**Srikanth. K**

**Email: srikh81@gmail.com**

**Sr Network Engineer Mobile: (469)756-3811**

**Summary**

* Over 8 years of expertise in design, implementation, troubleshooting, development, and maintenance of enterprise security network systems.
* Daily management of Checkpoint, Palo Alto, and Juniper Firewalls, along with Cisco Routers and Switches in a dynamic Data Center environment.
* 8+ years of experience in IT Security, Administration, and strategic security architecture.
* Implementation of security plans, controls, processes, and policies aligned with organizational standards and operational objectives.
* Dedicated professional with a background in mobile application support and cloud infrastructure for multi-enterprise mobility solutions.
* Seeking to contribute determination, drive, and innovation in the evolving cloud security industry.
* Design, implementation, troubleshooting, and support of Enterprise-Wide Windows Active Directory environments.
* Expertise in Multi-Forest environments, Trusts, migration, consolidation, Sites and Services, FSMO roles, and DNS troubleshooting.
* Design and configuration of AD Forests, Domains, Trusts, Group Policy, OU's, and domain controllers.
* Hands-on administration of Checkpoint, Palo Alto, and Juniper Firewalls, with experience in site-to-site VPN services.
* Implementation of IDS and IPS systems, Symantec DLP solutions, and Endpoint Security Solutions.
* Configuration and implementation of WinMagic Servers for Encryption.
* Implementation of Mail Security Solutions like Proofpoint and Barracuda.
* Proficient in Data Center standards, procedures, routing protocols (RIP, OSPF, EIGRP, BGP), VLANs, VTP, STP, and redundancy technologies.
* Excellent troubleshooting skills in NAT configuration, access lists, and DNS/DHCP issues within the LAN network.
* Proficient in preparing Tech Documentation using Microsoft VISIO.
* Developed IT strategies, policies, and procedures consistent with business strategies and vision.
* Ensured data confidentiality, integrity, and availability, providing security and limiting liability.

**Education, Training & Certification**

Bachelors in Electronics and Communication Engineering at SRM Uiversity-2015

**Technical Skills & Work Experience**

|  |  |
| --- | --- |
| **Cisco router platforms** | 2500, 2600, 2800, 2951, 3600, 3700, 3800, 3925E,4431,4461, 7200, 7609 |
| **Cloud Platforms** | Microsoft Azure, AWS. |
| **Routing Protocols** | RIP, OSPF, EIGRP, and BGP |
| **Cisco Switch platforms** | 2900XL, 2950, 2960, 3560, 3750, 4500,6500, Meraki-MS225, Nexus 5K, 7K, 9K |
| **Switching Protocols** | VTP, STP, RSTP, MST, VLANs, PAgP, and LACP |
| **Security Protocols** | IKE, IPsec |
| **Firewalls** | Checkpoint, Cisco ASA, Palo Alto, Cisco PIX, Cisco Meraki MX84 |
| **Cryptographic Algorithms** | DES, 3DES, RSA, SHA, MD5, Diffe-Hellman Key exchange |
| **Load Balancer** | Cisco ACE 4700 series, F5 Big-IP |
| **WAN Technologies** | FRAME RELAY, ISDN T1/E1 (PRI/BRI), PPP, ATM, MPLS, leased lines, DSL modems |
| **LAN Technologies** | Ethernet, Fast Ethernet, Gigabit Ethernet, NAT/PAT, FDDI |
| **VOIP Devices** | Cisco IP phones, Meraki Phones, Polycom |
| **Operating Systems** | Windows 2000/XP/Vista, Windows server 2003,2008,2012,2016, Linux, Unix |
| **Network Management** | Cisco Network Assistant, HP OpenView, Solar winds, Zabbix |
| **Encryption Tools** | WinMagic, BitLocker, FileVault, Dell Encryption |
| **Backup Solutions** | CrashPlan, Druva |
| **Endpoint Antivirus** | Symantec Endpoint protection, McAfee Endpoint Security |
| **Patch Management Tools** | SCCM, Marimba. |
| **Identity Management** | Microsoft Azure Active Directory, RSA SecurID, Okta. |
| **Endpoint Privilege Management** | Avecto Defend point, AD RMS, Intune |
| **Email Spam Filtering Tools** | Barracuda, Proofpoint, Microsoft |
| **Proxy Solutions** | Bluecoat. |

**Areas of Expertise:**

**End User and Operation Administration:**

* Spearheaded the installation, configuration, and management of networks, including the setup and configuration of Storage/Backup devices (such as disk arrays), Printers, Network Interfaces, and terminals.
* Oversaw the installation, maintenance, and repair of both hardware and software components.
* Administered the internal and hosted network infrastructure, server software, and associated backup routines.
* Configured and deployed antivirus tools, leading network security initiatives for end-users and clients.
* Streamlined the day-to-day functioning of e-infrastructure, troubleshooting all client/server-related issues across the LAN.
* Managed the daily onboarding and offboarding of users, showcasing expertise in O365 administration.
* Demonstrated experience in Exchange Administration, setting up mailboxes for users, and implementing litigation hold as part of compliance measures.
* Contributed to Active Directory (AD) Domain Consolidation and provided service delivery for Azure Active Directory and the Identity Management team within the Microsoft cloud platform (O365 Identity, Azure, etc.). Designed and implemented a new ROLE BASED admin model, deploying Quest Roles.
* Possessed strong hands-on administration experience on Windows 2012 server, covering Forest, Domain trust, AD, DFS, DNS, WINS, DHCP, Group Policy, Distribution lists, Windows folder security, and IP filter.
* **Routing and Switching:**
* Planned, designed, installed, and configured a range of Cisco routers, including models 1700, 1800, 2500, 2600, 3200, 3600, 3700, 3800, 7200, and 7609, along with Cisco L2 & L3 Switches such as 2900, 3560, 4500, and 6500.
* Configured and implemented various routed and routing protocols, including TCP/IP, OSPF, EIGRP, and BGP.
* Designed and implemented a Cisco 3-tier LAN Network Architecture, encompassing Core, Distribution, and Access layers.
* Configured STP, RSTP, VLAN, VTP, SPAN port, and Port binding for optimized network performance.
* Implemented HSRP and VRRP protocols on routers, along with configuring and implementing IPsec and GRE in VPNs.
* Configured Intrusion Prevention Systems (IPS) using Cisco Routers and implemented an Intrusion Detection System (IDS) using SNORT.
* Implemented Cisco Secure Access Control Server (ACS 4.0) for Tacacs+/Radius authentication.
* Configured Cisco Call Manager for VOIP solutions and designed video solutions, including video conferencing.
* Worked with different load balancing products, including F5's BIG IP and Cisco ACE.
* **Firewall & VPN Management:**
* Installed and configured various firewalls, including Checkpoint NG, NGX, Cisco ASA, and Pix, ensuring optimal network security.
* Planned and executed changes and upgrades to firewall software in accordance with licensing agreements.
* Managed changes and upgrades to the operating systems of servers supporting firewall components, ensuring seamless functionality.
* Implemented security policies using ACL, PIX firewall (515, 520), ASA, and routers, and executed change requests to the firewall rule base.
* Managed changes to authentication configurations at the user, client, and session levels.
* Implemented changes to network routing tables and ACLs for enhanced security.
* Executed changes to the system backup schedule and contributed to Disaster Recovery Planning.
* Planned, designed, and implemented VPN connections using Checkpoint, Palo Alto, ASA, Cisco PIX, and Cisco Routers, including site-to-site VPNs.
* Proposed and deployed security and network connectivity details for Offshore Development Centers (ODCs).
* Implemented changes to supported encryption configurations and domains for enabled clients in the firewall VPNs.
* Installed and maintained SSL VPNs, Cisco Easy VPN servers, facilitating the work-from-home concept.
* Designed and implemented Business Continuation Plans (BCP) for project connectivity.
* Designed and implemented Remote Access VPN servers using Checkpoint and Cisco ASA technologies.

**Hartford Insurance, Hartford | Sep 22 - Present**

**Role:** IT Network and Azure Support Engineer

* Generate monthly compliance reports and conduct security audits.
* Assess the impact and supportability of standard solutions on the managed environment.
* Develop configurations for new and existing devices, ensuring supporting documentation reflects the full post-implementation configuration.
* Assess technical deployment and operational requirements, developing detailed implementation solutions for complex environments.
* Plan and manage projects designed to test defenses against hacking, denial of service, spam, break-ins, or similar attacks; provide guidance to infrastructure or application staff participating in exercises.
* Support Premiere Microsoft customers in the implementation of Intune/Azure mobile device management with SCCM and Office 365/Exchange hybrid environments.
* Manage a user base of 5,000 and Windows server count of 1,000 running various Windows Operating Systems.
* Install, configure, and provide support for LDAP in development, testing, staging, and production environments.
* Demonstrate expertise in Active Directory design and support, covering GPOs, AD Schema, OUs, LDAP, Sites, Replication, etc.
* Execute user-related tasks, including registration, renaming, recertification, deletion, and handling mail file movements and modifications.
* Create Windows Management Instrumentation (WMI) queries in System Center Configuration Manager (SCCM) R2.
* Develop, deploy, and manage mobile applications and policies with Azure, including MAM and MAMWE.
* Lead a technical team, resolving complex issues, ensuring quality, managing escalations, submitting KBs, and providing ongoing training.
* Serve as a subject matter expert for Apple iOS APN certificates, device enrollment program (DEP), Configuration Manager, and cloud services.
* Proficient in on-premises to cloud and cloud to on-premises migrations.
* Communicate with high-priority enterprise businesses regarding the status of support incidents in critical situations.
* Administer and configure mobile devices for enterprise users, collaborating with various support areas.
* Possess working knowledge of PowerShell, Exchange Active Sync, SCEP, NDES certificates, and some Power BI.
* Demonstrate basic knowledge of networking concepts, including TCP/IP, DNS, WINS, DHCP, and routing.
* Configure TCP/IP and NFS server, effectively serving clients in a heterogeneous environment.
* Test, implement, and manage cloud security solutions on Azure, including the management and governance of core network functions.
* Implement and manage Hybrid Cloud Architectures, Cloud brokering solutions, or Cloud Management Solutions for Public/Private Cloud.
* Hands-on experience with Microsoft Azure Cloud services, including storage accounts and virtual networks.
* Experienced in provisioning IAAS & PAAS Virtual Machines and Web\Worker roles on Microsoft Azure Classic and Azure Resource Manager.
* Design and create Network Architecture Diagrams using Visio.
* Migrate Security Policies and NAT rules from Cisco ASA to Palo Alto.
* Create, manage, and troubleshoot Site-to-Site VPN tunnels from Cisco ASA to Palo Alto.
* Configure OSPF protocol on Palo Alto and coordinate with ISPs to implement EBGP on Flexware devices.
* Hands-on experience with Azure VPN-Point to Site, Virtual networks, Azure Custom security, endpoint security, and firewall.
* Maintain high availability production systems in a Public/Private Cloud environment.
* Experience with OS firewalls (Windows Firewalls) and Next-Gen Firewalls (Barracuda Firewalls).
* Work hands-on with Azure MFA (Multi-Factor Authentication) Servers and Phone factors for two-step security.
* Deploy VMs, Virtual Networks, Gateways, and Next-Gen Firewalls; hands-on experience with backup and restore Azure services.
* Involved in creating Azure Services with Azure Virtual Machine and implementing Active Directory in Windows Server environments.
* Identify opportunities to improve infrastructure utilizing Office 365 and Microsoft Azure for Windows server environments.
* Configure, deploy, and manage Cisco Meraki Switches and Firewalls through the Meraki Dashboard.

**BNY Mellon, Newyork city | Jan 20 – Aug 22**

**Role:** IT Network and Cloud Security Engineer

* Hands-on experience with Microsoft Azure Cloud services, including Storage accounts and Virtual Networks.
* Provisioned IAAS & PAAS Virtual Machines and Web\Worker roles on Microsoft Azure Classic and Azure Resource Manager.
* Designed and created Network Architecture Diagrams using Visio.
* Successfully migrated all Security Policies and NAT rules from Cisco ASA to Palo Alto.
* Created, managed, and troubleshooted Site-to-Site VPN tunnels from Cisco ASA to Palo Alto.
* Configured OSPF protocol on Palo Alto and coordinated with ISP to implement EBGP on Cisco Routers.
* Planned and managed projects to test defenses against hacking, denial of service, spam, break-ins, or similar attacks.
* Provided guidance to infrastructure or application staff participating in exercises.
* Supported Premiere Microsoft customers in the implementation of Intune/Azure mobile device management with SCCM and Office 365/Exchange hybrid environments.
* Managed a user base of 5,000 and Windows server count of 1,000 running various Windows Operating Systems.
* Installed, configured, and provided support for LDAP in development, testing, staging, and production environments.
* Expertise in Active Directory design and support, covering GPOs, AD Schema, OUs, LDAP, Sites, Replication, etc.
* Handled user-related tasks such as registration, renaming, recertification, deletion, mail file movements, and modifications.
* Created Windows Management Instrumentation (WMI) queries in System Center Configuration Manager (SCCM) R2.
* Experienced in migrating On-premises instances or Azure Classic Instances to Azure ARM Subscription with Azure Site Recovery.
* Worked on various Azure services, including Compute (Web Roles, Worker Roles), Azure Websites, Caching, SQL Azure, NoSQL, Storage, Network services, Azure Active Directory, API Management, Scheduling, Auto Scaling, and PowerShell Automation.
* Configured Internal load balancer, load-balanced sets, and Azure Traffic manager.
* Upgraded, migrated, and configured F5 LTM, including Routing, VLAN’s, SNAT, and route domains.
* Managed SSL certificates and configured iRules on the F5 load balancer to manage client traffic.
* Configured SSL-OFFLOADING & SSL-BRIDGING through Citrix NetScaler’s and F5 LTM’s.
* Wrote Security Policies for Global and Domestic Traffic, evaluating traffic for OWASP TOP 10 and other attack types.
* Worked on new critical vulnerabilities and built attack signatures in F5 WAF to mitigate vulnerabilities.
* Actively worked on deploying VMs, Virtual Networks, Gateways, and Next-Gen Firewalls.
* Hands-on experience on Backup and restore Azure services.
* Involved in creating Azure Services with Azure Virtual Machine and implemented Active Directory in Windows Server 2012.
* Identified opportunities to improve infrastructure utilizing Office 365 and Microsoft Azure for Windows server environments.
* Configured, deployed, and managed Cisco Meraki Switches and Firewalls through the Meraki Dashboard.
* Collaborated with various vendors to implement Express routing from On-Premises to Azure environment for various customers.
* Quality Control Leader responsible for formulating and implementing core KPIs, knowledge base, and training material.
* Built and maintained successful relationships with service providers, dealers, and consumers.
* Trained new employees, explained protocols clearly and efficiently, and researched issues on various computer systems and databases to resolve complaints and answer inquiries.
* Provided professional customer service consultations on MDM device enrollment and deployment methods.
* Researched, resolved, and followed up on customer issues, assessed customer bug and enhancement requests, and prioritized development.
* Developed documentation for common processes for support staff and end-users.
* Coordinated installation of software systems and collaborated on the design and implementation of new features.

**Vertify (Epam Systems, India) | Sep 17 – Nov 19**

**Role:** Network Security Engineer**,** Infra Ops

* Completed a comprehensive rename of all firewall objects and rules and upgraded Checkpoint firewalls.
* Designed traffic using AlgoSec and created firewall diagrams using MS-Visio.
* Managed the design, implementation, support, and administration of Checkpoint Provider-1 and VSX.
* Configured security solutions on the AWS platform, monitoring routers, switches, and firewalls.
* Decommissioned and migrated partner VPN tunnels to the new environment.
* Installed and configured Checkpoint R76 and Palo Alto Firewalls (PAN-5060,3220).
* Managed security tools such as Checkpoint Firewall and RSA Security.
* Designed and established the VPN environment for partner connectivity.
* Implemented Bluecoat Proxy and configured vSwitches for Port groups, NIC Teaming, Traffic shaping, Load Balancing, VLAN tagging, Failover, and Security Policies on vNetworks.
* Configured and managed Azure AD Connect, Azure AD Connect health, and Microsoft Azure Active Directory.
* Expertise in Active Directory setup, troubleshooting, and managing AD group policy Templates.
* Planned and managed server hardware, OS upgrades, software drivers, firmware upgrades, and disaster recovery procedures.
* Configured Resource Pool, Motion, Alerts, Alarms, and managed Virtual Machines and Templates.
* Conducted health checks and performance monitoring for all Windows servers.
* Installed and managed security reporting tools to monitor any Active Directory changes.
* Planned and managed migrations and upgrades related to Active Directory and Domain controllers.
* Managed and supported Application Security Manager or Web Application Firewalls.
* Worked with F5 load balancer, LTM, GTM, iRules, ASM, integration with Python (Rest API), and troubleshooting layer 7 application issues.
* Set up virtual F5 LTM’s in the DMZ environment, managed F5 APM-APM traffic processing, and configured access policies and access profiles.
* Troubleshooted network connectivity and established firewall rules.
* Migrated firewall rules from CISCO ASA to Checkpoint and automated the process of vulnerability management.
* Installed and maintained security infrastructure, including Firewall, IDS/IPS, log management, and SIEM tools.
* Performed operating system, network, and application vulnerability assessments.
* Documented and performed system upgrades, regular product updates, emergency patch applications, and defined monitoring requirements.
* Developed and maintained installation, configuration procedures for migration deployments.
* Implemented Full Disk Encryption (FDE) and Removable Media Encryption (RMCE) techniques using WinMagic.
* Worked with the Active Directory team to harden Group Policies and controlled rights management by implementing solutions like Avecto Defendpoint.
* Implemented Email Spam Filtering solutions like Barracuda and Proofpoint and experienced in implementing Endpoint Malware solutions such as Symantec Endpoint Protection as well as DLP.

**iGate, India | May 15 – Aug 17**

**Role:** Network Security Engineer

* Extensive experience in the Configuration, Implementation, and Change requests administration of Checkpoint, Palo Alto, and Juniper Firewalls.
* Configured and troubleshooted site-to-site IPSEC VPN tunnels on VPN concentrators and ASA firewalls with private vendors.
* Administered L2/L3 Switching Technology, including creating and managing VLANs, Port security, Trunking, STP, and InterVlan routing.
* Configured GLBP, VLAN Trunking 802.1Q, STP, and Port Security on Catalyst 6500 switches.
* Troubleshot network issues using Checkpoint Smart Tracker and CLI (clish and bash mode).
* Audited and removed old rules that are no longer in use, generating hit counts for rule prioritization.
* Prepared MOPs, Change Request Sheets, VPN Specification Sheets, and created/submitted Remedy tickets.
* Utilized LogRhythm Log servers for Security Information and Event Management (SIEM).
* Designed and implemented staging and production network scenarios in the LAB environment.
* Contributed to network design, support, and implementation of internal projects for establishing connectivity in various field offices and Datacenters.
* Managed enterprise BGP setup by configuring and troubleshooting BGP-related issues.
* Worked with Cisco Nexus 2148 Fabric Extender and Nexus 5000 series for a Flexible Access Solution in datacenter access architecture.
* Experience with Juniper JUNOS operating system.
* Analyzed network problems and coordinated resolutions.
* Worked on EasyIT and STIM Solution for Network Management System and Ticketing.
* Troubleshot network issues using the Checkpoint tracker tool.