A picture containing text, ax, weapon, knife

Description automatically generated 

Bairam

Cloud Network Engineer

Phone:

**SUMMARY:**

* Experienced Cisco certified network engineer with over 10+ years of expertise in routing, switching, data center environment, and cloud networking. Significant hands-on experience in seamlessly migrating remote sites to new MPLS links and establishing connectivity to data centers, leveraging SD-WAN technology for enhanced network performance and efficiency.
* Proficient in managing, monitoring, and supporting AWS and Azure cloud environments, with a focus on network security devices and services.
* Strong expertise in AWS technologies including CloudFormation, ECS Fargate, EC2, Network
* Security Groups (NSGs), VPC, S3, Lambda, and CloudWatch.
* In-depth knowledge of a wide range of AWS services such as EC2, VPC (NAT, Peering, VPN), IAM, Elastic Beanstalk, S3, RDS, DynamoDB, Redshift, and Route 53.
* Experience administering AWS services using both the AWS Console and AWS CLI.
* Significant hands-on experience in seamlessly migrating remote sites to new MPLS links and establishing connectivity to data centers, leveraging SD-WAN technology for enhanced network performance and efficiency.
* Proficient in troubleshooting and handling policy change requests for Cisco ASA, Checkpoint, and Palo Alto Firewalls, ensuring smooth network operations during planned network changes and new IP segment deployment.
* Proficient in firewall technologies, encompassing general configuration, risk analysis, security policy development, and creating and modifying rules for Checkpoint R65, R70, R77, Palo Alto, and Cisco ASA.
* Experienced in configuring all models of Palo Alto Networks Firewalls, including PA-2k, PA-3k, PA-5k, etc., and utilizing a centralized management system like Panorama for efficient management of large-scale firewall deployments.
* Proficient in configuring a wide range of security policies, including Network Address Translation (NAT), Port Address Translation (PAT), Virtual Private Networks (VPNs), route maps, prefix lists, and Access Control Lists (ACLs).
* Demonstrated proficiency in Cisco Identity Services Engine (ISE) and successfully managed the migration of wireless and TACACS systems to ISE.
* Proficient in Identity and Access Management (IAM) solutions, including designing, implementing, and managing access controls and policies for network resources, ensuring secure and authorized user access.
* Experienced in designing and configuring OSPF and BGP protocols on Juniper Routers, specifically MX960 and MX480 models, as well as SRX Firewalls like SRX240 and SRX550.
* Deep knowledge and significant expertise in a wide range of networking technologies, including Ethernet, 802.2/3, 802.1d, IP, TCP, VLAN, VTP, STP, BGP, OSPF, HSRP/RRP/GLBP, PIM, IGMP, MSDP, MPLS, LDP, DNS, HTTP, SSL, NetFlow.
* Familiarity with high-speed networking technologies such as 10G, 40/100G, and proficiency in Linux/Unix systems.
* Proficient in utilizing Ansible, a leading orchestration and automation tool, for network configuration management, provisioning, and deployment, ensuring efficient and consistent network operations.
* Experienced in leveraging Terraform, a widely adopted infrastructure-as-code (IaC) tool, to automate the provisioning and management of network resources, enabling scalable and reproducible network infrastructure deployments.
* Developed automation scripts for managing cloud core network using a Python scripting language.

**CERTIFICATIONS:**

* Cisco Certified Network Associate (CCNA)
* Cisco Certified Network Professional (CCNP)

**TECHNICAL SKILLS:**

|  |  |
| --- | --- |
| Switches | CISCO 2900, 3750, 2950, 2934, 3500, 4500, 4900, 5000, 6500, 7500 Nexus 7k, 5k, 2k. Arista 7280, 7010. |
| Routing Protocols | OSPF, IGRP, EIGRP, RIP, MPLS, BGP, Multicasting. |
| Routers | CISCO 2500, 2600, 2800, 3000, 3600, 3601, 3640,3800, 3825 4000, 7200, 7500, 7600 Juniper M & T Series, Cisco CRS-1, CRS -3, GSR. |
| Firewalls and Load Balancers | IPSEC, SSL VPN, F-5 BIGIP, Juniper net screen (500/5200), Juniper SRX (650/3600), Pix (500/525/535), ASA (5520/5550/5580). |
| Cloud | AWS (ELB, S3, EC2, AMI), Ansible, AWS-LAMBDA, Terraform, Kubernetes. |
| Networking Technologies | LAN/WAN Architecture, TCP/IP, Frame Relay, VPN, VLAN, VTP, NAT, PAT, STP, RSTP, PVST, MSTP. |
| LAN Networks | Ethernet, Fast Ethernet, Gigabit Ethernet & 10 Gigabit Ethernet, VLAN routing, Inter-VLAN Routing, VTP, STP, RSTP. |
| Networking Hardware | Cisco Switches, Cisco Routers, Cisco ASA firewalls, Palo Alto Juniper routers, Nexus Switches. |
| Security Technologies | PAP, CHAP, Cisco PIX, Nexpose, QRadar, Tenable. |
| Agile Tools | Rally and Jira |
| Monitoring tools | Cisco Works 2000, Wireshark, SNMP, TCP dump, Orion, Splunk. |
| Operating Systems | Cisco IOS, IOS XR, Windows 7, Vista, XP, 2000,2003, LINUX. |
| Programming Languages | Ansible, Terraform, Git. |

**PROFESSIONAL EXPERIENCE:**

**Comcast, Mt Laurel NJ NOV 2022 – Present**

**Cloud Network Engineer**

**Responsibilities:**

* Created a comprehensive AWS security roadmap that outlined the utilization of AWS services and third-party tools for effective security monitoring in the AWS Cloud.
* Implemented automated build pipelines using Jenkins for continuous integration, enabling streamlined software development and deployment processes.
* Developed custom Splunk dashboards and reports tailored to specific business needs and requirements.
* Deployed Chef Dashboard for efficient configuration management of existing infrastructure, ensuring consistency and scalability.
* Install and configure Red Hat Enterprise Linux Servers in box Physical and Virtual Environment.
* Collaborated with cross-functional teams to integrate Splunk with existing network infrastructure and security tools.
* Developed a robust AWS Security Group strategy, including establishing naming conventions, defining owners, and implementing an approval process for Security Group change requests in a promote-to-production environment.
* Enabled and configured CloudTrail logs for 26 AWS accounts, setting up a centralized, encrypted S3 Bucket to store all CloudTrail logs, and adjusting bucket policies to grant appropriate access for each account's CloudTrail.
* Proficient in securing AWS infrastructure using various security measures such as private subnets, security groups, Network Access Control Lists (NACLs), and Web Application Firewalls (WAF).
* Skilled in configuring and deploying instances on AWS environment and data centers, with expertise in Amazon EC2, CloudWatch, Elasticsearch, and managing security groups.
* Experienced in designing AWS CloudFormation templates for creating custom sized VPCs, subnets, and NAT gateways to ensure successful deployment of web applications and database templates.
* Responsible for maintaining user accounts (IAM), and managing AWS services such as RDS, Route 53, VPC, RDB, DynamoDB, SES, SQS, and SNS in the AWS cloud.
* In-depth knowledge of terraform for automation in cloud environments.
* Demonstrated proficiency in leveraging key AWS cloud services like EC2, auto-scaling, and VPC to build secure, highly scalable, and flexible systems capable of handling both expected and unexpected load bursts.
* Implemented and managed AWS Direct Connect to establish dedicated, high-performance connectivity between on-premises infrastructure and AWS cloud, ensuring secure and efficient data transfer for mission-critical applications and workloads.
* Working understanding of Linux Systems administration.
* Conducted regular performance tuning and optimization of Splunk search queries and data pipelines to ensure efficient data ingestion and processing.
* Developed and deployed serverless functions using AWS Lambda to streamline application workflows, optimize resource utilization, and achieve cost savings by executing code in response to events, eliminating the need for traditional server provisioning and management.
* Cloud technologies with focus on AWS. In depth knowledge of AWS technologies such as S3,EFS, EBS, SQS, EC2, VPC, ELB and Auto-scaling, Cloud Trail, Cloud formation for disaster recovery EC2, terraform for automation with AWS and Route53.
* Leveraged AWS CloudWatch extensively to monitor and troubleshoot AWS resources, configure custom metrics and alarms, and gain real-time visibility into system performance, ensuring proactive detection and resolution of issues, and driving continuous improvements in system reliability and operational efficiency.
* Proficient in configuring and troubleshooting F5 requests, including VIP (Virtual IP) creation, decommissioning servers from load balancers, iRule updates, and modifying health check monitors to align with customer requirements.
* Involved in F5 load balancer configurations, including migrating configurations from Cisco ACE to F5 platforms and providing general troubleshooting and support for F5 load balancers.
* Skilled in configuring and implementing F5 BIG-IP, LTM, and GTM load balancers to efficiently manage global and local traffic, ensuring optimal performance and high availability.
* Overseeing Level III Network operations at HCL, efficiently handling daily tickets, incidents, and service requests through the utilization of ticketing tools like PDSM (Process Driven Service Management), and delivering comprehensive technical support encompassing troubleshooting, maintenance, upgrades, patches, and fixes.
* Developed comprehensive URL filtering policies based on business requirements, leveraging Palo Alto Networks firewall capabilities to enforce granular controls and ensure compliance with acceptable use policies.
* Integrated Panorama with Palo Alto firewalls to centralize management and streamline administration across multiple Palo Alto firewall devices, enabling efficient policy management and monitoring.
* Developed SSL decryption policies for traffic decryption, ensuring robust antivirus and malware protection capabilities.
* Implemented an External Dynamic List in the URL filtering profile, allowing for real-time updates and enhanced security by dynamically blocking or allowing URLs based on external threat intelligence feeds.
* Proficiently managed complex routed LAN and Global Traffic Manager (GTM) networks, including configuring and administrating Cisco routers, switches, and firewalls.
* Managed an extensive network infrastructure spanning across the USA, overseeing the operations of over 90,000 network devices, including Nexus 7010, 5020, and 2000 Data Center switches, Cisco Catalyst 6500 series switches with WS-SUP720-3B SUP, Cisco Catalyst 3650 switches, as well as routers such as Cisco 7600, 7200, and 2900 series, and various firewalls.

**Environment:**

AWS Services: CloudFormation, ECS Fargate, EC2, CloudWatch, Elasticsearch, RDS, Route 53, Splunk, VPC, DynamoDB, SES, SQS, SNS, Jenkins (for automated build pipelines), Terraform, Chef Dashboard (for configuration management), F5 BIG-IP, LTM, and GTM load balancers, Palo Alto firewalls (Panorama, SNMP, SSL decryption), PDSM, Palo Alto Networks firewall, External Dynamic List, Cisco routers, switches, and firewalls, BGP, HSRP, 802.1Q, Catalyst switches, Nexus 7K and 5K switches, VSAN, VLAN routing, CloudTrail, CloudWatch, SNMP, Syslog.

**AT & T, Middletown NJ FEB 2022 – OCT 2022**

**Network Security Engineer**

**Responsibilities:**

* Proficient in configuring and maintaining Cisco ASA firewalls, including models ASA 5540, ASA 5520, and ASA 5510, as well as PIX 535 and FWSM firewalls. Skilled in implementing and troubleshooting site-to-site VPNs on ASA firewalls, ensuring secure and reliable connectivity between network locations.
* Completed the migration from PIX firewalls to ASA firewalls, leveraging an in-depth knowledge of both platforms to ensure a smooth transition with minimal downtime and preserving existing firewall policies and rulesets. Implemented best practices and conducted thorough testing to validate the functionality and security of the new ASA firewall environment.
* Implemented Site-to-Site VPNs between ASA Firewall and routers.
* Configured and carried out automated, manual, dynamic, and static testing for the mitigation of security flaws and attacks on Cisco devices and Web Security Appliances.
* Successfully led the migration of on-premises applications to AWS, ensuring a seamless transition and improved scalability, availability, and cost-effectiveness.
* Designed and deployed AWS services for applications, utilizing the AWS stack and leveraging services such as EC2, S3, RDS, Lambda, and CloudFront.
* Took responsibility for security and network administration of the AWS environment, implementing security measures, managing network infrastructure, and coordinating with internal and external audit teams.
* Managed and configured the OSPF, BGP, HSRP, VRRP, and ARP security vulnerabilities mitigation and protection systems.
* Analyzed and coordinated operations on the latest and upcoming security vulnerabilities with the Cisco Security Incident Management Team.
* Oversaw the migration from conventional WAN to Meraki SD-WAN, which streamlined network operations and cut costs by relying on cloud-based administration and intelligent traffic routing.
* Successfully integrated Meraki SD-WAN solutions for a global corporation, allowing for seamless branch-to-branch connection and centralized administration.
* Designed and implemented VeloCloud SD-WAN architecture for a large-scale network, improving user experience and application performance.
* Deployed BIG-IP F5 LTM Load Balancers for load balancing and traffic management of critical business applications.
* Implemented and maintained F5 LTM and GTM series such as 6400, 6800, and 8800 for ensuring high availability of corporate applications.
* Proficient in configuring Virtual Device Context in Nexus 7010 and successfully managing the configuration, upgrade, and verification of the NX-OS operating system.
* Experienced in configuring Virtual Chassis for Juniper switches, including EX-4200 models, as well as configuring and managing firewalls such as SRX-210.
* Effective collaboration with Cisco for opening TAC (Technical Assistance Center) cases and resolving issues within project deadlines.
* Expertise in checking and configuring Cisco 7600 routers at data centers to address remote site issues.
* Strong understanding and experience in physical infrastructure aspects like structured cabling, IP address management, racking, stacking, and Data Center concepts.

**Environment:**

Cisco ASA firewalls (ASA 5540, ASA 5520, ASA 5510, PIX 535, FWSM), Cisco routers (including 7600), switches (including Nexus 7010, EX-4200), and firewalls (such as SRX-210), EC2, S3, RDS, Lambda, CloudFront, Meraki SD-WAN, VeloCloud SD-WAN architecture, F5 BIG-IP LTM.

**Kaiser Permanente., Lake Oswego, OR AUG 2019 – DEC 2021**

**Network Operation Center(NOC) Engineer**

**Responsibilities:**

* Extensive experience in layer-3 routing and layer-2 switching, specifically with Nexus models such as 7K, 5K, and 2K series.
* Accountable for handling service request tickets generated by the helpdesk, providing technical support in troubleshooting, maintenance, upgrades, patches, fixes, and overall technical assistance.
* Supported OSPF-based networks by resolving level 2 problems for both internal teams and external customers across all locations.
* Effectively managed the configuration and ongoing maintenance of access points, utilizing the Cisco 4400 WLAN controller for seamless control and monitoring of wireless networks.
* Worked with F5 LTM and GTM series, including models like 6400, 6800, and 8800, to ensure the availability of corporate applications.
* Responsible for the administration of Checkpoint and Cisco ASA firewalls across global networks.
* Provided technical assistance and support to Cisco customers, specifically on routers like 2950, 7600, and 7200, addressing configuration, troubleshooting, and IOS upgrade tasks.
* Proficient in configuring and debugging policy-based routing, route filtering with route maps, and route redistribution.
* Hands-on experience in upgrading Cisco IOS and firmware across different Cisco devices and modules, including router memory and IOS upgrades using TFTP.
* Checked and configured Cisco 7600 routers at data centers to resolve remote site issues.
* Worked on system tests involving NXOS, IOS, and IOS-XR BXB to N7K-NXOS (MPLS) transitions.
* Familiarity with the JUNOS platform and experience in performing IOS upgrades on Juniper devices.
* Provided technical support for the full setup, troubleshooting, and debugging of OSPF, switching, and HSRP.
* Involved in network support and implementation-related internal projects.
* Experienced in stacking and racking equipment in data center environments to ensure appropriate setup and arrangement of servers, switches, routers, and other network devices.
* Knowledgeable of cable management practices, such as labeling, routing, and securing cables to maintain a tidy and organized data center infrastructure, reducing the likelihood of cable-related problems, and making maintenance and troubleshooting simpler.
* Proficient in terminating connections, carrying out cable testing, and debugging connectivity issues to guarantee reliable and efficient data transfer. Experience dealing with different cabling standards, including Cat5e, Cat6, and fiber optic cables.
* Ensured network, system, and data availability and integrity through proactive maintenance and upgrade activities.

**Environment**:

Nexus switches (7K, 5K, 2K series), Cisco WLAN controller (Cisco 4400) for wireless network control and monitoring, F5 LTM and GTM series (6400, 6800, 8800) for application availability, Checkpoint and Cisco ASA firewalls, Cisco routers (2950, 7600, 7200) for configuration, troubleshooting, and IOS upgrades, Policy-based routing, route filtering, and route redistribution, Cisco IOS and firmware upgrades (across different Cisco devices and modules), TFTP (for router memory and IOS upgrades), Juniper devices (familiarity with JUNOS platform, performing IOS upgrades), OSPF, switching, and HSRP troubleshooting and support, Network equipment stacking, racking, and cable management in data center environments, Cable termination, testing, and debugging (Cat5e, Cat6, fiber optic cables).

**Charter communications., Charlotte, NC MARCH 2016 – AUG 2019**

**Network Engineer**

**Responsibilities:**

* Actively participated in on-call responsibilities to ensure a seamless production environment.
* Coordinated network and security operations at the data center to provide dependable and secure connections.
* Maintained and administered firewall policies on Cisco and Checkpoint devices to guarantee correct access restrictions and adherence to security guidelines.
* Implemented suitable NAT settings on the firewall for DMZ traffic and third-party traffic to provide a secure and smooth connection.
* LAN/WAN level 3 assistance was offered, including diagnosis and resolution of problems at OSI model layers 1, 2, and 3.
* Expertise with redistribution between OSPF and EIGRP as well as routing protocols like EIGRP and RIP versions 1 and 2.
* efficient network addressing and name resolution through the configuration and support of DNS and DHCP services.
* Created trunk connections, configured server and client modes, and implemented VLANs to separate various departments.
* Configure client VPN technologies, such as Cisco's VPN client over IPSEC, to provide users with secure remote access.
* Implemented firewall logs, DMZ settings, and associated security policies, monitoring and adjusting them for greater network security.
* Performed installation, configuration, and testing of LAN/WAN devices to maintain network infrastructure.
* Managed printers, copiers, and other miscellaneous network equipment.
* Documented network problems and resolutions for future reference.
* Developed and maintained procedures for backup and recovery, virus scanning, and access control.
* Responsible for the administration of Checkpoint and Cisco PIX 525 firewalls across global networks.
* Provided desktop support, including creating client-specific images and resolving hardware and application issues.
* Configured and installed software and hardware, ensuring smooth operations.
* Conducted routine network maintenance checks and compiled data for special projects, preparing weekly status reports.
* Communicated effectively with vendors, peers, and clients to resolve problems and manage equipment.
* Provided technical support on hardware and software-related issues to remote production sites.

**Environment:**

Cisco ASA and Checkpoint firewalls for maintaining and administering firewall policies, NAT settings for secure DMZ and third-party traffic, DNS and DHCP services for efficient network addressing and name resolution, VLANs for departmental separation and trunk connections, Client VPN technologies, such as Cisco's VPN client over IPSEC, Firewall logs, and associated security, LAN/WAN devices for installation, configuration, and testing of network infrastructure, Checkpoint and Cisco PIX 525 firewalls.

**Client: St. Louis University, St. Louis, MO June 2014- Feb 2016**

**Role: Network Engineer**

**Responsibilities:**

* Deployed Cisco routers and switches and administered network monitoring services.
* Configured and troubleshoot issues with VLAN, Inter-VLAN routing, NAT/PAT, Access-List, and IOS Firewall.
* Updated benefits or pricing configuration to effectively administer the operational requirements of current and new business.
* Configuration and maintenance of Cisco ACE 4710 Load Balancer.
* Encouraged implementation of physical security to the access of network and security devices.
* Encouraged network redundancy for backup of network devices in case of disaster recovery.
* Managed network evaluation and troubleshoot various network problems.
* Configured and installed Aruba 5000 wireless network for Army users with WPA2 security.
* Configuring VMware HA, VMware DRS Clusters for VMotion- migrations between ESX Servers.
* Updated the Patches for ESX Servers using VMware Update Manager in vCenter server.
* Monitored firewall workload using smart view-monitor to enhance checkpoint firewall performance.
* Troubleshoot firewall issues through command-line using CLI commands and GUI interface using smart console.
* Implemented identity awareness using checkpoint software blade to track user activity as company policy demands.
* Maintained VMware Machine.
* Network Assessment and Documentation (including technical, operational, and economical assessment).
* Experience with Veritas volume manager (VxVM), Veritas File system (VxFS), Veritas net backup, Veritas clustering with SAN, NAS environment.
* Actively involved in planning and administering High availability and high-performance clusters using Veritas cluster server.