**Ram Reddy B**

**Sairamreddy985@gmail.com**

**430-901-2028**

**SUMMARY**

* Extensive experience in Networking Security and proven expert proficiency in designing, engineering, configuring, and maintaining of large enterprise network devices.
* Expert Level Cisco ASA, Fortinet Firewalls, PaloAlto, Vmware NSX, Check Point and Juniper SRX/Netscreen Firewalls Administrator.
* Configure all Fortinet Networks Firewall models (100E, 200E, 600D, 900D, 1500D, 3980E, 5001E etc.) as well as a FortiManager to manage large scale firewall deployments and FortiAnalyzer to collect logs from all FortiGate firewalls.
* Configure all Palo Alto Networks Firewall models (PA-500, PA-2000, PA-3000, PA-5000, NSX, PA-1000V etc.) as well as a centralized management system (Panorama) to manage large scale firewall deployments.
* Experience in Configuring, and managing the Cisco Cisco Firepower 4120, 9300 Series.
* Worked on Juniper devices MX-480, SRX-240, SRX-650, SRX-1500, SRX-5400, SSG-550 and EX-4300.
* Expert Level Experience in Configuring, Deploying and managing Pulse Secure Mag devices 2600, 4610, 6610 PSA 7000C, License Server.
* Experience in configuring and troubleshooting of routing protocols IGRP, EIGRP, OSPF, PIM and E/IBGP. Worked on core and edge routers configurations, with implementation of unicast-multicast, ipv4, ipv6, TCP/IP, UDP, Full mesh, Hub and Spoke, Hybrid and Virtual topologies with route reflector and SDWAN with Cisco Viptela and SILVERPEAK.
* WAN optimization utilizing Riverbed Steelhead, Cisco WAAS and Silverpeak appliances. Configured and installed devices into sites and production data centers
* Configuring and Implementing Security rules as per the business needs in Palo Alto Firewalls, Fortigate Firewall, Cisco ASA Firewall and Juniper SRX.
* Advanced Knowledge in Building IPSEC Site-to-site & Client VPN’s in Cisco ASA, Checkpoint and PaloAlto firewalls.
* Knowledge of DNS, Active Directory and Certificate Services (PKI).
* Experience in configuring and troubleshooting VLANS, VTP, STP, MST, Ether-channel, HSRP, VRRP, BGP, OSPF and EIGRP.
* Experience in deploying , troubleshooting and configuring Cisco Meraki Layer 2 and Layer 3 switches like MS 225 , MS 250 and MS 350.
* Expertise in installing, configuring, and troubleshooting of Cisco Routers (7200, 3800, 3600, 2800, 2600, 800) and installing, configuring, and maintaining Cisco Switches (2900, 3500, 3750 series, 6500 series).
* Configure and deploy Cisco 5508 and 5520 Wireless.
* Experience configuring Catalyst (2900, 3500, 3700 and 6500 Series), Nexus (7000, 5000 and 2000 Series) Switches, and Routers 9500,9350,7600,7200,2800, 3600, 4400 Series and Wireless AP's (1260, 3600) using CLI and GUI.
* Experienced setup, create test beds on Cisco LAP/WLC and Aruba IAP/Airwave/Clearpass
* Installing and Configuring Cisco ASA 5585 firewall with firepower module.
* Experience with Checkpoint Firewalls NG, NGX, NGR55, NGX R65, R70, R75, R80.10.
* Worked on the SIEM tools like SPLUNK and IBM QRadar.
* Extensive work experience on the firewall optimization tools like Tufin and Firemon
* Worked on Tipping point Intrusion Protection System management.
* Responsible for architecture, development, and maintenance of multi-vendor network environment, including, but not limited to Juniper, Arista, Cisco, F5, SD-WAN and SilverPeak
* Designed and configured Palo Alto Central Management Platform with Panorama.
* Designed Installed and Troubleshoot Palo alto firewalls with the cluster using Panorama.
* Completed Firewall, URL filtering, Anti-spam protection, Content filtering, Traffic shaping, IP address   
  filtering, Intrusion Detection System (IDS), and Intrusion Prevention System (IPS), configurations for various client sites.
* Experience in monitoring and analyzing the load balancing of network traffic using Wireshark and Solar Winds
* Experience Configuring VDC&VPC in Nexus Switches 7k, 5k and 2k.
* Configuring Nexus 2000 Fabric Extender (FEX) which acts as a remote line card (module) for the Nexus 7000.
* Experience with converting Cisco 6500 IOS to Cisco Nexus NX-OS in the data center environment.
* Configured URL and content filtering using Bluecoat SG Proxy’s.
* Ensure Firewall Policy compliance for standards including PCI, SOX auditing, and rule base remediation.
* Experience in configuring TACACS+, RADIUS and implementing with Cisco ACS.

CERTIFICATIONS & EDUCATION

* Cisco Certified Network Associate (CCNA)
* Palo Alto ACE Certified.
* Checkpoint Certified Security Associate (CCSA)
* Bachelors in Computer Science , JNTU Hyderabad 2013

WORK EXPERIENCE:

**Kaiser Permanante, San Jose, CA Jan 2022 - Till date**

**Network Security Engineer**

Responsibilities:

* Responsible for Palo Alto, ASA and Checkpoint firewalls configuration and administration across global networks.
* Integrating Panorama with Palo Alto firewalls, managing multiple Palo Alto firewalls using Panorama.
* Managed multiple Palo Alto Firewalls using Panorama.
* Designed and configured Palo Alto Central Management Platform with Panorama and Wildfire Deployment.
* Integrating Configuring RSA SecurID with ISE for Token based authentications using RSA Native method RSA RADIUS method for user's remote VPN users.
* Performed code upgrades to the Palo Alto Firewall from Panorama.
* Configuration and upgrading the Policies in the PaloAlto, Cisco ASA and Pulse Mag Devices.
* Configuring, deploying maintain SSL VPN in Pulse secure PSA 7000C devices.
* Migrating the Cisco ASA’s to PaloAlto using Palo Alto expedition tool.
* Configured and deployed the NGFW Firewall Features in PaloAlto, like SSL Decryption, User ID, Proxy, and DNS, IPS/IDS
* Implemented IPSEC Site-to-Site in Palo Alto Firewall, Cisco ASA.
* Worked on Source Fire, Tipping Point IPS/IDS Systems, vulnerability assessment tools like Nessus, Qualys, and SIEM tools like Arcsight, Rapid7, NetQos, Splunk and packet capture tools like WireShark, tcpdump.
* Design, Maintained, and upgraded various IDS and IPS solutions for clients. Vendors such as Snort, Tipping Point, McAfee, Cisco IDSM2, IOS IPS, ASA solution.
* Configuring of ACL’s, Implemented Static NAT and PAT for internet users to allow users all over the company to access different applications and also for the internet access.
* Implemented Proof Point Email protection and route all the corporate emails to Proof point.
* Responsible for all Forescout Nac Appliance Configure Monitor and Manage.
* Manage Bluecoat Proxy for our SSL Encryption and adding policy’s.
* implemented and managed Zscaler to Web security where allow the access to User based web policy’s
* Configuring, managing and maintaining the Cisco ISE, Forescout NAC appliances, Firemon, Microsoft EOP and proof point for email protection.
* Maintained and supported Solarwinds Orion Network Performance Monitor, Splunk, VMware Loginsight and LoginME.
* Cisco DN, Data Center with VxLAN / spine-leaf design, Cisco ACI POC, SD-WAN (SilverPeak) at more than 100 locations, Aruba ClearPass globally with profiles and policies for 802.1X and MAB, AnyConnect VPN ASA at all regional locations.
* Worked with team Managing and configuring Cisco Meraki Switches.
* Plan, document and deploy SDWAN solutions from different vendors ex. Cisco Meraki and VMWARE, Velocloud, Riverbed, Cisco DNA on 9300 and 9200 Cisco switches.
* Configured, management of and monitored SilverPeak SD-WAN product
* Co-ordinate with different application teams to figure out what firewall rules they needed in environment after the migration of their Firewall to new Firewall.
* Configuring networks to ensure their smooth and reliable operation for fulfilling business objectives and processes.
* Network connectivity design for AWS and Azure connectivity with best security practice including micro-segmentation, transport encryption and complete Account/VPC/VNET/AZ/Subnet design using AWS Transit Gateway & Transit Hub.
* Network security including NAT/PAT, ACL, and ASA/PIX Firewalls. Integrated Active Directory/LDAP with Palo Alto Next Generation Firewalls. Integrated LDAP with Palo Alto rule base and Global Protect Client VPNs.
* Perform daily maintenance, troubleshooting, configuration, and installation of all network components.
* In-depth knowledge of AWS and other public and private cloud infrastructure is required (including EC2, VPC, ELB, S3, EMR and IAM).
* Troubleshooted and deployed all servers in Azure.
* Experience in migration of IPv4 addresses to IPv6 addresses using mechanisms like Tunnel Broker, Transport Relay Translation (TRT), NAT64, DS-Lite and DNS64.
* Review requirements and migrate clients’s application and servers to either Azure or on premise from old Datacenters.
* Configuration of CISCO Routers 3600, 4000 Series and 3550, 4500 series switches.
* Migrated Cisco ACS from v5.4 to Cisco ISE for TACACS authentication. Build AWS cloud infrastructure. Automated network using Python
* Test all IPv6 connection technologies for performance and select those that meet or exceed our stringent guidelines.
* Trial, analyze, and gather information on IPv6 technologies and assess the impact on existing current infrastructure.
* Implemented and Configured IP Routing Protocols: OSPF, EIGRP, and RIPv2.
* Implemented and configured LAN Protocols: Ethernet, VLANs, VTP and STP.
* Overseeing security engineering aspects/Implementing content filtering/interception (Bluecoat, WAF) including SSL interception, authentication, and ICAP.
* Working with ticketing system ServiceNow to track and resolve problems and incidents

**Cisco, Raleigh, NC Jan 2020 – Dec 2021**

**Network Security Engineer**

**Responsibilities:**

* Design, Engineer, Deployment and Administration of Firewalls, Network Devices in for Datacenter /Cloud.
* Deployment, Migration of Palo Alto, 3220, 5260’s and 7050’s in HA pair for Multiple Data-centers without impacting Production
* Responsible for Migration from Legacy Cisco ASA firewall, Checkpoint, Juniper SRX to Palo Alto firewall. This includes objects. Object-groups, Security rules, NAT rules. Also move from Layer 4 port-based rules to Layer 7 application based rules.
* Implement the Next generation firewall features such as URL-filtering, AV, AS profiles, Vulnerability Protection, Threat Prevention. Also implement SSL Decryption Policies
* Deployment, Migrate form Cisco ASA to Cisco Firepower 2100/4100 with ASA logical system and FTD.
* Design, Engineer, Deploy, Remote Access VPN Solution for 15,000+ user with redundancy at multiple sites. On Cisco Firepower 4120 and 4150 appliances.
* Hands on experience in Aruba S2500 switches, Aruba 7200, 3600 series wireless controllers, Aruba IAP 105, Airwave Products and clear pass Servers.
* Configuring managing around 500+ Network Security Devices that includes Cisco Nexus and Juniper SRX Firewalls.
* Migrated from Cisco ACS to Aruba Clear pass.
* Configured 802.1X on all access layer switch ports for port security. Implemented MAC based, and Certificate based authentication to the end hosts.
* Working for a Large Environment with 100’s+ (Physical, Virtual) Firewalls spread across Multiple Data Centers, cloud with Cisco, Palo Alto, Juniper, Fortinet, and Checkpoint vendors.
* Expertise with Palo Alto Next-Generation devices.
* Monitoring Alerts on Tipping point IPS/IDS and running reports using NESSUS scanning tool.
* Monitoring Tipping point IPS/IDS and engage SOC team depends on the alerts and act accordingly.
* Deployment and Administration of Panorama to administer Palo Alto Firewalls.
* Collaborate with application owners to define dependencies, map dependencies for better application workflow within ACI or public cloud use.
* Support/Design deployment/ migration to ACI network
* Deployment ACI fabric to ensure each tenant is secured and has separation from other tenants. Use L3/L2 outs via common tenant
* Worked in an environment with Border leaf, Spine and Leaf architecture
* Incorporate Cisco Nexus 9000 NXOS to ACI fabric to work in concert with existing Nexus 7000s and ASRs for MPLS
* Deployment of Cisco Firepower 4150 Firewalls as edge Firewalls. Devices with FTD code for next generation features. Setup Cisco Firepower Management Center to manage Firepower Next generation Features such as IPS, Application Control, Advance malware protection (AMP)
* Deployment and administration of Fortinet Fortigate 3000, 1500D, 200D Firewalls
* Deployment, Administration with Of Firewalls with tools such as Forti Analyzer, Forti Manager
* Deployment and administration of Cisco ISE for NAC, AAA. This involves setup of Policy Elements, AV definitions, Profiling of Endpoints. End point compliance-posturing.
* Deploying Cisco ISE in wired environment to perform Dot1x port based authentication configure the Posture polices for users connecting to the corporate network.
* Implemented a wireless network infrastructure providing access to wired LANs to increase mobility and productivity on Cisco WLC 2106, Cisco 3550 switch, Cisco 1130AG and 1121G series APs.
* Created wireless LANs and configure interface association, security parameters, and radios used. Managed the wireless network through the WLC web GUI.
* Configured DHCP scope into Infoblox for new sites which includes subnets for wireless, voice, security, and data centers.
* Integrating Configuring Cisco Wireless LAN Controllers WLC with Cisco ISE to perform Dot1x authentication for Wireless users.
* Integrating Configuring Cisco ASA Firewalls with Cisco ISE to the Posture policy compliance for remote VPN IPSec, SSL AnyConnect users.
* Integrating Configuring RSA SecurID with Cisco ISE for Token based authentications using RSA Native method RSA RADIUS method for user's remote VPN users.
* Strong experience with Automation. Automation of large number of repetitive tasks for Multiple Vendors for backups, blocks etc using Ansible Playbooks and Python Scripts.
* Administer and use orchestration Suite Firemon/ Tufin / Algosec to manage configurations, Backups, check compliance on firewalls.
* Experience with Deployment of Firewalls on AWS
* Experience with AWS, VPC, NAT’s, networking on Cloud, Troubleshoot issues leveraging VPC flow logs and researched Security incidents, alerts based on Splunk network Flow and Log Activity.
* Worked on Standardizing nonstandard configurations and reduced hardware and software variability.
* Experience with Splunk Security Infrastructure and Event Management. (SIEM). Using Splunk for search and analysis of logs.
* Troubleshoot and researched Security incidents, alerts based on Splunk Network Traffic Flow and Log Activity.
* Dedicated security monitoring and analysis of Cyber security events (Triage) of tracking phishing URLs, and emails and deep dug investigations.

**CFS, Boston, MA Dec 2017- Dec 2019**

**Network Security Engineer**

**Responsibilities:**

* Assisting with Zscaler cloud security deployment and configuration of ZPA (Zscaler Private Access) VPN solution.
* Employing Zscaler ZTNA (Zero Trust Network Access) to replace currently used Cisco any - connect VPN.
* Configuration of Zscaler internet access, ZIA, for system security outside of the office.
* Also took part of Call manager upgrade project. Controlled & monitored network traffic, route policy setup, web-filtering with Palo Alto 3020, Cloud base Zscaler firewall and various models of Fortinet Firewalls in US and overseas.
* Worked with vendors like Zscaler proxy and content filtering also using their expertise for recommendation of enforcing security policies using Cisco ISE/NAC for Centralized Policy, Posture Assessment, Guests Access Services and Device Profiling
* Responsible for answers and solutions about security related new technologies security related and any new cyber threats.
* Experience in Network Security that includes perimeter security for Internet, Extranet, DMZ, Internal Server farms, Web-traffic security with Proxies, Web Application firewalls. Worked and migrated multi-vendor equipment and Next generation firewall technologies. Worked on ASA, Firepower, Checkpoint and Palo Alto firewalls. Experience on MWG, Bluecoat and Zscaler proxies.
* Worked on Zscaler cloud proxies. Migration from Bluecoat Proxies to Zscaler cloud solution. Implemented GRE tunnels from Data Centers on F5 to Zcloud. Configuration of Policies, AD groups, Azure AD authentication, Whitelist, Blacklist and SSL inspection rules.
* Worked on FortiGate firewalls. Worked on migration from cisco ASA to FortiGate Firewalls. Worked on deploying site to site VPN tunnels, Security policies, NAT policies, URL filtering, VDOM, Forti Manager, User ID based Security policies, SSL forward proxy, SSL decryption.
* Worked on Software Defined Network (SDN) controllers Cisco ACI, Open Daylight and SDN protocols OpenFlow and Netconf, SD-WAN and Network Function Virtualization (NFV).
* Designed for SD-WAN team and deployed Silverpeak SD WAN devices to branch offices; member, Z-Scaler project using Z-Scalers on top of Silverpeaks to replace Palo Alto firewalls.
* Design virtualized/Cloud computing network with the SAAS leveraging Amazon AWS. Assess current network routing and switching to identify mission critical real-time solution and define best path.
* Extensive knowledge in configuring and deploying Next Generation Firewalls including Palo Alto, Cisco ASA, and Checkpoint Firewalls.
* Profound working knowledge of administration and management of Palo Alto firewalls using centralized Panorama M-100 and M-500 devices

**Emblem Health, New York, NY Feb 2016- May 2017**

**Sr Network Engineer**

**Responsibilities:**

* Worked primarily as a part of the Security team and daily tasks included firewall rule analysis, rule modification and administration.
* Installed, configured and troubleshooted firewall issues on the Checkpoint R77 Gaia, MDM, Smart Console, Checkpoint 12k Appliances and open platform servers.
* Configuration of Palo Alto firewalls per client topology and features such as Application & URL filtering, Security Profiles and Global Protect VPN solutions.
* Experience in building VPN’s in global protect and Knowledge to manage wildfire.
* Configure and implement URL filtering PAN DB
* Configuration and Maintenance of ASA 5585 firewalls with firepower, 5540, 5525 Firewalls using Cisco Security Manager (CSM).
* Worked on the migration of Cisco ASA 5540 Firewalls to PaloAlto firewalls using PaloAlto conversion tool.
* Have experience in building different firewall vendor technologies like Checkpoint, Cisco and PaloAlto from scratch.
* Experience in working with Cisco Nexus 7K, 5K & 2K Switches.
* Performed network implementation that includes configuration of routing protocols, leased lines, ISDN lines, VLANs and IOS installations
* Configured and deployed VPC, OTV, FABRIC PATH between Nexus 7k and Nexus 5k,5548 switches along with FEX2248
* Provided ongoing administration and support for authentication service using RSA SecurID and Cisco RADIUS servers for internet-based remote access vpn solution.
* Installation, configuration and troubleshooting of Cisco Routers (ASR 9K, NSX 5K, Meraki MX84, CISCO ISR 1K, 7600, 3800, 2800, 2600, 1800 series) and Juniper Routers (MX, PTX, T4000-series)
* Worked on the Tufin secure track and Tufin Secure change module to clean up and optimizing the security policies.
* Performed upgrade process for Cisco ISE software from version 1.0.4 to 1.1 ADE-OS, patch management and data backup management.
* Replaced old 6500 and WAN routers from DR testing site and Installed Nexus 7K and ASR 6800routers.
* Supported Infoblox appliances grid environment for DNS, DHCP and IP Address Management tools (IPv4).
* Managing AD, DHCP, DNS and Print Services for end client for different projects
* Configured Palo Alto Networks Firewall models (2k, 3k, and 5k) as well as a centralized management system (Panorama) to manage large scale firewall deployments.
* Experience on working with Palo Alto Next Generation firewall with security, networking, and management features such as URL filtering, Anti-virus, IPsec VPN, SSL VPN, IPS, Log Management etc.
* Installed Solar Winds Network Performance Monitor with traffic analysis, application & virtualization management, configuration management and other modules additionally installed.
* Implement URL filtering requests in Bluecoat Proxy SG for website blocklist and whitelist purpose.
* Provided redundancy in a multi homed Border Gateway Protocol (BGP) network by tuning AS-path.

**Global Aviation Services Pvt. Ltd, Hyderabad, India Sep 2014 – Jan 2016**

**Network Engineer**

**Responsibilities:**

* Cisco ASA 5505, 5510 design, implementation, configuration and troubleshoot. Basically, creating Lan Firewall, VPN, access-list, remote VPN.
* Migration from 2500 series to 2600 series Routers.
* Installed, configured (through CLI & SDM) and managed CISCO routers and Catalyst switches.
* Performed Troubleshooting and monitored routing protocols such OSPF, EIGRP & BGP.
* Configured ACL & NAT through CLI.
* Experience with protocols such as IEEE 802.11 and VLAN, OSPF and BGP, DNS, DHCP, FTP, NTP, SNMP, SMTP and TELNET.
* Provides updates and upgrades to the Palo Alto Firewall and Panorama devices
* Implemented firewall rules in Palo Alto firewalls using Panorama for one of the environment.
* Monitoring and troubleshooting traffic on Palo Alto firewall.
* Creating and managing admin users and troubleshooting the issues by using juniper SRX.
* Firewall filtering and NAT, Adding and modifying the policies in juniper SRX.
* Maintained and supported Solarwinds Orion Network Performance Monitor.
* Designing, configuring and troubleshooting ASA failover for the customer network
* Involved in customer escalations and troubleshooting issues related to connectivity, STP, VLAN, Trunking, VTP, Layer 2/3 switching, Ether channels, Inter-VLAN routing, log messages, high CPU utilization and parameters that can degrade performance of network.
* VLAN Configurations, troubleshooting and Firewall ACLs and Object-Groups configuration and support.
* Upgrade the network by translating protocols like EIGRP to OSPF.
* Provided technical support and problem resolution for the LAN and its environment by analyzing the problem, identifying the cause and circumstances of the problems and finding a solution to the identified problem.
* Add, delete, and modify rules on Checkpoint firewalls.
* Experience with working on some ecommerce technologies.
* Set up Internet, implementing Networking products like Servers, Proxy servers, Switches, Firewalls, Routers.
* Analyze IP data using industry standard tools i.e. Wireshark, SolarWinds.