**MARK CHRIS**

**Network Security Engineer**

**Markkchris1947@gmail.com**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**PROFESSIONAL SUMMARY:**

* Having 7 years of experience in routing, switching, firewall technologies, systems design and administration and troubleshooting.
* Experience in Supporting and troubleshooting Checkpoint (R80, R77 Gaia, R75, R70, R65, Provider-1, VSX, SPLAT, Cluster XL, Smart Center Server) Juniper (SRX, JUNOS, ScreenOS, Netscreen SSG and NSM), Palo Alto (Pa-500, PA-3k,PA-5k, PA-7k, VSYS and Panorama) and Cisco firewall (ASA 5550, 5540, 5520, FWSM,5585 with Firepower module, VPN 3000 concentrator, PIX 535, CSM and ASDM) technologies.
* Experience in installing, configuring and troubleshooting of Cisco 7600, 7200, 3900, 3600, 2900, 2600, 2500 and 1800 series routers, Nexus 3k, 5k, 7k, 9k series, Cisco Catalyst 6500, 4500, 3750, 2950 and 3500XL series switches.
* Performing migrations from Cisco PIX to ASA, Juniper SSG to SRX and Checkpoint to Palo Alto DNA
* Expertise in Cisco ACS and Cisco ISE Authentication, Authorization and Accounting Protocols. Expert Hands On Experience in Cisco ACS & Cisco ISE for 802.1x, AAA Configurations.
* Worked on F5 LTM, GTM series like 6400, 6800, 8800 for the corporate applications and their availability.
* Worked with Cisco ASA security appliances including Source fire, FirePOWER services, and Fire Sight Management Console.
* In-depth knowledge in designing, implementing, configuring with best practices on NexGen IDS/IPS Firewalls such as Palo Alto, Cisco Firepower (Source fire).

**CERTIFICATIONS:**

Cisco Certified Network Professional (CCNP- Trained)

Cisco Certified Network Associate (CCNA) June 2018 – June 2021

**TECHNICAL SKILLS**:

|  |  |  |
| --- | --- | --- |
| **Routing** | | Routers such as 2900, 3800, 3900, 4000, 7200, 7600, 3900 & Juniper MX40/240/2020 series routers |
| **Switching** | Cisco Multilayer Switches 2960, 3850, 4500, 4900, 6500 & Juniper SRX 540, 1400, EX2200/3300/4200 | |
| **Data Center** | Nexus-9K, 7K, 5K, 3K | |
| **Firewall** | Palo Alto, Checkpoint, ASA Firewalls | |
| **AWS Cloud** | VPC, EC2, S3, ELB, Auto Scaling Groups(ASG), EBS, RDS, IAM, Cloud Formation, Route 53, Cloud Watch, Cloud Front, Cloud Trail | |
| **F5 Load Balancers** | LTM, GTM, SSL, iHealth, iRules, VIP, Troubleshooting etc | |
| **Load Balancer** | F5 LTM 6400 & 11.2 | |

**PROFESSIONAL EXPERIENCE:**

**VERIZON, NY Oct 2019 – Present**

**Network Security Engineer**

**ROLES & RESPONSIBILITIES:**

* Install, upgrade and configure Next-Gen Palo Alto Firewall series PA-500, 3000, 5000, 7000 and Installed Palo Alto PA-3060 Firewalls to protect Data Center.
* Configuring rules and maintaining Palo Alto, checkpoint VSX Firewalls & Analysis of firewall logs using various tools.
* Experience in deploying the Azure Cloud infrastructure and integrating it with Cisco ACI Fabric including the APIC Cluster, Leaf and Spine Switches and integrate them with different Cisco Nexus 2232, 2248 fabric extender for better Network Performance and Manageability.
* Upgrading the code from Pan OS 7.1.X to 8.0.X. Experience working on Panorama M100. Migration from Cisco checkpoint to PA firewalls.
* 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.
* Design, Build, and Implement various solutions on Check Point Firewalls (R75, R77.30), Blue Coat Proxies, F5 Load balancers and F5 Global Traffic Managers.
* Part of the New Product development team and responsible for User Acceptance Testing (UAT), SDWAN, Viptela, Versa, Meraki.
* Experience on Cisco DNA and ISE knowledge.
* Worked on Riverbed devices for WAN bandwidth Optimization in the data centers for the sensitive.
* Created virtual systems (firewalls) in the Palo Alto and Checkpoint firewalls.
* Configuring VPN, clustering and ISP redundancy in Checkpoint firewall.
* Configuring the security policies to ensure the data protection in Azure Cloud.
* Experience with configuring Nexus 2000 Fabric Extender (FEX) which acts as a remote line card (module) for the Nexus 5000/9000
* Strong knowledge and understanding with IPsec, Remote Access VPN, and Source Fire IPS.
* Utilized knowledge of STP, BGP, MPLS, OSI model layers 1-2 to create network layouts, Configure and troubleshoot Routing protocols such as OSPF and EIGRP for routing internally and BGP for external routing.
* Experience in Azure network, VPN and Express route, Azure DNS, Traffic Manager, and Load Balancers
* Worked on configuring Monitoring metrics for CISCO ISE using Big Query through SQL scripting
* Worked on deploying SD-WAN solution using VIPTELA Router.
* Build, configure, test and provide production cloud systems support that may include duties such as deployment, configuration, monitoring and troubleshooting in Azure load balancers, firewall policies, VPN tunnels, DNS and Linux servers
* Application Centric Infrastructure (ACI) L4-L7 services deployment: Develop L4 to L7 service chaining and traffic steering for ACI controller. Develop ACI model and implement resource management for service deployment.
* Designed & Deployed Cisco ISE 1.2/1.3 and 2.1 for Enterprise RADIUS Authentication with Active Directory.
* Implemented Quality of Service (QoS), Policy Maps, ACI, Class-maps, and Policy Routing in the network infrastructure throughout all the different sites
* Designed and configured Azure Virtual Networks (VNets), subnets, Azure network settings, DHCP address blocks, DNS settings, security policies and routing.
* Worked with internal/external customers including partners by delivering the ACI Jumpstart program to help customers and speed up technology adoption.
* Experience in Cisco Routing and Switching with strong Cisco hardware/software experiences with Routers such as 2900, 3800, 3900, 4000, 7200, 7600, 3900; Cisco Multilayer Switches 2960, 3850, 4500, 4900, 6500.
* Experience in configuration of Juniper security appliances SRX 220, SRX 240, SRX 550, NS 50, SSG 550M, SSG 520M.
* Continually upgraded Meraki security devices as all store locations and kept current firmware, verified Meraki was upgraded, both circuits were functioning through the Meraki and wireless clients were using the Meraki appliances.
* Experience in deploying and supporting **SD-WAN** module in the production network environment
* Setup Azure Virtual Appliances (VMs) to meet security requirements as software-based appliance functions (firewall, WAN optimization and intrusion detections).
* Extensive design and operational experience with; Enterprise/carrier-class routers and switches (Cisco Viptela SD-WAN
* Provided leadership in architecting and implementing security solutions towards Qualys and SIEM tools like Splunk.
* Assisted in designing and programming of object oriented databases with Python and other languages.
* Hands on experience in designing SD-WAN (Silver-Peak & Viptela) solution for Customer Networks.
* Worked in configuring Azure AD and Conditional access policies.
* Configured F5 Big-IP LTM 6400. Responsible for troubleshooting of F5 load balancers.
* Supporting EIGRP and BGP based on the network by resolving level 2 & 3 problems of internal teams & external customers of all locations.
* Installing virtual PA100 devices in Azure Cloud Environment.
* Worked on Ansible and Ansible Tower to automate repetitive tasks, to deploy critical applications quickly, and proactively manage the changes.
* Knowledge on usage of Queries in Smart View Tracker to monitor IPS and common network traffic and troubleshoot events using packet data.
* Configuring the Palo 3020 devices in enterprise and Azure Cloud Environment.
* Creation of ASM policies (Application security) on F5 Virtual servers.

**OHIO HEALTH, OH Jul 2016– Sep 2019**

**NETWORK ENGINEER:**

**ROLES & RESPONSIBILITIES:**

* Maintained multi-vendor firewalls PaloAlto 3k, 5k and 5k series firewalls, Checkpoint 12k and 15k appliances, Checkpoint R77.30, R75 firewalls with firepower and Juniper SRX 540, 1400 series firewalls.
* Implemented Cisco Firepower NGIPS, Imperva WAF, OOB solutions, perimeter protection, DMZs
* Implementing firewall rules using Palo Alto panorama, Checkpoint smart dashboard, Provider- 1, Cisco CSM and Juniper NSM.
* Installed and configured Amazon's Inspector. Created Targets and Templates and scheduled Assessment runs on all EC2 instances in the AWS account.
* Worked on PaloAlto APP-ID, User-ID and other security profiles like Anti-virus, Threat Prevention, URL-filtering and Wildfire etc.
* Implemented Zone Based Firewalling and Security Rules on the Palo Alto Firewalls and Juniper firewalls.
* Experienced with event-driven and scheduled AWS Lambda functions to trigger various AWS resources.
* Performed IOS Software upgrades on switches 6500, 3750 and 4500s and Cisco ASR for compatibility with Cisco ISE 1.0.3/1.0.4 setup.
* Experience with Cisco DNA solutions ISE, NGFW, Prime, ESA, WSA, VPN and CWS implementations
* Gathering information and co-ordinate with business before we migrate checkpoint to Palo Alto firewalls.
* Enabled and configured Cloud Trail logs for 26 AWS accounts. Created and managed an encrypted S3 Bucket for all Cloud Trail logs and adjusted bucket policy for each accounts CloudTrail to access.
* Experience on Code Upgrade for Cisco Routers including 7200, 3900, 2900, 881, 891 and Switches including 6500, 4500
* Experience in designing SD-WAN (Viptela) solution for Customer Networks.
* Worked on Nexus 9K, Nexus 7k, Nexus 6k, and Nexus 5k, Nexus 4k, ASR 9K, and ASR 1K data center switches.
* Involved in AWS EC2/VPC/S3/SQS/SNS based automation through Terraform, Ansible, Python, and Bash Scripts. Adopted new features as they were released by Amazon, including ELB&EBS.
* Worked with integration of Cisco ACI with SD-WAN and automate the WAN path based on the SLA configured.
* Deploy and support Viptela solution in production
* Responsible for the secure development lifecycle for Cisco's Nexus line of products, including Application Centric Infrastructure (ACI), Application Policy Infrastructure Controller (APIC)
* Developed cisco ACI templates for new device onboarding using APIC.
* Worked on Upgrading multiple Versions and Patches on CISCO ISE based on Vendor Released best security Practices.
* Experience on Software-Defined technology (SD-WAN) vendor products like VIPTELA
* Providing the operational support to Cisco Viptela SD-WAN technology and WAN technology.
* Proficient in AWS services like VPC, EC2, S3, ELB, Auto Scaling Groups(ASG), EBS, RDS, IAM, Cloud Formation, Route 53, Cloud Watch, Cloud Front, Cloud Trail.
* Worked on upgrading Cisco ISE 3300 Appliances and 1.0.4 Cisco ISE software on VMware’s.
* Used security groups, network ACL's, internet gateways and route tables to ensure a secure zone for organization in AWS public cloud.
* Working on migration from traditional MPLS platform to SD- WAN technologies (Silver Peak, Cisco)
* Managed relational database applications with UI designing services and Python languages.
* Used SIEM tool called Splunk SIEM tool to Analyse firewall logs and incident event analysis.
* Performing Firewall rule audit and Firewall policy optimization using Tufin analyzer tool.
* Working on trouble tickets in remedy ticketing system which comes to our queue.
* Configure and troubleshoot Routing protocols such as OSPF and EIGRP for routing internally and BGP for external routing.
* Installing and configuring F5 LTM 11.2 load balancer in Active-Standby mode and Creating Virtual Servers, VIP’s and server pools based upon application requirements.
* Participating in 24\*7 on-call support and implementing changes in different time zones as per the client requirements.
* Experience in designing cloud based networks on top of AZURE, AWS, and Alibaba frameworks
* Provided application level redundancy and availability by deploying F5 load balancers LTM.
* Experience with Cisco Meraki wireless managed network infrastructure.
* Configured 6500, 3750 and 4500 for Network Access Solution integration with Cisco Identity Service Engine on ESX 5.0 VMware and physically with Cisco ISE appliances.
* Perform testing of all SourceFire IPS/NGFW appliances and open source snort. Create packet captures and snort rules to test SourceFire sensor operation and verification of traffic.
* Worked on extensively on troubleshooting multiple issues and driving Incident calls to resolution by doing packet capture techniques and performing other troubleshooting scenarios.
* Worked on the Bluecoat proxies for URL and content filtering solutions.

**BNY MELLON , NY April 2015 – June 2016 NETWORK ENGINEER**

**ROLES & RESPONSIBILITIES:**

* Documented the company’s design, implementation and troubleshooting procedures.
* Intermediate working of using python development skills- ability to develop solutions for network and system automation use cases.
* Performed routine network maintenance checks as well as configure and manage printers, copiers, and other miscellaneous network equipment.
* Performed scheduled Virus checks and updates on all servers and desktops.
* Got Hands-on experience in maintaining and troubleshooting **RIP, OSPF** and **EIGRP** routing protocols.
* Configured and performed software upgrades on Cisco Wireless LAN Controllers 2504, 4404, 5508 for Wireless Network Access Control integration with Cisco ISE.
* Provided high availability for IaaS VMs and PaaS role instances for access from other services in the VNet with Azure Internal Load Balancer
* Configured **RIP** and **EIGRP** on **2600, 2900** and **3600** series Cisco routers.
* Implemented VTP and Trunking protocols (802.1q and ISL) on **3560, 3750** and **4500**series Cisco Catalyst switches.
* Deploy Azure IaaS VMs and Cloud services PaaS with high availability by designing availability sets, VMSS
* Performed **IOS** upgrades on **2900, 3500** series Cisco Catalyst switches and **1800, 2600, 3600** series Cisco routers using TFTP.
* Worked on installation, maintenance, and troubleshooting of **LAN/WAN** (**ISDN**, Frame relay, NAT, DHCP, TCP/IP).
* Configured Access List (Standard, Extended, and Named) to allow users all over the company to access different applications and blocking others.
* Involved in Viptela SD-WAN technology in discovery design and implementation of client's network.
* Configured **STP** for loop prevention and **VTP** for Inter-VLAN Routing.
* Done trouble shooting of **TCP/IP** problems and connectivity issues in multi-protocol Ethernet environment.
* Check routing and ports, WAF configuration, Azure Firewall, NSG, NVA, Load Balancer configuration.
* Worked on network-based IT systems such as Racking, Stacking and Cabling.
* Basic Experience working with API