**Aluri Bangar**

**Senior Network Engineer**

**Email:** **bangarualluri@gmail.com**

**Contact no: +1 910-446-8180**

### Professional Summary

* CCNA, CCNP, CEH, PCNSE Certified professional with 10 years of experience with networking installations, Configurations testing, troubleshooting, implementing, optimizing, maintaining enterprise data network and service provider systems.
* Worked on Cisco Nexus 9000 family of switches whose hardware is based on Cisco ACI.
* Experience in configuring on latest cisco switches like Nexus 2000, 5000, 6000 and 7000 series switches while implementing advanced features like VDC, VPC, OTV and Fabric Path.
* Configured Access policies, static bindings, EPG's, Bridge Domain and VRF.
* Designed and implemented Cloudflare Zero Trust Network Access (ZTNA) to securely connect users to internal applications without using traditional VPNs.
* Designed and deployed IPsec-based VPN solutions using Cisco ASA and ISR platforms, ensuring high availability and compliance with security standards.
* Deployed, configured, and managed Cisco Meraki MR series wireless access points across enterprise and branch locations.
* Implemented and supported Cisco Unity Connection for voicemail integration and auto-attendant configurations.
* Deployed and maintained IPsec VPN tunnels using Cisco ISR routers, ASA firewalls, and next-gen firewalls to securely connect remote sites and cloud services.
* Provide technical support on Nexus 2000/9000 switches and operating systems (NX-OS) create vPC domain, design single sided vPC, design double sided vPC, design vPC peer-keepalive, vPC peer-link, vPC member ports.
* Used Prime Collaboration and Cisco Unified Reporting tools for system health checks and capacity planning.
* Deployed, configured, and managed Silver Peak SD-WAN edge devices to optimize branch-to-branch and branch-to-cloud connectivity.
* Deployed the Nexus 9000 Application Virtual switch to support network telemetry applications and 9000 Core with VPC and 3172 TOR.
* Designed, implemented, and troubleshot Layer 3 networks using TCP/IP protocols for routing, addressing, and network segmentation.
* Configured ACI integration with VMware and Worked on integrating existing Layer 2 and Layer-3 networks with ACI.
* Configured, deployed, and managed Citrix Netscaler (ADC) devices for load balancing, traffic optimization, and secure remote access across enterprise environments.
* Configured, deployed, and managed Next-Generation Firewalls (NGFWs) for enterprise environments, ensuring deep packet inspection, application awareness, and intrusion prevention.
* Worked on Bridge Domains, VXLANs, VTEPS, VNID. Configuration of routing using BGP among multiple Leaf to spine switches. Thorough understanding of Application Profile, Tenants, End Point Group, Inter Subnet Tenant Routing, Routing within Tenants, Router Peering and Redistribution.
* Hands on Experience in configuring and troubleshooting Cisco routers, WIFI wireless Controller, Cisco catalyst, Nexus switches, Citrix net scalar, ASA, Palo Alto Next generation and Firepower Threat Défense FTD Next generation Cisco Firewalls.
* Designed and deployed enterprise Wi-Fi networks using Cisco Wireless LAN Controllers (WLC) and Cisco Access Points (APs), including 2800, 3800, and 9100 series.
* Integrated Cloudflare ZTNA with SSE (Secure Service Edge) architecture for comprehensive secure remote access to SaaS, internal, and cloud applications.
* Designed and implemented network redundancy using dual-homed architectures, HSRP/VRRP, and redundant uplinks to ensure high availability and minimize downtime.
* Implement & manage around 500+ Network & Security Devices that includes Cisco Nexus & Catalyst Switches, Cisco ASA, Juniper EX Series Routers, Juniper SRX Firewalls.
* Google Cloud hybrid networking with interconnect through service providers to connect gcp infrastructure to on-prem and setting up on VPNs as a backup
* Possess a solid understanding of Internet architecture, including BGP routing, autonomous system (AS) relationships, and global routing table operations.
* Creating, managing, and optimizing firewall rules to allow or block specific types of traffic based on security policies.
* Participated in incident response and mitigation efforts during large-scale volumetric DDoS attacks affecting critical network infrastructure.
* Troubleshot DNS resolution failures and DHCP lease issues, coordinating with application and server teams to ensure resolution.
* Palo Alto design and installation (Application and URL filtering, Threat Prevention, Data Filtering). Configured and maintained IPSEC and SSL VPNs on Palo Alto Firewalls.
* Participated in Configuration of Palo Alto NGFW, Cisco ASA to create security profiles and VSYS based on client topologies and Palo Alto Networks 5220 application firewalls (NGFW)
* Experienced in implementing network security using NAT, PAT, ACL, IDS, IPS and ASA Firewalls.
* Updated training SilverPeak SDWAN, SolarWinds, Splunk, Aruba wireless, F5 LTM/GTM & Cisco SD-WAN - Silver Peak & Cisco Viptela
* Configured LDP and Segment Routing on core Cisco/Arista routers to enable deterministic routing paths for high-priority services.
* Experience with Firewall migrations from Cisco ASA to Cisco Firepower.
* Designing and architecting Checkpoint, Fortinet firewalls solutions based on the organization's security requirements and network infrastructure.
* Implemented advanced security policies on NGFWs to control traffic based on user identity, applications, and content rather than traditional IP/port-based rules.
* Configured dynamic routing protocols (OSPF, BGP) with path preferences and route failover to support resilient network topologies during link or device failures.
* Experience in Network Intrusion detection/Intrusion Prevention System and Firewalls.
* Experience in Implementing & managing Symantec Data Loss Prevention.
* Designed and deployed enterprise-grade Wi-Fi networks, ensuring optimal coverage and performance for high-density environments.

### TECHNICAL SKILLS:

|  |  |
| --- | --- |
| * Router and VoIP Platforms | * Cisco Routers series 7300, 4000, 3800, 2000, 1900; Juniper T4000, MX10, MX40, ACX2200, ACX5000; On SIP, Avaya products, cisco IP phones |
| * Routing Fundamentals and Protocols | * Routed and Routing protocols RIP, EIGRP, IS-IS, OSPF, BGP, IPX; MPLS, IPv4 and IPv6 addressing, subnetting, VLSM, Static routing, ICMP, ARP, HSRP, VRRP, Route Filtering, Multicast, 802.11, Policy Based Routing, Redistribution, Port forwarding, Arista. |
| * Switch Platforms | * Cisco Catalyst series 2960, series 3560, 3850, 4500, 6500, 7000, 9000; Nexus series 2K, Netgear switches,5K, 7K; Nortel/Avaya 5510, 5520; Juniper EX3300, EX4600, EX4300, EX3400 |
| * Switching Fundamentals and Protocols | * Ethernet technologies, LAN networks, MAC, VLAN and VTP, STP, PVST+, Multicast, * RSTP, Multi-Layer Switching, 802.1Q, EtherChannel, PAGP, LACP, CDP, HDLC, RARP |
| * Firewall Platforms | * Palo Alto (PA series 2K, 3K and 5K), Juniper Net screen 6500, 6000, 5400, Juniper SSG, SRX5600, SRX5800, Checkpoint (NGX R65, 3100, 5100, 5900), Cisco (ASA 5505, 5506-X, 5585), Net gear Firewall, WAF, ACI, Fortinet (101F, 201F, 401F, 601D, 1000D, 1500D), |
| * Security Protocols | * Standard and Extended ACLs, IPsec, VPN, Port-Security, SSH, SSL, IKE, AAA, Prefix-lists, Zone-Based Firewalls, NAT/PAT, HIPAA standards, Ingress & Egress Firewall Design, Content Filtering, Load Balancing, IDS/IPS, Blue Coat URL Filtering, L2F, IDS, TCP Intercept, Router Security, SNMP trap |
| * Network Management and Monitoring | * Wireshark, Infoblox, HP OpenView, Cisco Prime, Security Device Manager (SDM), Cisco Works; TCP Dump and Sniffer; SolarWinds NetFlow Traffic Analyzer, Network Performance Monitor (NPM), Network Configuration Manager (NCM), SevOne, SiteScope. |
| * Load Balancers | * F5 (BIG-IP) LTM, GTM/DNS, WAF, ASM, APM,Velocloud, Citrix NetScaler |
| * WAN technologies | * Frame-Relay, ISDN, ATM, MPLS, PPP, DS1, DS3, OC3, T1 /T3 lines, SONET OC3-OC192, SDH, POS, PDH |
| * Cloud Computing and Automation | * AWS, Microsoft Azure, Cisco Meraki, C, Python scripting, Shell, Cloud Migration |
| * Other Networking Protocols and Fundamentals | * DHCP and DNS server, Shell, Active Directory Management, NTP, NDP, TCP, UDP, FCP, Network Implementation, Troubleshooting techniques, NHRP, NetBIOS, NFS, FTP, TFTP, HTTP, PAP, PPTP, SIP Trunking, SNMP logging, BitTorrent, SMTP, RADIUS and TACAS+, PBX servers, SDN, SAN |
| * Operating Systems | * Windows 10/7/XP, MAC OS, Windows Server, Nexus OS, Cisco IOS-XR, Linux, UNIX |

### Certifications

* CCNP- Cisco Certified Network Professional
* CCNA- Cisco Certified Network Associate
* PCNSE- Palo Alto Networks Certified Network Security Engineer

### EDUCATION DETAILS

* Masters Degree in Informatics, Northeastern University -2016
* BE in Computer Science, JNTU-2012

### PROFESSIONAL EXPERIENCE

**Client: Optum,OH**

**Role: Senior Network Engineer Aug 2024 to Till Date**

**Responsibilities**:

* Works with client engineering groups to create, document, implement, validate and manage policies, procedures and standards that ensure confidentiality, availability, integrity and privacy of information.
* Extensive experience in designing, implementing, and managing Layer 3 network infrastructures for large-scale enterprise environments.
* Designed and implemented SSID configurations, VLAN tagging, and access policies via the Meraki Dashboard.
* Configured Access Control Lists (ACLs) to control traffic flow and enhance network security.
* Integrated Cisco Firepower with existing security infrastructure, including SIEM systems and endpoint protection, to create a cohesive and multi-layered security posture.
* Integrated NGFWs with threat intelligence feeds to enable real-time blocking of known malicious IPs, domains, and malware signatures.
* Subnetted IP networks (IPv4 and IPv6) using VLSM and CIDR to efficiently allocate addresses and support scalable network growth.
* Configured and managed Cisco WLC (AireOS and/or Catalyst 9800) for centralized wireless control, SSID broadcasting, and policy enforcement.
* Designed and implemented SD-WAN overlays, traffic steering policies, and QoS to ensure application performance and reliability.
* Developed and maintained complex firewall rules and policies, optimizing network traffic flow and ensuring compliance with organizational security standards.
* Performed troubleshooting and traffic analysis using Cloudflare logs and analytics to resolve ZTNA policy violations and application access issues.
* Configured and managed IKEv1 and IKEv2-based IPsec tunnels, ensuring secure data encryption and integrity for critical business communications.
* Managed and troubleshot SIP trunks, H.323, and MGCP voice gateway protocols across multisite environments.
* Implemented SSL offloading and acceleration using Citrix Netscaler to enhance application performance and reduce server load.
* Led training sessions and created user guides to support end-user adoption of new VoIP and collaboration tools.
* Configured Layer 2 and Layer 3 functionalities, including VLANs, spanning tree protocols, and routing protocols, on Catalyst 9000 switches.
* Deployed redundant firewalls, switches, and routers across core, distribution, and access layers to support seamless failover and traffic continuity.
* Administered network devices for authentication and accounting using Cisco ISE's TACACS+ and RADIUS services.
* Configured port security measures to control access and prevent unauthorized devices from connecting to the network.
* Conducted regular security audits and vulnerability assessments to identify and mitigate potential threats.
* Aruba 802.11ac wireless access points deliver superb Wi-Fi performance, Aruba 330 series, 501 wireless client bridge, 7220, 7010 MOBILITY CONTROLLER.
* Managed interconnectivity with Internet Exchange Points (IXPs) to optimize latency, reduce transit costs, and improve routing efficiency.
* Managed and updated switch firmware and software for security and feature enhancements.
* Migration of ASA firewalls to Meraki next gen Firewalls. Migration IPSEC tunnels, ACL’s, NAT rules and policies to SD-WAN Solution. Expertise in configuring and optimizing advanced routing protocols, including OSPF, BGP, EIGRP, and IS-IS, to ensure efficient and reliable network performance.
* Conducted QoS (Quality of Service) configurations to prioritize voice traffic across LAN/WAN, ensuring minimal latency and jitter.
* Integrated Meraki APs with RADIUS/Active Directory for 802.1X authentication to enhance wireless security.
* Replacing Checkpoint VPN and BlueCoat proxy with Zscaler and worked on implementing Zscaler in Production.
* Leveraged DNAC's analytics and assurance features to monitor network health, performance, and security, proactively identifying and resolving issues.
* Configured and managed Cloudflare Tunnel (formerly Argo Tunnel) for secure, outbound-only connections to internal applications, eliminating inbound firewall rules.
* Worked on Arista Cloud Vision (CVP) & Cloud Vision Exchange (CVX) Deployed on VMs.
* Experience in configuring, trouble shooting and deploying of various IP Routing Protocols (RIP, EIGRP, OSPF and BGP) on both Cisco and Juniper devices.
* Troubleshot WAN connectivity, routing, and failover issues to ensure high availability and minimal downtime.
* Hardened internet-facing routers by disabling unnecessary services, restricting management access, and applying control plane policing (CoPP).
* Designed and deployed high-availability configurations for Citrix Netscaler to ensure continuous service delivery and minimize downtime.
* Configured and verified core TCP/IP services including DHCP, DNS, NAT, and PAT across routers, firewalls, and layer 3 switches.
* Led multiple site-to-site and remote access VPN deployments using Cisco ASA and Firepower appliances, ensuring high availability and redundancy.
* Worked with internal stakeholders to migrate from traditional perimeter security to a Zero Trust architecture using Cloudflare's security stack.
* Built disaster recovery (DR) network environments with automated failover capabilities between primary and secondary data centers using technologies like IP SLA and BFD.
* Performed wireless site surveys and coverage analysis to optimize AP placement and ensure reliable connectivity.
* Conducted wireless site surveys using tools like Ekahau or NetSpot to optimize AP placement and ensure proper coverage and capacity.

**Client: MISO, IN Nov 2022 – July 2024**

**Role: Senior Network Engineer**

**Responsibilities:**

* Design and Implemented IOS, Nexus 9K/7K/ & Catalyst 6500/4900/3750- X, 1000V in a Complex DC Core/ Aggregation/ Access layer on a 10G backbone in Production and Data Canter Architecture.
* Deals with F5 migration of 3DNS to Global traffic managers (GTM) of BIG 8900 series to GTM 6800 series
* Data center Planning and Architecture by Maintaining Active Directories.
* Involved in migration of F5 Local traffic managers of LTM 5100 series to LTM 6800 series for higher capacity of data process and load balancing the web traffic within the data center
* Provide Layer 3 and Layer 4 support regarding DNS, DHCP and Load Balancing.
* Installation and maintaining AAA servers.
* Integrated Silver Peak appliances with existing WAN infrastructure, firewalls, and cloud platforms (Azure, AWS, etc.).
* Implemented dynamic and static crypto maps to manage encryption and traffic flow policies across enterprise IPsec VPN architectures.
* Analyzed packet flows and TCP/IP headers using tools like Wireshark to diagnose latency, retransmissions, and connectivity issues.
* Created granular application access policies using Cloudflare’s Zero Trust Dashboard to control access based on identity, device posture, and network conditions.
* Tuned RF profiles, channel assignment, and transmit power to minimize interference and improve performance.
* Utilized Infoblox APIs and scripting tools (Python/Perl) for automating DDI tasks and bulk provisioning.
* Implementation of HSRP, DHCP, DNS, FTP, TFTP, MRTG.
* Migrated legacy PBX systems to Cisco VoIP solutions, improving call quality and reducing operational costs.
* Assisted with migration of applications/VMs into cloud environments (AWS, Azure, GCP)
* Gathering details from customers and providing best security infrastructure solutions with F5 load balancers, Check Point/Net screen firewalls and Blue Coat proxies
* Integrated Cisco IPsec VPNs with technologies like GRE, DMVPN, and FlexVPN for scalable branch connectivity and dynamic routing support.
* Configured and supported guest Wi-Fi networks with splash page authentication and bandwidth shaping.
* Implemented secure wireless authentication using WPA2/WPA3-Enterprise with 802.1X and RADIUS integration (Cisco ISE or Windows NPS).
* Deployed and managed high availability (HA) NGFW clusters to ensure uninterrupted security services during maintenance or failover events.
* Integrated Citrix ADC with existing authentication systems such as LDAP, Active Directory, and RADIUS to streamline user access and improve security.
* Configured L3 protocols (IP, BGP, OSPF), redistribution, summarization, Filtration (using distribute list, route map, prefix list, access list).
* Implementation and troubleshooting of 802.11a/b/g/n technology with primary focus on Cisco Unified Wireless Network /Configure Aruba wireless Controller 7210
* Troubleshoot WAN, LAN, security, access, and Cisco wireless connectivity using BBSM for guest wireless access and Sniffer software for troubleshooting, Cisco Works, HP Openview, Tivoli or related tools.
* Experience with wireless survey tools (Air Magnet or Ekahau Site Survey).
* Experience with wireless survey methodologies for office, factory, warehouse, outdoor, and mesh designs.
* Maintenance and configuration of Cisco ASR1000 series and 7200VXR routers at data center and deployment of 3900, 3800, 2951 and 2821 for branch connectivity.
* Coordinated with cross-functional teams to support VoIP deployments, user training, and system upgrades across multiple sites.
* Implemented routing protocols (OSPF, EIGRP, BGP) for dynamic path selection and failover in TCP/IP-based enterprise environments.
* Monitored wireless performance and client connectivity using Meraki Cloud Dashboard analytics and health reports.
* Configuring and implementing F5 BIG-IP, LTM, GTM load balancers to maintain global and local traffic.
* Hands on experience with troubleshooting and configuring terminal servers.
* Palo Alto, and Cisco ASA design and installation (Application and URL filtering, Threat Prevention, Data Filtering). Configured and maintained IPSEC and SSL VPN's on Palo Alto Firewalls.
* Configuring rules and Maintaining Palo Alto Firewalls & Analysis of firewall logs using Panorama.
* Configured and maintained IPSEC and SSL VPN's on Palo Alto, and Cisco ASA Firewalls and also implemented Zone Based Firewall and Security Rules on the Palo Alto Firewall, and Cisco ASA.
* Exposure to Palo Alto Wildfire, and Cisco Firepower.
* Implemented Positive Enforcement Model with the help of Palo Alto Networks
* Worked on zia for internet web traffi security.
* Automated deployment and policy updates using Terraform and Cloudflare API for scalable and consistent Zero Trust configuration.
* Deploying and decommission of VLANs on core ASR 9K, Nexus 9K, 7K, 5K and its downstream devices and configure 2k, 3k,7k series Routers.
* Integrated NGFWs with SIEM platforms for centralized logging, correlation, and alerting on security incidents.
* Implemented load balancing strategies (round robin, least connections, etc.) to distribute network traffic efficiently.
* Integrated IPsec VPNs with GRE tunnels and DMVPN to support scalable, multi-branch connectivity.
* Implemented security best practices by designing VPC security groups, network ACLs, and AWS Firewall Manager policies to protect cloud environments.
* Monitored SD-WAN performance, link utilization, and application visibility using Silver Peak Orchestrator.
* Instrumental in the planning and architecture development of SDN based virtual enterprise gateways (infrastructure as a service -IaaS) reducing the customer time to deployment from months to days.
* Set up tunnels from NetScaler devices to Zscaler cloud.
* Conducted regular DR tests and simulated failover scenarios to validate network resilience and recovery time objectives (RTO).
* Worked on Cisco ISE to prevent unauthorized access to the network.
* Implementing, configuring, and troubleshooting various routing protocols like RIP, EIGRP, OSPF, and BGP.
* Integrate with business owners and Scheduled Windows servers patch using patch management and install Windows service pack.
* Designed and implemented IPAM strategies for large-scale enterprise environments to reduce IP conflicts and improve visibility.
* Designed and supported BGP Flowspec-based DDoS mitigation to allow granular traffic filtering based on dynamic threat patterns.
* Performed advanced troubleshooting of VPN tunnels using debug crypto, show crypto, and syslog analysis to resolve phase 1/2 negotiation and data traffic issues.
* Configured, implemented and troubleshooted different business policies in Velocloud SDWAN
* Conducted Wi-Fi site surveys using tools such as Ekahau and AirMagnet to optimize access point placement and minimize interference.
* Implemented secure wireless access solutions using WPA2, WPA3, and 802.1X protocols, safeguarding sensitive data and ensuring user authentication.
* Managed and maintained Citrix Netscaler Virtual Appliances (VPX), ensuring proper configuration and performance for virtualized environments.
* Created detailed documentation and runbooks for voice infrastructure, including change control procedures and disaster recovery plans.
* Created and managed multiple SSIDs with VLAN tagging, QoS policies, and role-based access control for different user groups (staff, guest, BYOD).
* Configured and maintained ACLs and firewall rules based on TCP/UDP ports and IP address ranges for secure access control.
* Troubleshot Wi-Fi connectivity issues related to signal strength, interference, and device compatibility, improving network stability and user experience.

**Client: Hackensack Meridian Health, NJ Sep 2020 to Oct 2022**

**Role: Cloud Network Engineer**

**Responsibilities:**

* Worked for the Global Deployment and Operations team to support multiple migrations in switching, routing, firewalls, LB and Proxies
* Tuning and configuring rate control parameters for complex protocol methods in Akamai WAF
* Configured and designed OSPF, EIGRP and BGP at Distribution and Core layers. Configured OTV layer 2 connection between Data centers on Nexus (Cisco ASR 9K, Nexus 7k and 9K) Worked on Juniper devices like M, MX, T routers on advanced technologies like MPLS VPNs, TE and other service provider technologies (EX-2200, EX-4200, EX-4500, MX-480, M Series, SRX650, SRX240)
* Automated routine administration tasks for Citrix Netscaler using scripting (e.g., PowerShell, bash) and the Netscaler API to improve operational efficiency.
* Troubleshot connectivity and application issues caused by NGFW policies, NAT rules, or traffic inspection, using packet captures and session logs.
* Troubleshot wireless roaming, latency, and interference issues using Meraki packet capture and spectrum analysis tools.
* Administered and monitored voice gateway hardware including Cisco ISR routers with voice DSP modules and FXO/FXS ports.
* Experience with configuring BGP, OSPF in M and MX series routers. Worked on several BGP attributes like MED, AS-PATH, Local Preference for route optimization. Worked on Route-Reflector, Route-Redistribution among routing protocols
* Configured secure tunnels, dynamic path control, and application-based routing to improve network efficiency.
* Implemented route filtering, prefix limits, and BGP communities to enforce traffic engineering and security best practices across transit and IXP peers.
* Deployed Cloudflare Gateway to inspect and filter DNS, HTTP, and network traffic, enhancing threat protection and compliance across user devices.
* Verified automatic rerouting behavior, OSPF reconvergence, and BGP route withdrawal handling across failover paths.
* Integrated load balancers into existing firewall and security frameworks to ensure secure and seamless data flows.
* Developed Infrastructure as Code (IaC) templates using AWS CloudFormation and Terraform to automate AWS network architecture provisioning.
* Optimized VPN performance and security by implementing AES encryption, SHA integrity algorithms, and perfect forward secrecy (PFS).
* Remotely monitoring and managing servers using utilities like VMware Vsphere Clients, VCOPs, Veeam MP, Terminal Services, RDP, HP-ILO, HP Insight Manager, Citrix APP Center, Citrix Management Console, PC anywhere, and maintained Cisco LANs and WAN devices Cisco Routers and Switches.
* Managed AD Domain Controller, DNS and DHCP Servers and configurations. Worked on Cisco ISE for user Authentication, Security Group Tags, MAC based authentication for Wireless and Wired users, 802.1X, EAP, PEAP etc.
* Performed migration of legacy VPNs to Cisco FlexVPN using IKEv2, improving security and interoperability.
* 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, Zscaler Proxy and Versa SD-WAN appliances
* Migrated Nexus 7Ks &amp; Nexus 5Ks to an ACI Fabric consisting of 9336PQ Spines &amp; 9332PQLeafs in a brownfield Data Center
* Worked on PAC file updates, Internet proxy migration from IronPort to Zscaler cloud. Access policies, AD based, user based, location-based access. (Tools: ZAPP client)
* Worked on connections handoff using Bridged Interface to an External Route. L3- EPG configurations, AEP configurations. Integrated existing Layer 2 and Layer 3 networks with ACI Play a key role in the company’s direction towards Cloud Computing platforms by creating a strategy for transition plans. (Tools: Azure AD and AWS, Office 365)
* Design, implement, and develop network designs for applications used in TMO. Worked on Checkpoint Firewall to create new rules and allow connectivity for various Applications. Checkpoint is used as an internal firewall for application security in Kodiak network.
* Implemented Firewall rules and NAT rules by generating precise methods of procedure (MOPs). Responsible for packet capture analysis, syslog and firewall log analysis.
* Maintaining and updating security policies and configurations in response to evolving threats and business needs.
* Experience in F5, Cisco ACE 4710 Load balancers. Migration Experience from ACE to F5 and NetScaler to F5. Worked on critical applications on Layer 4 and layer 7 load balancing.
* Experience with Virtual server, Pool, Node, Profiles – TCP, http, https, ftp, fastl4, Persistence – Source IP, SSL, Cookie, SNAT, iRules, iAPP, SSL offloading.
* Worked on Orion (Solar Winds) for mapping network diagrams, updated Orion with commissioned and decommissioned network devices.
* Monitored and optimized Wi-Fi networks using advanced tools like Cisco Prime and Aruba AirWave, ensuring consistent performance and uptime.
* Integrated redundancy into VPN and WAN connectivity using dual ISPs, redundant IPsec tunnels, and routing policies for failover and load balancing.
* Supported application-level troubleshooting by analyzing TCP three-way handshakes, session timeouts, and port usage.
* Troubleshot wireless connectivity issues using packet capture tools, WLC logs, and spectrum analyzers to resolve interference, roaming, and performance issues.
* Conducted regular firmware updates and patches on Citrix ADC appliances to ensure up-to-date security and functionality.
* Created and managed DNS zones, records, DHCP scopes, and IP address blocks via the Infoblox Grid Manager and API.
* Validated encryption domains and NAT-T configurations to ensure successful IPsec tunnel negotiation and traffic encryption.
* Collaborated with IXP operators and upstream providers to provision and troubleshoot Layer 2 cross-connects and BGP sessions.
* Applied firmware upgrades and patches to Meraki APs to maintain stability and security compliance.
* Collaborated with cross-functional teams and vendors during VPN migrations and disaster recovery planning involving IPsec connectivity.
* Integrated AWS native services such as Route 53, CloudFront, and Global Accelerator to optimize DNS, CDN, and global application delivery.
* Integrated Wi-Fi networks with VLANs and network access control (NAC) systems, providing seamless connectivity and enforcing security policies.

**Client: Cisco, CA May 2018 – Aug 2020**

**Role: Network Security Engineer**

**Responsibilities:**

* Creating, managing, and optimizing firewall rules to allow or block specific types of traffic based on security policies.
* Designing and architecting Checkpoint firewall solutions based on the organization's security requirements and network infrastructure.
* Upgraded Cisco 7200, 3600 Router IOS Software, backup Routers and Catalyst 3560, 4500 switch configurations.
* Administered Infoblox DNS, DHCP, and IPAM (DDI) appliances to maintain robust IP address management and name resolution services.
* Collaborated with security teams to enforce IPsec policies aligned with corporate security frameworks and external compliance requirements.
* Delivered highly specialized support to worldwide customers that run Checkpoint, and Fortinet in their network infrastructure.
* Deployed QoS policies to prioritize TCP/IP traffic such as voice, video, and critical business applications.
* Regularly updated and patched VPN endpoints to mitigate vulnerabilities and maintain IPsec tunnel stability.
* Integrating Checkpoint, and Fortinet firewalls with other security solutions and network devices for a cohesive and robust security infrastructure.
* Ensuring the firewall's performance is optimized to handle the network traffic efficiently without compromising security.
* Supported international and remote offices by configuring region settings, device location settings, and codecs to optimize bandwidth usage.
* Integrated threat intelligence feeds and automated detection systems to dynamically block malicious IPs at the edge routers and firewalls.
* Applying industry best practices to configure security features, such as intrusion prevention, anti-virus, and URL filtering, to safeguard against evolving threats.
* Deployed, configured, and managed of 802.1x solutions to include Cisco Identity Services Engine (ISE), ACS (Radius and TACACS+), and Cisco Prime Infrastructure.
* Implement SSL VPN solutions including Fortinet Networks Global Protect with single and multiple gateway solutions including integration of PKI certificates. Integrate multiple vendor IPSEC site to site VPNs, including Fortinet Network, Checkpoint, and Juniper SRX firewalls.
* Deployed and managed guest Wi-Fi portals using Cisco ISE or built-in WLC features, ensuring secure access and bandwidth limitations.
* Collaborating with other IT teams to integrate firewalls with other security technologies like SIEM systems, threat intelligence feeds, and endpoint protection tools.
* Evaluated existing external BGP route policies and identified inefficient paths across transit providers.
* Designed and Implemented a MPLS network for a new subsidiary with BGP redistribution into OSPF
* SD-WAN role integration with worldwide locations with Multiple Cloud Providers.
* Maintained McAfee Web washer proxy to control the user traffic.
* Worked on F5 LTM series like 7050, 5050, 2200 for several applications and their availability.
* Designed VPN and Direct Connect architectures for secure, low-latency on-premises to AWS connectivity.
* Updated training Silver Peak SDWAN, SolarWinds, Splunk, Aruba wireless, F5 LTM/GTM & CiscoSD-WAN - Silver Peak & Cisco Viptela
* Used Remedy ticketing system to track and resolve trouble tickets.
* Collaborated with ISPs and upstream providers to implement blackholing and RTBH (Remote Triggered Black Hole) techniques for effective DDoS mitigation.
* Used tools Wireshark, Packet Sniffer and Microsoft Network Analyzer for monitoring LAN’s and WANs for Network connection and failure issues.
* Led integration efforts with multiple Internet Exchange Points (IXPs) to improve path diversity and reduce dependency on upstream transit.
* Experience in deployment of Nexus 7010, 5548, 2148T, 2248 devices
* Deployed and Manage SD-WAN network (Cisco Meraki Solution) for WAN connectivity.
* Experience with Web Content Filtering, Proxy, Firewalls, IDS/IPS, Malware Inspection. Protecting the client Network from DDOS, Vulnerability and attacks from the internet.
* Firsthand experience on all software blades of Check Point Firewall. 24x7 on-call step-up support as a part of the safety operations team.
* Performed end-to-end network testing (ping, traceroute, telnet, netcat) to verify TCP/IP connectivity and identify bottlenecks.
* Supporting deployment of SD-WAN MPLS implementation via Viptela vEdge devices.
* Provided technical leadership in upgrading Wi-Fi networks to the latest standards (Wi-Fi 5, Wi-Fi 6) to meet growing bandwidth demands and support modern applications.

**Client: Availity, FL Feb 2016 – Apr 2018**

**Role: Network Security Engineer**

**Responsibilities:**

* Deployed the switches in high availability configuration with HSRP.
* Configured UDLD, port-fast, uplink fast and other spanning tree features.
* Support Complex 6500 /5500 Series Switches.
* Worked with telecom providers to provision and troubleshoot DID numbers, PRI circuits, and SIP trunk connectivity.
* Troubleshoot network problems using Packet Analysis tools like Ethereal.
* Configured various routing protocols including OSPF, BGP, analyzing throughput of WAN link
* Worked on the implementation of Cisco Meraki Enterprise Cloud Wireless Bridge/Repeater to extend the LAN for multiple buildings.
* Worked on Cisco Layer 2 switches (spanning tree, VLAN).
* Deployed IP filtering policies at the edge using ACLs, uRPF (Unicast Reverse Path Forwarding), and prefix-lists to prevent spoofing and unauthorized traffic.
* Troubleshooting IOS related bugs based on past history and appropriate release notes.
* Work on different connection medium like Fiber and Copper Connectivity.
* Performed and technically documented various test results on the lab tests conducted.
* Working Knowledge of SD-WAN technologies Such as Meraki, OpenStack, and Silver Peak.
* Deployed FTD code on ASA platform, Firepower appliances (4110, 2110) running on FXOS and managed through FirePower Management Center (FMC).
* Planning and configuring the entire IP addressing plan for the clients' network.
* Assist the certification team and perform configuration of LAN\WAN technologies such as Ethernet, Fast Ethernet, and Gigabit Ethernet.
* In-depth expertise in the implementation of analysis, optimization, troubleshooting and documentation of LAN/WAN networking systems.
* WAN Infrastructure running OSPF as a core routing protocol.
* Follow process & procedures for change & configuration management.
* Implemented BGP best practices for secure internet routing, including prefix filtering, max-prefix limits, and BGP session authentication using MD5.
* Supported nationwide LAN infrastructure consisting of Cisco 4510 and catalyst 6513.
* WAN Infrastructure running OSPF & BGP as core routing protocol.
* Support various Routers like 2600/3600/7200 series routers.
* Tested authentication in OSPF and BGP.

**Client: DXC , India Sep 2012 – Nov 2014**

**Role: Network Engineer**

**Responsibilities:**

* Installation and configuration of Cisco Routers 3600, 3900 and Switches 3550, 3560, 3560E, 3750, 6500, 7200 for VLANs, Routing Protocols (OSPF, BGP), VPNs etc.
* Implemented Cisco ACS for wired and wireless user authentication utilizing certificates and MAB for all known company assets.
* Installed WAN and LAN access for internet and intranet access.
* Configured Ether channels, Trunks, VLANs, HSRP in a LAN environment. Worked on Access, Core and Distribution layers.
* Implemented route redistribution between OSPF and EIGRP.
* Experience in AWS cloud platform and its features which includes EC2, VPC, EBS, SNS, RDS, EBS, Cloud Watch, Cloud Trail, Cloud Formation, AWS Config, Auto Scaling, Cloud Front, IAM, S3 and Route53.
* Provided end-user technical support for LAN and remote users in a 24/7 environment. Assisted in deploying WAN projects. Connectivity and configuration of routers, switches, end to end monitoring in new campuses.
* Planning, designing and implementing high availability solutions with Net screen & Juniper SRX Firewalls (500 & 650 series).
* Troubleshoot and hands on experience on security related issues on Cisco ASA/PIX, Juniper Net screen 6500, 6000.
* Provided WAN/LAN Cisco router/switch configuration, implementation, and support to internal customer tickets involving BGP, OSPF and EIGRP.
* Configuration and Maintenance of ASA 5585 firewalls with firepower, 5540, 5525 Firewalls using Cisco Security Manager (CSM).
* Perform configuration, deployment and support of cloud services including Amazon Web Services.
* Troubleshooted and worked with security issues related to Cisco ASA/ PIX, Checkpoint, IDS/IPS and Juniper Net screen firewalls.
* Configuring advanced threat prevention features such as intrusion prevention systems (IPS), anti-malware, and sandboxing to identify and mitigate security threats.
* Implement and modify DNS entries and manage IP Addresses using Windows DNS and DHCP. Experience configuring and troubleshooting on Citrix NetScaler Load Balancer.
* Performed Access Control Lists (ACLs) to set up usage for the intended users. Responsible for IOS installations and upgrades using TFTP Server.
* Troubleshooting Routing/Switching/Security Configuration problems/errors encountered to Clients in Head/Remote Campuses.
* Performed subnetting of the IP addresses. Configuration and allocating IP and network resources to Storage, Virtualization, Server, and Application teams.
* Responsible for design/implementation/maintenance of Site-to-Site VPNs, and remote access VPN using Cisco solutions (ASA 5520 and 5540), including head-end and remote client-side connections.