**Trupti Patel**

**Senior Security Analyst / Engineer**

**ktruptee1008@gmail.com**

**Professional Summary:**

* Senior Security Analyst and L3 support engineer with 12 years of experience in Information Security, Networks, Network Security, and Engineering & Implementation.
* Creative, Strategic, Focused, Multi-functional with Cross-domain, Cross industry experience.
* Experienced working on multiple Hardware/Software environments and comfortable with complex heterogeneous systems environments.
* Excellent knowledge about Fireeye (NX, CM and Helix), Zscaler ZIA, Firewalls, AWS Cloud Services and Splunk.
* Expertise in Next Generation Firewalls, Load Balancers, Intrusion Detection System, Intrusion Prevention System, SIEM, Complex Network Infrastructure troubleshooting, managing security incidents, Management Reporting and Presentations.
* Experienced and comfortable hands-on working with Security Technologies. Comfortable in articulating low level details to various Implementation, Testing and Support Teams.
* Effective communicator, adept in bridging the business and technical communities
* Excellent skills to build productive relationships with partners, stakeholders and customers to foster business
* Experienced in working in SOC 24x 7 and with customers across Europe, Asia and America.

**Technical Skills:**

|  |  |
| --- | --- |
| **Vendors - Extensive Hands-on Experience** | Fireeye (NX, CM, Helix), Zscaler ZIA/ZPA, Palo-Alto, Gigamon, Checkpoint, Provider – 1, Cisco, Juniper, F5 Networks, SPLUNK, Remedy, Service now, Citrix |
| **Security Technologies** | Firewalls, Next Gen Firewalls, Load Balancers, Local Traffic Manager (LTM), Global Traffic Manager (GTM), Intrusion Detection System / Intrusion Prevention System (IPS/IDS), IPsec / SSL VPN, Advance Networking and Clustering, Antivirus, URL Filtering, Threat Prevention, Data Loss Prevention, Application Control, Palo Alto Global Protect |
| **Networking Hardware** | Fireeye (NX7400, NX5500), Checkpoint (26000/15000/16000/7000/6XXX & more), Palo Alto (7000/5000), Cisco ASA (5520/5550/5580), Juniper Net Screen (500/5200), Juniper SRX (4200/3600), Juniper SRX (4200/3600) F5 Load balancers (i5000/i7000), Cisco Switches, Cisco Routers. |
| **Network Monitoring** | Solar winds, Wireshark, HRping, TCP Dump, Infoblox, SPLUNK, fw monitor |
| **Operating Systems** | Gaia (Checkpoint), PAN-OS (Palo Alto), CentOS Linux (F5 BIG IP), Cisco IOS, Windows, KALI LINUX, MAC OS, Unix |
| **Simulation Tools** | VMware, GNS3, VMware, Cisco Packet tracer |
| **AAA Architecture** | TACACS+, RADIUS, Cisco ACS, Active Directory, Captive Portal |
| **Security Tools** | Qualys Guard, Metasploit, Nessus, Threat connects, Tenable, Nikto, Burp Suite, Alien Vault, Splunk, QRadar, Rapid 7, Proof point. |
| **Cloud and Distributed Computing, Proxy** | Amazon Web Services AWS, Zscaler ZIA |
| **Project Management Skills** | Task management, prioritization, delegation, task separation, scheduling, risk management, Scrum/Agile Methodologies |

**Professional Experience:**

**Senior Security Engineer**

**Hines,TX**

**Jan‘20–Now**

**Responsibilities:**

* Proficient in building, managing, administrating and troubleshooting of Fireeye Helix, CM and NX appliances.
* Worked extensively with Fireeye project including the following:
  + - Installing SSL/TLS certificate on each NX 5500 appliances
    - LDAP configuration.
    - Splunk configuration – making each NX device to send logs to Splunk.
    - Upgrade and licenses
    - Alert white listening
    - Adding device to Helix and CM for management and monitoring.
* Analyze logs generated by various sources including Palo-Alto, Fireeye, Zscaler and various tools using Splunk.
* Part of the project group involves in Designing, deploying and supporting Zscaler Cloud based Infrastructure across various Data Centers and Disaster Recovery environments.
* Migrating the policies from on premise Bluecoat to Cloud Based Zscaler Proxy service in tandem with various application owners.
* Work on Palo Alto Zone based Firewalls to create Zones and Policies for various segment of the network and accordingly troubleshoot any connectivity issues thereof across various Security Zones.
* Experience in Network Intrusion/ Host Intrusion detection/prevention systems and firewalls.

**Senior Security Engineer**

**T Rower Price, MD**

**Jan‘18–Dec 19**

**Responsibilities:**

* Configured, Troubleshoot and Maintained Firewalls policies on Palo alto including Security, NAT policy definitions, application filtering, Regional based rules, URL filtering, Data filtering, file blocking, User based policies.
* Proficient in design, implementation, management and troubleshooting of Check Point firewalls, Palo Alto IDS/IPS modules, F5 Load Balancers
* Advanced knowledge, design, installation, configuration, maintenance and administration of Checkpoint Advanced Knowledge in IPSEC VPN design connection and protocols, IPSEC tunnel configuration, encryption and integrity protocols
* Analyzing security incidents and providing timely resolution.
* Device management (log management, upgrades, configuration)
* Complex VPN troubleshooting and configuration.
* Specializing in Checkpoint, Palo Alto, F5 and Cisco Firewalls

**Senior Security Analyst**

**NTT Security (Nippon Telegraph and Telephone Corporation) - United Kingdom**

**Apr’13 – Apr’17**

**Responsibilities:**

* Member of an EU-SOC Security team providing Security support facility for Firewalls, IDS and IPS and associated devices for a Global client base.
* Providing – fault analysis / rectification of Ticketed issues, design and implementation of changes, and general day-to-day monitoring and managing of tickets and changes through ‘Remedy’ CRM.
* Hands on experience with Check Point, F5 LTM, Cisco, Juniper and Palo Alto.
* Performed Installation, Enrollment and Maintenance of 1200+ Checkpoint devices.
* Built and deployed Check Point Provider-1 new Customer Management Add-on (CMA) and Multi-domain Log Module (MLM) for new sites.
* Configured and tested scripted backups of the Provider-1 system and CMAs, verified scheduled backups of Check Point firewalls.
* Deliver security monitoring and alerting services, assisting with investigations as a result of escalated problems and security alerts from security information & event management systems
* Member of team tasked with enrolling devices into Integralis Managed Service.
* Providing proactive technical support in a timely and professional manner in alignment with SLA

**Senior Network Engineer**

**BSNL (Bharat Sanchar Nigam Limited) – Gujarat, India Jun’09 – Feb’13**

**Responsibilities:**

* Pre-sales consultant/support: Building and maintaining strong relationship with customers. Understanding technical requirements, responding to RFP’s and producing bill of materials (BOM), working with procuring team to create rough order of magnitude (ROM) cost, providing high quality presales technical consultation. Interpret and translate technical and business requirements into cost effective and reliable security solutions to meet customer’s needs.
* Responsible for producing the network designs and architectures, including TCP/IP and VLAN Engineering and associated Requests for Proposals (RFPs) for various BSNL Clients like Call Centers, Banks and SME business related information security technologies such as Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Access Control, Vulnerability Assessment, Anti-Virus, Cisco PIX Firewalls, VPN.
* Managed corporate Checkpoint Firewall implementing security rules and mitigating network attacks. Checkpoint security policies including NAT, VPN and anti-spoofing for internal, external networks as well as Internet gateways. Protect and authenticate local-net and DMZ.
* Responsible for setting up and secure deployment of information security system Firewalls, managing Software license and implementation of security policies, procedures and standards into the technical security environment and managing core network connectivity ensuring delivery of a scalable, secure, resilient network infrastructure.
* Developed quality documentation for internal organization ensuring that all detailed designs adhere to network standards.
* Address questions from internal and external audits and examinations.
* Develop policies, procedures and standards that meet existing and newly developed policy and regulatory requirements

**Trainings and Certifications**

* CCSA – Check Point Certified Security Administrator (Current).
* CCSE – Checkpoint Certified Security Expert (Certification due this month)
* ACE - Accredited Configuration Engineer (Palo Alto)
* CCNA – Cisco Certified Network Associate (Security)
* F5 - 101 - Application Delivery Fundamentals
* CISSP - Certified Information Systems Security Professional
* AWS - AWS Certified Security

**Educational Qualification**

* Masters of Science (MSc.) in Telecommunications – University College London (UCL)
* Bachelor of Engineering (B.E.) in Electronics and Communications
* Diploma in Electronics and Communications