**Bhargav**

**Network Security Engineer**

**Professional Summary**

* Experience working in large-scale environments on L1/L2 troubleshooting, Network Design, IDF and MDF architecture, Datacenter Architecture, Spine Leaf Architecture, and support roles, IOS upgrades, downtime procedures, Migration projects to different vendor equipment.
* Experience working in complex environments which includes Layer 2 Switching, L3 routing, Network security with perimeter and VPN firewalls, Load balancing and Access policies management in F5 and Wireless LAN Controllers.
* Experience in installing, configuring, and maintaining Cisco Switches (2960, 3500, 3750, 3850, 4500, and 6500) in enterprise Environment and Nexus 2k, 3k, 5k, 7k and 9k in Data Center Environment.
* Expertise in installing, configuring, and troubleshooting Juniper EX Switches (EX2200, EX2500, EX3200, EX4200, EX4500, EX8200 series).
* Experience in VSS, VPC, and VDC technologies. Experience working on Gateway redundant protocols HSRP, VRRP, and GLBP. Experience with Access, Distribution and Core Layer Architecture and Spine Leaf Architecture in Datacenter.
* Expertise in installing, configuring, and troubleshooting of Cisco Routers (3800, 3600, 2800, 2600, 1800, 1700, 800, ASR 9k) and Juniper Routers (E, J, M, and T-series).
* Experience and high-level technical knowledge in OSPF, EIGRP, RIP and BGP routing protocols. L1/L2 troubleshooting skills in Routing in complex environments. Worked with MPLS over BGP. Worked on upgrading Edge routers, failing over ISP circuits for maintenance. Knowledge in EVPN, VXLAN, VTEPS.
* Advanced knowledge of OSI model, TCP/IP, Internet technologies, system security, firewall infrastructure, network architecture and Cisco network routing / switching (Layer 2 and 3) experience, including LAN and WAN, design and implementation which includes Layer 1 to Layer 7 experience
* Strong experience in Network security using Juniper SRX, ASA Firewall, Checkpoint, Palo Alto, Cisco IDS/IPS and IPSEC/SSL VPN.
* Worked on different firewall & security appliance such as, Checkpoint 4400,4600,4800, 21700,Palo - Alto 200,500,3020,3060, 5020,5060, Panorama M-100/500, Juniper SRX 240, 650, 1400, 3400. Junos Space, Cisco Sourcefire, FireEye, Imperva (WAF).
* Manage, operate, and analyze data from corporate security systems including Sourcefire IDS.
* Expertise in network protocols, Firewalls and Communication Network design.
* Migrated and implemented new solutions with Juniper SRX 240, 650, 1400, 3400.
* Configuring Site-Site VPN on Juniper Firewall with SRX 1400, 3400.
* Managed multiple security devices in order to protect the Enterprise’s network - Vulnerability Scanners, Malware Detection, Intrusion Detection; Host based Firewalls, SIEM, Web Application Firewall
* Implemented Juniper FW Interface, NAT and VLAN using Junos Space..
* Advanced knowledge, design, installation, configuration, maintenance, migration and administration on Juniper SRX device.
* Experienced in handling Junos Space Network management to administer Juniper devices.
* Checkpoint VPN-1/ Firewall-1, 3D Analysis, GAiA, Standalone & Distributed setup, Security management, Log server, Secure platform (SPLAT), License management.
* Advanced knowledge, design, installation, configuration, maintenance and administration of Juniper SRX Firewall, Juniper EX 2500, 4500 and Juniper MX 240,480 devices.
* Implemented security policies using ACL, Firewall, IPSEC, SSL, VPN, IPS/IDS, AAA(TACACS+ & RADIUS)
* Hands on experience with packet sniffer, TCP DUMP and Wireshark for packet monitoring.
* Configuring & Managing LAN, WAN, VPN and Firewall of Juniper MX Routers for End Users and VLAN on Juniper EX series switch 2500, 4500.
* Work experience on Bluecoat Proxy SG for Content filtering and URL filtering.
* Proficient in design, implementation, management and troubleshooting of Check Point firewalls, Check Point Provider-1 / VSX, Palo Alto IDS/IPS modules, Data Center Migration, F5 Load Balancers, Blue coat URL filtering.
* Experienced in Deploying Wireless Network Infrastructure and Wireless Survey Best Practices
* Basic knowledge of CISCO ACE and F5 Load Balancers.
* Advanced knowledge in TCP/IP suite and routing protocols, such as OSPF, EIGRP, and BGP.
* Knowledge of Python and Linux shell scripting language.
* Knowledge in Documenting and preparing the Process related Operational Manuals.
* Finely tuned analytical/critical thinking and debugging skills with excellent verbal and written communication skills.
* Highly enthusiastic, creative team player, project implementation, analytical, interpersonal and communication skills

**TECHNICAL SKILLS**

Firewalls: Juniper SRX, Cisco ASA, Palo Alto, Checkpoint

Juniper Routers: 40, 80, 240, 480, 980

Juniper Switches: 2200, 2500, 3300, 4200, 4500, 8200

Nexus Switches: 7000, 5500, 5000, 2000

Other Hardware: F5 BIG-IP LTM Load Balancer, 7960 IP Phone

Networking: TCP/IP, UDP, ICMP, LAN, WAN, DHCP, DNS, FTP, TFTP, SNMP, ARP

Other Protocols: HSRP, GLBP, VRRP, QoS/CoS, VoIP, IPv4, IPv6, IP SLA

Security: ACL, NAT/PAT, ASA (5505, 5510) FirewallLoad Balancer: F5 Networks (Big-IP) LTM 6400, 1600

Routing: EIGRP, OSPF, RIP, BGP, MPLS, PPP

Switching: VLAN, VTP, STP/RSTP, Ether-Channel (PAgP, LACP), CEF

Operating Systems: Win XP, Win 7, Win 8, Win Server 2003, working knowledge of Mac OS X and Linux

Applications: Wire shark, PRTG, VMware, MS Visio, MS Office, Adobe Photoshop and Illustrator

**Professional Experience**

[**Harbor Freight Tools USA, Inc.**](https://www.indeed.com/cmp/Harbor-Freight-Tools?campaignid=mobvjcmp&from=mobviewjob&tk=1iavftf77go79800&fromjk=93780649304b8d18) **Calabasas, CA Sep 2022 to till the date**

**Network Security Engineer/ Firewall Engineer**

**Responsibilities:**

* Designs, tests and deploys IT security systems, solutions and ecommerce environment.
* Working on Secure Change/Remedy ticket management tool by providing support service to client by implementing and working on change request, Incident request and troubleshooting.
* Configuration of Juniper and Palo Alto firewall according to client topology and features such as Application & URL filtering, Security Profiles, VPN, Data filtering and file blocking. Antivirus
* Configuration of Palo Alto Next-Generation Firewall mainly VSYS according to client topology and working on Content-ID, User-ID, App-IP
* Experience on working on Cisco IPsec VPN, SSL VPN and natting
* Firewall technologies including general configuration, optimization, security policy, rules creation and modification of Palo Alto and Juniper Firewall
* Experience in Qualys policy compliance in detecting internal and external threats and vulnerability
* Worked on IBM QRadar SIEM tool for network/log monitoring an troubleshooting.
* Experience in working with designing, installing and troubleshooting of Palo Alto firewalls
* Create policies, alerts and configure using SIEM tools (Splunk, IBM QRadar)
* Installation of Palo Alto (Web Application and URL filtering, Threat Prevention, Data Filtering)
* Experience in Configuration, Management, Deployment, Optimization and Troubleshooting Juniper Firewall
* Performed upgradation of Palo Alto firewall from old platforms to new platforms 6.1.5 to 6.1.10
* Implemented Zone Based Firewalling and Security Rules on the Palo Alto Firewall
* Worked on network packet analyzer tools such as, Wireshark, Microsoft Network Monitor, Snort, Tcpdump
* Experience with working on Palo Alto centralized management GUI PANORAMA
* Experience with working on Palo Alto Next-Generation firewalls security profiles and Cisco ASA VPN
* Experience in working with Cisco 5500-X Firepower and Cisco Sourcefire IPS & FireEye
* Experience on working with migration with both Juniper and Palo Alto Next-Generation.
* Worked on security tools and software’s like Cisco WSA, Qualys, Splunk, Symantec Endpoint Protection, QRadar.
* Upgrading Impervav WAF (Web application firewall) and fixing hot fixes and patches.
* Exposure to wild fire advance malware detection using IPS feature of Palo Alto
* Experience on working in datacenter and on different devices console
* Maintain a thorough understanding of the basics behind the Internet and its workings (DNS, Security, IP Routing, HTTP, VPN)
* Configured Site to Site IPsec VPN tunnels and Split tunnel to peer with different clients. Routing and Switch protocols: BGP,OSFP, VLAN,VTP, STP, RIP, RSTP
* Firewall deployment, rules migrations, firewall administration and converting existing rule based onto new Checkpoint and Palo Alto Next-Generation Firewall platforms.
* Responsible for planning, documenting and implementation of complex Firewall and VPN solutions
* Represent the changes at the weekly change review and application migration meetings.

**Client:** [**Indiana University**](https://www.indeed.com/cmp/Indiana-University?campaignid=mobvjcmp&from=mobviewjob&tk=1iavfvn2pge6t800&fromjk=1d1a403a47ba3775)**, Bloomington, IN**

**Role: Sr Network Information Security Engineer Jan 2021 – Aug 2022**

Role - To Design, Maintain and troubleshoot issues in Datacenter Network in all areas which include switching, routing, Firewalls and Load balancer. Project includes several migrations from Cisco routers to Juniper, ACE to F5, ASA to PA firewalls etc. Design of DMZ trained in Spine Leaf Architecture.

Responsibilities:

* Worked as a part of network team where my daily tasks included configuring, monitoring, and troubleshooting of TCP/ IP networks. Configuring & managing around 500+ Network &Security Devices that includes Cisco Routers & Switches, Nexus Switches, Juniper and Palo Alto Firewalls, F5 BigIP Load balancers, Blue Coat Proxies and Riverbed WAN/MAN Optimizers.
* Palo Alto design and installation (Application and URL filtering, SSL decryption, SSL Forward Proxy). Configured and maintained IPSEC and SSL VPNs on Palo Alto Firewalls. Successfully installed PA-5000 series firewalls in Data Center as perimeter Firewalls.
* Collaborate with network engineering teams, software developers, and DevOps practitioners to leverage YAML as a common language for expressing infrastructure requirements, automation workflows, and operational procedures.
* Configure and manage FortiGate firewalls to enforce security policies, control traffic, and protect the network perimeter from unauthorized access and cyber threats. Managed day-to-day operation of the company's network infrastructure, including routers, switches, firewalls, and VPNs.
* Configured and maintained Windows Server 2019 and 2022 servers, ensuring high availability and reliability.
* Led the deployment and configuration of WAN routers across multiple locations, ensuring secure, reliable, and high-performance WAN connectivity using Cisco and Versa platforms.
* Managed the end-to-end configuration of WAN routers, including IP routing, VPN setup, QoS policies, and redundancy configurations to optimize network performance and ensure business continuity.
* Designed and implemented SD-WAN solutions using Cisco and Versa platforms, enabling intelligent traffic management, dynamic path selection, and enhanced security for WAN links.
* Developed Python scripts to automate network configuration tasks such as VLAN provisioning, IP address management, and firewall rule updates, significantly reducing manual effort and minimizing errors.
* Created Python scripts to interact with network devices via RESTful APIs, automating tasks such as device configuration, status monitoring, and data retrieval across a multi-vendor environment.
* Automated the management of network configurations using Python, enabling version control, automated backups, and deployment of configurations to Cisco, Juniper, and Palo Alto devices.
* Wrote Python scripts to parse and analyze logs from network devices, generating alerts and reports for anomalies, security events, and performance metrics.
* Utilized Bash scripting to automate routine system administration tasks, such as user account creation, file system management, and system updates on Linux/Unix servers.
* Developed Bash scripts to automate network diagnostic tasks, including ping sweeps, traceroutes, and interface status checks, providing quick insights into network health.
* Implemented automated backup processes for configuration files and critical data using Bash scripts, ensuring regular backups and secure storage of network configurations.
* Created Shell scripts to monitor system performance metrics (CPU, memory, disk usage) and network statistics, triggering alerts when thresholds were breached.
* Automated the deployment of software and patches across multiple servers using Shell scripts, streamlining the update process and ensuring consistency across the environment.
* Successfully deployed and managed Cisco ISR routers (2800, 2900, 4000 series) for branch office and WAN connectivity, including configuration of MPLS, VPN, and dynamic routing protocols such as OSPF, BGP, and EIGRP.
* Hands-on experience with Cisco Nexus switches (5K, 7K, 9K series) running NX-OS, including the deployment of VPCs, FabricPath, and OTV for scalable, high-performance data center networks.
* Managed IOS and NX-OS software upgrades on both Catalyst and Nexus platforms to ensure devices run the latest security patches and features, minimizing downtime during maintenance windows.
* Configured and managed IPSEC VPN tunnels for secure communication between remote sites and data centers, including the integration of IPSEC with dynamic routing protocols such as BGP to maintain connectivity during failover.
* Expertise in configuring BGP for WAN routing and OSPF for intra-enterprise routing across large-scale networks, ensuring optimal path selection and load balancing across multiple WAN links and ISPs.
* Configured and implemented FHRP protocols like HSRP, VRRP, and GLBP to provide high availability and automatic failover for critical network gateways.
* Deployed and managed WLAN solutions, including setting up wireless access points, configuring SSIDs, and applying QoS policies to prioritize voice, video, and critical data traffic in enterprise networks.
* Experience managing and troubleshooting DNS and DHCP services in enterprise environments, including the configuration of IP address pools, static reservations, and domain resolution to ensure network efficiency.
* Configured VLANs, trunking, and STP technologies (RSTP, MSTP, PVST) on Cisco switches to ensure proper segmentation, loop prevention, and optimal forwarding across complex Layer 2 networks.
* Configured and managed SonicWall firewalls, including setting up rules, NAT policies, and VPNs for both site-to-site and client-to-site connectivity.
* Experience configuring Fortinet firewalls with advanced security features, including IPSEC VPNs, intrusion prevention (IPS), and application control, ensuring the protection of critical network resources.
* Hands-on experience deploying Cisco FTD for integrated firewall and security management, including configuring next-generation firewall policies, intrusion prevention, and URL filtering.
* Performed firewall rule audits and optimization on SonicWall, Fortinet, and Cisco FTD platforms to eliminate unnecessary rules, enhance security, and improve performance.
* Proficient in using SolarWinds NPM (Network Performance Monitor) for proactive network monitoring, generating alerts for critical network events, and providing visibility into bandwidth usage, device health, and performance trends.
* Developed custom dashboards in SolarWinds to display real-time performance data for critical devices and links, allowing for quick identification of potential network bottlenecks or issues.
* Utilized SolarWinds, Wireshark, and other tools to diagnose and resolve complex network issues related to latency, packet loss, and security breaches, ensuring rapid incident response and resolution.
* Managed network configuration backups, automated device configuration changes, and monitored compliance with SolarWinds NCM (Network Configuration Manager), reducing configuration drift and improving security compliance.
* Employed NetBrain for real-time network visibility, mapping, and automated troubleshooting workflows, enabling efficient
* Generated detailed network performance and security reports using SolarWinds and NetBrain to analyze trends, optimize network traffic, and ensure alignment with organizational objectives.
* Extensive experience in configuring, managing, and troubleshooting MS Windows Server environments, ensuring high availability and optimal performance.
* High-level network troubleshooting and diagnostic experience using Packet capture tools like Wireshark.
* Regular upgrade and maintenance of Infrastructure, Installing, configuring, and maintaining Cisco Switches (2960, 3500 ,7600, 3750, 3850 series, 6500 series) Cisco Routers (4800, ASR 9K, 800), Juniper Routers and Firewalls, Nexus 7k,5k & 2k, f5 BIG IP, Palo Alto Firewalls, Bluecoat Proxy, Meraki and Riverbed Steelhead appliances.
* Assist in creating network design standards for hardware and software. Developing and maintain Network Documentation (Visio diagrams, Excel spreadsheets, Word documents, etc.) Configure and troubleshoot network elements in a test/dev environment.
* Worked on Orion (Solar Winds) for mapping network diagrams, updated Orion with commissioned and decommissioned network devices.
* Environment: Cisco Routers (4800, 3800, 3600, 2800, 2600, 2900, 1800, 1700, 800), switches (6500/3750/3550 3500/2950), F5 Load balancing (LTM, GTM, APM, AFM, ASM), EIGRP, RIP, OSPF, Voice Gateways, BGP, VPN, MPLS, Ether Channels, Cisco Catalyst Switches, Firewalls (Cisco ASA, Palo Alto), Cisco Voice (CCM, UCCE), Shell Scripting.

**Crum & Forster Insurance, Morristown, NJ Nov 2019 to Dec 2018**

**Firewall Specialist**

**Responsibilities:**

* Manages, maintains and support Juniper, Palo Alto Firewalls, IPS/IDS, Endpoint Security products, PKI and network security Infrastructure.
* Designed and implemented an enterprise wide Intrusion Detection system utilizing IBM/ISS Proventia IPS sensors and IBM/ISS SiteProtector
* Ability to configure and monitor security tools such as security information and event management (SIEM).
* Extract the logs, Perform real time log analysis using SIEM technologies and Forensics Analysis of logs as per the request.
* Engineered Juniper infrastructure which consists of 500+ firewalls running different flavors of Juniper hardware (SRX-240, 650, 1400, 3400, 3600) and vSRX.
* Configured, installed and maintained McAfee endpoint security on management and policy servers.
* Migration and implementation; new solutions with Juniper firewall administration across our global network.
* Responsible for planning, documenting and implementation of Juniper Firewall and VPN solutions
* Experience on working with Juniper SRX and 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.
* Provide initial fault isolation, proactive maintenance and monitoring of Company’s Network Equipment. Perform monitoring and support of internal network security.
* Configure all Palo Alto Networks Firewall models (PA-2k, PA-3k, PA-5k etc.) as well as a centralized management system (Panorama) to manage large scale firewall deployments
* Installation of Junos SPACE Network management for creating policy, Application and URL filtering
* Exposure to wild fire advance malware detection using IPS feature of Palo Alto
* Successfully installed Palo Alto Next-Generation PA-3060, PA-5060 firewalls to protect Data Center with the use of IPS feature.
* Configured Site to Site IPsec VPN tunnels to peer with different clients and each of client having different specifications of Phase 1 and Phase 2 policies using Juniper SRX 3400 series firewalls.
* Implemented Positive Enforcement Model with the help of Palo Alto Networks
* Checkpoint log server upgrade from R71.40 to R75.40 to take advantage of Smart logs.
* Firewall management server redesign and consolidation to one management server environment.
* Configuring Site-Site VPN on Checkpoint Firewall and Palo Alto firewall.
* Experience with convert Checkpoint VPN rules over to the Cisco ASA solution. Migration with both Checkpoint and Palo Alto rules.
* Experience with Cisco ASA firewall Cisco security Manager (CSM) and migration from Cisco to Palo Alto
* Experience on Palo Alto Advanced Endpoint Protection (TRAPS) and Migration tool 3.0
* Worked on Blue coat Proxy SG 600, 900 appliance for content filtering, Blue coat policy align with corporate security policy with VPM (Visual Policy Manager).
* Worked extensively on policy construction, policy optimization on Blue coat SG appliance.
* WAN Optimization using Blue Coat Packet Shaper appliance for monitoring, traffic shaping and compression for better bandwidth utilization.
* Worked on Sourcefire for virus detection and source vulnerability detection.
* Bluecoat Administration - Blocking/Unblocking URL's.
* Experience with using F5 Load balancer in providing worldwide data and file sharing, continuous internet connectivity, optimized web performance.
* Working knowledge of frame relay, MPLS services, OSPF, BGP and EIGRP routing protocols, NATing, sub-netting, also including DNS, WINS, LDAP, DHCP, http, HTML, HTTPS, TCP/IP, UDP, SNMP, OSPF, RIP, IPSEC, PPTP, VLAN, STP (Spanning tree Protocol), RTSP & Multicasting protocols
* Experience with Using GTM, APM & LTM F5 component to provide 24“7 access to applications
* Worked on Sourcefire for application control, malware detection and URL filtering.
* Third Party VPN migration from old data center to new data center.
* Cyber Security assessment using traffic analysis tools (i.e. WireShark, TCPDump, etc.)
* Creating object, groups, updating access-lists on Check Point Firewall, apply static, hide NAT on smart dashboard.

**Soft Tech services Bangalore India July 2014 to Aug 2017**

**Juniper Network Engineer**

**Responsibilities:**

* Provided technical and vendor support services, designing and planning Network Planning, Implementing, Configuring, SRX210, SRX240 Ex4200 EX4300, QFX5100
* Troubleshooting and Testing of networking system
* Evaluated network performance and activities on layer 3 routing and layer 2 switching.
* Coordinated with internal technical groups for delivery of telecommunication services and network infrastructure
* Managed routers, switches, and firewall as part of day to day operations
* Assisted in effective operation and maintenance of enterprise based network solutions and applications
* Implemented procedures for configuration and management of routers and switches and firewalls Confidential local and remote sites
* Upgraded network equipment, software and hardware components and system configuration
* Maintained technical detailed documentation of LAN and WAN systems and applications.
* Monitor tickets through HPSM to either trouble shoot or open TACACS case with Confidential for assistance
* Some F5 Load Balancer firewall ( Confidential ASA, Juniper & Check Point)
* Layer 3 IPSec, Routing BGP, GRP/EIGRP, OSPF, RIP, NAT, HSRP, MPLS
* Layer 2 switching - VLAN, VTP, Ether Channel, Port channel
* Troubleshooting of complex LAN/WAN infrastructure including routing protocols EIGRP, OSPF, MPLS & BGP
* Worked on Routing/Security/Wireless domains while ensuring multi-vendor network
* Confidential Catalyst 65XX, Confidential ASA 5505 Firewalls, Confidential 29XX
* Configured Confidential 6500, 4500 and 3750 Catalyst switches Confidential the core, distribution and access layers.
* Installation Implementing security policies using ACL, Firewall,
* Enterprise wireless support of Confidential Aruba