.200.1.254	2
	ac Guest	IN VLAN Switch	🗮 internal4	192.16.1.1/255.255.255.0	PING		192.16.1.2-192.16.1.254	2
	⊐# MGMT (internal)	34 VLAN Switch	internal1	192.168.1.99/255.255.255.0	PING HTTPS SSH Security Editor Connection	1	192.168.1.110-192.168.1.210	3
					Secondy Patric Connection			

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

EXEED-SITE •	≡ Q.						>_ @• 42	• \varTheta admin •
Bashboard →     Hetwork →     Interfaces ☆	FortiGate 40F-3G4G LA	N 3 A WAN R R R						
DNS IPAM	+ Create New • PEdit 🐵	Delete 🕨 Integrate Interfac	e Search		Q			Group By Type 💌
Fort/Extenders	Name 🗘	Type \$	Members \$	IP/Netmask \$	Administrative Access \$	DHCP Clients \$	DHCP Ranges \$	Ref. ¢
SD-WAN	🖃 📴 802.3ad Aggregate 🕚							
Static Routes Diagnostics	₽ fortilink	Bo 802.3ad Aggregate	🗎 a	Dedicated to Fort/Switch	PING Security Fabric Connection		10.255.1.2-10.255.1.254	2
💄 Policy & Objects 🔹 🔹	🖃 😅 Hardware Switch 🚳							
Security Profiles  VPN  VPN  User & Authentication	DOD (ian)	34 Hardware Switch	📻 lan1	172.200.2.1/255.255.255.0	PING HTTPS SSH Security Fabric Connection		172.200.2.2·172.200.2.254	4
	🕫 Guest	⊐\$ Hardware Switch	📻 lan3	192.16.2.1/255.255.255.0	PING		192.16.2.2-192.16.2.254	2
System     Security Fabric	24 Office	24 Hardware Switch	😁 lan2	172.16.2.1/255.255.255.0	PING		172.16.2.2-172.16.2.254	2
L≝ Log & Report >	Physical Interface 2							
	🖮 wan	Physical Interface	6	192.168.111.158/255.255.255.0	PING HTTPS			1
	🗎 www.an	Physical Interface		0.0.0.0/0.0.0.0	PING			1
	Tunnel Interface 1							
	NAT interface (naf.root)	Tunnel Interface		0.0.0.0/0.0.0.0				0
FURTIDET V7.4.6	1 Security Rating Issues						10 Update	d: 19:57:00 🛛 -

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:

EXEED-HO -	= Q				>_ 0·	<b>₽0</b> -	\varTheta admin •
Dashboard >	Address Address Group						
✤ Network >	+ Create new / Edit / Clone 🗎 Delete	O Q Search					Q
Policy & Objects	Name	Type	Interface	Details	IP		Ref.
Addresses	BOD address	Interface Subnet	24 BOD		172.200.1.0/24	2	
Internet Service Database	FABRIC DEVICE	Subnet			0.0.0.0/0	0	
Services	FIREWALL AUTH PORTAL ADDRESS	Subnet			0.0.0.0/0	0	
🔄 🔂 🔂	Guest address	Interface Subnet	I Guest		192.16.1.0/24	0	
Virtual IPs	Office address	Interface Subnet	⊐‡ Office		172.16.1.0/24	2	
IP Pools	SSLVPN_TUNNEL_ADDR1	IP Range			10.212.134.200-10.212.134.210	2	
Protocol Options Traffic Shaplog	Site 1 BOD	Subnet			172.200.2.0/24	0	
Security Profiles	Site 1 Office	Subnet			172.16.2.0/24	0	
□ VPN →	all	Subnet			0.0.0.0/0	8	
Luser & Authentication	dmz address	Interface Subnet	😸 dmz		10.1.100.0/30	2	
☆ WiFi & Switch Controller >	gmail.com	FQDN		gmail.com		1	
🗘 System 🚺 >	internal	Interface Subnet	34 MGMT (Internal)		192.168.1.0/24	0	
Security Fabric	login.microsoft.com	FQDN		login.microsoft.com		1	
um Log & Report	login.microsoftonline.com	FQDN		login.microsoftonline.com		1	
	In Ingin.windows.net	FQDN		login.windows.net		1	
	Ø none	Subnet			0.0.0.0/32	0	
	wildcard.dropbox.com	FQDN		*.dropbax.com		0	
	wildcard.google.com	FQDN		*.google.com		1	
	Security Rating Issues						18

Gambar 3.4. Addresses SITE pada HO

EXEED-SITE -	≡ Q				>_ 0•	<b>↓2 - ⊖</b> admin -
Dashboard	Address Address Group					
+ Network	+ Create new Clone A Delete	Q Bearch				Q
Policy & Objects 🗸	Name	Tuno	Interface	Datalle	ID	Pof
Addresses		Subnat	interiese	Details	172 200 1 0/24	No.
Internet Service Database		Subnet			0.0.0.0/0	0
Services	EIREWALL AUTH PORTAL ADDRESS	Subnet			0.0.0.0/0	0
Schedules	Guest address	Interface Subnet	24 Guest		192.16.2.0/24	0
Virtual IPs	Office HO	Subnet			172.16.1.0/24	0
IP Pools	Office address	Interface Subnet	34 Office		172.16.2.0/24	0
Traffic Shaping	SSLVPN_TUNNEL_ADDR1	IP Range			10.212.134.200-10.212.134.210	2
A Security Profiles →	Server	Subnet			10.1.100.0/30	0
⊒ VPN →	🖬 all	Subnet			0.0.0/0	5
♣ User & Authentication >	😐 gmail.com	FQDN		gmail.com		1
☆ WiFi & Switch Controller >	🖸 lan	Interface Subnet	pr BOD (lan)		172.200.2.0/24	1
System     System     Security Exterio	Iogin.microsoft.com	FQDN		login.microsoft.com		1
M Los & Report	Iogin.microsoftonline.com	FQDN		login.microsoftonline.com		1
	Iogin.windows.net	FQDN		login.windows.net		1
	Ø none	Subnet			0.0.0/32	0
	wildcard.dropbox.com	FQDN		*.dropbox.com		0
	wildcard.google.com	FQDN		".google.com		1
	Security Rating Issues					17
47.40						

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.

EXEED-HO -	≡ Q.					_	-	≻. Q A.2 Oradmit
a Dashboard >	New VPN Tunnel	<b>D</b> 000						
be beautoputs         Activation         Activ	Phase 1 Pr Encryption Encryption Encryption Diffie-Hell Key Lifetin Local ID XAUTH Type	According to the second	32 21 15 Ø B6400	Authentication Authentication Authentication Authentication 31 30 30 20 19 1 14 2 5	SHA256 SHA256 SHA1 SHA1 27 28 18 17 2 1	27 16	× × ×	Additional information Additional information API Preview in IPsec VPNs Gains Preve VPN Control Redges [2] With Sequen Precident Configure in IPsec VPN Connection [2] Ordina Gaides Relevant Documentation [2] Video Tartiset [2] • Tortiset Community
Security Fabric	Phase 2 Selecto	rs Local Ad	dress	Rem	ote Address			Fortigate with Mikrotik Site to site - Fortigate without public ip # 4 Answers # 1 Votes # 3,999 Views
🖃 Log & Report 🔹 🔹	но	0.0.0.0/0	.0.0.0	0.0.	0.0/0.0.0.0		1	BGP is flapping Hold Timer Expired to AWS S Answers      + 0 Votes      + 69 Views
	New Phase 2 Name Comments Local Address Remote Address Remote Address	H G S A	IO Comments ddr_subnet	<ul> <li>■ 0.0.0.0.0.0</li> <li>■ 0.0.0.0.0.0</li> </ul>	10.0		0	BCP routing strategy with the vol BSec Connections # 6 A revew See More (2* See More (2*
				c	к	Cano	cel	

Gambar 3.6. Konfigurasi Phase 2 Selector pada FortiGate-HO

Image: Dashboard     Edit Vin       Image: Dashboard     Common Vin	Q PN Tunnel						
Orchestrator Presc Turnel Complete Proce VUsrid Proce VUsrid Proce Content Map VVRI Content Map ♥ Writ IS Anktic Controler ♥ Security Tahris ♥ Security Tahris ■ Security Tahr	me menuestis Network Remote Guteway: Static Authentication Authentication Authentication Method: ICT Version: 1, Mode: M Plane 1 Proposal Magnithms: ACS120-SH Ditthe-Inflamma Groups: 1 XAUTH Mype: Disabled prop. Stat.p.10 2 Version 2 Methods Method	Site1_to_HO           Comments           IP Address (192.168.111.159), I           Pre-shared Key           tain (ID protection)           A256, AC5256-51 (A256, AC5120           Local Address           Coloc., Site1_to_HO           Office, Site1_to_HO           Office, Site1_to_HO	Interface; wan	Edit     Edit     Edit     Edit	Additional information Additional information Provider References All Provider Pr	0- 42- 9	dmin •
	mote Address Advanced	addr_subnet • 0.0.0,0/0.0.0	0.0	d			

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.

REED-SITE	- = Q				
Dashboard	+ Create New / Edit >_ Edit in CLI	Te Clone B Delete Search	٩		III 1DHCP route(s)
Network	✓ Destination ₽	Gateway IP ©	Interface ©	Status ©	Comments ©
Interfaces	0.0.0.0/0	Dynamic Gateway (192,168,111,1)	The war	C Enabled	
IPAM	10.1.100.0/30		③ Site1_to_HO	Enabled	1
	172.200.1.0/24		③ Site1_to_HO	C Enabled	
	172.16.1.0/24		③ Site1_to_HO	C Enabled	
	\$				-
🕭 Policy & Objects	•				
Security Profiles	•				
Q VPN	•				
▲ User & Authentication					
<ul> <li>Will a Switch Controller</li> <li>Controller</li> </ul>					
Security Fabric					
Let Log & Report					
		۲.			





Gambar 3.10. Tabel Konfigurasi Static Route pada FortiGate-HO

	≣ α,				≻_ 0• 4 <b>0•</b> elad
ward ~	Routing				C Static & Dynamic *
r					
		Type	Interfaces		
+		Granected O	HO 0		
Aew Sources			5 Total		
flew Destinations					
/lew Applications					
New Web Sites	Q. Route Lookup O. Create Address	2 Edit 0 9 Bearch			
new Inreats					
ewcompromiseu	Network #	Gateway IP #	Interfaces #	Distance #	Type #
ew Policies	0.0.0.0/0	192.168.111.1	🗮 wan1	5	Static
ew Sessions	172.16.2.0/24		⊕ H0	15	Static
Inventory	172.200.2.0/24		⊕ H0	15	Static
t Modilar I	192.168.1.0/24	0.0.0.0	24 MGMT (Internal)	0	Connected
Meelior	192.168.111.0/24	0.0.0.0	🗮 want	0	Connected
AN Monitor					
ward Onota					
Suard Quota or					
ward Quota or Monitor					
ivard Quota or Monitor all User Monitor					
uard Quota or Honitor III User Monitor ntine Monitor					
uard Quota of Monitor ill User Monitor ntine Monitor Hent Monitor					
eard Quota or Monitor all User Monitor ntine Monitor Hent Monitor P Clients Monitor					
euerd Quota or Monitor all User Monitor ntine Monitor Hent Monitor P Clients Monitor APs Monitor					
aard Quota X denitor III User Monitor nthe Monitor Bent Menitor P Clients Monitor APs Monitor +					
Juard Quota or Monitor all User Monitor intine Monitor Allent Monitor ₽ Clensts Monitor et APs Monitor + erk ≯					
Juard Quota Jord Quota Ior Monitor antine Monitor antine Monitor 2 Clents Monitor e APS Monitor e APS Monitor e APS Monitor e APS Clents Monitor					

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.

🖙 exeed-site 🔹	≡	۹											>_ 0· 40·	⊖ admin •
Dashboard	+	Create new Q Pe	olicy match OQ	Search								Q	Export • By Sequence •	iew layout 🝷
Network      Network      Network      Network		Policy	From	То	Source	Destination	Schedule	Service	Action	IP Pool	NAT	Туре	Security Profiles	Log
Firewall Policy		1	⊐⊄ BOD (lan)	🖮 wan	4 all	🛃 all	lo always	🖸 ALL	✓ ACCEPT		🔿 NAT	Standard	sa. no-inspection	UTM
Addresses		2	=# BOD (lan)	🗮 wwan	4 all	🛃 all	6 always	ALL ALL	✓ ACCEPT		🖉 NAT	Standard	ss. no-inspection	UTM
Internet Service Database Services		BOD_to_VPN (3)	54 BOD (lan)	Site1_to_HO	🛃 lan	🔄 all	🚺 always	😡 ALL	✓ ACCEPT		Oisabled	Standard	ss. certificate-inspection // default is default	S VII
Virtual IPs IP Pools		VPN_to_BOD (5)	Site1_to_HO     Site1	⊐⊄ BOD (lan)	all all	🖬 lan 🔥	lo always	😡 ALL	✓ ACCEPT		Oisabled	Standard	ss. certificate-inspection default is default	S VI
Protocol Options Traffic Shaping Security Profiler		Office_to_VPN (4)	24 Office	Site1_to_HO	Office address	4 all	lo always	😡 ALL	✓ ACCEPT		Oisabled	Standard	se certificate-Inspection // default is default	Ø All
User & Authentication		VPN_to_Office (6)	Site1_to_HO	⊐⊄ Office	🔁 all	Office address	🚺 always	😨 ALL	✓ ACCEPT		Oisabled	Standard	ss. certificate-inspection /// default us default	Ø All
		implicit_deny (0)	any any	any any	4 all	🛃 ali	lo always	ALL ALL	O DENY					O Disabled
© System (														
ENPTIOET	0	Security Rating Issues												▶
V7.4.6					-					-				

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.

etwork >	+	Create new Q Pol	icy match O Q Searc	h								Q	Export • By Sequence •	New layou
		Policy	From	То	Source	Destination	Schedule	Service	Action	IP Pool	NAT	Type	Security Profiles	Lo
blicy & Objects 오이지 아이지 않는 아이지 않는 아이지 않는 아이지 않 아이지 않는 아이지 않 아이지 않는 아이지 않는 아이지 않는 아이지 않는		MGMT-Internet (1)	⊐ MGMT (internal)	i wan1	🛃 all	🖾 all	. always	😨 ALL	✓ ACCEPT		🖉 NAT	Standard	xx         certificate-inspection           xv         default           usi         default	🔊 Ali
ternet Service Database rvices hedules		HO_to_server (2)	@ но	🕅 dmz	🛃 all	4 dmz address	👩 always	😰 ALL	✓ ACCEPT		Oisabled	Standard	certificate-inspection  default  default	O AI
tual IPs Pools		Server_to_HO (3)	🗯 dmz	⊕ HO	dmz address	🖾 all	. always	😰 ALL	✓ ACCEPT		Oisabled	Standard	certificate-inspection  default  default	S AI
itocoyOptions 合 ffic Shaping surity Profiles >		BOD_to_HO (4)	⊐≭ BOD	⊕ но	BOD address	🖸 all	. always	🕢 ALL	✓ ACCEPT		O Disabled	Standard	certificate-inspection     default     default	O AI
& Authentication		HO_to_BOD (5)	<u>© но</u>	⊐4 BOD	🖸 all	BOD address	. always	😨 ALL	✓ ACCEPT		O Disabled	Standard	certificate-inspection     default     default	<b>O</b> A
n (1) tyFabric (1)		Office_to_HO (6)	⊐⊄ Office	. но	Office address	🛃 all	. always	😨 ALL	✓ ACCEPT		O Disabled	Standard	certificate-inspection     default     default	🔊 Al
Report >		HO_to_Office (7)	⊡ но	⊐‡ Office	🛃 all	Office address	. always	😨 ALL	✓ ACCEPT		O Disabled	Standard	certificate-inspection     default     default	<b>O</b> A
		implicit_deny (0)	🗆 any	any	🛃 all	🛃 all	lo always	ALL ALL	O DENY					O D

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.

EXEED-SITE •	Ξ	۹											>_ 0 - 40-	⊖ admin +
Dashboard >	+	Create new Q P	olicy match	Search								Q [	Export • By Sequence •	New layout •
Network     Network		Policy	From	То	Source	Destination	Schedule	Service	Action	IP Pool	NAT	Туре	Security Profiles	Log
Firewall Policy		1	=# BOD (lan)	🖮 wan	🖪 all	🛃 all	G always	🕢 ALL	✓ ACCEPT		🖉 NAT	Standard	ss. no-inspection	<b>©</b> UTM
Addresses		2	⊐⊄ BOD (lan)	🗮 wwan	🖸 all	🛃 all	lo always	ALL ALL	✓ ACCEPT		Ø NAT	Standard	ss. no-inspection	O UTM
Internet Service Database		BOD_to_VPN (3)	od BOD (lan)	Site1_to_HO	4 Ian	🛃 all	6 always	👿 ALL	✓ ACCEPT		Oisabled	Standard	ss. certificate-inspection	🗢 All
Services													Av default us default	
Schedules		VPN to BOD (5)	Site1 to HO	⊐⊈ BOD (lan)	<b>5</b> all	El ian o	G always	ALL.	✓ ACCEPT		O Disabled	Standard	ss. certificate-inspection	🖸 All
Virtual IPs													M default	
Protocol Options		000	nt 0/0	0.0000	E otto da	<b>n</b>	<b>R</b>	<b>F1</b>	ALCOURT	_	O Disabled	Charles	es default	
Traffic Shaping		Office_to_VPN (4)	J4 Office	(1) Site1_to_HO	<ul> <li>Ornce address</li> </ul>	E au	UG anways	D VII	✓ ACCEPT		Uisabled	Standard	default	O All
Security Profiles												_	us default	_
□ VPN →		VPN_to_Office (6)	Site1_to_HO	⊐4 Office	4 all	4 Office address	lo always	ALL ALL	✓ ACCEPT		Oisabled	Standard	certificate-inspection	S VII
Luser & Authentication													default	
		implicit_deny (0)	🗆 any	🗆 any	4 ali	🛃 all	6 always	🕢 ALL	O DENY					O Disablec
System 1 >														
Let Log & Report														
	4 0													Þ
	0	Security Rating Issues												7

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

EXEED-HO	- =	۹											≻_ 0· 4 <b>2</b> ·	\rm 9 admin -
Dashboard	° (+	Create new Q Pol	icy match	h								Q	By Sequence •	New layout •
Motwork	°.	Policy	From	То	Source	Destination	Schedule	Service	Action	IP Pool	NAT	Туре	Security Profiles	Log
Firewall Policy Addresses	\$	MGMT-Internet (1)	X MGMT (internal)	🕅 wan1	🖾 all	🛃 all	. atways	🕢 ALL	✓ ACCEPT		🛇 NAT	Standard	certificate-inspection default default	🛛 Ali
Internet Service Database Services Schedules		HO_to_server (2)	⊡ но	i drnz	🖸 all	dmz address	🐻 always	🕢 ALL	✓ ACCEPT		O Disabled	Standard	certificate-inspection default default	Ø All
Virtual IPs IP Pools	-	Server_to_HO (3)	🖮 dmz	⊕ но	dmz address	🛃 all	. atways	🕢 ALL	✓ ACCEPT		Oisabled	Standard	certificate-inspection  default  default	S All
Protocol Options Traffic Shaping Security Profiles	☆ >	BOD_to_HO (4)	⊐⊄ BOD	. но	BOD address	🛃 all	🚺 always	😰 ALL	✓ ACCEPT		O Disabled	Standard	certificate-inspection     default     default	Ø All
User & Authentication	> = = >	HO_to_BOD (5)	<u>© но</u>	⊐‡ BOD	🖸 all	BOD address	. always	😱 ALL	✓ ACCEPT		O Disabled	Standard	certificate inspection  default  default	Ø All
System 1	,	Office_to_HO (6)	⊐‡ Office	€ HO	Office address	🛃 all	to always	🕢 ALL	✓ ACCEPT		Oisabled	Standard	certificate-inspection default default	Ø All
f Log & Report	<b>`</b>	HO_to_Office (7)	⊡ но	office	🛃 all	Office address	to always	🕢 ALL	✓ ACCEPT		O Disabled	Standard	certificate-inspection default default	Ø All
		implicit_deny (0)	any any	any	🛃 all	🛃 all	. always	ALL ALL	O DENY					O Disable
	4.0							_		_		_		
ps://192.1dE	46.0	Security Rating Issues												

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.

Note of Capacity     Note of Capacity <th>de Manuala</th> <th>Č.</th> <th>+ (</th> <th>Create new Q Po</th> <th>licy match O Q \$ea</th> <th>rch</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>Q</th> <th>Your changes have been seen and the second secon</th> <th>nsawed</th>	de Manuala	Č.	+ (	Create new Q Po	licy match O Q \$ea	rch								Q	Your changes have been seen and the second secon	nsawed
Construction         Construction<	Policy & Objects	, v		Policy	From	То	Source	Destination	Schedule	Service	Action	IP Pool	NAT	Type	Cundo Changes	
binner Growing     is foreigned binner     is foreigned binner </td <td>Firewall Policy Addresses</td> <td>ŵ</td> <td></td> <td>HQ_to_serves (2)</td> <td><u>⊕ HQ</u></td> <td>🕅 dmz</td> <td>al al</td> <td>dmz.address</td> <td>always</td> <td>🖳 ALL</td> <td>✓ ACCEPT</td> <td></td> <td>O Disabled</td> <td>Standard</td> <td>// default</td> <td></td>	Firewall Policy Addresses	ŵ		HQ_to_serves (2)	<u>⊕ HQ</u>	🕅 dmz	al al	dmz.address	always	🖳 ALL	✓ ACCEPT		O Disabled	Standard	// default	
Vinue (%)         DOD, 0x 10/10         2000         (%)         Disclosion	Internet Service Database Services Schedules	•		Server_to_HO (3)	🗯 dmz	@ HO	dmz address	<b>2</b> all	. always	😰 ALL	✓ ACCEPT		O Disabled	Standard	certificate-inspection     ///     default     default	Ø Al
MICRODOPUID         IN Display         IN Display <thin display<="" th="">         IN Display         IN Disp</thin>				BOD_to_HO (4)	34 BOD	@ HO	BOD address	all all	l i always	🕢 ALL	✓ ACCEPT		O Disabled	Standard	<ul> <li>certificate-inspection</li> <li>default</li> <li>default</li> </ul>	S Al
UNN         Others (b / 10 / 10 / 10 / 10 / 10 / 10 / 10 / 1	Traffic Shaping Security Profiles	,		HO_to_BOD (5)	⊙ но	34 BOD	<b>13</b> at	BOD address	. always	😨 ALL	✓ ACCEPT		O Disabled	Standard	xx. certificate-inspection x default es default	O AI
System         Image: Description (Control (Contro) (Contro)(Control (Control (Contro) (Control (Control (Contro) (	VPN User & Authentication WEI & Switch Controller	> >		Office_to_HO (6)	of Office	⊕ HO	Office address	E all	. always	🕢 ALL	✓ ACCEPT		O Disabled	Standard	certificate-inspection default default	🕲 Ali
Log & Report ANY to Internet any Mission 1 B RDD address 1 all a ANY to Internet any Mission 1 B RDD address 1 all ANY to Internet any CEPT I NATI Standard The restlicate insertion	System Security Fabric	1) (1) (1)		HO_to_Office (7)	⊕ но	34 Office	🖬 all	Office address	Co always	🕢 ALL	✓ ACCEPT		O Disabled	Standard	ss certificate-inspection default default	S All
definit     definit     definit     definit		,	•	ANY_to-Internet	🗆 any	M wan1	<ul> <li>BOD address</li> <li>dmz address</li> </ul>	<b>2</b> all	l always	😨 ALL	✓ ACCEPT		🔊 NAT	Standard	certificate-inspection default default	S Al
□ implicit,deny(0) □ any □ any □ at ■ atl				implicit_deny(0)	🗆 any	any arry	<b>2</b> at	all all	l always	ALL ALL	O DENY					O Disabi

Gambar 3.16. Kebijakan Akses Internet untuk Pengguna

21 Implementasi dan konfigurasi..., Ignatius Steven, Universitas Multimedia Nusantara

EXEED-HO	- = c	ι						>_ @ · 48	• 🛛 admin •
Dashboard	> Traffic	Shaping Policies Tra	ffic Shapers Traffic Shaping Profi	les					
+ Network		ata annu an Cata	Classe Delate 00 Kessel						O Shurd -
Policy & Objects	~ + CR	are new a cont							Silared •
Firewall Policy		Name \$	Guaranteed Bandwidth \$	Max Bandwidth \$	Bandwidth Utilization 🖨	Dropped Bytes \$	Priority \$	DSCP \$	Ref. ≑
Addresses	D BC	D	10 Mbps	1 Gbps	0 bps	0 B	High		0
Internet Service Database	Gu	est	0 bps	2 Mbps	0 bps	0 B	Low		0
	Of	fice	2 Mbps	50 Mbps	0 bps	0 B	Medium		0
Schedules	🗆 gu	arantee-100kbps	100 kbps	1.05 Gbps	0 bps	0 B	High		0
IP Poole	🗆 hig	h-priority	0 bps	1.05 Gbps	0 bps	0 B	High		0
Protocol Options		-priority	0 bps	1.05 Gbps	0 bps	0 B	Low		0
Traffic Shaping	🕁 🗆 me	dium-priority	0 bps	1.05 Gbps	0 bps	0 B	Medium		0
A Security Profiles	> 🗆 sh	ared-1M-pipe	0 bps	1.02 Mbps	0 bps	0 B	High		0
L VPN	>								
🚨 User & Authentication	*								
	*								
🕸 System 🚺	•								
Security Fabric 6	• •								
🖼 Log & Report	*								
FURTIDET	746								8
v	1100								



EXEED-HO -	≡ ٩									>_ 0·	<b>42</b> • € admin •
Dashboard >	Traffic Shaping Policies	Traffic Shapers	Traffic Shaping Profi	les							_
Network	+ Creste new # Ed	It Delete	Search								O P Event -
🛃 Policy & Objects 🛛 🗸	- Create new		Deut-ut-					0	0		
Firewall Policy	Name	Source	Destination	From T	To	Shared Shaper	Reverse Shaper	Per-IP Shaper	Service	Schedule	Status
Addresses						200	0.00				
Services	BOD_Policy	BOD address	<b>M</b> all		Jm wan1	BOD	BOD		Sec. ALL		S Enabled
Schedules	Office_Policy	Office address	all all		m wan1	Office	Office		LE ALL		C Enabled
Virtual IPs	Guest	Guest address	4 ali		📩 wan1	Guest	Guest		L ALL		C Enabled
IP Pools	Implicit	_	_		-		_	_		-	
Protocol Options					L any	Priority: medium			ALL	Lo always	C Enabled
Traffic Shaping 🛱											
Security Profiles >											
LL VPN											
S WELS Switch Controller											
Svstem (1)											
Ø Security Fabric (1) >											
네 Log & Report >											
											4
47.400							_	_			

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

# J N I V E R S I T A S

#### F Implementasi dan Verifikasi Fitur Keamanan NGFW

Untuk memberikan perlindungan berlapis terhadap ancaman modern, fiturfitur 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.

EXEED-SITE -	≡	۹		
Dashboard >	+	Create new Q Poli	icy match	Edit Policy
+ Network >	-			Service V
🛃 Policy & Objects 🛛 🗸 🗸		Policy	From	Service 2 ALL +
Firewall Policy 🏠		BOD_to_VPN (3)	⇒\$ BOD (I	Action ACCEPT O DENY
Addresses				
Internet Service Database		VPN_to_BOD (5)	() Site1	Firewall/Network Options
Services				NAT
Schedules				10 mod configuration Lice Outgoing laterface Address Lice Dunamic ID Deal
Virtual IPs		Office_to_VPN (4)	>\$ Office	Manage and Configuration Proof
IP Pools				Manage source port
Protocol Options	- 11	VPN to Office (6)	() Site1	Protocol options default
Traffic Shaping				Security Profiles
Security Profiles				
므 VPN ›	:: 🗹	ANY_to_internet (1)	any	AntiVirus C default 👻
Loser & Authentication				Web filter C VEB default •
☆ WiFi & Switch Controller >			_	DNS filter 🔘
System (1) >				Application control C APP Block Games and Streaming
Security Fabric 0 >			=4 BOD (	IPS 🔘 🕫 default 👻
I Log & Report →			any any	
				SSL inspection
				Lorging Options
				Log allowed traffic O Security events All sessions
				Comments
				ľ
				0/1023
				Enable this policy

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].

# UNIVERSITAS MULTIMEDIA NUSANTARA



Gambar 3.20. Bukti Pemblokiran Berkas Tes Antivirus EICAR

EXEED-SITE -	≡ Q.		>_ 0- 4 <mark>0</mark> -
a Dashboard	Edit Web Filter Profile		
Network     Policy & Objects     Security Profiles     AntiVirus	Name default Comments Default web filtering.	22/255	Additional Information                • API Preview                • References             ~ Edite In CU
Web Filter C DNS Filter Application Control Intrusion Prevention SSL/SSH Inspection	Warning: This device is not lice service. Traffic may be blocked if this	r sensed for the FortiGuard web filtering option is enabled.	Online Guides     Relevant Documentation     C     Vistor Tutoriais     C     C     Control Community
Application Signatures IPS Signatures	Pre-configured filters Custom	G PG-13 R	Fortinet Community URL Filter for Let's Encrypt HTTP-01 challenge  3 Answers  0 Votes  199 Views
Web Rating Overrides	Name	Action	Web Filtering while utilizing the Fortinet SSO Agent - With multiple Fortigate Firewa
VPN >		Piction	web filtering not working on 90D
Luser & Authentication	custom1	Q Disable	P Answers      O Votes      P 999 Views     See More      C
	custom2	O Disable	
🗘 System 🔹 🤨	Potentially Liable 12		
Security Fabric 🛛 🕄 🕨	Drug Abuse	Monitor	
≝ Log & Report >	Hacking	Monitor	
	Illegal or Unethical	<ul> <li>Monitor</li> </ul>	
	Discrimination	<ul> <li>Monitor</li> </ul>	
	Explicit Violence	Monitor	
		0% 🚱	
	<ul> <li>Allow users to override blocked of</li> </ul>	ategories	

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 3.23. 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.
- 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

27







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,

28 Implementasi dan konfigurasi..., Ignatius Steven, Universitas Multimedia Nusantara

Network								- станову - Шою
Policy & Objects	Date/Time	ø	Source	Device	Destination	Application Name	Result	Policy ID
Security Profiles	2025/05/29 20:31:43		172.200.2.2		10.1.100.2	udp/137	Accept (1.58 kB / 1.58 kB)	BOD to VPN (3)
l VPN	2025/05/29 20:30:00		10.1.100.2		35 172.200.2.2	PING	<ul> <li>Accept (276 B / 276 B)</li> </ul>	VPN_to_BOD (5)
	2025/05/29 20:29:09		172.200.2.2		172.16.1.1	udp 37	Accept (468 B / 0 B)	BOD_to_VPN (3)
WIFI & Switch Controller	2025/05/29 20:28:52		10.1.100.2		<b>I72.200.2.2</b>	PING	✓ Accept	VPN_to_BOD (5)
System (1)	2025/05/29 20:28:52		10.1.100.2		35 172.200.2.2	PING	✓ Accept	VPN_to_BOD (5)
Security Fabric 0	2025/05/29 20:28:52		10.1.100.2		IT2.200.2.2	PING	✓ Accept	VPN_to_BOD (5)
Log & Report v	2025/05/29 20:28:39		172.200.2.2		<b>IF 172.200.1.1</b>	udp/137	Accept (468 B / 0 B)	BOD_to_VPN (3)
Local Traffic	2025/05/29 20:28:20		172.200.2.2		10.1.100.2	PING	<ul> <li>Accept (672 B / 396 B)</li> </ul>	BOD_to_VPN (3)
Solffer Traffic	2025/05/29 20:28:20		172.200.2.2		10.1.100.2	icmp/0/8	✓ Accept (ip-conn)	BOD_to_VPN (3)
System Events	2025/05/29 20:27:36		172.200.2.2		10.1.100.1	udp/137	Accept (468 B / 0 B)	BOD_to_VPN (3)
Security Events	2025/05/29 20:27:17		172.200.2.2		172.16.1.1	PING	Accept (276 B / 276 B)	BOD_to_VPN (3)
Reports	2025/05/29 20:26:48		172.200.2.2		III 172.200.1.1	PING	Accept (276 B / 276 B)	BOD_to_VPN (3)
Log Settings	2025/05/29 20:26:11		172.200.2.2		172.16.1.1	PING	✓ Accept	BOD_to_VPN (3)
	2025/05/29 20:26:11		172.200.2.2		172.16.1.1	PING	✓ Accept	BOD_to_VPN (3)
	2025/05/29 20:26:11		172.200.2.2		172.16.1.1	PING	✓ Accept	BOD_to_VPN (3)
	2025/05/29 20:25:45		172.200.2.2		10.1.100.1	PING	Accept (516 B / 516 B)	BOD_to_VPN (3)
	2025/05/29 20:25:45		172.200.2.2		10.1.100.1	icmp/0/8	Accept (ip-conn)	BOD_to_VPN (3)
	2025/05/29 20:25:40		172.200.2.2		UE 172.200.1.1	PING	✓ Accept	BOD_to_VPN (3)
	2025/05/29 20:25:40		172.200.2.2		<b>I72.200.1.1</b>	PING	✓ Accept	BOD to VPN (3)
	2025/05/29 20:25:40		172 200 2 2		SE 172 200 1 1	PING	Accent	BOD to VPN (3)

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 ERSITA

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.

