Archana G

ganjiarchana08@gmail.com

**(410) 368 0706**

Sr Network Engineer

**PROFESSIONAL SUMMARY:**

* Highly skilled Network Engineer with 12+ year’s of experience in designing, deploying, and supporting complex enterprise network infrastructures, specializing in Fortinet, and Meraki environments, Load Balancing with a proven track record of troubleshooting complex LAN/WAN issues, managing SD-WAN implementations, and driving security-focused network infrastructure improvements.
* Expertise in routing, switching, firewall configurations, SD-WAN, and network security to optimize performance and ensure security.
* Strong knowledge of Cisco, Juniper, Fortinet, Palo Alto, and F5 network devices, with hands-on experience in troubleshooting and configuring multi-vendor environments.
* Strong hands-on experience on Cisco Catalyst (series 3850, 3560, 4500, 6500), Cisco Nexus (series 2K, 5K, 7K), Cisco Routers (series 7300, 4000, 3800, ASR 9000), Firepower (4100), Load Balancers (Citrix NetScaler, Cisco ACE, F5 BIG-IP LTM/GTM, Virpion), IDS/IPS (HIDS, NIDS, NIPS, HIPS), Fire eye, Splunk, Palo Alto Networks Firewalls (PA-820, series PA-3K, 5K), Checkpoint IP Appliances (NXG R60, R70, 3100, 5900), FortiGate (7060E and 7030E)
* Experience in working with Cisco Nexus Switches like 5000, 7000 and 9000 series and configuring VDC, VPC, EVPN, VRF, and OTV on the Nexus switches.
* Experience on Fortinet FortiGate Appliances including 3200D, 1500D, 1200D running Latest 5.2 FortiOS.
* Experience in configuration of Cisco ACI environment; configuring APICs, Spine and Leaf switches for Cisco ACI and
* Experience in configuring Virtual Local Area Networks (VLAN) with IEEE 802.1Q, VLAN trunking protocol (VTP), shortest path bridging, Multiple VLAN Registration Protocol and VLAN Cross Connect (CC).
* Experience in installing, configuring Firewalls like Cisco ASA,SonicWall and Fortigate.
* Experience in designing and implementing IPsec based Site - to-Site, Remote Access VPN and ADVPN projects using Cisco Routers, Cisco Pix/ASA Firewall, SonicWALL.
* Experience on EVPN, MLAG, Symmetric and Asymmetric routing in Spine Leaf, VXLAN, VTEPS, VNI, MAC flood lists updates using BGP Route distinguishers, RT1,2,3 and 5 updates.
* Installed, configured, deployed Network Virtualization (NSX) VMware platform for the software defined data center.
* Experience in testing Cisco routers and switches in lab scenarios and deploy on site for production.
* Experience in Tier II ISP Routing Policies, Network Architecture, NAT, DHCP, DNS.
* Experience in configuration of LAN protocols such as Ethernet and Fiber Distributed Data Interface (FDDI) on Cisco Switches. Experience in documenting and preparing process related operational manuals.
* Experience of various wireless 802.11 standards, controllers, Access Points, Wi-Fi analytics from various vendors (Cisco Meraki, HPE, D-Link and Net gear).
* Implemented and maintained Sourcefire intrusion detection/ prevention (IDS/IPS) system and hardened protection standards, IDS/IPS signatures on Firewall for Fine-tuning of TCP and UDP services.
* Experienced with Cisco Firewalls Cisco ASA 5500, Series 5500 - X, and Cisco Next-Generation Firepower 4100 Series security appliances in standalone and high availability configurations.
* Hands-on experience with IXIA Packet generator. Developing TCL scripts for automation
* Experience with Aruba WLAN infrastructure in large scale global deployments.

**EDUCATION:**

**Rajiv Gandhi university of knowledge and technologies, Bachelors of Computer science, 2012**

**CERTIFICATION:**

**CCNA** - **Cisco Certified Network Associate**

**CCNP** - **Cisco Certified Network Professional**

**TECHNICAL SKILLS:**

* **Networking Protocols**: Cisco ISE, Cisco ACI, BGP, OSPF, EIGRP, MPLS, STP, VLANs, HSRP, VRRP
* **Network Security**: Cisco ACI, SD-WAN, Fortinet NGFW, Firewall (Cisco ASA, Palo Alto, Fortinet), IPS/IDS, VPNs, NAC
* **Cloud Networking**: AWS VPC, Azure Virtual Network, Google Cloud Networking, hybrid cloud integration
* **Wireless Technologies**: Wi-Fi 6, Cisco Meraki, Aruba Wireless, RADIUS, 802.1X authentication
* **Network Monitoring**: Extrahop, NetFlow, SolarWinds, Wireshark
* **VoIP & Unified Communications**: Cisco CUCM, SIP, QoS, Microsoft Teams Voice integration
* **Load Balancing & Optimization:** F5 BIG-IP, F5 LTM/GTM, A10, WAN Optimization, SD-WAN solutions
* **Operating Systems**: Linux, Windows Server, Cisco IOS, JunOS, FortiOS
* **Networking Protocol & Fundamentals:** DHCP and DNS server, Active Directory Management, NTP, STP, NDP, TCP/IP, UDP, FCP, NFS, FTP,, PAP, PPTP, SIP Trunking, SNMP logging, SMTP, RADIUS and TACAS+, PBX servers, SDN, SAN.
* **Wireless Technologies:** D-Link Point-to-point Wireless, D-Link APs, CISCO 1200 series APs, Aruba wireless and APs, Cisco Meraki, Linksys Wireless/Wi-Fi Routers, Cisco WLC, Access Points, DNAC + DNA Spaces, Ekahau, Aruba 225, Aruba 3000 controller & Airwave, ISE, Clear Pass 6.0,6.2,6.5
* **Scripting:** Bash, Python, Ansible

**PROFESSIONAL EXPERIENCE:**

**Client: First Republic, CA March 2023 – Present**

**Role: Sr. Lead Network Engineer**

* + Led architecture for secure remote access using SSL VPNs and TLS encryption, ensuring compliance with enterprise security standards.
	+ Designed network solutions using Meraki SD-WAN in combination with Fortinet’s WAN optimization tools.
	+ Designed and maintained highly available network infrastructure using F5 BIG-IP LTM, GTM, and AFM modules across multi-site environments.
	+ Working with customers and educating them on latest security features of wireless products we use and the differences. (WEP,WPA, WPA2, WPA3)
	+ Wrote Python scripts to parse JSON documents and load the data in PostgreSQL database.
	+ Designed and deployed VMware vSphere 7.x environments with 100+ ESXi hosts across multiple clusters, enabling high availability (HA) and dynamic resource scheduling (DRS) to achieve 99.99% uptime for critical workloads.
	+ Automated network device configurations across 300+ multi-vendor devices (Cisco, Juniper, Arista) using NAPALM's unified API, reducing manual CLI work by 75% while ensuring configuration consistency.
	+ Worked with different models of Cisco/Juniper/Arista switches, routers, firewalls, load balancers, VPNs and wireless systems.
	+ Managed and troubleshoot NET Cloud, Cradle Point and Aruba access points wireless devices on Citrix and Airwave. Aruba VPN, customer public and private wireless networks. Aruba mobility and Clearpass training.
	+ Responsible for performing predictive wireless designs/site surveys with AirMagnet Planner (Cisco 3500/3600/3700/ Aruba 105 access points) and conducting physical wireless site surveys with AirMagnet Survey.
	+ Heavily involved with data center migration from Cisco to primarily Arista with minimal downtime utilizing VxLAN.
	+ Deployed and optimized A10 ADCs, creating custom aFleX rules and SSL templates to support secure application delivery.
	+ Demonstrated proficiency in Network Administration in large datacenter environment - DNS/DHCP, Load Balancing (F5 Networks, AWS ELB), Firewalls (Cisco Systems, Juniper Networks), IDS/IPS, IPSEC VPN)
	+ Setup datadog monitoring across different servers and aws services.
	+ Configured resilient uplinks with Catalyst 9500's EVC/PBR, maintaining sub-50ms failover during fiber cuts between buildings.
	+ Designed a Python-based health checker that validated IOS-XE-specific parameters (PLIM counters, memory leaks) before maintenance windows.
	+ Designed and developed web applications using Flask web framework for python models or scripts.
	+ Developed network validation framework using pyATS that executed 200+ test cases pre/post-change, catching 95% of configuration errors before production impact.
	+ Deployed Nautobot as network source of truth for 5,000+ devices, modeling complex relationships (devices, circuits, VRFs) that reduced CMDB inaccuracies by 90%.
	+ Participate in planning, implementation, and growth of our customer's Confidential Web Services (AWS) foundational footprint.
	+ Deployed and configured FortiGate firewalls across multiple sites to ensure secure WAN connectivity.
	+ Configured dynamic routing protocols (BGP, OSPF) and MPLS for scalable WAN solutions.
	+ Acted as SD-WAN SME for a multi-state deployment using Fortinet SD-WAN solutions.
	+ Automated F5 configuration tasks using iControl REST API and Ansible scripts.
	+ Troubleshot AFM-related network issues, minimizing downtime and maintaining service availability.
	+ Troubleshot network route, gateway, and DNS resolution issues using dig, nslookup, traceroute, and ping.
	+ Configured and managed A10 Thunder ADC appliances to ensure high availability and load balancing for web applications.
	+ Built a BGP policy compliance checker that compared live network states (via pyATS) against intended designs, identifying 30+ route leaks in 6 months.
	+ Experienced in writing the web applications for the code written in python which is migrated from SPSS.
	+ Migrated legacy physical servers to VMware virtual machines (VMs) using VMware Converter and vMotion, reducing hardware costs by 40% while improving scalability and disaster recovery readiness.
	+ Developed a network compliance engine that used NAPALM to validate device configurations against security baselines, identifying and auto-remediating 200+ drift violations weekly.
	+ Migrated from traditional IOS to IOS-XE on Catalyst 9300s, leveraging programmability features (gRPC, NETCONF) while maintaining legacy protocol support.
	+ Work with application and architecture teams to conduct proof of concept (POC) and implement the design in production environment in AWS
	+ Created datadog dashboards for various applications and monitored real-time and historical metrics.
	+ Configured NAT/PAT policies on Cisco ASA firewalls to manage internal and external traffic.
	+ Update Miami International Airport wireless network to allow for future expansion and support of Real Time Locations Services (RTLS) design.
	+ Survey site and Design an upgrade for the Miami International Airport (MIA) Aruba Wireless Networks to support user capacity of 20,000 subscribers and RTLS to assist the traveling public moving through MIA and in corporate advanced delivery services.
	+ Experience as a Cisco Wireless LAN Specialist with hands-on 802.11 implementation and support experience.
	+ Experience with Real Time Location Systems (RTLS) tracking
	+ Implemented custom AFM rules to block malicious traffic and reduce false positives in firewall events.
	+ Implemented SSL offloading and SSL inspection on A10 devices to improve application performance and visibility.
	+ Implemented GTM (DNS) solutions for global traffic distribution and failover across multiple data centers.
	+ Supported Cisco ISE and 802.1x NAC to enforce secure access policies across wired and wireless networks.
	+ Performed regular upgrades, patching, and troubleshooting of Cisco ACI and Nexus OS, implementing automation solutions for streamlined operations.
	+ Automated IP address management by integrating Nautobot with Ansible, enabling self-service IP allocations that reduced provisioning tickets by 70%.
	+ Built a zero-touch provisioning system leveraging NAPALM's merge capabilities to deploy standardized configurations to new devices, cutting deployment time from 4 hours to 20 minutes.
	+ Troubleshot complex TCP/IP connectivity issues across LAN, WAN, and VPN networks using tools like Wireshark
	+ Designed and managed VPN tunnels through Panorama for secure communication between remote healthcare facilities and the UHG central network.
	+ Implemented Cisco DNAC and DNA Spaces, optimizing network visibility and spatial analytics for organizational needs.
	+ Proficient with deployment and management of AWS services - including but not limited to: VPC, Route 53, ELB, EBS, EC2, S3
	+ Experienced in working with Session Initiation Protocol (SIP) trunking for voice over IP (VoIP) to facilitate the connection of a Private Branch Exchange (PBX) to the Internet.
	+ Created system alerts using various datadog tools and alerted application teams based on the escalation matrix.
	+ Wrote Python scripts to parse JSON documents and load the data in database.
	+ Implemented Palo Alto VM-series firewalls in virtual environments, ensuring comprehensive network security in cloud deployments.
	+ Performed migrations from Check Point firewalls to Palo Alto using the PAN Migration Tool MT3.3.
	+ Implement advanced Palo Alto Firewall features like URL filtering, User-ID, App-ID, Content-ID on both inbound and outbound traffic.
	+ Deployed Palo Alto firewalls using Confidential NSX through L2 and L3 interfaces on models such as VM-300, VM-500, and VM-1000-HV.
	+ Enable file forwarding to Wildfire cloud through Content-ID implementation to identify new threats.
	+ Leveraged Palo Alto Networks’ Wildfire inspection engine to prevent Zero-Day attacks.
	+ Manage multiple Palo Alto firewalls centrally through the Palo Alto Panorama M-500 centralized Management appliance.
	+ Implement the Global Protect VPN, IPSec VPNs and SSL VPNs through IKE and PKI on Palo Alto firewalls for site-to-site VPN Connectivity.
	+ Deployed Active/Standby modes of High Availability (HA) with Session and Configuration synchronization on multiple Palo Alto firewall pairs. Knowledge on the application of Active/Active HA mode.
	+ Integrated SSL offloading on F5 LTM to reduce backend server load and enhance performance.
	+ Optimized UHG’s firewall configurations through Panorama by setting up hierarchical device groups, templates, and shared policies, reducing network management overhead.
	+ Developed and maintained network documentation detailing TCP/IP subnet schemes and device IP assignments.
	+ Configured and managed VPN tunnels between Virtu’s global trading offices and co-location data centers using Fortinet IPsec and SSL VPN.
	+ Configured and monitored GlobalProtect VPN to provide secure remote access, enabling reliable remote work solutions for end users
	+ Configured, monitored, and optimized Cisco network infrastructure, including routers, switches (Catalyst, Nexus, ACI), and security devices, ensuring high availability and efficiency across WAN/LAN environments.

**Client: NorthWestern Medicine July 2020 – Feb 2023**

**Location: Newark, CA**

**Role: Sr. Network Engineer**

* Designed and implemented site-to-site and client-to-site VPN tunnels using Fortinet IPsec and SSL VPNs.
* Designed and deployed Arista Spine-Leaf architecture to optimize network performance.
* Managed security devices, ASA, juniper, Palo Alto firewalls, routers, switches. Configured rules and maintained Palo Alto Firewalls and analysis of firewall logs using various tools
* Worked on Arista Cloud Vision (CVP) & Cloud Vision Exchange (CVX) Deployed on VMs.
* Worked on Routing protocols Eigrp and BGP. Working on Infoblox for IPAM, DHCP and DNS. Working on Linksys, SG500, Cisco, Arista switches and Cisco routers.
* Managed the F5 BigIP GTM/LTM appliances to include writing iRules, SSL offload and everyday task of creating WIP and VIPs
* Integrated cloudcheckr, Datadog, Splunk Dashboard with aws accounts.
* Implemented Business logic, data exchange, and XML processing and graph creation using Python.
* Automated policy enforcement using Catalyst Center's (DNA) APIs to push ACL updates to 300+ access switches within minutes.
* Implemented model-driven telemetry with IOS-XE's YANG models, streaming interface counters to Kafka at 30-second intervals for real-time analytics.
* Work with our current application teams to understand our current applications and make migration recommendations and to-be architectures in AWS
* Optimized VMware storage performance by configuring VMFS6 datastores with SSD caching and Storage I/O Control (SIOC), reducing latency by 35% for high-demand databases and applications.
* Created a golden configuration manager with NAPALM and Git, enabling version-controlled network changes and rollback capabilities that reduced outage risks by 60%.
* Migrated load balancing infrastructure to modern platforms from Cisco ACE to F5.
* Configured and optimized Cisco Nexus, Catalyst, and ASR series routers and switches, ensuring robust and high-performance network communications across enterprise environments.
* Designed a PoE monitoring system for Catalyst 3560-CX switches that alerted on power budget exhaustion before IP phone outages occurred.
* Monitored performance and history of infrastructure with tools such as CloudWatch, Datadog etc.
* Developed views and templates with Python and Django's view controller and templating language to created user-friendly website interface.
* Provided Tier 2/3 support for incidents involving Meraki-managed networks and Fortinet NGFWs.
* Migration of ASA firewalls to PA next gen Firewalls using migration tool in PA. Migrated all IPSEC tunnels, ACL’s, NAT rules and policies.
* Work with team to build out automation templates in Fugue or AWS Cloud Formation in support of the managed services platform
* Provisioned Datadog monitoring metrics at build time using Terraform.
* Hardened IOS-XE devices per CIS benchmarks, disabling unnecessary services (HTTP, CDP) and implementing AAA with TACACS+ fallback.
* Designed and implemented Layer 4–7 load balancing for internal and external business-critical applications.
* Enabled TLS offloading on ADCs (e.g., F5, A10, NGINX) to reduce backend server CPU usage.
* Supported VMware-based virtual environments, integrating networking layers for multiple VMs and virtual switches.
* Used AWS Beanstalk for deploying and scaling web applications and services developed with Java.
* Extensively used Python requests urllib and urllib2 module to call web services.
* Integrated NAPALM with NetBox as source of truth, automatically synchronizing device facts (interfaces, VLANs) and eliminating IPAM discrepancies.
* End to end deployment ownership for projects on AWS. This includes Python scripting for automation, scalability, builds promotions for staging to production etc.
* Troubleshot complex VMware vCenter issues, including HA failover failures and vSAN synchronization problems, by analyzing logs and applying patches to restore service within SLAs.
* Assisted in the transition from legacy load balancers to F5 appliances, enhancing application resilience.
* Managed SSL decryption policies on Palo Alto devices, ensuring visibility into encrypted traffic while maintaining compliance with data security policies.

**Client: Valero Energy, TX July 2018 – May 2020**

**Role: Cisco Network Engineer**

* Worked on Cisco Viptela, Versa SD-WAN solutions. Migrated from DM-VPN and MPLS circuits to SD-WAN solutions.
* Create Config templates in DNAC for WLCs as per customer demand.
* Integrated VeloCloud with existing MPLS and broadband networks to provide hybrid WAN solutions.
* Integrated Meraki wireless networks with authentication protocols like 802.1X and RADIUS for enhanced security.
* Designed and implemented secure VPN connections using Prisma Access to ensure encrypted communication for remote users.
* Implemented and maintained the monitoring and alerting of production and corporate servers/storage using AWS Cloud Watch.
* Developed scripts in Python and Excel VBA to automate the data analysis, generating statistics isolating trends in memory failures.
* Integrated QoS configurations into the SDN framework, enhancing flexibility and responsiveness to changing network demands.
* Designed webhook-based workflows that triggered Nautobot data updates from change management systems (ServiceNow), ensuring audit trail accuracy.
* Performed routine maintenance and upgrades of Cisco VoIP systems, ensuring alignment with industry standards and best practices.
* Experience in Building and Managing Hadoop EMR clusters on AWS.
* Managed global traffic distribution using F5 BIG-IP GTM (now DNS), improving performance and redundancy.
* Monitored real-time performance statistics via SNMP and A10 dashboards.
* Connection of Edge routers and perimeter firewalls to Super Spines in Spine leaf Architecture. (Cisco ACI).
* Responsible for L2 & L3 support of customer’s Network and Security Infrastructure devices.
* Created and maintained documentation, runbooks, and standard operating procedures (SOPs) for load balancing systems.
* Expertise python scripting with focus on DevOps tools, CI/CD and AWS Cloud Architecture.
* Used tools like Qualys SSL Labs, OpenSSL, and Nmap to audit and validate TLS implementations.
* Installed and configured LAN/WAN Networks, Hardware, Software, and Telecommunication services- Cisco Routers and Switches. Implemented IPv4 and IPv6 on PTX platforms.
* Configuring and deploying multiple vendor firewalls like Palo Alto, Fortigate, Juniper SRX and ASA firewalls.
* Worked on Cisco wireless LAN technologies and switching.
* Developed test scripts in Python that are used to test embedded systems via their debug UART port.
* Worked closely with vendors to troubleshoot and resolve Panorama-related issues affecting network performance.
* Worked with Cisco Wireless products and technologies including Cisco Wi-Fi access points, Catalyst 9800 wireless controllers, DNAC, ISE, DNA spaces, Meraki.
* Experience AWS services (VPC, EC2, S3, RDS, Redshift, Data Pipeline, EMR, Dynamo DB, Redshift, Lambda, SNS, SQS).
* Built a network topology visualizer using Nautobot's GraphQL API and D3.js, helping engineers quickly identify single points of failure.
* Developed Views and Templates with Python and to create a user-friendly website interface Django's view controller and template.
* Optimized spanning tree protocol (STP) configurations on Catalyst switches to prevent broadcast storms and loops.
* Routing protocol configuration such as OSPF, IS-IS, EIGRP and BGP, Router redundancy configuration (HSRP, VRRP and GLBP) and Wireless LAN (Access point, LWAPP).

**Client: Hitachi, Ind Sept’ 2013 – Feb’ 2018**

**Network Support Engineer**

* Performed RIP & OSPF routing protocol administration. Support services to reduce the downtime on leased lines.
* Deploy and Maintain SD-WAN solution, routers and Switches, Cisco ASR, Juniper SRX and Fortinet firewalls.
* Worked as a customer facing engineer to Deploy new hardware, Upgrade IOS, troubleshoot any ongoing issues with Routing, Security, SD-WAN and coordinate with support and professional services.
* Designed and Implemented plan for migration from existing Catalyst switches to Nexus and configured NX-OS Virtual Port Channels, Nexus port profiles, Nexus VPC peer links on Nexus 5k and 7k.
* Involved in designing and deploying multiple applications utilizing almost all the AWS stack (Including EC2, Route53, S3, RDS, Dynamo DB, SNS, SQS, IAM) focusing on high-availability, fault tolerance, and auto- scaling in AWS Cloud Formation.
* Implemented routing protocols (BGP, OSPF, EIGRP) and configured QoS policies to enhance WAN/LAN performance for Cisco VoIP and data traffic.
* Monitored and analyzed network traffic using Panorama, identifying and mitigating potential security threats in real time.
* Implemented SNMP agents and traps on Linux for network monitoring and alerting.
* Managed Cisco Wireless LAN Controllers and Access Points, ensuring seamless Wi-Fi connectivity with DNAC and DNA Spaces for location-based services.
* Supported VPN configurations with IPSec, providing secure connections for remote users and ensuring compliance with organizational security policies.
* Leveraged AWS cloud services such as EC2, auto-scaling and VPC to build secure, highly scalable and flexible systems that handled expected and unexpected load bursts.
* Providing support to networks containing more than 2000 Cisco devices.
* Performing troubleshooting for IOS related bugs by analyzing history and related notes.
* Carrying out the documentation for tracking network issue symptoms and large-scale technical escalations.
* Troubleshot network interfaces, VLANs, and bonding on Linux systems.
* Managed DNS, DHCP, NTP, and TFTP services on Linux for internal network support.
* Managed the service request tickets within the phases of troubleshooting, maintenance, upgrades, fixes, patches and providing all-around technical support.
* Used AWS Beanstalk for deploying and scaling web applications and services developed with Java.
* Monitor the traffic of the network via NTA and IPAM
* Provided Technical Support to customers and partners on Palo Alto security appliances
* Completed service requests (i.e. – IP readdressing, bandwidth upgrades, IOS/platform upgrades, etc.)