**A logo of a company

Description automatically generatedA logo for a company

Description automatically generatedA close-up of a logo

Description automatically generatedDatta**

**Senior Network Engineer (Cloud, Data Center, Security Firewalls, SDWAN)**

**A blue hexagon with white text

Description automatically generatedA logo with black and red squares

Description automatically generatedContact: 6099179484**

**Email : dattanetwork1234@gmail.com**

**Professional Summary:**

* Highly skilled and experienced Network Engineer with over 9 years of hands-on experience in designing, implementing, and supporting enterprise-level network infrastructures.
* Proficient in a wide range of networking technologies, including Cisco/Juniper Networking, Security which includes designing, deployment and providing network support, installation, and analysis for a broad range of LAN / WAN protocols. routing and switching protocols, security solutions, and cloud computing.
* Hands On experience Networking Technologies: LAN/WAN Architecture, **TCP/IP, VLAN, VTP, BGP, OSPF, EIGRP, MPLS, SD-WAN, VPN.**
* Proficient in implementing and maintaining ISO 27001-compliant **information security management systems (ISMS)**
* Strong understanding of information security principles, frameworks, and best practices, including **ISO 27001**, **NIST** Cybersecurity Framework, and **GDPR.**
* Routing and Switching: **Cisco IOS, Cisco Nexus, Cisco Catalyst, Juniper JUNOS, Arista EOS.**
* Security Solutions: **Cisco ASA, Palo Alto Networks Firewall, Check Point Firewall, IDS/IPS, VPN.**
* Cloud Computing: **AWS, Azure, Google Cloud Platform (GCP), Virtual Private Cloud (VPC).**
* Network Management: **SNMP, NetFlow, Syslog, Cisco Prime, SolarWinds, Wireshark.**
* Load Balancers: **F5 BIG-IP, Citrix NetScaler, Cisco ACE**
* **Cisco IOS/IOS-XR/NX-OS**, **Juniper JUNOS** for configuration & troubleshooting of routing protocols: **MP-BGP, OSPF, EIGRP, RIP, BGP v4.**
* Wireless Technologies: **Cisco Meraki, Aruba Wireless, WLAN Controllers**
* Experience **Arista Cloud** Vision. Working on Data center Architecture and Spine Leaf Architecture.
* Worked on EVPN, **VXLAN**, VTEPS, Bridge Domains, **MP-BGP** etc.
* Troubleshooting of **DNS, DHCP** and other IP conflict problems.
* Experience in **Palo Alto Firewalls** and the **Panorama** Network Security Management Box.
* Configuring Virtual Chassis for **Juniper** switches EX-4200, Firewalls SRX-210
* Experience with TACACS+, RADIUS implementation in Access Control Network.
* Experience in upgrading IOS in the Data center switches and routers.
* Migration Experience from Cisco ACS to Cisco ISE.
* Datacenter experience create new cable run list (L1), document runbook and Solution planning and upgrading, architect VXLAN, ACI and ASA cluster firewall with NAC, ISE.
* Implemented and managed Tripwire File Integrity Monitoring Points to detect unauthorized changes to critical system files and configurations.
* Designed, implemented, and maintained personal area networks (**PANs**) for clients, ensuring seamless connectivity and data security.
* Configured PAN devices such as Bluetooth, Wi-Fi Direct, and **Near Field Communication** (**NFC**) to establish efficient and secure connections between devices.
* Conducted thorough network assessments to identify potential vulnerabilities and implemented appropriate security measures to mitigate risks.
* Configured and fine-tuned Tripwire policies to align with industry best practices and organizational security requirements.
* Conducted regular integrity checks and audits using Tripwire FIM to identify potential security breaches or compliance violations.
* Collaborated with cross-functional teams to remediate security incidents and maintain a secure IT environment.
* Provided training and support to system administrators and security analysts on Tripwire FIM usage and best practices.
* Proficient in deploying, configuring, and managing Cisco Mobility Services Engine (CMX) and Prime Infrastructure for wireless network optimization
* Strong understanding of wireless network protocols, standards, and technologies, including IEEE 802.11, RF spectrum analysis, and location-based services
* Experience with network monitoring and management tools, including Cisco Prime Infrastructure, for centralized control and visibility of wireless infrastructure
* Knowledgeable in network security principles and best practices, particularly related to wireless network access control, encryption, and intrusion detection/prevention
* Excellent troubleshooting and problem-solving skills for diagnosing and resolving wireless network issues effectively
* Ability to communicate technical concepts and recommendations clearly and concisely to non-technical stakeholders
* Extensive work experience with **Cisco Routers, Cisco Switches**, **Load Balancers** and **Firewalls**.
* Experience working with **Cisco Nexus 2148** Fabric Extender and **Nexus 9K, 7010, 5000** series to provide a Flexible Access Solution for a datacenter access architecture.
* Experience with Cisco DNA solutions ISE, NGFW, Prime, ESA, WSA, VPN and CWS implementations.
* Experience with Spine Leaf Architecture, **EVPN, VXLAN, VTEPS, VNI, BGP**. Experience with Overlay and underlay technologies. Experience on scripting in **bash**
* **and Ansible**.
* Responsible for **Check Point** (Secure Platform R70) and **Cisco ASA firewall** administration across global networks.
* Experience in working with Cisco Nexus Switches and **Virtual Port Channel** configuration.
* Implementing and maintaining Sourcefire intrusion detection/ prevention **(IDS/IPS)** system and hardened protection standards, **IDS/IPS** signatures on Firewall for Fine-tuning of **TCP** and **UDP** services.
* Implementing traffic filters using standard and extended **access-lists**, distribute-lists and **route maps**.
* Implementing and troubleshooting complex layer 2 technologies such as **VLAN** Trunks**, VTP, Ether channel**, **STP, RSTP and MST**. Implementation of **HSRP, VRRP** for Default Gateway Redundancy.
* Proficiency in **Cisco ASAs, ISRs, Catalyst/Nexus**, **HP Switches, Cisco Meraki, Aruba, EIGRP, OSPF, BGP**.
* Experience with configuring **Nexus 2000** **Fabric Extender** (FEX) which acts as a remote line card (module) for the Nexus 5000.
* Experience with SD-WAN, DMVPN, NSX, HCX, BIG-IP F5 load balancers, version 9.x, 10.x, 11.x, Citrix NetScaler and Web Accelerators.
* Participating in troubleshooting SDN/SD-WAN deployments. Provide consultation regarding segmentation, security, and policy of the SDN network.
* Configuring and maintaining Quality of Service (QoS) protocols (SIP, BroadSoft, SRTP, SDP, IAX) on VoIP along  
   with PBX servers, VoIP Gateways and Cloud-based PBX servers, Active Directory Database.
* Deploying, Managing, monitoring, and supporting **Bluecoat Proxy** for content filtering, internet access between sites and VPN client users, forward proxy scenario and reverse proxy scenario for security and worked on adding URLs in **Bluecoat Proxy SG's** for URL filtering.
* Working extensively on **Cisco ASA 5500(5510/5540) Series**. Experience with **Palo Alto 5K** series. Migration from **ASA** to PA.
* Extensive experience in cloud management systems and integrated with **Azure** for AD.
* Working with Meraki **Wireless** access points MR 16, MR 18, MR 32, MR 42, MR 72 etc.
* Experience with **SSL decryption, APP ID, Threat ID, URL filtering** in PA firewalls.
* Working on upgrading **Aruba** controllers and Access points in troubleshooting the onboarding devices with the networks.
* **ClearPass** Deployment & Integration Experience - ClearPass TACACS, Onboard, and OnGuard policy features.
* Working on **Cisco Firewalls Cisco ASA 5500(5510/5540) Series and Checkpoint R75, 76, NGX R70 Firewalls.**
* Working with Automation script with **Python** module like **Chef & Ansible**.
* Experience on **Fortinet** FortiGate Appliances including 3200D, 1500D, 1200D running Latest 5.2 FortiOS.
* Configuring **Cisco Wireless Controllers** and **AP’s.**
* Excellent customer management/resolution, problem solving, debugging skills and capable of quick learning, effectively analyze results, and implement and deliver solutions as an individual and as part of a team.

|  |  |
| --- | --- |
| **Networking Technologies** | LAN/WAN Architecture, TCP/IP, Frame Relay, VPN, VLAN, VTP, NAT, PAT, STP, RSTP, PVST, MSTP, SDN, SDWAN, GNAC. |
| **Cloud Computing and Automation** | AWS, Microsoft Azure, Cisco Meraki, C++, Python scripting, Ansible, Cloud Migration. |
| **Networking Hardware** | Cisco Switches, Cisco Routers, ASA/Pix firewalls, IronPort |
| **Routing Protocols** | OSPF, IGRP, EIGRP, RIP, IS-IS, BGP, Multicasting |
| **Network Management and Monitoring** | Wireshark, Infoblox, Cisco Prime, Security Device Manager (SDM), CiscoWorks; TCP Dump and Sniffer; SolarWinds, Extrahop, NetFlow Traffic Analyzer, Network Performance Monitor (NPM), Riverbed |
| **Routers** | CISCO 2600, 2800,3600,3800,7200, Juniper M & T Series, Cisco CRS-1, CRS -3, GSR |
| **Load Balancers** | Cisco CSM, F5 Networks (BIG-IP), Citrix NetScaler, CISCO ADC |
| **Capacity & performance** | Cisco works |
| **Switches** | CISCO 2900, 3500,4500,5000,6500, Nexus 7k,5k,2k |
| **Simulation Tools** | GNS3, VMware, OPNET IT GURU, OPNET Modeler, Cadence |
| **Layer Three Switching** | CEF, MLS, Ether channel (PAGP and LACP, Load Balancing). |
| **Wireless** | Cisco Meraki Wireless Access points (MX-65, MX-64, MS-225-48PS, MS-220-48PS, MR-42), Aruba Access points 200, 207,300,320, Wireless controllers 7280, 7240, Cisco Wireless controller 5508 and Cisco Aironet 3700 series. |
| **Firewalls** | Juniper Net Screen (500/5200), Juniper SRX (650/3600), Pix (525/535), ASA (5520/5550/5580), McAfee Web Gateway, Checkpoint, Palo Alto firewalls. |
| **AAA Architecture** | TACACS+, RADIUS, Cisco ACS |
| **Features & Services** | IOS and Features, HSRP, GLBP, IPAM IRDP, NAT, SNMP, SYSLOG, NTP, DHCP, CDP, DNS, TFTP and FTP Management, Open Stack, IVR’s, HLD and LLD documents, Dell equal logics |

**Certifications:**

* CCNA – Cisco Certified Network Associate
* CCNP – Cisco Certified Network Professional
* AWS
* Palo Alto accredited configuration engineer (ACE).

**Education Details:**

* Bachelor of computer science and engineering., CVSR College of Engineering (Anurag University) – Hyderabad, India

**Professional Experience:**

**Client: Invesco, Houston, TX Feb 2022 – Till date**

**Role: Senior Network Engineer (Cloud, Data Center, Palo Alto, Firewall, SDWAN)**

**Project Description:** Build new and maintain existing capabilities in our public and private (on-premises) Cloud platforms. Building blocks, go language, Terraform, Ansible, and work with on-premises infrastructure OpenStack and Cloud services in AWS.

**Responsibilities:**

* Deploy and Maintain SDWAN solution, routers and Switches, Cisco ASR, Juniper SRX and Fortinet firewalls. Working as a customer facing engineer in deploying new hardware, Upgrade IOS, troubleshooting any ongoing issues with Routing, Security, SDWAN and coordinate with support and professional services.
* ACI
* Creating detailed AWS Security Groups which behave as virtual firewalls that control the traffic allowed to reach one or more AWS EC2 instances.
* Deploy Reveal(x) 360 sensors via a distributed grant from AWS License Manager using with Extrahop network monitoring tool.
* Implementing and maintaining Sourcefire intrusion detection/ prevention (IDS/IPS) system and hardened protection standards, IDS/IPS signatures on Firewall for Fine-tuning of TCP and UDP services.
* Updating customer networks by configuring routers, switches, and incorporate the SDWAN into the network design.
* Working with NAT/PAT, Policies, SSL Forward proxy, Decryption, URL Filtering on PA firewalls.
* Designing interfaces, defining integration workflows and solutions using vArmour products and other systems within the customer environments.
* Collaborated with cross-functional teams to integrate PAN solutions into larger network infrastructures, ensuring compatibility and scalability.
* Provided technical support and troubleshooting for PAN-related issues, ensuring minimal downtime and optimal performance for clients.
* Stayed updated on emerging PAN technologies and industry trends to recommend innovative solutions and enhance network efficiency.
* Configuring LACP, OSPF protocols on Arista 7250qx-64 Cloud switches.
* Daily Support of F5 environment to include Creation of new VIPs/WIPs and irules.
* Working and demonstrating experience on the PAN-OS 8, 9.1, and 10.0 versions; Palo Alto: PA 220, PA 820, PA-2K, PA-3K and PA-5K firewalls.
* Working with Load Balancing team to build connectivity to production and disaster recovery servers through F5 Big IP LTM load balancers.
* Working on the URL filtering and upgradation of Palo Alto firewall from PAN-OS 8.1 to PAN-OS 9.0.
* Working on the migration from Cisco ASA to the Palo Alto firewall and the configuration of User-ID’s, App-ID’s, SSL Decryption, URL Filtering, Policies, Zone Protection, High Availability, Certification Management, Migrated all IPSEC tunnels, ACL’s, NAT rules and policies.
* Troubleshooting Fortinet Firewall, issues, edited policies and created rules.
* Providing Level 3 Support for converged infrastructure Nexus 5Ks, Cisco MDS, EMC XtremIO/VMAX3s) and non-vBlock Storage - VNX2, ECS (cloud), Isilon (FILE), Pure Storage, HP3Par. Migrated data from Datacenters and on-premises to Cloud using AWS Import/Export Snowball service.
* Configuring user's role and policies for authentication using cisco NAC and monitoring the status of logged users in network using Cisco ISE.
* Day-to-day work includes certifying new code across multiple vendor Firewalls by testing them with the Charter requirements for PCI Compliance.
* Infrastructure Services, Business Relationship Managers, and Engineering teams supporting, and implementing Cloud-native and over the top networking in GCP.
* Cisco advanced security products including tetration, Stealthwatch, NAC and Client.
* Objectives for Security Operations, which includes perimeter security, endpoint security, malware protection systems and implementation of Cisco EA (ISE, Stealthwatch and Umbrella).
* Deployment of Cisco AAA product ISE and its integration with other Cisco Security products such as DNAC, StealthWatch, Firepower.
* Successfully implemented PAN solutions for clients, resulting in improved data accessibility and productivity.
* Reduced security risks through the implementation of advanced encryption protocols and access control mechanisms on PANs.
* Received recognition from management for exceptional problem-solving skills and dedication to delivering high-quality PAN services to clients.
* Setting up and Managing Virtual Machines on AWS Cloud including working on EC2, Route53, RDS, Lambda.
* Supporting centralized **DNS** and **DHCP** administration using Infoblox.
* Working on **Azure AD SAML** authentication for **Zscaler** authentication and AD group-based policies.
* Deployed and Manage **SDWAN** network (Cisco Viptela Solution) for WAN connectivity.
* Implementing and managing hybrid cloud connectivity - Arista, Express Route.
* Configuring and testing source, static and destination NAT/NAT64 policies as part of the certification process.
* New code updates in the lab environment help Charter to identify and detect any unknown bugs that may cause downtime or vulnerability in the production environment.
* Working on the SDWAN implementations at all Greenfield and Brownfield medical facilities/hospitals by deploying Viptela hardware.
* Fortinet Firewall administration configuration of FortiGate 3000, 3815 series as per network diagram.
* Participating actively in proof-of-concept projects implementation which included storage and backup solutions from private cloud providers Amazon AWS & Microsoft Azure.
* Working on the ISE integration in DNA Center.
* Application traffic security with WAF, F5 ASM, F5 APM for Authentication, defend NetScaler’s for ICA proxy, Citrix VDI, Microsoft Office 365, Azure AD, AWS, Zscaler Cloud based proxies, Cisco IronPort, and Blue Coat proxies.
* Working on setting up tunnels from F5 devices to Zscaler cloud. Worked on Zscaler Private Access- ZPA for app based per user VPN. Experience with APP connectors, access policies, APP segments, LSS connectors in ZPA.
* Upgrading 3x data centers’ network and Optical fiber infrastructures with an Arista spine-leaf.
* Configuring cisco DNA for Secure remote workforce with zero trust policies and dynamic segmentation of endpoints.
* Configuring DNA for Policy-driven provisioning and guided remediation to increase network uptime.
* Documenting the network design using Microsoft Visio and GNS3.
* Working on issues with IPS/IDS servers, Zscaler and Bluecoat Proxies.
* Working and configuring devices using Ansible and Python for automation.
* Performing network monitoring, providing analysis and network topologies using various tools like NS3, Wireshark, SolarWinds etc.
* Redundancy &Management HSRP, VRRP, Wireshark, SolarWinds, SNMP, CISCO Works, GNS3, Riverbed.
* Working on configuring and deploying the Arista switches and creating MLAG for the switches and firewalls.
* Working with Cloud Exchange providers like Equinix. Worked on Direct Connect and IPSEC tunnels. Configuration of BGP o peer with On-premises and Internet.
* Working with IronPort, Bluecoat and Zscaler cloud Proxies for Internet Web Security. Worked on migration project from IronPort’s to Zscaler Internet Security.
* Rapid firewall security assessments through Python automation.
* Plan, Install, upgrade, and configure F5 load balancer 11X to 15X and A10 harmony controller install using CLI (TMSH and BASH) commands.
* Working on Route53 in AWS to register domain names, route internet traffic to resources in AWS, Health monitoring of resources and DNS failovers. Experience with DNS resolution between VPCs and on premises.
* Working with SDN, Cisco ACI, VXLAN, VTEPS, VNI, Bridge Domain, Arista Cloud Vision, EVPN, MP-BGP, Spine and Leaf Architecture.
* Designing, implementation, and managing network security countermeasures including firewalls and intrusion detection/prevention systems such as: Palo Alto, Pfsense, and Cisco's Sourcefire.
* Responsible for maintaining multi-vendor network environment including Juniper JUNOS, Fortinet firewalls, Palo Alto PA-200 and configuring different policies to provide connectivity.
* Configuring and administering network devices consisting of F5 load balancers, Bluecoat proxies, Juniper SRX's, Palo Alto Network Firewalls.
* Administrating on F5 LTM, GTM, ASM, APM on series 5050, 10000 8900.
* Working on products for Wi-Fi alliance and WLAN testing & pre and post deployment Wireless security WEP, WPA, EAP.
* Network segmentation using Illumio and Palo Alto firewalls for traffic filtering and applying polices on Illumio central manager.
* Responsible for troubleshooting on Cisco ISE added new devices on network based on policies on ISE.
* Implementing Cisco ISE 1.2 for Wireless 802.1x Authentication and Authorization with Flex Connect
* Configuring and performing software upgrades on Cisco Wireless LAN Controllers 2504, 4404 ,5508 for Wireless Network Access Control integration with Cisco ISE.
* Upgrading Cisco ISE appliances company wide. Recently rolled out OpenDNS including onsite VM appliances.
* Configuring Cisco NAC for Secure access by utilizing 802.1X. Cisco TrustSec.
* Understand OSPF configuration and authentication settings for migration routing over to the Firepower platform.
* Implementing Cisco and Aruba Wireless Controllers, Aruba Wireless Access Points at corporate site as a part of WLAN Infrastructure.
* Deploy and manage with advanced security and network management tools like Aruba ClearPass Policy Manager.
* Monitoring and responding to network anomalies utilizing SolarWinds/Orion's software and recommended appropriate network solutions for issues.
* Firewall policy provisioning on Fortinet FortiGate appliances using Forti Manager.
* Working with NSX, HCX and on IP Address Data Mining and Management over using Men and Mice Management Console.
* Working with Cisco Channel partners to build practices around Cisco ACI.
* Using Cisco ACI (Application Centric Infrastructure) SDN architecture to reduce operating costs, automate IT tasks, for greater scalability and visibility in a data center environment.
* Deployed and configured Cisco Mobility Services Engine (CMX) to provide location-based services, including real-time location tracking, proximity marketing, and analytics, enhancing the overall user experience for wireless network users.
* Integrated CMX with existing wireless infrastructure, including Cisco Wireless LAN Controllers (WLC) and Access Points (AP), to collect location data and provide actionable insights for network optimization and troubleshooting.
* Utilized CMX APIs and SDKs to develop custom applications and integrations, enabling innovative use cases such as asset tracking, geofencing, and indoor navigation for various industries, including retail, healthcare, and manufacturing.
* Designed and implemented wireless network designs using Cisco Prime Infrastructure, leveraging its centralized management capabilities to streamline configuration, monitoring, and troubleshooting of Cisco wireless devices across distributed environments.
* Creating Azure Virtual Firewalls, VPNs, VLANs, Load Balancers and Route Tables. Implemented Checkpoint firewall rules according to business requirements and verifications.
* Configuring and maintained IPSEC and SSL VPNs on Palo Alto Firewalls.
* Creating firewall policies and NAT rules to provide access for websites internal and externally on Palo Alto and Juniper firewalls.
* Pushing Firewall rules staged during the day to respective comes at night includes the juniper and Palo Alto firewalls.
* Working with Cisco Meraki wireless managed network infrastructure.
* Configuring Cloud Computing Engineering, concepts, service models (IaaS, PaaS, etc.)
* Configuring and Maintained rules on Palo Alto Firewalls & Analysis of firewall logs using various tools.
* Configuring Palo Alto policies and setting different device configurations.
* Working on SCIM provisioning from Azure AD to Zscaler ZIA for users and groups sync.
* Participating in the deployment, configuration and maintenance of a multiple data center infrastructure consisting of over 50 Palo- alto firewall clusters and 10 Panorama devices along with supporting routers and switches.

**Environment:** Cisco 3500, 3700, 3900 series Routers, Cisco ASA Firewalls, F5 ADC, Cisco ACI, VMware, Aruba, VTP, Juniper SSG-140, Extrahop, Palo Alto Wildfire, Juniper EX series switches, Cisco Firepower, Bluecoat, Aruba Wireless, WLC, Juniper SRX, Routing Protocols: BGP, OSPF, AAA (TACACS+ & RADIUS), TCL Scripting, ACL Configuration.

**Client: AT&T, Redmond, WA Aug 2021 - Jan 2022**

**Senior Automation Network Engineer**

**Project Description:** During this project, my main aim was to maximize network performance by monitoring performance, troubleshooting network problems and outages, scheduling upgrades and collaborating with security architects on network optimization for providing better security to the firm.

**Responsibilities:**

* Configured auto scaling in customized VPC, based on elastic load balancer (ELB) traffic and using ELB health check in order to trigger auto scaling actions.
* Configure / Troubleshoot CISCO 12000, 7500, 3800 series routers and 3560 series switches for LAN/WAN connectivity.
* Integrate Microsoft active directory (LDAP) into checkpoint for identity awareness and user authentication.
* Performing network monitoring, providing analysis using various tools like Wireshark, SolarWinds etc.
* Installed, configured, and maintained with vendors Cisco, Juniper, Alcatel-Lucent, Arista, Brocade, Riverbed, Enterasys, Fortinet networking and Wireless technologies and protocols.
* Performing standard network operations via ITIL standard with Incident Management and Change Management.
* Hands on experience of NSX, HCX, McAfee Proxy, Nexus 9K, 7k, 6K, 5k and 2K FEXs and Cisco switch 3560.
* Extensively done all the LTM upgrades. Troubleshoot User connectivity issues on CLI utilities and handled GUI too for upgrading other components DNS, Firewall, AMS,
* Experience with Palo Alto and checkpoint firewalls with next gen firewall features that includes app id, threat id, URL filtering, user id, SSL decryption.
* Implemented Palo Alto 7050 Firewall in HA Pairs as an internet firewall, configured rules and Zones based on traffic.
* Deploying AWS Solutions using EC2, S3, EBS, Elastic Load balancer (ELB), auto scaling groups, RedShift and OpsWorks.
* Working in identity and access control policy related technologies such as authentication, authorization, accounting (AAA), 802.1X.
* Worked extensively in Configuring, Monitoring and Troubleshooting Cisco's ASA 5500/PIX security appliance, Failover DMZ zoning & configuring VLANs/routing/NAT with the firewalls as per the design.
* Cisco PRIME to manage Wireless LAN Controllers.
* Replacing Checkpoint VPN and Bluecoat proxy with Zscaler and worked on implementing **Zscaler** in Production.
* Design and build out a very large **100G Layer3 Leaf & Spine architecture (eBGP)** using Arista switches to support the network consolidation in the new data center.
* Automation practice and coding in Terraform and Ansible.
* Performed Switching Technology Administration including **VLANs, inter-VLAN Routing, STP, RSTP** and Port Aggregation on Cisco catalyst devices and Arista 7K.
* Worked on the installation and configuration of **Cisco ISR 800, 1000 series and ASR 1000 series** routers.
* Working as a network access controls **(NAC) ISE** engineer in planning and designing client’s global network for network access solution.
* Conducted risk assessments and gap analyses to identify security vulnerabilities, threats, and risks to the organization's information assets, prioritizing remediation efforts and implementing controls to mitigate identified risks.
* Established and monitored key performance indicators (**KPIs**) and metrics to measure the effectiveness and performance of the **ISMS**, conducting regular internal audits and compliance reviews to ensure adherence to ISO 27001 standards.
* Facilitated external audits and certifications for **ISO 27001** compliance, collaborating with auditors, stakeholders, and certification bodies to demonstrate compliance with regulatory requirements and industry standards.
* Expertise with Installation of **Arista 7250QX** series switches on **Spine Platform**.
* Configured CSP hypervisor to support NFV platform for both Cisco and third-party VNFs.
* Configured CSP hypervisor Increased automation and operational agility.
* Using Palo Alto Networks Linux Access Platform.
* Provide the network and security boundary between the borderless cloud infrastructures and regular cloud DMZs.
* Configuration management and infrastructure automation tooling – Jenkins, Terraform, Ansible/Tower, Puppet/Chef, vRA/vRO, and other orchestrators and configuration management frameworks.
* Deploy, configure, and support CISCO Wireless LAN controllers and AP devices globally.
* Serve as part of a team of network engineers responsible for base wide network upgrade from Cisco Layer 3 Catalyst switches to Juniper Layer 3 EX4200 & EX3200 switches.
* Worked on Zscaler policies, cloud app control policies, advanced threat, malware, sand box-based policies.
* Worked on Azure AD SAML authentication for Zscaler authentication and AD group-based policies.
* Managed successful delivery of massive security response portfolio including Splunk and Cisco ISE.
* Worked with Cisco Umbrella to manage policies and evaluate effectiveness related to client and server DNS protection.
* Palo Alto design and installation (Application and URL filtering, Threat Prevention, Data Filtering). Configured and maintained IPSEC and SSL VPN's on Palo Alto Firewalls.
* Integrate Splunk with AWS deployment using puppet to collect data from all EC2 systems into Splunk.
* Monitored and Created traffic Pattern on Arista 7250 switches using Open flow.
* Working with Nexus 7010, 5548, 5596, 2148, 2248 devices.
* Perform troubleshooting and issue resolution related to SIEM solution, including reports.
* Managed DHCP, DNS and IP address through Infoblox, and Admin for Internet sites access thru Zscaler.
* Configuring VPC (Virtual Port Channel), VDC (Virtual Device Context) in Nexus 7010/7018
* Created documents for various platforms including Nexus 7k, ASR9k, and ASR1k enabling successful deployment of new devices on the network.
* administer IPv4 enterprise network infrastructure utilizing Juniper routers like Juniper MX80, MX 480 and MX960.
* Devised new VPN solution utilizing Cisco Firepower and Cisco AnyConnect.
* Design and implement Catalyst/ASA Firewall Service Module for various LAN’s.
* responsible for managing Cisco routers, switches, HP switches, F5 load-balancers using SNMP MIBs for fault detection and for fault isolation.
* Providing second/third level technical support for ACI (Application Centric Infrastructure), APIC technologies.
* Responsible for the secure development lifecycle for Cisco's Nexus line of products, including Application Centric Infrastructure (ACI), Application Policy Infrastructure Controller (APIC) - Cisco's Software Defined Network (SDN).
* Deploying Application Centric Infrastructure, Spine-Leaf, APIC and VXLAN.
* Automation frameworks (Terraform, Ansible, Chef, Puppet) and automation scripts to support the Azure environment tools (Azure Resource Manager Templates).
* Function as part of a Firewall and Security team in support of Checkpoint Firewalls, Zscaler Proxy, Juniper Portals, SecAuth, Open LDAP, and Active Directory.
* Change control / ITIL Service Controls / PCI compliance. Coordinating with various teams to perform Network Changes.
* Migrated to Juniper EX series switches from Cisco 3500, 3700 series and 6500 series switches. Worked on setting up Cisco ASR as edge routers. Worked on BGP for inter Data center connectivity.
* Migrated Virtual Machines and applications from on premises cloud to AWS.
* Architect, plan and deploy SIEM solution migration for splitting one SIEM into two environments.
* Successful Data Center Migration Planning and Successfully developed Python automation scripts to perform Cisco firewall rule assessments.
* Configured Nexus 2000 Fabric Extender (FEX) which acts as a remote line card (module) for the Nexus 5000 to connect servers and storage devices.
* Deployed applications and host websites on AWS cloud involving blackboard.
* Created the AAA servers for LDAP and Active Directory authentication in F5 APM.
* Configure and manage LDAP User management with Checkpoint Smart Directory. Implemented the policy rules and DMZ for multiple clients of the state on the Checkpoint firewall.
* Worked with several network engineers for the understanding of Juniper SRX firewalls along with the changeover to Palo Alto. Palo Alto Firewall Management-Panorama.
* Performed configuration for end users on CUCM, IM&P, Jabber, Webex, Telepresence Video Communication Server, SX80 and end points DX80's, SX20's and SX10's.
* Configured and managed APM as an SSL VPN solution for remote management.
* Implementation and Configuration (Profiles, iRules) of F5 Big-IP LTM-6400 load balancers
* Implemented Access lists and policy mapping on Juniper router installed in each branch across all the states.
* Configuring policies on ASM using manual policy enforcement and auto policy enforcement with F5 ASM, LTM, APM.
* Implemented, analyzed and recommended appropriate system for the out of band management monitoring. Utilizing SolarWinds for primary and disaster recovery sites.
* Installing & configuring firewalls – NSX, HCX, Checkpoint NG & NGX, Cisco ASA (5500), Cisco Pix, ISA, and IP tables.
* Configured Connectors along with Zscaler TAM and DAS team.
* Perform WLAN testing of newly installed WLAN controllers and Aps. Interface daily with customers and NOC reporting production milestones and any issues
* Performed virtualization and deployed various VMs using VMware ESXI 6.5
* Involved in working with Data Center hardware and management software.
* Worked on issues with IPS/IDS servers, Zscaler and Bluecoat Proxies.
* Performed in-depth analyses and complex troubleshooting overall Network telecom infrastructure and IT system using Compuware Dynatrace, and Wireshark.
* Implementing large Data Center infrastructures with Cisco ACI, Cisco N9K, N7K, N5K, N3K, Cisco Cat 9500/9300, 6500, 4500/4900, Cisco ISR 4451, Cisco ASR1001.
* Planning and development of designs for Migrating to AWS cloud.
* Configuration and Administration of Cisco and Juniper Routers and Switches.

**Microsoft, Seattle, WA April 2019 – July 2021**

**Role: Senior Network Engineer**

**Responsibilities:**

* Deploying and decommissioning of VLANs on core ASR 9K, Nexus 9K, 7K, 5K and its downstream devices and also configure 2k, 3k, 7k series Routers.
* Designed and Implemented Cisco PIX525 and ASA5550 Firewall's interfaces with FTP, DNS, HTTP servers on DMZ with different security levels.
* Hands on experience in managing IT Network infrastructure in Meraki Dashboard (Access points, Switches etc.).
* Working on network monitoring and analysis tools like, SOLAR WINDS, CISCO works and Riverbed and Wireshark.
* Experience with configuring Cisco 6500 VSS in Distribution layer of the Data center network.
* Managing and configuring Aruba Wireless devices and Cisco Access Points.
* Networking 802.1x - ClearPass Deployment & Integration Experience.
* Configuring and managing F5 ASM (Application security manager). Developed security policies.
* Configure and troubleshoot Juniper EX series switches.
* Integrating Configuring Cisco Wireless LAN Controllers WLC with ISE to perform Dot1x.
* Designed & Deployed Cisco ISE and Provided comprehensive guest access management for Cisco ISE administrators.
* Configured Cisco ISE for Domain Integration and Active Directory Integration.
* Configured and performed software upgrades on Cisco Wireless LAN Controllers 5508 for Wireless Network Access Control integration with Cisco ISE.
* Performed WLAN validation of newly installed APs using NetScout SurveyPro analytical software.
* Hands on Experience working with security issues like applying ACL's, configuring NAT and VPN.
* Responsible for design and implementation/migration from Cisco Wireless platform to Aruba Wireless platform.
* Worked on integrating existing Layer 2 and Layer-3 networks with ACI.
* Conducted wireless site surveys and RF spectrum analysis using Cisco Prime Infrastructure tools to assess wireless coverage, interference, and performance metrics, identifying optimization opportunities and resolving connectivity issues.
* Developed and maintained network policies and configurations within Cisco Prime Infrastructure, ensuring compliance with industry standards and best practices for security, performance, and reliability.
* Automated routine network tasks and workflows using Cisco Prime Infrastructure features such as templates, policies, and scheduled tasks, improving operational efficiency and reducing manual errors.
* Provided training and support to IT staff and end-users on Cisco Prime Infrastructure and CMX usage, functionality, and best practices, empowering them to effectively manage and troubleshoot wireless networks.
* Collaborated with cross-functional teams, including network engineering, system administration, and application development, to integrate CMX and Prime Infrastructure with other IT systems and applications, enabling seamless data exchange and workflow automation.
* Stayed updated on emerging technologies and industry trends related to wireless networking, attending training sessions, webinars, and conferences to enhance skills and knowledge in CMX and Prime Infrastructure.
* Well Experienced in configuring protocols HSRP, GLBP, PPP, PAP, CHAP, and SNMP.
* Configured & Implemented Cisco Firepower Services with Cisco ASA 5500-X advanced security defenses.
* Switching tasks include VTP, ISL/ 802.1q, IP Sec and GRE Tunneling, VLANs, Ether Channel, Trucking, Port Security, STP and RSTP.
* Configure and install Aruba Wireless controllers 7210 and access points.
* Implementing PCI policies and procedures, ITIL practice in customer infrastructures.
* Responsible for layer 2 securities which was implemented using a dedicated VLAN ID for all trunk ports, setting the user ports to non-trucking, deployed port security, when possible, for user ports.
* Involved in configuring Juniper SSG-140 and Cisco ASA firewall.
* Implemented Cisco Application Centric Infrastructure (ACI) as a solution for data centers using a Spine and Leaf architecture.
* Strong hands-on experience on ASA Firewalls, Palo Alto Firewalls. Implemented Security Policies using ACL, Firewall, IPSEC, SSL VPN, IPS/IDS, AAA (TACACS+ & RADIUS).
* Supported Bluecoat Proxy in explicit mode for users trying to access Internet from Corp Network.

**Environment:** Cisco ASA Firewalls, F5 ADC, Cisco 3900 Routers, Cisco Catalyst switches 6500, 3750, 3550, 2960 Switches, Juniper SSG-140, Palo Alto Wildfire, Juniper EX series switches, Riverbed, Cisco Firepower, **Aruba** **Wireless**, **WLC**, Nexus 9k, 7k, 5k, ASR 9k, ASR 1k, Nexus 2000 FEX, Juniper SRX, Routing Protocols: BGP, OSPF, AAA (TACACS+ & RADIUS), TCL Scripting, ACL Configuration.

**Adobe, San Jose, CA Sept 2017 – March 2019**

**Role: Senior Network Engineer**

**Responsibilities:**

* During this project my main aim was to maximize network performance by monitoring performance, troubleshooting network problems and outages, scheduling upgrades, and collaborating with security architects on network optimization for providing better security to the firm.
* Involved in design and implementation of Data Center Migration, worked on implementation strategies for the expansion of the VPN networks.
* Designed and implemented support for streaming Open config models in model driven telemetry.
* Actively involved in Switching Technology Administration including creating and managing VLANS, Port security- 802.1x, Trucking 802.1Q, RPVST+, Inter-VLAN routing, and LAN security on Cisco Catalyst Switches4507R+E, 6509-E and Cisco Nexus Switches 2232, 5596, 7009.
* Experience with deploying PIM Sparse-mode/Dense-mode multicasting in Campus locations.
* Used Cisco ACI Fabric which is based on Cisco Nexus 9000 series switches and Cisco Application Virtual Switch (AVS)
* Implemented Cisco ACI infrastructure for supporting rapid application change by reducing complexity with a common policy framework that can automate provisioning and resource management.
* Installed and configured latest Cisco equipment including Cisco catalyst switches 6500, Nexus 7010, Nexus 5548 and Nexus 2k as per business requirements.
* Collaborated with cross-functional teams, including IT, legal, compliance, and risk management, to integrate information security requirements into business processes, systems, and applications, aligning with organizational objectives and priorities.

**Environment:** Cisco 12000, 7500, 3800 series routers and Cisco 3560 series switches, Juniper EX4200, EX3200 Switches, Juniper MX80, MX480, MX960 Routers, F5 ADC, FHRP: HSRP, GLBP, ASR 9000, Cisco Firepower, Juniper SSG-140, Cisco Nexus Switches 2232, 5596, 7009, Checkpoint Firewall, VLAN, 802.1Q Trunking.

**Wipro Aug 2014 – Aug 2017**

**Role: Technical Support Analyst**

**Responsibilities:**

* Involved in implementation of trunking using Dot1Q, and ISL on Cisco Catalyst Switches.
* Involved in Local Area Network (LAN) design, troubleshooting, and maintenance as per company’s requirements.
* Worked with sniffing tools like Ethereal to analyze the network problems.
* Maintenance and troubleshooting of network connectivity problems using PING, Trace Route.
* Performed replacements of failed hardware and upgraded software.
* Configured VLANS to isolate different departments.
* Troubleshoot issues related to VLAN, VLAN Trunking, HSRP failovers, related issues.
* Configured IPSEC VPN on SRX series firewalls.
* Used TFTP server to backup Cisco configuration files.
* Network layer tasks included configuration of IP Addressing using FLSM, VLSM for all applications and servers throughout the company.