Tharakeshwar Navarathinam

tharakeshwar007@gmail.com | +1 (814) 280-6258 | PA, USA | LinkedIn | Portfolio

SUMMARY

Network Security Engineer with 2+ years of experience securing hybrid enterprise networks through firewall policy enforcement, segmentation, routing, VPN connectivity, and cloud network controls. Applies Palo Alto, FortiGate, AWS, and Azure to strengthen access boundaries, while using Splunk, Wireshark, Python, and Ansible to investigate traffic behavior, validate changes, automate checks, and improve network reliability and security operations.

TECHNICAL SKILLS

Network Security & Architecture: Network Security, Zero Trust, Network Segmentation, Secure Network Design, Defense-in-Depth, High Availability

Firewalls & Secure Connectivity: Palo Alto Networks, Fortinet FortiGate, Cisco ASA, VPN (IPSec, SSL VPN), NAT, ACLs
Routing & Switching: TCP/IP, BGP, OSPF, VLANs, STP, MPLS, DNS, DHCP

Threat Detection & Monitoring: IDS/IPS, SIEM, Wireshark, Splunk, Syslog, SNMP, Packet Analysis, Network Traffic Analysis
Cloud & Infrastructure Security: AWS (VPC, Security Groups, NACLs, Transit Gateway), Azure (VNet, NSG, VPN Gateway), Load Balancers, SASE

Automation & Security Operations: Python, Bash, Ansible, REST APIs, Incident Response, Vulnerability Management, Patch Management, Change Management

PROFESSIONAL EXPERIENCE

Network Security Engineer, *PJM Interconnection* Jan 2026 - Present | PA, USA

- Configured Palo Alto firewalls and segmented network zones supporting PJM grid operations, applying ACLs and least-privilege policies to reduce unnecessary east-west access by 18% overall.
- Evaluated routing paths, VPN connectivity, and firewall logs across critical network segments, using Splunk and packet captures to isolate recurring latency, policy, and access-control issues.
- Integrated AWS VPC security groups, NACLs, and Transit Gateway controls with on-premises connectivity, strengthening hybrid segmentation while preserving required communications between monitored infrastructure zones securely.
- Automated recurring firewall rule validation and configuration checks with Python and Ansible, standardizing monthly security reviews and reducing inconsistent manual verification across approved network changes.
- Validated failover behavior, IDS alerts, and approved change implementations during controlled maintenance windows, resolving misconfigurations before release and reducing post-change network incidents by 15% overall.

Network Security Engineer, *Prodapt* Mar 2023 - Jul 2024 | Chennai, India

- Configured Cisco routing, switching, VLANs, and FortiGate firewall policies for 25+ telecom client sites, supporting secure branch connectivity across managed enterprise network service environments reliably.
- Analyzed BGP and OSPF routing behavior, IPSec tunnels, and packet captures with Wireshark, resolving recurring connectivity faults across customer WAN and internet edge paths efficiently.
- Integrated Azure VNet, VPN Gateway, and network security groups with customer WAN connectivity, enabling secure cloud access for distributed sites without disrupting existing routing policies.
- Monitored SNMP alerts, syslog events, and firewall health across managed network devices, applying standardized diagnostic workflows to accelerate incident triage and escalation handling consistently daily.
- Tested SD-WAN policy changes, VPN recovery, and routing convergence during maintenance windows, documenting validation results and reducing recurring connectivity escalations by 14% across managed sites.

PROJECTS

C2 Beaconing Discovery via Periodicity and Behavioral Features in Network Flow Logs | Python, pandas, scikit-learn, Gradio

- Built a Python, pandas, scikit-learn, and Gradio pipeline that standardized CTU-style flow logs, engineered pair-level periodicity features, and classified suspicious beaconing behavior.
- Added severity scoring, reason codes, DNS allowlisting, and CSV export, reducing analyst review effort by 35% and lowering false-positive investigations by 20%.

End-to-End Network Traffic Examination for Network Intrusion Detection using Feature Embedding Learning | Python, CNN-LSTM, Feature Embedding Learning

- Implemented feature embedding from raw network traffic, reducing manual feature engineering effort by 80% while preserving discriminative patterns for intrusion classification overall.
- Engineered a CNN-LSTM architecture combining spatial and temporal traffic features, improving intrusion detection accuracy by 25% over traditional baseline models during evaluation

CERTIFICATIONS

- **CompTIA Security+** | Issued Mar 2025 · Expires Mar 2028
- **Web Security and Bug Bounty, Udemy** | Issued Nov 2023
- **CyberSecurity and Ethical Hacking - Advanced, HCL GUVI** | Issued Jun 2023
- **IBM Cybersecurity Analyst - IBM** | Issued Sep 2022

EDUCATION

Master of Science in Cybersecurity Analytics and Operations, *Pennsylvania State University* Aug 2024 - May 2026 | PA, USA

Bachelor of Technology in Computer Science, *SRM Institute of Science and Technology* Sep 2020 - May 2024 | Chennai, India