BAB III
PELAKSANAAN KERJA PROFESI

3.1 Bidang Kerja

Bidang Teknologi Informasi (TI) memiliki peran yang sangat penting dalam operasional perusahaan modern. Di dalam struktur organisasi, departemen TI biasanya bertanggung jawab atas berbagai aspek yang berkaitan dengan teknologi dan sistem informasi. (Ulrich Beck 2000) menyoroti perubahan bidang kerja di era globalisasi dan digitalisasi, di mana pekerjaan berbasis teknologi dan fleksibilitas menjadi semakin dominan. TI mengelola infrastruktur teknologi perusahaan, termasuk jaringan komputer, server, dan sistem keamanan data. Tim TI juga bertugas mengembangkan dan memelihara aplikasi perangkat lunak yang digunakan untuk mendukung berbagai fungsi bisnis, seperti manajemen keuangan, sumber daya manusia, dan operasional

Salah satu tanggung jawab utama departemen TI adalah memastikan ketersediaan dan kepraktikanlan sistem informasi perusahaan. TI harus memantau kinerja sistem, melakukan pemeliharaan rutin, dan menangani masalah teknis yang muncul. Selain itu, tim TI juga berperan dalam perencanaan strategis teknologi, mengidentifikasi peluang untuk meningkatkan efisiensi melalui solusi teknologi baru, dan membantu dalam pengambilan keputusan terkait investasi teknologi.

Keamanan informasi juga menjadi fokus utama departemen TI. Teknologi Informasi bertanggung jawab untuk melindungi data perusahaan dari ancaman keamanan siber, mengimplementasikan kebijakan keamanan, dan memastikan kepatuhan terhadap regulasi yang berlaku terkait privasi dan perlindungan data. Tim TI juga sering kali terlibat dalam proyek-proyek transformasi digital, membantu perusahaan mengadopsi teknologi baru untuk meningkatkan daya saing dan efisiensi operasional.

Sebagai praktikan di divisi teknologi informasi, Praktikan saat ini terlibat dalam berbagai aspek pengelolaan TI perusahaan. Salah satu tugas utama Praktikan adalah membantu tim helpdesk dalam menangani permintaan dukungan teknis dari karyawan. Sehari-hari, Praktikan menangani troubleshooting masalah perangkat keras dan perangkat lunak sederhana, membantu proses instalasi software, dan memberikan panduan penggunaan sistem kepada pengguna. Pengalaman ini membantu Praktikan mengembangkan keterampilan komunikasi dan pemecahan masalah yang penting dalam industri TI.

Dalam aspek infrastruktur dan jaringan, Praktikan membantu dalam pemeliharaan rutin server dan perangkat jaringan. Tugas-tugas Praktikan meliputi pemantauan kinerja sistem, membantu dalam proses backup data, dan terlibat dalam proyek-proyek upgrade hardware. Pengalaman ini membantu Praktikan memahami kompleksitas infrastruktur TI perusahaan dan pentingnya menjaga kepraktikanlan sistem.

Keamanan informasi juga menjadi bagian dari tanggung jawab Praktikan. Praktikan membantu dalam pelaksanaan audit keamanan rutin, memantau log keamanan, dan terlibat dalam pengembangan materi pelatihan keamanan untuk karyawan. Hal ini memberikan Praktikan pemahaman yang lebih baik tentang pentingnya keamanan siber dalam lingkungan bisnis modern.

Sebagai praktikan, Praktikan juga diberikan kesempatan untuk terlibat dalam proyek-proyek inovatif yang sedang dikerjakan oleh divisi TI. Ini mencakup penelitian tentang teknologi baru, membantu dalam proof of concept untuk solusi-solusi inovatif, dan berkontribusi pada inisiatif transformasi digital perusahaan. Keterlibatan ini membantu Praktikan tetap up-to-date dengan tren terbaru dalam industri TI dan memahami bagaimana teknologi dapat mendorong inovasi bisnis.

3.2 Pelaksanaan Kerja

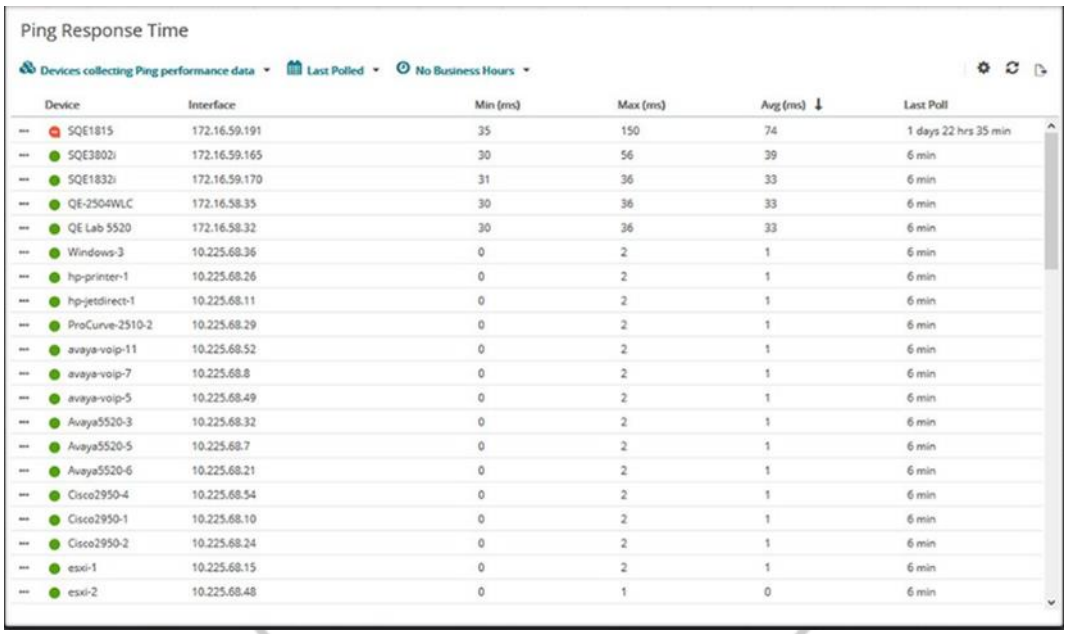
3.2.1 Pemantauan Jaringan (Network Monitoring)

1. Pelaporan Real-time dan Historis

Kerja praktik pemantauan jaringan dimulai dengan tahap persiapan yang melibatkan pengaturan peralatan dan software yang diperlukan. Peserta akan menginstal software pemantauan jaringan seperti *WhatsUp Gold* pada komputer mereka dan memastikan akses ke perangkat jaringan yang akan dipantau. Penting untuk memverifikasi bahwa semua perangkat terhubung dengan benar sebelum memulai praktikum.

Setelah persiapan selesai, praktikan akan mempelajari cara memantau ketersediaan jaringan. Mereka akan menggunakan metode sederhana seperti ICMP Ping untuk memeriksa konektivitas dasar ke berbagai perangkat dalam jaringan. Selanjutnya, akan mengkonfigurasi SNMP pada router atau switch dan menggunakan software monitoring untuk mengumpulkan data yang lebih rinci tentang status perangkat.

Analisis kinerja jaringan menjadi fokus utama dalam sesi berikutnya. Praktikan akan menggunakan *WhatsUp Gold* untuk melakukan *packet sniffing*, mengamati lalu lintas jaringan secara *real-time*. Mereka akan melakukan berbagai aktivitas jaringan dan menganalisis paket yang tertangkap, mencari pola dan potensi masalah. Selain itu, mereka akan mempelajari cara memantau penggunaan *bandwidth* dan mengidentifikasi aplikasi atau layanan yang mengkonsumsi *bandwidth* terbanyak.



Gambar 3.1 Pelaporan *Real-time dan Historis*

Admin jaringan terlibat dalam siklus hidup berkelanjutan dalam mendesain, menganalisis, dan mendesain ulang jaringan.

Untuk mendukung siklus hidup ini, sistem NMS menyediakan data pemantauan historis dan waktu nyata. Informasi ini memungkinkan admin Jaringan:

- Untuk memvalidasi bahwa desain jaringan memberikan hasil yang diinginkan

- Untuk mengungkap tren yang dapat memengaruhi kemampuan jaringan dalam memberikan kinerja yang diminta oleh pengguna, aplikasi, dan bisnis.

- Untuk mengisolasi dan memperbaiki masalah kinerja dengan cepat

- Untuk memberikan bukti bahwa komitmen SLA dipenuhi.

NMS memberikan informasi pemantauan di halaman web yang disebut dasbor. Dasbor terdiri dari tampilan siap pakai. Misalnya, tampilan 10 penggunaan CPU teratas atau tampilan 10 penggunaan Memori teratas.

Admin Jaringan memindai dasbor ringkasan untuk menilai kesehatan seluruh jaringan. Lalu menelusurinya dengan dasbor terperinci

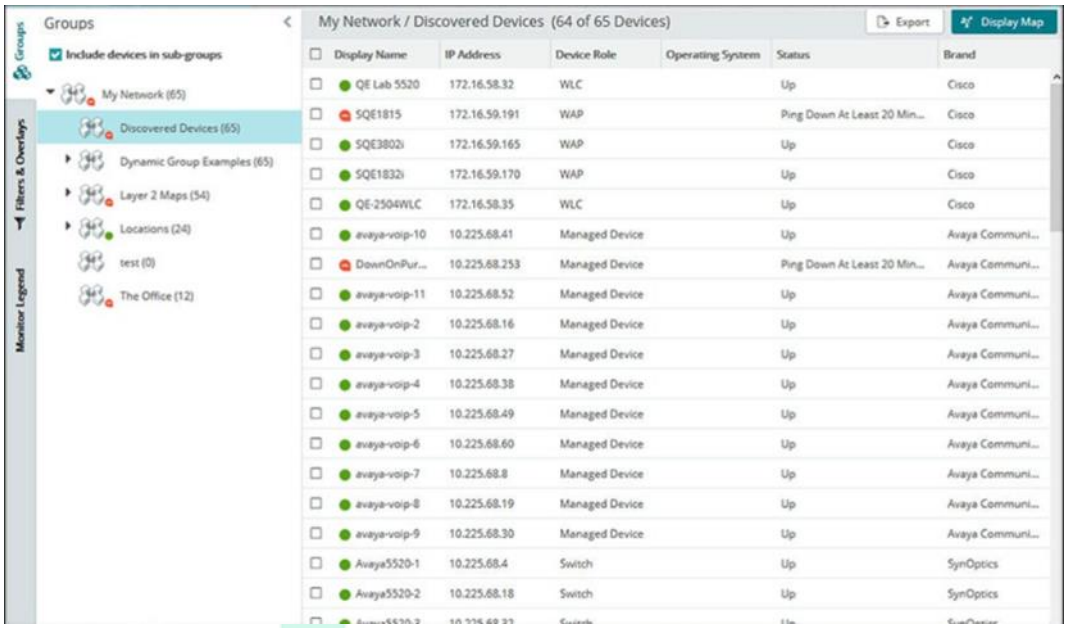
dari perangkat dan monitor tertentu untuk mengisolasi masalah kinerja dengan cepat.

Sebagian besar NMS dapat disesuaikan. Admin jaringan dapat membuat dasbor untuk klien internal mereka – Manajer mereka, pemilik lini bisnis, Help Desk, dan rekan yang mengelola sistem dan aplikasi.

2. Daftar Perangkat yang Terhubung

Sistem Pemantauan Jaringan, seperti WhatsUp Gold, menemukan semua perangkat di jaringan – router, switch, *firewall*, server, printer, dan banyak lagi. NMS mencakup pustaka templat pemantauan, yang menentukan cara memantau perangkat. Di WhatsUp Gold, kami menyebut templat ini sebagai Peran Perangkat. Peran perangkat bersifat khusus untuk jenis dan vendor. Misalnya, apa yang Anda pantau pada Router Cisco akan berbeda dengan apa yang Anda pantau pada Server Dell.

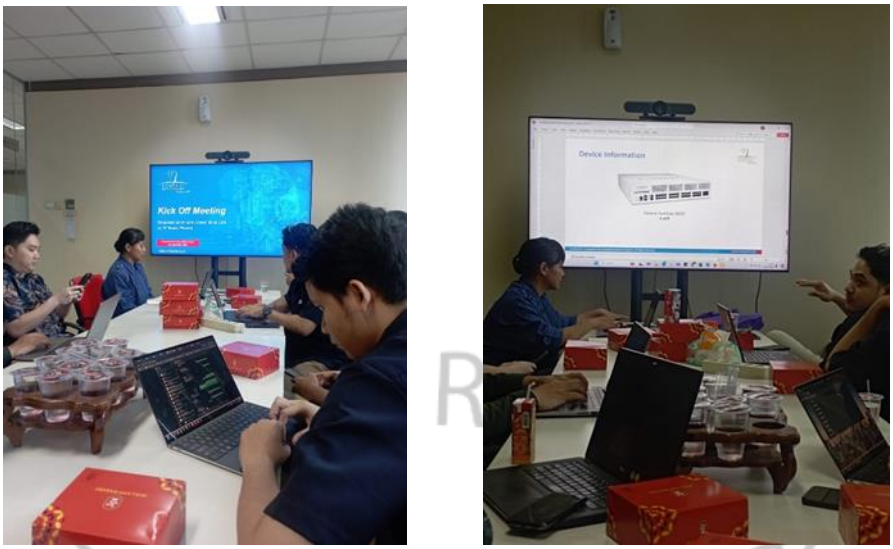
Ketika sistem pemantauan jaringan menyelesaikan proses penemuan, secara otomatis menetapkan peran perangkat yang sesuai untuk setiap perangkat yang ditemukan. Sistem Pemantauan Jaringan berbeda dalam kemampuan penemuannya. Semua NMS menemukan perangkat di jaringan. Namun, tidak semua akan menemukan bagaimana perangkat terhubung ke jaringan. Misalnya, NMS mungkin telah mengidentifikasi server di jaringan tetapi tidak akan tahu saklar mana yang terhubung dengannya.



Gambar 3.2 Daftar Perangkat yang Terhubung

3.2.2 Training Pengadaan *Server farm Firewall*

Training Pengadaan *Server farm Firewall* oleh CompNet adalah profesional IT tentang bagaimana mengelola pengadaan dan implementasi *firewall* dalam infrastruktur *server farm*. *Server farm* merupakan kumpulan server yang bekerja secara bersamaan untuk menangani beban kerja besar, sehingga memerlukan perlindungan keamanan yang kuat. Dalam pelatihan ini, peserta akan diajarkan cara menganalisis kebutuhan spesifik *server farm*, seperti lalu lintas data, jenis aplikasi yang digunakan, dan potensi risiko keamanan, untuk memastikan *firewall* yang dipilih dapat memberikan perlindungan optimal.



Gambar 3.3 Melakukan Training Pengadaan *Server farm Firewall*

1. Perencanaan Pengadaan *Firewall* untuk *Server farm*

Analisis Kebutuhan Jaringan: Mempelajari cara menilai kebutuhan spesifik *server farm*, termasuk *throughput*, jumlah koneksi, segmentasi jaringan, dan jenis aplikasi yang digunakan untuk memilih *firewall* yang sesuai.

Identifikasi Risiko dan Mitigasi: Menilai ancaman potensial terhadap *server farm*, seperti serangan DDoS, *malware*, atau penyusupan, dan bagaimana *firewall* dapat membantu mengurangi risiko tersebut.

2. Konfigurasi dan Manajemen *Firewall*

Konfigurasi Kebijakan Keamanan: Cara mengonfigurasi *firewall* untuk mengelola kebijakan akses, aturan keamanan, serta mengatur *Access control list* (ACL) untuk membatasi akses berdasarkan zona keamanan atau tipe koneksi.

Segmentasi Jaringan dan NAT: Mempelajari pengaturan untuk memisahkan IP publik dan privat, serta mengelola akses dari luar ke dalam *server farm*.

VPN dan *Bandwith*: Mengonfigurasi VPN melalui *firewall* untuk mendukung koneksi aman dari jarak jauh ke *server farm*.

3. Pemantauan, Logging, dan Pelaporan

Monitoring *Firewall*: Pelatihan tentang penggunaan alat pemantauan untuk melacak kinerja *firewall* secara real-time, termasuk analisis lalu lintas jaringan dan penggunaan *bandwidth*.

Log dan Audit Keamanan: Mempelajari cara mengonfigurasi *logging firewall* untuk mencatat aktivitas jaringan dan serangan yang terdeteksi, serta membuat laporan keamanan yang berguna untuk audit dan kepatuhan regulasi.

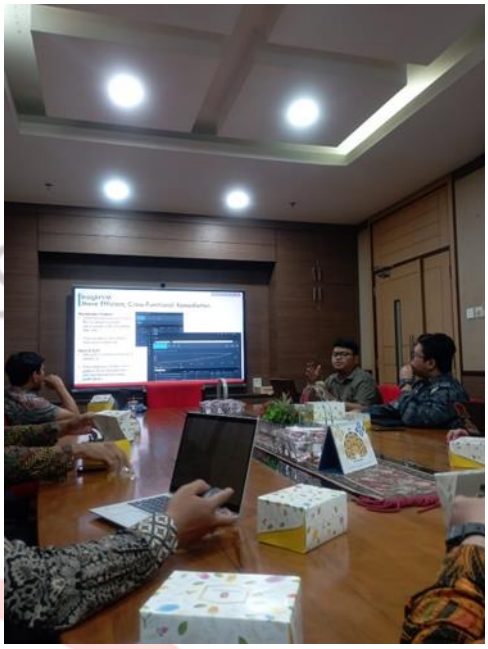
Deteksi dan Tanggapan Terhadap Ancaman: Menggunakan *firewall* untuk mendeteksi ancaman seperti serangan DDoS atau penyusupan, serta merespons insiden keamanan dengan cepat dan efektif.

3.2.3 Training *Rapid 7 Vulnerabeility Management*

Rapid7 adalah penyedia terkemuka dalam solusi keamanan dan manajemen kerentanan, dengan platform *Insightvm* yang populer untuk penilaian dan perbaikan kerentanan. Pelatihan manajemen kerentanan menggunakan *Rapid7* biasanya dimulai dengan pemahaman dasar tentang *Insightvm*, termasuk fitur-fitur utamanya seperti pengelolaan kerentanan, siklus manajemen risiko, serta cara menavigasi antarmuka dan dashboard. Langkah awal yang penting adalah mempelajari proses instalasi dan konfigurasi, seperti penerapan platform di jaringan, pengaturan situs, dan aset yang akan dipindai.

Setelah *Insightvm* diatur, praktikan pelatihan akan belajar cara melakukan pemindaian penemuan dan kerentanan. Pemindaian ini mencakup identifikasi aset di jaringan dan deteksi potensi kerentanan yang ada pada sistem dan aplikasi, baik melalui metode pemindaian berbasis agen maupun tanpa agen. Hasil pemindaian ini kemudian dianalisis, di mana peserta akan dilatih untuk memahami laporan pemindaian, memprioritaskan risiko berdasarkan tingkat keparahan dan faktor-faktor lain, serta mengkategorikan aset yang memerlukan perhatian khusus. *Insightvm* menawarkan fitur skor *Real risk*, yang memperhitungkan probabilitas eksploitasi selain skor CVSS standar, membantu dalam

pengambilan keputusan yang lebih tepat dalam memprioritaskan kerentanan.



Gambar 3.4 Rapid Vulnerability Management

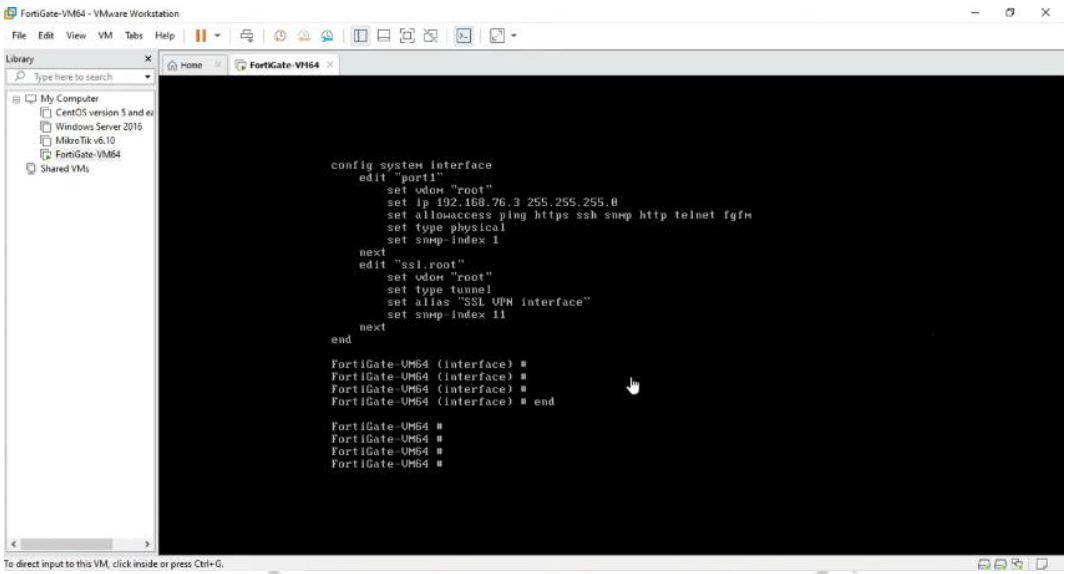
Praktikan pelatihan akan belajar cara melakukan pemindaian penemuan dan kerentanan. Pemindaian ini mencakup identifikasi aset di jaringan dan deteksi potensi kerentanan yang ada pada sistem dan aplikasi, baik melalui metode pemindaian berbasis agen maupun tanpa agen. Hasil pemindaian ini kemudian dianalisis, di mana peserta akan dilatih untuk memahami laporan pemindaian, memprioritaskan risiko berdasarkan tingkat keparahan dan faktor-faktor lain, serta mengkategorikan aset yang memerlukan perhatian khusus. *Insightvm* menawarkan fitur skor *Real risk*, yang memperhitungkan probabilitas eksploitasi selain skor CVSS standar, membantu dalam pengambilan keputusan yang lebih tepat dalam memprioritaskan kerentanan.

3.2.4 Intalasi dan Konfigurasi *Firewall Fortigate*

Fortigate adalah perangkat keamanan jaringan yang dikembangkan oleh *Fortinet* dan dikenal sebagai salah satu solusi *firewall* yang paling komprehensif di pasaran (Michael E. Whitman & Herbert J. Mattord 2018). Dikenal sebagai *firewall* generasi berikutnya atau *Next-Generation Firewall (NGFW)*, *Fortigate* tidak hanya menyediakan fungsi *firewall* tradisional, tetapi juga berbagai fitur keamanan tambahan untuk melindungi jaringan dari ancaman modern. Dengan kemampuannya yang canggih, *Fortigate* menjadi pilihan utama bagi banyak organisasi yang ingin memastikan keamanan jaringan mereka tetap tangguh terhadap berbagai jenis serangan siber yang semakin kompleks.

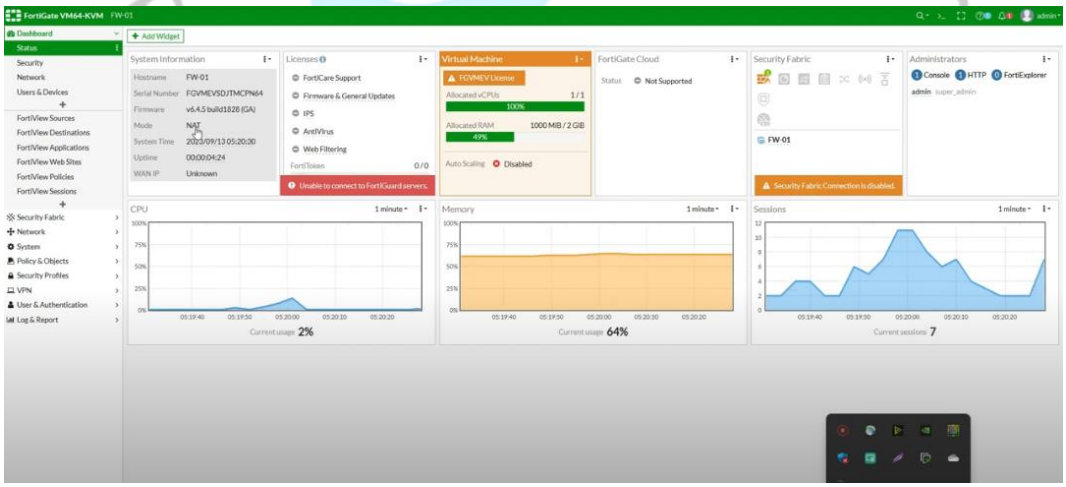
Salah satu fitur utama *Fortigate* adalah fungsionalitas *firewall-nya*. Seperti *firewall* pada umumnya, *Fortigate* dapat memonitor, mengontrol, dan memfilter lalu lintas data yang masuk dan keluar dari jaringan berdasarkan aturan yang ditentukan oleh administrator. Fitur ini memberikan kontrol penuh atas lalu lintas jaringan, sehingga memungkinkan organisasi untuk melindungi sistem. Selain itu, *Fortigate* mendukung kemampuan stateful inspection yang memungkinkan firewall memantau status koneksi jaringan dan memastikan bahwa hanya lalu lintas yang diotorisasi yang melewatinya.

Di samping kemampuan *firewall* tradisional, *Fortigate* juga dilengkapi dengan sistem *Intrusion Prevention System (IPS)*. IPS bertugas untuk mendeteksi dan menghentikan ancaman atau serangan yang berusaha mengeksploitasi kerentanan dalam sistem. *Fortigate* dapat memantau lalu lintas secara *real-time* dan mendeteksi pola serangan yang mencurigakan, lalu menghentikannya sebelum merusak sistem. Dengan integrasi IPS, *Fortigate* dapat memberikan perlindungan yang lebih proaktif daripada *firewall* tradisional yang umumnya hanya berfokus pada pemblokiran berdasarkan aturan statis.



Gambar 3.5 Konfigurasi *Firewall Fortigate*

Langkah pertama dalam mengkonfigurasi *Fortigate* adalah mengakses antarmuka admin untuk pengaturan awal. Untuk ini, Anda perlu menghubungkan komputer ke perangkat *Fortigate* melalui salah satu port LAN, lalu mengakses antarmuka web-nya melalui alamat IP default, biasanya https://192.168.76.3 Setelah masuk dengan kredensial default, praktikan bisa mulai mengatur parameter dasar, seperti alamat IP pada antarmuka WAN dan LAN, agar perangkat dapat terhubung dengan jaringan lokal dan jaringan internet. Proses ini memastikan *Fortigate* terhubung dengan baik pada infrastruktur jaringan yang ada.



Gambar 3.6 Masuk ke halaman *Fortigate* setelah di konfigurasi

Setelah antarmuka jaringan dikonfigurasi, langkah berikutnya adalah mengatur kebijakan *firewall* yang akan mengontrol lalu lintas data antara jaringan internal dan eksternal. Kebijakan *firewall* ini memungkinkan menentukan aturan mana yang memperbolehkan atau memblokir lalu lintas berdasarkan beberapa parameter seperti sumber, tujuan, layanan, dan antarmuka jaringan. Misalnya, Anda dapat membuat kebijakan untuk memperbolehkan lalu lintas dari LAN ke WAN untuk layanan web (HTTP/HTTPS) atau memblokir akses ke port yang tidak digunakan untuk keamanan tambahan. Dengan fitur ini, *Fortigate* memungkinkan pengendalian lalu lintas yang sangat terperinci dan aman.

Setelah kebijakan *firewall* diterapkan, biasanya Anda juga perlu mengaktifkan *Network address translation* (NAT) untuk memungkinkan banyak perangkat di jaringan internal berbagi satu alamat IP publik saat mengakses internet. *Fortigate* mempermudah pengaturan NAT dengan opsi untuk mengaktifkan NAT di dalam kebijakan *firewall* yang Anda buat. Ini sangat berguna terutama dalam situasi di mana organisasi memiliki beberapa perangkat di belakang satu alamat IP eksternal yang sama, sehingga semua lalu lintas dapat diterjemahkan dengan baik saat melewati *firewall*.

3.3 Kendala Yang Dihadapi

3.3.1 Kurangnya Pengalaman atau Keterampilan

Bagi praktikan yang baru memasuki dunia kerja, salah satu kendala terbesar adalah kurang pengalaman atau keterampilan yang relevan dengan industri atau bidang yang digeluti. Sebagai praktikan, banyak yang mungkin hanya memiliki pengalaman teoritis dari perkuliahan tanpa pernah terjun langsung ke lapangan. Ketika praktikan mulai magang, keterampilan teknis yang diperlukan untuk menyelesaikan tugas-tugas tertentu mungkin belum dimiliki, sehingga menimbulkan rasa cemas atau bahkan frustrasi.

Selain itu, keterampilan soft skills, seperti komunikasi yang efektif, kerja sama tim, atau manajemen waktu, mungkin juga masih belum terasah dengan baik. Hal ini bisa menyebabkan praktikan mengalami kesulitan dalam beradaptasi dengan tuntutan pekerjaan sehari-hari yang berbeda dari rutinitas akademik. Misalnya, seorang praktikan teknik mungkin

menguasai teori tentang pemrograman atau desain, namun ketika dihadapkan pada proyek nyata, mereka merasa kewalahan karena tidak terbiasa dengan alat atau software yang digunakan di dunia industri.

Rasa tidak percaya diri sering muncul ketika mereka membandingkan diri dengan karyawan tetap yang lebih berpengalaman. Mereka mungkin merasa tidak mampu untuk memenuhi standar pekerjaan atau takut membuat kesalahan. Kekhawatiran ini wajar di lingkungan profesional. Namun, perasaan ini bisa menghambat pembelajaran dan perkembangan diri jika tidak dikelola dengan baik.

3.4 Cara Mengatasi Kendala

Praktikan harus lebih proaktif dalam mencari bimbingan dari mentor, supervisor, atau rekan kerja yang lebih berpengalaman. Tanyakan hal-hal yang kurang dipahami, baik terkait tugas yang sedang dikerjakan maupun mengenai keterampilan yang dibutuhkan untuk menyelesaikan pekerjaan dengan baik. Jangan malu ketika bertanya, karena magang adalah tempat untuk belajar dan mengembangkan diri. Bimbingan yang baik akan membantu praktikan memahami ekspektasi perusahaan dan cara kerja yang lebih efektif di lingkungan profesional.

Selain belajar dari rekan kerja, praktikan harus juga memanfaatkan berbagai sumber daya lain yang ada di perusahaan. Misalnya, jika perusahaan memiliki pelatihan internal, program pengembangan keterampilan, atau sesi bimbingan profesional, praktikan manfaatkan kesempatan ini sebaik mungkin. Banyak perusahaan menyediakan program pelatihan bagi karyawan atau peserta magang untuk meningkatkan kemampuan mereka. Praktikan juga bisa memanfaatkan materi pelatihan *online*, buku, atau tutorial yang relevan dengan bidang kerja praktikan untuk menambah wawasan dan keterampilan.

3.5 Pembelajaran Yang Diperoleh dari Kerja Profesi

Praktikan sangat efektif dalam mengembangkan soft skills yang penting dalam lingkungan kerja profesional. Keterampilan seperti komunikasi efektif, kerja tim, manajemen waktu, dan problem solving

adalah aspek yang terus diasah selama magang, baik rekan kerja maupun atasan, sehingga keterampilan komunikasi yang baik sangat penting.

Selain itu, praktikan juga belajar mengelola waktu dengan lebih baik karena harus memenuhi tenggat waktu tertentu dan mengatur prioritas antara tugas-tugas yang berbeda. Soft skills ini bermanfaat di mana kemampuan berkomunikasi, berkolaborasi, dan mengelola waktu sangat penting untuk mencapai keseimbangan hidup.

Magang juga memberikan kesempatan untuk membangun jaringan profesional. Selama magang, praktikan berinteraksi dengan rekan kerja, atasan, dan profesional lain yang mungkin bisa menjadi mentor, pemberi saran, atau bahkan membuka peluang kerja di masa depan. Jaringan ini bisa sangat berharga dalam mengembangkan karier karena referensi dari kolega atau atasan di tempat magang dapat membantu dalam mendapatkan pekerjaan di masa depan.

Selain itu, melalui jaringan ini, peserta magang bisa mendapatkan wawasan tentang berbagai posisi dalam industri, memahami dinamika kerja yang ada, dan mempelajari berbagai peluang yang mungkin tidak mereka ketahui sebelumnya.