

Ahmed Fathi Mahmoud Elesawi

Network Security Engineer | Cybersecurity Instructor

Professional Summary

Dynamic and results-oriented Network Security Engineer with expertise in managing and securing enterprise-level infrastructures in the banking and telecommunications sectors. Proficient in firewall administration, VPN configuration, and automation, with hands-on experience in industry-leading platforms like Palo Alto, FortiGate, and Cisco ASA. Adept at aligning technical strategies with organizational goals to enhance security and operational efficiency. Trainer and mentor, passionate about empowering the next generation of cybersecurity professionals through engaging instruction and practical labs. A proven track record of implementing robust security measures, reducing vulnerabilities, and fostering proactive defense mechanisms.

Personal Information

Name: Ahmed Fathi Mahmoud Elesawi

Phone Number: 01158373746

Email: ahmed@elesawi.com

LinkedIn: [linkedin.com/in/elesawi](https://www.linkedin.com/in/elesawi)

Residence: Cairo, Egypt

Military Status: Served

Education and Certifications

Bachelor of Engineering – BE in Electrical, Electronics, and Communications Engineering

Marg High Institute for Engineering and Technology | 2013 – 2018

- **Overall Grade:** Very Good (GPA: 2.92), reflecting strong academic performance and a solid foundation in engineering principles.
- **Graduation Project:** Designed and implemented a **Robotic Arm with Computer Vision** capable of identifying and manipulating objects. Applied advanced **image processing algorithms** and **embedded systems** to develop an efficient, automated solution. This project demonstrated proficiency in **emerging technologies**, **problem-solving**, and **team collaboration** while showcasing effective **project management** skills. (Grade: Excellent)

Certifications

- **Certified Ethical Hacker (CEH)** | Verification: <https://elesawi.com/url/CEH>
- **Fortinet FortiManager 7.0 Administrator** | Verification: <https://elesawi.com/url/FMG>
- **Fortinet Enterprise Firewall 7.0 Administrator** | Verification: <https://elesawi.com/url/EFA>

Professional Experience

Network Security Engineer

Banque Misr | 07/2024 – Current

- Manage and troubleshoot Palo Alto and FortiGate firewalls to ensure the security and operational stability of critical banking infrastructure.
- Monitor and optimize NGFW security profiles, integrating features such as IPS, URL filtering, application control, and SSL decryption to enforce comprehensive security policies.
- Maintain **SSL-VPN configurations** to provide secure connectivity for internal systems and remote users.
- Oversee **site-to-site VPNs** for secure communication between internal systems and extranet partners, ensuring uninterrupted data flow.
- Conduct regular policy reviews and fine-tune firewall configurations to enhance performance and align with InfoSec policies and Central Bank of Egypt (CBE) regulations.
- Automate operational tasks, including firewall rule audits and configuration consistency checks, using Python scripting to improve efficiency and reduce manual errors.
- Centralize log collection and analysis through syslog servers, FortiAnalyzer, Panorama, and SIEM platforms to support proactive threat monitoring and incident response.

Network Security Engineer

Raya Information Technology | 07/2023 – 06/2024

- Deployed and configured FortiGate and Palo Alto NGFWs to replace legacy systems, enhancing the organization's overall security posture.
- Migrated firewall policies from legacy systems to FortiGate and Palo Alto platforms, ensuring seamless transitions and compliance with organizational standards.
- Implemented advanced NGFW features, including sandboxing, malware detection, and application control, as part of deployment processes.
- Troubleshooted and optimized newly implemented firewalls and associated features to ensure performance and operational reliability.

Network Security Engineer Trainee

BARQ Systems | 05/2023 – 06/2023

- Shadowed experienced engineers to gain hands-on exposure to advanced network security technologies and operations.
- Assisted in the installation and initial configuration of FortiGate firewalls, FortiManager, and F5 LTM/ASM systems.
- Participated in troubleshooting sessions to resolve network issues and ensure the operational reliability of deployed solutions.
- Acquired foundational skills in deploying and managing security solutions, including endpoint protection and load balancing systems.

Electrical Site Engineer

ECS - Energy and Contracting Solutions, Cairo Business Park Project | 07/2021 – 01/2023

- Supervised electrical installations, including power distribution systems, cabling, and lighting, ensuring adherence to project specifications and timelines.
- Coordinated with cross-functional teams, including civil and mechanical engineers, to align project phases and meet deadlines.
- Managed workforce and resources effectively to maintain project schedules and ensure quality control across electrical works.
- Provided technical support to resolve on-site issues, ensuring compliance with industry standards and safety regulations.
- Conducted inspections and testing to verify the integrity and functionality of completed installations.

Teaching Experience

Instructor (Part Time)

NTI - National Telecommunication Institute | 06/2023 – Current

- Deliver specialized training courses in **Certified Ethical Hacker (CEH)**, **Cisco CyberOps Associate**, and **Network Security**, tailored for IT professionals.
- Teach advanced methodologies in penetration testing, network intrusion analysis, and security operations, preparing students for industry certification exams.
- Conduct hands-on labs focusing on configuring NGFWs, setting up VPNs, performing log analysis, and implementing threat mitigation techniques.
- Develop and present real-world scenarios and case studies to reinforce learning and practical application of security concepts.

Instructor (Part Time)

YAT learning Centers | 06/2023 – 03/2024

- Teach foundational cybersecurity concepts and principles as part of the Digital Egypt Cubs Initiative in collaboration with Udacity.
- Conduct practical training sessions covering ethical hacking, incident response, and basic network security for young learners.
- Design interactive simulations and exercises to engage students in understanding real-world cybersecurity challenges.

Technical Skills:

- **Network Security and Firewalls:**
 - Expert in managing and optimizing enterprise firewalls, including Palo Alto, FortiGate, and Cisco ASA, to secure critical banking infrastructure.
 - Proficient in configuring and managing security profiles for NGFWs, integrating multiple advanced features such as intrusion prevention systems (IPS), URL filtering, application control, malware protection, and SSL decryption into cohesive policies.
 - Configured application-aware security profiles to monitor and control traffic based on application types, enhancing resource utilization and overall network security
 - Configured security profiles with FortiSandbox and Palo Alto WildFire integration for sandboxing and malware analysis, enabling detection of zero-day threats.
 - Applied security profiles to enforce URL filtering policies, blocking access to malicious or non-compliant web categories.
 - Enforced URL filtering policies to block access to malicious or non-compliant web categories using integrated NGFW features
 - Integrated SSL/TLS traffic decryption with Gigamon for secure traffic inspection, ensuring seamless analysis without disrupting critical services.
 - Migrated legacy IP-based policies to user-based policies through Active Directory integration using Fortinet's FSSO and Palo Alto User-ID, improving dynamic access control.
 - Configured Host Information Profiles (HIP) in Palo Alto to enforce VPN access restrictions based on trusted user devices.
 - Managed **Palo Alto Prisma Access** to enable secure VPN connectivity for user, ensuring compliance with organizational security policies
- **Threat Detection and Incident Response:**
 - Centralized firewall log collection and monitoring by directing logs to syslog servers, FortiAnalyzer, Panorama, and SIEM platforms for enhanced visibility and proactive threat detection.
 - Maintained dynamic blocklists of malicious IPs and domains within NGFWs, ensuring continuous updates from vendor threat intelligence feeds.
- **Automation and Optimization:**
 - Automated repetitive tasks, including firewall rule audits, configuration validations, and backups, using Python scripting to enhance operational efficiency.
 - Developed custom scripts to streamline bulk configuration updates across firewalls, ensuring consistent application of security policies.
- **Networking Foundations for Security:**
 - Strong knowledge of VLANs, OSPF, and Layer 2/3 protocols, tailored to secure banking network environments.
 - Configured advanced QoS policies to prioritize critical security traffic, such as IPS updates and log transmissions.
 - Experienced in integrating secure networking practices with firewall deployments to ensure robust protection for sensitive data
- **Tools and Platforms:**
 - Advanced proficiency with Palo Alto Panorama, FortiManager, and FortiAnalyzer for centralized policy management, monitoring, and incident reporting.
 - Skilled in using Python to automate firewall-related tasks and improve consistency in network security operations.

Soft Skills:

- **Critical Thinking:** Strong analytical abilities to evaluate security challenges, identify vulnerabilities, and implement effective solutions.
- **Decision-Making Under Pressure:** Skilled at making sound decisions during high-pressure security incidents to mitigate risks and restore operations.
- **Problem-Solving:** Proficient in diagnosing and resolving complex network and security issues, ensuring operational integrity.

- **Strategic Planning:** Capable of designing and executing long-term security strategies aligned with organizational objectives and compliance requirements.
- **Attention to Detail:** Meticulous in reviewing security configurations, logs, and processes to identify and address potential vulnerabilities.
- **Collaboration:** Experienced in coordinating with cross-functional teams, ensuring seamless communication between IT, InfoSec, and management.
- **Change Management:** Effective at leading teams through transitions, such as adopting new security technologies or workflows, while maintaining productivity.
- **Negotiation and Persuasion:** Skilled at advocating for security best practices and gaining support from stakeholders, including upper management.
- **Technical Writing and Documentation:** Proficient in creating clear and detailed security policies, procedures, and incident reports.
- **Cultural Awareness:** Comfortable working in diverse teams and adapting communication styles to foster global collaboration.
- **Continuous Learning:** Committed to staying updated on cybersecurity trends, emerging threats, and new technologies to remain effective in dynamic environments.
- **Time Management:** Proven ability to handle multiple high-priority projects and meet tight deadlines in fast-paced settings.
- **Effective Communication:** Adept at explaining complex technical concepts to both technical teams and non-technical stakeholders, ensuring alignment and understanding.
- **Leadership and Mentorship:** Experienced in guiding teams and junior engineers, fostering collaboration and professional growth.
- **Empathy in Teaching:** Patient and supportive when helping students or junior engineers navigate complex concepts, ensuring they build confidence and skills.

Courses and Training

Modern Defensive Security Solutions

NTI, Digital Egypt Youth Initiative | 02/2023 – 05/2023

- Gained hands-on experience with security appliances, including ASA, FortiGate, FortiManager, FortiAnalyzer, FortiSIEM, FortiWeb, Palo Alto Firewall, and Sophos Firewall.
- Conducted real-world scenarios and lab exercises to configure, deploy, and troubleshoot various security solutions.
- Strengthened communication and teamwork skills through collaborative troubleshooting and group projects.

Network Attacks and Mitigations

NTI | 09/2022

- Gained hands-on experience in network intrusion analysis, endpoint threat detection, and forensic investigation techniques.
- Explored SOC operations, threat intelligence integration, and security data visualization for enhanced decision-making.
- Learned to detect, analyze, and mitigate network threats using real-world scenarios and SOC workflows.
- Developed skills in continuous monitoring, compliance, and incident response for effective security operations.

Ethical Hacking and Network Monitoring

NTI | 08/2022

- Gained hands-on experience in ethical hacking techniques, including reconnaissance, vulnerability analysis, and system exploitation.
- Used network monitoring tools to detect and prevent attacks against protocols, services, and endpoints.
- Applied penetration testing methodologies to evaluate and secure networks against threats.
- Strengthened skills in identifying vulnerabilities, mitigating attacks, and analyzing network security alerts.

CCNA

NTI | 07/2022

- *Gained practical knowledge in configuring and managing Cisco routers, switches, and VLANs.*
- *Learned to implement and troubleshoot OSPF, Layer 2 protocols, and IP services for network optimization.*
- *Developed skills in securing network devices using techniques like Port Security.*
- *Applied expertise to real-world scenarios, ensuring efficient communication and resolving network issues through systematic troubleshooting.*

Languages:

- **Arabic:** Native
- **English:** Very Good

References:

References are available upon request.