**Sowmya Veeravalli**

**Mobile:** (669)799-6266 **Email:** sowmyaveeravalli67@gmail.com

**Professional Summary:**

**Network Security:**

* Certified Network Security Engineer | Ethical Hacker with extensive experience in cybersecurity, network security engineering, and Python development. Proficient in penetration testing, vulnerability assessment, and incident response. Skilled in utilizing a variety of cybersecurity tools and technologies to secure networks and systems against sophisticated threats. Strong background in developing and automating solutions with Python. Holds multiple certifications including CCNA, CCSA, AWS Associate Developer, OSCP, CISSP.
* Experience in working on Enterprise Network and Security devices both on-prem and Cloud.
* Experience with both Implementation and Operational type of work on Network and Security Platforms.
* Enterprise scale experience with Firewalls, Routers and Switches as well as next generation threat prevention.
* Experience with Security Gateway from Checkpoint R80 in Multi Domain Security environment with several hundreds of gateways as well as Palo Alto Firewalls, Fortinet and Cisco
* Working with Advanced blades such as Application and URL filtering, Intrusion Prevention (IDS/IPS)
* Working with amazon cloud services AWS including building and managing VPC’s, NACL, Security Groups, IAM.
* Experience working in an environment with Compliances such as PCI, HIPAA, SOX etc.
* Proven analytical, decision making, and problem-solving abilities.
* Basic understanding and implementation experience with Python and Ansible for network automation tasks that include automatic backups, config templates, tasks automation like software upgrades etc.
* Flexible, Capable of quickly learning new technologies and adapting to new environments.

**Certifications:**

* Cisco Certified Network Associate (CCNA)
* Check Point Certified Security Administrator (CCSA)
* AWS Certified Developer – Associate

**Education:**

* Master’s in computer science – Silicon Valley University, USA
* Bachelor of Technology (BTech) – Jawaharlal Nehru University, INDIA

**Cloud Engineer:**

* Cloud Network Engineer in designing and configuring AWS network infrastructure such as including IAM, EC2, EBS, VPC, RDS, Cloud Watch, Autoscaling, Cloud Front, SNS, S3, SQS, Lambda and Route53.
* Experience with IAM requirements for cloud - based services, including strategies, trust models, and open standards, encryption, etc. used to improve manageability, access governance, provisioning, information security, and privacy.
* Designing and configuring secure Virtual Private Cloud (VPC) through private and public networks in AWS by creating various subnets, routing table, Network ACL, NAT gateways.
* Configured AWS Elastic Block Storage (EBS), different volume types and use of various types of EBS volumes based on requirement.
* Setting up databases in AWS using RDS, storage using S3 buckets and configuring instance backups to S3 bucket.
* Excelled on creating AMI (AWS Machine Images) that utilizes ELB (Elastic Load Balancer) and Auto Scaling.
* Implemented a 'server less' architecture using API Gateway, Lambda, and Dynamo DB and deployed AWS Lambda code from Amazon S3 buckets. Created a Lambda Deployment function and configured it to receive events from your S3 bucket.
* Experience on the TCP/IP protocols RSH, SSH, RCP, SCP analyzing the error logs, analyzing the User logs, analyzing the /var/log/messages.
* Experienced with different kinds of Load Balancers in AWS Cloud to control the flow of traffic in AWS Cloud.
* Experienced in provisioning and deployed API Gateways by configuring different stages and writing rules.
* Creating Shell Scripts and Cron jobs to ease administration tasks and monitoring security issues.
* Configuring and maintenance of networking services and protocols on Linux including NIS/NFS, TFTP, FTP, DNS, SSH, DHCP, TCP/IP, SNMP, SSL, FTP, LDAP, HTTP, HTTPS, firewalls and VLANS and Routers.

**Other Security Skills:**

* Configure and tweak Checkpoint IPS Blades for false positives and Alerts.
* Build and troubleshoot Site to Site IPsec VPN and work with various business partners.
* Troubleshoot Phase 1 and Phase 2 Configurations and debug the VPN connectivity.
* Extensive hands-on experience in mitigating different DDOS attack types (UDP/ICMP Flood, SYN Flood
* HTTP Get Flood, TCP Connection Attack, TCP Flag-based Attacks) using Arbor systems.
* Investigates and resolves security incidents and recommends enhancements to improve security.
* Experience deploying and configuring URL Filtering Firewalls as well as Blue Coat Proxy series appliances and manage using Bluecoat Director.
* Identifying security risks and exposures, determining the cause of security violations and suggesting procedures to halt future incidents.
* Implemented data extraction, transformation, and loading (ETL) processes using Python.
* Built web applications using Python frameworks such as Django and Flask.
* Performed automation task as per the client requirement for devices using python and increased performance through automating network security tasks.
* Developed RESTful APIs to facilitate communication between different systems.
* Automated repetitive tasks using Python scripts, improving efficiency and accuracy.
* Integrated third-party APIs and services to extend application functionality.
* Conducted security assessments and implemented best practices for application security.
* Utilized containerization technologies like Docker to streamline development and deployment.

**Routing and Switching:**

* Planning, Designing & Implementing Secure IPsec based VPN solutions for both B2B and Remote Access
* Hands-on experience in routing with multiple VRF especially using EIGRP, OSPF and BGP routing protocols as well as route redistribution.
* Advance experience in STP, RSTP and MST.VLAN mgmt. and VTP. Layer 2 high availability using VRRP, HSRP
* Planning, designing, Installing and Configuring of Cisco Routers (ASR 1000, ISR 4000, 7600, 7200, 3900, 2900, 2800) & Cisco L2 & L3 Switches (Nexus 7000, 5000, 2000 and IOS 6500, 4500, 3750 series,).
* Designing & implementing Cisco 3-tier LAN Network Architecture (Core, Distribution and Access).
* Configuring Spanning Tree, Rapid Spanning Tree, MST, VLAN, VTP
* Redistribution of routing protocols, Route-maps (Policy Based Routing), access list and NAT.
* Implementation of HSRP, VRRP protocol on routers. VRF on Routers and build GRE Tunnels between Cisco routers.
* Configuring HPE routers and switches such as Procurve, 3COM, Aruba.
* Managing HPE aruba airwave systems and supporting wireless systems and access points.
* Configuring different WiFi networks such as Gust, Corporate and special as required.

**PROFFESSIONAL EXPERIENCE:**

**Client: Citizens Bank June 2021 – Till now**

**Role: Senior Network Security Engineer Springfield, OR**

* Conducted comprehensive security assessments and vulnerability scans to identify and mitigate risks.
* Implemented and managed firewalls, intrusion detection/prevention systems (IDS/IPS), and VPNs.
* Developed and maintained security policies and procedures in compliance with industry standards.
* Monitored network traffic for unusual activity and responded to security incidents in real-time.
* Configured and managed network security tools including Nmap, Wireshark, and Nessus.
* Implemented encryption protocols (SSL/TLS) and managed certificate authorities.
* Performed security audits and risk assessments to ensure compliance with security frameworks.
* Automated security tasks using Python scripts to improve efficiency and response times.
* Collaborated with IT and development teams to secure network architecture and applications.
* Provided training and support on cybersecurity best practices and tools to internal teams.
* Implementation, configuration and support of Checkpoint firewalls, Palo Alto Firewalls and Cisco Firewalls.
* Experience working with Data Center migration from Physical to AWS Cloud and implement security
* Responsible for performing security assessments on applications deployed within AWS
* Manage the Cisco ASA Hardware through CLI, ASDM as well as CSM. (CSM 4.6)
* Perform Zero down time upgrades on Check Point and Cisco ASA Firewalls as well as build and configure Active/Standby high availability with Stateful replication/sync
* Configured High Availability in active/standby mode on Checkpoint, Palo alto appliances.
* Firewall Policy provisioning and work with firewall requests submitted by users through change system.
* Cleanup and Optimize firewall rule base and database. Reorder rules for optimal firewall performance.
* Packet Capture using tools such as TCP DUMP to analyze traffic and troubleshooting connectivity issues
* Configuration and support of Check Point VSX and configure load sharing VS in VSLS Mode.
* Deploy Palo Alto Firewalls in Virtual VWIRE mode and enable zone protections.
* Installation, Configuration and troubleshooting of Palo Alto Firewalls running PAN OS 8.X and 9.X
* Firewall Policy provisioning on PAN devices using PANORAMA management platform.
* Manage Palo Alto Firewalls using Panorama configuring Device Groups and Templates
* Configuring Palo Alto Firewalls with multiple zones based on traffic segregation requirements.
* Configuring and support different types of NAT on PAN devices. Source/Destination based NAT
* Work with App-ID for application visibility and URL Filtering on PAN devices
* Work with different types of nat including Static, Destination, Source NAT
* Firewall Policy provisioning and work with Fortinet, Cisco ASA and Check Point firewall requests submitted by users through change system.
* Vulnerability Management including Assessments and security threat analysis.
* Build and provision new Checkpoint and Cisco ASA firewalls ground up and migrate existing rule base.
* Document all the errors and logs recorded during upgrade process on the staging hardware and work with
* Configuring B2B VPN tunnels with Business partners on various platforms such as ASA, Checkpoint
* Run packet captures and analyze for any VPN issues with phase 1 and Phase 2
* Implementation and Support of Checkpoint, Fortinet and Cisco ASA Firewalls in the network for various clients.
* Ensure Firewall Policy compliance as per client required standards.
* Troubleshooting connectivity issues within the server zones of the Data center.

**Client: Verizon June 2017 - June 2021**

**Role: Network Security Engineer West St, NY**

* Implementation, configuration and support of Palo Alto, Checkpoint, and Fortinet products.
* Firewall Policy provisioning and troubleshooting connectivity issues related to firewall.
* Setting up a Panorama Management Appliance on VMware ESX host.
* Experience with Implementing Windows Based User-ID agent and group mapping on PAN firewall.
* Perform Firewall cross platform migration from Cisco ASA to PAN firewall.
* Import PAN firewall into a Panorama Management Appliance.
* Experience with Template Stack and Device Group with Panorama to manage multiple PAN firewall.
* Configuration and administering the security policies on Panorama.
* Perform upgrades on PAN-OS devices in High Availability pair.
* Rapid firewall security assessments through Python automation.
* Successful Data Center Migration Planning and Successfully developed Python automation scripts to perform Cisco firewall rule assessments.
* Worked with various Security profiles, including antivirus, Anti-Spyware, Wild-fire analysis, Data Filtering,
* File Blocking, Wildfire and DOS Protection.
* Configure and implement URL Filtering on Palo Alto Firewalls.
* Cleanup and Optimize firewall rule base and database. Reorder rules for optimal firewall performance.
* Manage checkpoint security gateways split through multiple CMA’s and administer using provider-1.
* Work with Threat management from Palo Alto and tweak false positives and configure Security Profiles.
* Build site to Site VPN tunnels using communities on Checkpoint.
* Work on day to day changes on VPN wrt change of crypto access list / encryption domain
* Build and support IPsec site to site VPN for various extranet partners connected through internet.
* Maintain Configuration and network documentation using Visio and SOP documentation.
* Responsible for Checkpoint Firewall support and Troubleshooting, IOS Security Configurations, IPsec VPN Implementation and Troubleshooting, DMZ Implementation and Troubleshooting.
* Actively take part in Disaster Recovery exercise to failover and troubleshoot any underlying issues
* Documentation and draw network diagrams using MS Visio and use SharePoint portal as site repository.
* Firewall Policy provisioning and work with firewall requests submitted by users through Remedy system.
* Build and Upgrade Checkpoint Security Gateways as well as support upgrades of Checkpoint Clusters
* Troubleshoot complex problems, providing root cause analysis and remediation to mitigate future risk
* Worked on migration from Checkpoint to Palo Alto firewall using expedition tool.
* Configuring and rolling out Global Protect solution for the corporate users.
* Configured global protect portal, gateways, certificates, SSL/TLS profiles.
* Configured HA on Palo-Alto in Active and Passive mode.
* Perform migration from Websense URL filtering to PANDB URL filtering.
* Perform software upgrades on PA firewalls and Panorama in High Availability pair.
* Configuring Palo Alto Firewalls with multiple zones based with traffic segregation requirements.
* Troubleshoot IPsec Site to Site VPN connectivity including Phase1 (ISAKMP) & Phase2 (IPSEC)
* Review Firewall rule conflicts and misconfigurations as well as redundant rules.
* Identify unused rules and schedule change to revoke them and mark it for permanent deletion
* Updating Network Diagrams using MS Visio and Network documentation.
* Firewall Policy provisioning on platforms such as Checkpoint, Cisco ASA firewalls
* Work on B2B VPN Tunnels with business partners and Remote access VPN using ANYCONNECT
* Build High Availability using ClusterXL on checkpoint, Active/Standby HA mode on Cisco ASA.
* Configured Firewall logging, DMZs and related security policies and monitoring.
* Configuring VLAN, VTP, Spanning Tree, Trunking and Port channel configurations.
* Debugging abilities at lower levels of OSI layer (Switching, Network and Transport Layer).
* Implementation, configuration and support of Checkpoint and Fortinet firewalls for clients at data center.
* Installation and configuration of New Check Point Security Gateways, Fortinet and Cisco ASA Firewalls
* Performance Tweaking on firewalls including CoreXL, SecureXL etc.
* Firewall Policy provisioning and work with Fortinet, Cisco ASA and Check Point firewall requests submitted by users through change system.
* Troubleshooting Firewall Connectivity issues through packet capture utilities and debug level logs
* Creating object, groups, updating access-lists on Check Point Firewall, apply static, hide NAT using smart dashboard.
* Configure and administer Provider-1 with multiple CMA’s and manage CLM, CMA’s
* Perform Zero down time upgrades on Check Point and Cisco ASA Firewalls as well as build and configure Active/Standby high availability with Stateful replication/sync
* Work with different Check point platforms including IP Appliances, SPLAT and GAIA Products.
* Experience working with Check Point VSX and spin virtual firewalls in VSLS mode
* Manage policies in VSX and ensure the VS are equally distributed across all the physical nodes.
* Work in a Check Point VSX environment with Virtual firewalls including Virtual System Load Sharing
* Resource management on Check Point VSX and work in a Shared as well as dedicated modes

**Client: Piramal Pharma June 2015 - May 2017**

**Role: Network Engineer. Sellersville, PA**

* Responsible for Crossroads rollout of LAN/WAN, problem determination and diagnosis, provide project leadership (onsite, offsite)
* Working with local IT personnel on troubleshooting, problem determination, diagnosis of performance issues, bandwidth issues, throughput traffic prioritization to improve overall application response time cross WAN.
* Responsible for executing planned network infrastructure installations and configurations associated with the relocation of the NC FAST Camden and Bath Buildings networks into a new building
* Participating in the design and planning aspects of the network infrastructure that installed in the new building.
* Configuration and installation of LAN switches and wireless network infrastructure equipment and cabling all uplink and user network connections.
* Working with the DIRM Networking team and NC FAST IT staff to review current VLAN configuration, IP routing and firewall access control for existing networks, and applying the necessary network and security access rules to the installed equipment.
* Configuring & managing around 500+ Network &Security Devices that includes Juniper SRX Firewalls, F5 BigIP Load balancers and Nexus Devices
* Participating in testing of the internal network infrastructure in the new building, and troubleshooting and remediating any issues.
* Worked with network services like DNS, DHCP, DDNS, IP4, IP6, IPSec, VPN etc
* Worked with F5, CISCO ACE 4710 Load balancers, GSS and Wireless networks.
* Deployed Cisco Catalyst 6500, 4500, 4000, 3750, 3850, 3560 switches
* Installed and monitored extreme networks S-series, 7100 stackable switches and E4G-400, 1800 router to support VMware machines in NCFAST.
* Deployed and configured Cisco ASR 1000, 7000, 9000 series routers
* Also worked with Extreme networks wireless devices like Access points AP3705, AP3610.
* Experienced working with Nexus OS, IOS, CATOS and Nexus 7K, 5K & 2K Switches
* Have experience and worked with configuring session persistence and web services.
* Deployed Juniper switches EX4500 and EX4200, routers M7i and M10i and Junos OS
* Deployed Cisco 2500 and 5800 Series Wireless Controllers and Access Points
* Working with Cisco ASA 5525 firewalls with current and demonstrated expertise with ACL security in a multi-VLAN environment
* Worked with Firewall DMZ zones and configuring them.
* Worked with storage team in installing IBM Store wise V5000
* Experience in working with load balancer for converting CSS to F5
* Experience in working with LTM and GTM for scaling and securing DNS infrastructure during high volumes.
* Configured Multiprotocol Label Switching (MPLS) VPN with Routing Information Protocol (RIP) on the customer’s stage.
* Worked and performed troubleshooting, implementing, optimizing and testing of static and dynamic routing protocols such as EIGRP, OSPF, and BGP ability to interpret and resolve complex route table problems.
* Experience with Security- Firewalls, NAT / PAT, IPSEC, S2S.
* Experience with ALG (RTP, RTSP and FTP, DNS, HTTP), DHCP
* Worked with ITIL (Information and technology information library) for managing our services.
* Working with ITS networking teams to install an Avaya VoIP phone system and test phone system connectivity and functionality.
* Knowledge of with API’s for troubleshooting Network issues using Wireshark and NTOP
* Configured static NAT, dynamic NAT, dynamic NAT overloading.
* Back up a Cisco IOS to a TFTP server and Upgraded and restored a Cisco IOS from TFTP server.
* Configured and perform trouble shooting on Dell Power Connect Switch 5548 used to connect VM Servers and Flex Systems.
* In-depth expertise in the implementation, optimization, troubleshooting and documentation of LAN/WAN networking systems.
* Worked on a broad range of topics such as proactive monitoring and maintenance, disaster recovery exercises, and core network repairs
* Worked independently, meted deadlines provided detailed written status reports, documentation, work on multiple simultaneous projects and track status and progress on each.

**Environment:** Cisco 2948/3560/4500/3560/3750/3550/3500/2960/6500 switches and Cisco 3640/12000 /7200/3845/3600/2800 routers, Cisco Nexus 7K/5K/2K, Cisco ASA5510, Checkpoint, windows server 2003/2008: F5 BIGIP, LTM, OSPF, EIGRP, RIP, BGP, VLAN, VPN, Checkpoint, Juniper SRX

**Client: DEF Security Solutions Feb 2013 - March 2015**

**Role: Ethical Hacker India**

* Conducted comprehensive penetration tests on various systems, including web applications, mobile applications, network infrastructure, and cloud environments, identifying and mitigating security vulnerabilities.
* Led red teaming engagements simulating advanced persistent threat (APT) scenarios to evaluate the organization’s incident detection and response capabilities.
* Performed vulnerability assessments using tools such as Nessus, OpenVAS, and Nexpose to identify and prioritize security weaknesses.
* Developed and implemented custom scripts and tools for automation of repetitive penetration testing tasks, improving efficiency and consistency.
* Conducted social engineering exercises, including phishing campaigns, to assess and improve organizational awareness and response to such attacks.
* Performed security audits and compliance checks against standards such as PCI-DSS, HIPAA, and ISO 27001, ensuring adherence to regulatory requirements.
* Utilized advanced exploitation frameworks like Metasploit, Core Impact, and Cobalt Strike to simulate real-world attacks and identify weaknesses in security defenses.
* Executed wireless network penetration tests, assessing the security of wireless protocols (WEP, WPA, WPA2) and recommending enhancements.
* Performed thorough post-exploitation activities, including data exfiltration simulations, to evaluate the potential impact of successful attacks and inform remediation strategies.
* Collaborated with development and operations teams to remediate identified vulnerabilities, providing guidance on secure coding practices and configuration settings.

**Client: GHI Tech Solutions June 2012 - Feb 2013**

**Role: Junior Network Security Analyst India**

* Assisted in monitoring and analyzing network traffic to detect potential security threats.
* Conducted regular vulnerability scans and assessments on network infrastructure.
* Assisted in the configuration and management of firewalls and other security appliances.
* Developed and maintained network security documentation and incident response plans.
* Supported senior security engineers in the investigation and resolution of security incidents.
* Performed regular security audits to ensure compliance with organizational policies.
* Assisted in the implementation of security measures to protect sensitive data.
* Provided support for network security tools and applications.
* Participated in security training sessions to enhance knowledge and skills.