**A close-up of logos

Description automatically generated**A logo for a company

Description automatically generatedA close-up of a logo

Description automatically generated**Bindhu**

**Phone: +1 (609)-738-8321**

**Email: bindhu.network001@gmail.com**

**PROFESSIONAL SUMMARY:**

* 6+ years of experience in **Cisco** and **Juniper networking** and security, I focus on network design, deployment, support, and analysis using the latest tools like **Cisco DNA Center**, **Junos OS**, **Nexus** and **Catalyst** **switches**, and security platforms like **Cisco ISE** and **Juniper SRX.**
* Demonstrated mastery in architecting and deploying secure multi-tier applications on **AWS** and **Azure**, leveraging services like VPC, EC2, Route 53, and CloudFormation for highly scalable, available, and cost-efficient cloud solutions.
* Proficiently designed, implemented, and managed network security solutions utilizing **Palo Alto Networks**, **Checkpoint**, and **Fortinet technologies**, deploying advanced features like SSL inspection, intrusion detection, and micro-segmentation strategies for robust threat prevention.
* And
* Configured and managed **Zscaler Internet Access (ZIA)** to secure internet access for users, implementing advanced **threat protection** features to block **malware** and **phishing** attacks.
* Engineered high-availability architectures using **F5 load balancers**, implementing GSLB and disaster recovery solutions, ensuring seamless failover and traffic distribution across multiple data centers for uninterrupted services.
* Led the design and deployment of **Illumio's** Adaptive Security Platform (**ASP**) to implement micro-segmentation strategies, enhancing security posture and significantly reducing attack surfaces across the network.
* Led successful deployments and optimizations of **Viptela SD-WAN** solutions across global branches, integrating intelligent traffic steering, dynamic path selection, and application-aware routing for enhanced performance and reliability.
* Designed and deployed **Cisco ACI** in a multi-site environment, configuring **APIC controllers** and **fabric switches** for application-based network policies and centralized management.
* Developed **Python scripts** to automate network configuration and management tasks, integrating with **RESTful APIs** of **Cisco**, **Juniper**, and **Arista** network devices to streamline operations, reduce manual effort.
* Designed and deployed **AWS VPCs** (Virtual Private Clouds) to create isolated network environments, configuring **subnets**, **route tables**, and **security groups** to secure and optimize network connectivity.
* Deployed **SolarWinds** Network Performance Monitor (NPM) to monitor and manage network performance, ensuring high availability and quick issue resolution for **Cisco**, **Juniper**, and **Arista** devices.
* Configured and managed **Infoblox DNS, DHCP, and IPAM (DDI)** solutions, ensuring efficient allocation and management of IP resources across enterprise networks. Enhanced operational efficiency by automating **IP address assignments** and **DNS provisioning**.
* Utilized **Cisco ISE** profiling features to identify and classify network devices dynamically, automating access policy enforcement and improving network visibility.
* Designed and deployed **VMware vSphere 8.0** environments, configuring **ESXi hosts** and **vCenter Server** for high availability, resource optimization, and seamless management of **virtual machines**.
* Designed and implemented a high-density wireless network using **Cisco Catalyst 9800 Series Wireless Controllers** and **Cisco Aironet 4800** access points, providing reliable and high-performance **Wi-Fi coverage**.
* Managed and configured diverse infrastructure elements including **Cisco Nexus switches (9300, 9500, 9300X, 9500X)**, **Arista networking solutions (7280R, 7500R**, **7280R2**, **7500R2**), and structured cabling systems compliant with **CAT6A** and **fiber optics**, ensuring high reliability and performance.
* Expertly addressed complex network issues across **Layer 2** and **Layer 3** environments, utilizing various tools like **Wireshark**, **Splunk**, and network analysis tools, ensuring rapid identification and resolution of issues.
* Integrated **Ekahau** with Cisco Prime for detailed wireless network management and performance monitoring.
* Proficiently deployed and managed wireless **LAN**s across diverse environments using **Cisco**, **Aruba**, and **Meraki** access points, conducting site surveys and configuring robust security protocols for secure wireless access.
* Utilized dynamic routing protocols (e.g., **BGP**, **OSPF**, **EIGRP**) to manage **WAN connectivity** and ensure optimal path selection and failover capabilities.

**TECHNICAL SKILLS:**

|  |  |
| --- | --- |
| Routers | Catalyst 8300 Series, 8200 Series, ISR 4000 Series, 1000 Series, 900 Series, 800 Series, Catalyst 8300 Series Edge Platforms, ASR 1000 Series, Asr 1013 Router, ASR 901 Series, ASR 9000 Series, 1013 Router. Juniper MX304, MX10008 and MX10004, SDN-enabled MX10003, SDN-enabled MX2020 |
| 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. |
| Switch Platforms | Cisco Catalyst series 2960, series 3560, 3850, 4500, 6500, 7000, 9000; CISCO Nexus series 2K, 5K, 3K, 7K, and 9K |
| 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 | Checkpoint (NGX R65, 3100, 5100, 5900), Cisco Firewalls (ASA 5505, 5506-X, 5585), Palo Alto Networks (PA series 2K, 3K and 5K) with panorama 8.0, WAF |
| 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, URL Filtering, L2F, IDS, TCP Intercept, Router Security, SNMP trap. |
| Network Management and Monitoring | ServiceNow, Wireshark, Infoblox, HP NView, Cisco Prime, Splunk, Security Device Manager (SDM), Cisco Works, TCP Dump and Sniffer, SolarWinds Net Flow Traffic Analyzer, NetScout, Network Performance Monitor (NPM), Network Configuration Manager (NCM), SAM, IP Address Manager, Additional Polling Engine. |
| Load Balancers | F5 (BIG-IP) LTM 2000, 3900Viprion, Cisco ACE, Citrix NetScaler |
| Other Networking Protocols and Fundamentals | DHCP and DNS server, Active Directory Management, NTP, NDP, TCP, UDP, FCP, Network Implementation, Troubleshooting techniques, NHRP, NetBIOS, NFS, FTP, TFTP, HTTP, PAP, PPTP, SIP Trunking, SNMP logging, SMTP, RADIUS and TACACS+, PBX servers, SDN, SAN. |
| Operating Systems | Windows 10/7/XP, MAC OS, Windows Server, Nexus OS, Cisco IOS XR, Linux, UNIX, Cumulus. |
| Wireless Technologies | Canopy Wireless Devices, D-Link Point-to-point Wireless, D-Link APs, CISCO 1200 series APs, Clear pass wireless and APs, Cisco Meraki, Linksys Wireless/Wi-Fi Routers, Prime Infrastructure, Ekahau, Air Magnet, AirWatch and WLC’s (8510, 5508, 5706), Cisco Aironet AP’s (2600, 3600, 3700), ISE, MSE, Aruba 225, Aruba 3000 controller & Airwave, Clear Pass 6.0,6.2,6.5 |
| Scripting | Shell Scripting, Python, and Ansible |

**EDUCATION:**

* Bachelor of Information Technology Engineering from RVR&JC College of Engineering, India
* Master’s in Computer Engineering from Wright State University, USA

**CERTIFICATIONS:**

* Cisco Certified Network Professional (**CCNP**)
* Cisco Certified Network Associate (**CCNA**)
* Palo Alto Certified Network Security Engineer (**PCNSE**)

**PROFESSIONAL EXPERIENCE:**

**Client: Catholic Health Initiatives,** **Houston, TX Jan 2024 – Till Date**

**Role: Network Security Engineer (Palo Alto, AWS, Cloud, SDWAN, VXLAN, Infoblox)**

**Project Description:** Led the successful deployment of **Viptela SD-WAN** solutions across 20 branch offices, optimizing network performance and reducing **WAN** costs by 30%. Designed and configured Virtual Device Contexts (**VDC**) and Virtual Port Channels (**VPC**) for scalable and flexible network segmentation.

**Responsibilities:**

* Integrated **SD-WAN solutions** with existing **MPLS networks** to optimize hybrid WAN architecture, improving cost efficiency and performance for enterprise applications.
* Implemented **Viptela SD-WAN policies** for **QoS** and **application-aware routing**, using intelligent traffic steering and centralized management to optimize network performance and simplify monitoring.
* Configured and maintained **Palo Alto firewalls** to ensure appropriate segmentation and traffic filtering across IT and OT systems, optimizing security posture.
* Utilized **Viptela vEdge routers** to establish a secure and scalable **SD-WAN fabric**, ensuring seamless connectivity across distributed sites and enhancing network resilience.
* Deployed **Cisco ACI** in data centers, streamlining network management and enhancing application performance, while implementing **micro-segmentation** strategies to enforce granular security policies and isolate sensitive workloads.
* Managed and configured **Cisco switches** to ensure secure communication between IT and OT networks, enforcing **VLANs** and access control for critical infrastructure.
* Deployed and managed **Cisco DNA Center (DNAC)**, providing end-to-end network visibility, automation, and assurance across the enterprise network.
* Designed, deployed, and managed **Palo Alto Networks firewalls** globally, including **PA-5000 (5220, 5250), PA-3000 (3220, 3250), and PA-7000 (7050, 7080) Series**, to establish secure networks and enforce detailed application-based security policies.
* Designed and secured **ICS** and **SCADA** network architectures, ensuring minimal latency and high availability while implementing security controls to protect critical OT infrastructure.
* Developed and implemented disaster recovery plans and security protocols for IT and OT networks to ensure business continuity in case of incidents.
* Configured **Aviatrix Transit Network** with **Palo Alto VM Network Service** for robust firewall traffic inspection and enhanced network security.
* Created and managed security policies within **Illumio** to enforce zero trust principles, ensuring that only authorized users and devices have access to critical applications and data.
* Successfully integrated **Illumio** with existing next-generation firewalls (e.g., **Palo Alto**) to enhance visibility and control across network segments, improving overall network security.
* Utilized **Illumio’s** real-time monitoring capabilities to identify and respond to anomalies, enabling proactive threat detection and incident response.
* Integrated OpenShift with **AWS**, enabling hybrid cloud deployments that leverage the benefits of both platforms, enhancing flexibility and scalability for enterprise applications.
* Monitored and troubleshot containerized applications using tools like **Prometheus** and **Grafana**, ensuring optimal performance and quick resolution of issues in production environments.
* Developed Helm charts for **Kubernetes**, standardizing application deployments and facilitating easier management of complex applications within the Kubernetes ecosystem.
* Implemented security best practices for containerized applications, including image scanning, role-based access control (**RBAC**), and network policies within **Kubernetes** and **OpenShift**.
* Collaborated with the Load Balancing team to connect production and disaster recovery servers using **F5 Big-IP LTM** and **Citrix NetScaler**, configuring profiles for high availability.
* Designed and implemented **F5 BIG-IP LTM** version 17.x to optimize application delivery and ensure high availability. Configured virtual servers, pools, and load-balancing algorithms to distribute traffic efficiently across backend servers.
* Deployed **F5 BIG-IP DNS** version 15.x and 16.x to manage global traffic and ensure high availability across multiple data centers. Configured **DNS load balancing** and **Global Server Load Balancing (GSLB)** to direct users to the best-performing sites.
* Configured and managed **Infoblox DDI (DNS, DHCP, IPAM)** services to provide centralized IP address management and efficient network infrastructure operations.
* Deployed and configured **SolarWinds Network Performance Monitor (NPM)** to monitor real-time network performance, detect bottlenecks, and ensure uptime.
* Monitored network traffic and responded to security incidents, investigating threats across IT and OT environments to mitigate risks and prevent breaches.
* Configured and deployed **Cisco Identity Services Engine (ISE)** for **network access control (NAC)**, ensuring secure and authorized access to the corporate network.
* Managed **FortiManager** for centralized firewall management and **FortiAnalyzer** for detailed security analysis, log correlation, and reporting, boosting network visibility and control.
* Handled **FortiGate firewalls**, local servers, **Load Balancers**, **LAN**, **VLAN**, Switching, and access controllers to ensure secure and efficient network operations.
* Worked closely with IT and OT teams to align cybersecurity strategies, ensuring compliance with industry standards and seamless communication across environments.
* Managed **Zscaler Cloud Proxy Architecture**, including traffic forwarding with **GRE tunnels**, **Azure AD Authentication**, and access policies, using the latest **Zscaler ZCC 3.6** and **ZIA 6.2** tools.
* Configured and managed **Zscaler Internet Access (ZIA)** to secure user access, block threats, filter harmful sites, and ensure compliance with security policies and controls.
* Worked with **software-defined network solutions** such as **OpenFlow**, **OpenStack**, **Cisco SD-WAN (Viptela)**, **Cisco ACI**, **DDI Implementation** (e.g. **Infoblox**), **Cisco Meraki**, **VMware NSX**.
* Engineered scalable and fault-tolerant **AWS architectures**, leveraging services like **VPC**, **EC2**, **S3**, **RDS**, **IAM**, **Route 53**, and **CloudFormation** to design and deploy robust cloud solutions.
* Developed and implemented disaster recovery strategies with **AWS services**, including **AWS Backup**, **Storage Gateway**, and **Glacier**, and supported **Splunk** across **Unix**, **Linux**, and **Windows** platforms while adapting to AWS cloud strategies.
* Integrated monitoring and logging tools for real-time network visibility, threat detection, and automated alerting across the IT and OT environments.
* Designed and implemented **Azure Virtual Networks (VNets)** to create isolated network environments, configuring subnets, route tables, and network security groups to secure and optimize network connectivity.
* Integrated **OSPF** with **BGP** on **Cisco Catalyst 9600 Series switches** for smooth route redistribution and improved routing flexibility.
* Configured traffic aggregation, replication, and filtering in tools like **SolarWinds Network Performance Monitor (NPM)** and used **Cisco DNA telemetry** features to optimize monitoring and trigger alerts based on network health thresholds.
* Deployed and maintained **Arista Network Packet Broker (NPB)** solutions and **7300X Series switches** as packet brokers, configuring **Arista Wi-Fi 6E solutions** and access points, and managed the network through **CloudVision** for unified wired and wireless management.
* Demonstrated deep knowledge of interoperability between **Cisco Meraki** and **Viptela SD-WAN** solutions, facilitating a smooth transition process.
* Automated firewall rule deployment and network configurations to ensure consistency in enforcing security policies across **IT/OT** interfaces.
* Configured **ClearPass Device Insight** for automated device classification and policy enforcement, ensuring proper access controls according to device type and behavior.
* Worked with **CloudVision**, including setting up **CloudVision Portal (CVP)** for centralized management, enabling network-wide visibility, and automating configuration push to multiple **Arista devices**.
* Configured **EIGRP** over **DMVPN** on **Cisco ISR 4000 Series routers** to enable secure and adaptable routing for remote sites.
* Implemented robust security measures using **Meraki security appliances**, configuring **VPN tunnels**, **site-to-site VPNs**, and advanced security features such as **content filtering** and **intrusion prevention** to safeguard network integrity.
* Deployed **Juniper MX Series routers** for advanced routing and traffic engineering, improving network performance and reliability.
* Monitored and analyzed **ICS**-specific protocols such as **Modbus**, **DNP3**, and **OPC** for performance and security, ensuring uninterrupted and secure communication between control systems.
* Implemented **SDN technologies** (**OpenFlow**, **OpenDaylight**) to centralize network control and automate provisioning and management, reducing overhead and enabling quick changes.
* Implemented **BGP** on **Cisco ASR 9000 Series routers** to handle routing between multiple ISPs, enhancing route optimization and ensuring reliable connectivity.
* Monitored and reported on compliance metrics related to **NIST** and **ISO** frameworks, providing insights to management and stakeholders on the organization's security posture and areas for improvement.
* Utilized security information and event management (**SIEM**) tools to analyze security events and incidents, applying **NIST** and **ISO** guidelines to prioritize response actions.
* Integrated real-time monitoring tools to capture logs and detect abnormalities in **SCADA** environments, providing visibility into system health and potential security risks.
* Implemented advanced networking features on **Cumulus devices**, including **VXLAN**, **EVPN**, and **Layer 2/3 protocols**, to optimize network performance.
* Integrated **Cisco Meraki** with third-party solutions using **APIs**, enabling cross-platform functionality and data exchange to enhance network orchestration and automation.
* Automated network infrastructure tasks using **Ansible playbooks** and **Python scripts**, streamlining configurations, updates, and deployments across diverse network devices and services.
* Deployed **SNMP** and **Syslog** on **Cisco ASA** to monitor firewall performance and log security events, integrating with **SIEM solutions** for complete security analysis.
* Proficient in **Palo Alto Next-Generation Firewalls**, **HP ArcSight**, **Splunk Enterprise**, **Wireshark**, **FireEye**, and various network analysis tools.
* Configured **DHCP failover** on **Windows Server** and **Cisco IOS** to ensure continuous IP address management and minimize downtime.

**Client: State Street Bank and Trust Company,** **Princeton, NJ Jan 2023 – Dec 2023**

**Role: Senior Network Engineer**

**Responsibilities:**

* Enhanced network security and connectivity by integrating **Palo Alto Next-Gen** firewalls with overlay **VMware NSX SDN** technology, allowing firewall traffic inspection and secure communication between **VPCs** and on-premises data centers.
* Implemented **IPsec VPN** with **QoS** policies on **Juniper MX Series** routers to prioritize critical traffic and optimize performance over secure connections.
* Implemented advanced threat protection and **sandboxing** in **Zscaler Internet Access (ZIA)** to block malware, phishing, and unknown threats, strengthening defenses against zero-day attacks and APTs.
* Configured **Palo Alto firewalls** and **Cisco switches** in high availability (**HA**) mode, ensuring failover and redundancy for critical OT and IT network segments.
* Configured **Cisco ASA 5500-X** **Series** firewalls with version 9.14, deploying advanced security policies, intrusion prevention, and **VPN** services to ensure robust network protection.
* 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.**
* Implemented network segmentation for **ICS/SCADA** systems, isolating critical operational technologies from IT environments to mitigate cyber risks and prevent lateral movement.
* Monitored access patterns with **ZPA** and adjusted policies using advanced analytics to mitigate risks and improve security.
* Engineered disaster recovery solutions using **F5's GTM** functionalities, enabling seamless failover and load distribution across multiple data centers.
* Implemented advanced security features and policies on **Palo Alto firewalls**, such as App-ID, User-ID, and decryption capabilities, to bolster threat prevention and application visibility.
* Implemented **BGP** multipath on **Juniper QFX5100** switches to enable load balancing and redundancy across multiple links.
* Provided incident response support using insights from **Illumio** to mitigate risks and secure vulnerable assets, contributing to a robust security framework.
* Conducted training sessions for internal teams on best practices for using **Illumio**, fostering a culture of security awareness and effective policy adherence.
* Collaborated with cloud engineering teams to implement **Illumio** in public cloud environments, ensuring secure access and segmentation for cloud-native applications.
* Led the deployment of **ZTNA** solutions to support remote workforces, allowing employees to securely connect to internal resources from anywhere, without the need for a traditional **VPN**.
* As for my experience with Wi-Fi platforms, while my primary expertise is with **Arista**, I've also worked with other commercial Wi-Fi solutions including **Cisco Meraki**, Ruckus, and Ubiquiti Networks.
* Employed ClearPass OnGuard’s reporting tools to oversee endpoint compliance and create audit reports for security and regulatory needs.
* Configured **EIGRP** with **MPLS** on **Cisco CSR 1000V** to enhance routing scalability and efficiency in virtualized environments.
* Created and maintained **Dockerfiles** to streamline the build process for container images, ensuring consistency and efficiency in application deployment across various environments.
* Managed Kubernetes clusters using tools like **kubectl** and **kubeadm**, implementing best practices for resource allocation, scaling, and health monitoring to ensure high availability.
* Automated deployment processes with **Kubernetes** Operators, enhancing application lifecycle management and facilitating self-healing capabilities for stateful applications
* Developed and implemented custom Helm charts for complex application deployments, enabling version control and easy rollback of releases to ensure stability in production environments.
* I did integrate **NPBs** with security tools and performance monitoring solutions to get visibility across the network.
* Administered **Viptela SD-WAN** enterprise deployment, implementing networks and devices for **SDWAN** environments.
* Effectively managed a hybrid network environment, utilizing both **Cisco Meraki** and **Viptela SD-WAN** platforms, to balance network workloads and maintain service continuity.
* Implementation and management of **F5** Global Traffic Manager (**GTM**) and Local Traffic Manager (**LTM**) solutions, architecting highly available and scalable network infrastructures.
* Spearheaded the migration process from **Checkpoint** firewall infrastructure to **Palo Alto Networks**, ensuring a seamless transition while mitigating potential risks and service disruptions.
* Configured and optimized load balancing algorithms, SSL offloading, persistence, and health checks, ensuring efficient traffic distribution and high application availability.
* Proficiently configured and managed **Viptela SD-WAN** components, including **vEdge** routers, **vSmart** controllers, and **vManage**, ensuring 99.9% network uptime.
* Led the design and deployment of **Azure** cloud services, leveraging its suite for infrastructure as a service (**IaaS**), platform as a service (**PaaS**), and software as a service (**SaaS**).
* Configured **Azure Application Gateway** for load balancing and application firewall capabilities, ensuring secure and reliable application delivery.
* Configured **Google Cloud VPCs** to create isolated network environments, setting up subnets, firewall rules, and route tables for secure and efficient networking. Implemented custom route tables and private Google access to enhance security and control over network traffic.
* Configured **SolarWinds** **NCM** to automate configuration, compliance, and backups for multi-vendor devices, improving efficiency and security.
* Deployed **Blue Coat** **SSL** Visibility Appliance to decrypt and inspect encrypted traffic, detect hidden threats, and ensure policy compliance.
* Developed and enforced security policies aligned with **ICS/SCADA** security standards, such as **NIST SP** **800-82** and **IEC 62443**, to ensure robust protection of operational technologies.
* **OSPF** configuration and authentication settings to migrate routing over to the **Firepower** platform.
* Implemented logging and monitoring solutions for **Docker** containers and **Kubernetes** clusters using tools like **ELK** **Stack** (Elasticsearch, Logstash, Kibana) and **Fluentd**, providing visibility into application performance and troubleshooting.
* Developed multi-container applications using **Docker** Compose, simplifying local development environments and ensuring compatibility across various stages of the application lifecycle.
* Integrated **DNAC** functionalities into existing IT ecosystems through **API** integrations, enabling seamless communication with third-party tools and orchestrating complex workflows.
* Developed custom applications and scripts using **DNAC's** **APIs** to extend platform capabilities and address specific business requirements.
* Developed and maintained security policies and procedures in alignment with **ISO** standards, ensuring that organizational practices meet regulatory requirements and industry best practices.
* Participated in security audits and assessments, utilizing **NIST** and **ISO** frameworks to evaluate the effectiveness of existing security controls and recommend improvements.
* Collaborated with cross-functional teams to integrate security measures into the software development lifecycle (**SDLC**), ensuring compliance with **NIST** and **ISO** guidelines throughout the development process.
* Expert in **Ansible** for automating infrastructure, provisioning, configuration management, and application deployments, with experience in creating efficient workflows for network provisioning and orchestration.
* Implemented and managed **Blue Coat** proxy servers to replace existing **ISA** Proxy servers, layered with Websense content filtering.
* Involved in the Configuration of Access lists (**ACL**) on checkpoint firewalls for the proper network routing for the B2B network connectivity.
* Configured **Bluecoat** proxies for content and URL filtering and ensured data loss prevention and zero-day exploit prevention.
* Conducted migrations to **ACI** from traditional networking, ensuring seamless transitions, **L2/L3** connectivity, and traffic flow mapping.

**Client: Syntel, India Dec 2017 – July 2022**

**Role: Network Engineer**

**Responsibilities:**

* Implemented early adoption and integration of emerging networking technologies such as **Software-Defined Networking (SDN)** and **Network Functions Virtualization (NFV)** to enhance network flexibility and reduce operational costs.
* Utilized **Cisco ACI’s API** and automation tools to streamline network configuration and management, reducing manual effort and operational complexity.
* Configured **Meraki MX Series** security appliances for secure and scalable network connectivity, including **SD-WAN** capabilities to optimize traffic routing and performance.
* Conducted regular security assessments and vulnerability scans on both IT and OT systems, remediating identified weaknesses to improve overall network security.
* Configured **IPsec VPN tunnels** on **Cisco ASA 5500-X Series** firewalls to provide secure site-to-site and remote access connectivity, ensuring data confidentiality and integrity with strong encryption algorithms.
* Utilized **SolarWinds Network Configuration Manager** (NCM) to automate configuration management, compliance auditing, and backup for multi-vendor network devices, improving operational efficiency and security.
* Developed comprehensive documentation for **Illumio** deployments and security policies, while continuously assessing and optimizing configurations to align with evolving business needs and compliance requirements.
* Configured **Viptela vEdge routers** to establish secure and scalable **SD-WAN fabric**, ensuring seamless connectivity across distributed sites and enhancing network resilience.
* Integrated **SD-WAN solutions** with existing **MPLS networks** to optimize hybrid **WAN** architecture, improving cost efficiency and performance for enterprise applications.
* Monitored network traffic for anomalies and potential threats specific to **ICS/SCADA** environments and led incident response efforts to quickly address any security breaches.
* Worked with enterprise-level **Wi-Fi configuration**, troubleshooting, **IP routing**, network design, architecture, protocols, and topologies.
* Involved in troubleshooting **network traffic** and its diagnosis using tools like **ping**, **traceroute**, **Gigamon**, **Wireshark**, **TCP dump,** and **Linux** operating system servers.
* Established **BGP peering** with external **ASNs** on **Arista 7500R Series switches**, enhancing network resilience and optimizing inbound and outbound traffic flow.
* Utilized **BGP** route reflectors on the **Cisco Nexus 7000 Series** to streamline route advertisement and reduce the number of **BGP** sessions required within the AS.
* Utilized **OSPF** authentication and **MD5** hashing on **Arista 7050X Series** switches to secure routing updates and prevent unauthorized route injections.
* Updated and maintained security documentation, ensuring that configurations and policies align with industry standards (e.g., **NIST**, IEC 62443) and corporate security policies.
* Configured **OSPF** route summarization on **Cisco ASR 1000 Series** routers to reduce the size of routing tables and improve network efficiency.
* Enhanced the security of both IT and OT networks by implementing access control lists (**ACLs**), firewall rules, and security policies to mitigate cyber threats.
* Conducted training sessions for development and operations teams on **Docker** and **Kubernetes** best practices, fostering a culture of containerization and **DevOps** principles within the organization.
* Implemented horizontal pod autoscaling in **Kubernetes**, dynamically adjusting the number of running pods based on traffic load to ensure optimal resource utilization and application performance.
* Used service meshes like Istio to manage traffic flow, security, and observability in microservices architectures, improving communication between services and enhancing resilience.
* Configured **EIGRP** unequal-cost load balancing on **Cisco ISR 4331** routers to optimize traffic distribution across multiple paths.
* Monitored **EIGRP neighbor relationships** and **route updates** using **SolarWinds NPM** for proactive issue resolution.
* Deployed **SolarWinds** IP Address Manager (**IPAM**) to manage and track IP address allocation, ensuring efficient utilization and avoiding conflicts within the network.
* Configured **RSTP** (Rapid Spanning Tree Protocol) on **Cisco Catalyst 9500 Series** switches to prevent network loops and ensure fast convergence in **Layer 2** networks, enhancing network stability and reliability.
* Implemented **MST** (Multiple Spanning Tree Protocol) on **Juniper EX4300** switches to manage multiple **VLANs** with a single spanning tree instance, optimizing network performance and scalability.
* Configured **NAT** (Network Address Translation) policies on **Cisco ASA 5516-X** to manage IP address translation and enhance network security.
* Diagnosed and resolved network performance issues, ensuring reliable communication across **IT/OT** interfaces while maintaining security controls.
* Configured and optimized firewall rules to secure **ICS/SCADA** traffic while ensuring minimal disruption to operational processes.
* Used network analyzers like **Wireshark**, **ethereal,** and **Sniffer** for packet analysis.
* Integrated **Palo Alto Networks PA-7050** with **LDAP** and **Active Directory** to enforce user-based policies, utilizing user identification features to apply security measures based on user identity.
* Configured zone-based firewall policies on **Palo Alto Networks PA-5220** to segment network traffic, enforcing security controls based on data sensitivity and minimizing the attack surface.
* Maintenance and troubleshooting of network connectivity problems using **PING**, and **Trace Route**.
* Conducted Evaluated and tested **next-generation firewalls** to enhance network security and prevent sophisticated cyber threats.
* Assisted in migrating from **IPv4** to **IPv6**, ensuring seamless transition and compatibility with the latest internet standards.