**Sandesh Jung Thapa  
405-796-8729**

**sandeshjungthapa9@gmail.com**

**Summary**

* Expertise of 7 plus years with rich Computer Networking experience. Solid understanding of Designing, Implementation, Administration, Operational and troubleshooting of enterprise data networks.
* Implementing & troubleshooting **Cisco 2900, 3600, 3900, 7200, 7600** series routers, CAT OS **2960, 3560, 3750, 4500, 6500** series switches and **Nexus 2k, 5k, 7k** series switches.
* Provide scalable, supportable military grade **TCP/IP** security solutions along with **expert TCP/IP network designs** that enable business functionality.
* Conduct cyber analysis on events throughout the Enterprise Network using McAfee ePO, SIEM and ATD.
* Worked on F5 LTM/GTM, BIG-IP, load balancing, iRules and WAN acceleration.
* Administration, Engineering and Support for various technologies including proficiency in **LAN/WAN routing, switching, security, application load balancing and wireless**.
* Working experience on tools and devices like **Gigamon, Source Fire, Fireeye, Aruba, Cisco ASA, Cisco ISE**.
* Experience in creating User/Group Accounts and attaching policies to User/Group Accounts using AWS IAM service.
* Experience in F5 Load Balancing.
* Managed all network and devices to include Cisco routers, switches, VPNs, SSL, Check Point, Cisco PIX, Cisco ASA, Cisco FWSM as well as content delivery networks (CSS, Citrix Net scalar and F5 Big IP LTM and GTM 1600 and 3400 load balancers) enterprise environment.
* McAfee ePO 5.1.1 administration (VSE, SAE, DLP), PM on Open DNS deployment, incident management of threat alert concerning, McAfee products, Fire Eye, Source fire, establishing best policy and procedure for incident management.
* Provides technical support, development and implementation expertise and leadership in Antivirus and Malware prevention services (presently McAfee ePO 5.3 endpoint securities (ENS) suite).
* Knowledge of web application firewalls and data loss prevention technologies.
* Configuration and troubleshooting of CISCO & ARUBA wireless devices
* Worked on **Juniper Net Screen Firewalls NS50, SSG 550M, SSG520M, ISG 1000, ISG 200** and **Cisco PIX 535, 520, 515, ASA -5500 and 5505.**
* Very good knowledge in scripting languages like TCL/TK, Perl and Python.
* Experience in **Deployed Check Point Provider-1 NGX** and configured **CMAs**
* Responsible for **Check Point** and **Cisco firewall administration** across global networks.
* Worked on **Cisco Catalyst Switches 6500/4500/3500 series.**
* Policy development and planning/programming on **IT Security, Network Support and Administration**.
* Experience in Configuring and Troubleshooting **BIG-IP F5 LoadBalancer LTM.**
* Creating **Virtual Servers, Nodes, Pools** and **iRules on BIG-IP F5 in LTM module.**
* Experience with **Firewall** migrations from **PIX firewall to Cisco ASA** and **Juniper SRX firewall appliances**
* Experience in analyzing security logs generated by **Intrusion Detection/Prevention Systems (IDS/IPS), firewalls, network flow systems**, **Anti-Virus** and/or other **security logging sources.**
* **Monitor SIEM and IDS/IPS** feeds to identify possible enterprise threats. Actively investigate, respond to and remediate security incidents.
* Experience in implementation of F5 GTM based on topology load balancing methods.
* Experience in migration of data to cloud environment. Good working knowledge of Azure and AWS.
* Experience with **Bluecoat Proxy servers, LAN & WAN management.**
* Excellent knowledge in Routing, Switching, Firewall and Gateway technologies, system design, wireless design, data network design, capacity management and network growth.
* Deployed the Cisco 3500 Access Points using Cisco Wireless controllers 5500 and 2500 and WCS System.
* Experience in working with **Cisco Nexus Switches** and **Virtual Port Channel Configuration.**
* Experience with **Checkpoint VSX,** including **virtual systems**, **routers and switches**.
* Experience in **Network LAN/WAN** deployment.
* Experience with **DNS/DFS/DHCP/WINS Standardizations** and Implementations.
* Extensive understanding of networking concepts, (IE. Configuration of networks, router configuration and wireless security, **TCP/IP, VPN, Content Filtering, VLANs** and routing in **LAN/WAN**, **Ethernet Port, Patch Panel and wireless networks.)**
* Experience with management platforms such as **Panorama, Juniper NSM and Smart Center.**
* Configuration of **Network** and **Security** devices such as **Cisco routers** and **switches (Cisco 7600/3500/Nexus 7K/5K), Firewall (Checkpoint R75/Gaia and Cisco FWSM), Load Balancers and DNS and IP Manager (Infoblox)**
* **Black listing** and **White listing** of web URL on **Blue Coat Proxy Servers**.
* Administration of production Windows Servers infrastructure that includes **Domain Controllers, IIS Web Servers, SharePoint, File and Print and FTP/SFTP servers.**
* Experienced with routing protocols **(RIPv1/2, IGRP, EIGRP, OSPF, BGP),** switching **(VLANS, VTP Domains, STP** and **trunking)**,
* Extensive experience in **Windows 2008 R2/2008/2003 Wintel Servers** at single or multi-domain platforms.
* Provide consultancy services to customers on a variety of network security products including firewalls, VPNs, authentication, load-balancing, data loss prevention and security information and event management.
* Proficient in installing and configuring Windows Server 2003, 2008, 2012 and Windows XP, 7 & 8Professional Client Operating Systems
* **IDS** and **IPS** event management using CSM including signature updates for **SSM Modules, IDSM.**
* Provides management level **reporting of firewall** and **Intrusion Protection System (IPS)** activity on a periodic basis.
* Optimize, secure and control the delivery of all enterprise and cloud services and maximize the end user experience for all users including mobile clients using Net scalar.

|  |
| --- |
| **TECHNICAL SKILLS** |

|  |  |
| --- | --- |
| Networking | OSI, TCP/IP, Cisco IOS, IOS-XR, LAN/WAN interconnection, Frame-Relay, ISDN, RIP, OSPF, EIGRP, IS-IS, BGP, MPLS, STP, RSTP, MST, VTP, NAT, ACLs, VPN, IP-Sec |
| Hardware Routers | Cisco (1800/2600/3600/3800/7200/7600 series), Cisco ASR 9Ks) |
| Switches | Cisco (2900/3500/3700/5500/6500 Series, Nexus 7k) |
| Firewalls | Cisco ASA (5510,5540), Checkpoint R65, R70, R75, R77 Gaia, Juniper SSG, SRX, Palo Alto |
| Other Tools | Tufin Secure Track, Forescout Counter ACT, F5 Big IP (LTM/GTM/ASM), DNS, Bluecoat Proxy, Solar Wind, Wireshark, BMC Remedy, Citrix Net scalar, Cisco Prime, VM Ware |
| Operating Systems | Win 95/98, NT, XP,VISTA, LINUX, UNIX |

**CERTIFICATIONS:**

(CCNA) – Cisco Certified Network Associate

(CCNP) – Cisco Certified Network Professional

**Professional Summary:**

**Network Security Engineer**

**Molina Healthcare - Long Beach, CA July 2016 to Present**

**Responsibilities:**

* Works with client engineering groups to create, document, implement, validate and manage policies, procedures and standards that ensure confidentiality, availability, integrity and privacy of information.
* Researched, designed and replaced aging Cisco ASA firewall architecture with new next generation Palo Alto appliances serving as firewalls and URL and application inspection.
* Performed site refreshes on **Cisco switching** and **Aruba wireless** infrastructure at several locations.
* Configured, implemented and troubleshooting issues on **Checkpoint R77.10 Gaia, R75, Cisco ASA 5540, 5000 series firewalls** for the client environment.
* Manage project task to migrate from **Cisco ASA firewalls to Check Point firewalls**.
* Worked on VPN configuration, routing, NAT, access-list, security contexts and failover in ASA 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, Cisco ASA** Firewalls.
* Configuring, Administering and troubleshooting the **Checkpoint**, **Palo Alto** and **ASA** firewall.
* Configured **IPSec VPN** (Site-Site to Remote Access) on **Cisco ASA (5200)** series firewalls.
* Working with the rule base and its configuration in **Cisco ASA, Palo Alto, Juniper and Checkpoint** firewalls.
* Experience in layer-3 Routing and layer-2 Switching. Dealt with Nexus models like **9K, 7K, 5K, 2K** series, Cisco router models like 7200, 3800, 3600, 2800, 2600, 2500, 1800 series and Cisco catalyst 6500, 4500, 3750, 3500, 2900 series switches.
* Rule consolidation and rule lockdown process in the **ASA** firewalls.
* Supported 200 Cisco ASA firewalls in configuring and maintenance.
* Deployment of Cisco ASA firewalls and migration of end of life **ASA firewalls** to New **ASA firewalls**
* Cisco Firewalls include ASA 5585x, 5580, 5550 Series Hardware managed through CLI, ASDM as well as CSM.
* Configuring & Administration of the Checkpoint Firewall that includes creating Hosts, Nodes, Networks, Static & Hide NAT's.
* Involved in iRule management on F5 Load Balancers like loading rules, writing iRule syntax using TCL language and iRule extension to TCL.
* Experience in creating multiple policies and pushing them into Checkpoint Firewall (Gateways) and hands-on experience in managing the Checkpoint Management Server and Gaia operating system.
* Experience working with Palo Alto firewalls managed through Panorama management platform.
* Configure High Availability on Palo Alto firewalls.
* Currently working on migration to Cisco ACI and **Nexus 9K, 7K, 6K, 5K** switching in a fully fault-tolerant design model.
* Defining, tracking and maintaining the standard baselines and configuration sets of security devices and implementing industry best practices with regards to **Firewall, IDS/IPS, IPsec VPN, SSL VPN**.
* Applied security enhancement by implementing certificates and RSA keys for authentication.
* Installed and administered RSA Secure ID token authentication servers.
* Support Citrix Net Scaler F5 platform, configuring, implementing, & troubleshooting Citrix Net Scaler VIP configuration with health check, policy configurations Access Gateway, & content switching configuration solutions.
* Configured F5 GTM solutions, which includes Wide IP, Pool Load Balancing Methods, probers and monitors.
* Work with the Cisco Meraki Sales team and on strategic sales initiatives like customer outreach and channel training to grow business in targeted regions.
* Defined AWS Security Groups which acted as virtual firewalls that controls the incoming traffic and configured the traffic allowing reaching one or more AWS EC2 instances Virtual private cloud (VPC), subnets, Internet Gateways.
* Privileged and access management using AWS and Microsoft Azure.
* Physically deployed new Cisco Nexus devices, Catalyst and Nexus replacement blades, FWSMs, Cisco ASAs, Citrix Net scalar MPX and SDX chassis.
* Verify Firewall status with Checkpoint Monitor. Creation and implementation of Application delivery architectures which includes load balancing on **F5 BIG IP** modules.
* Worked with **F5 Load balancing**, **IDS/IPS**, Bluecoat proxy servers and Administrating.
* Use of Web application firewall providing reverse proxy based protection for applications deployed in physical, virtual / public cloud environments.
* Involved in the deployment and decommission of VLANs on core **ASR 9K, Nexus 7K, 5K** and its downstream devices.
* Involved in F5 LTM GTM and ASM planning, designing and implementation. Actively involved in F5 ASM policy configuration and deployment. Troubleshoot and Worked with Security issues related to Cisco ASA/PIX, Checkpoint, IDS/IPS and Juniper Net screen firewalls
* Configured High availability, User ID on Palo Alto firewall.
* Configured and utilized many different protocols such as OSPF, ISIS, BGP/MP-BGP, OER, MPLS, LDP, Multicast, IPv4/IPv6 protocols.
* Utilized knowledge of Spanning Tree Protocol, BGP, MPLS, OSI model layers 1-2 to create network layouts.
* Stateful firewall, VLAN to VLAN routing, Link bonding / failover, 3G / 4G failover, Traffic shaping / prioritization, WAN optimization, Site-to-site VPN, Client VPN, MPLS to VPN Failover, Active Directory and LDAP integration.
* Responsible for investigating Data Loss Prevention using Symantec DLP.
* Configured EIGRP routing and BGP route maps to allow traffic from subnets out to the core to Datacenter on the ASR 1002 devices.
* Implementation and configuration of Cisco L3 switches 3750, 4500, 6500 in multi VLAN environment with the use of inter-VLAN routing, dot1Q trunk, ether channel
* Configure and troubleshoot Routing protocols such as OSPF and EIGRP for routing internally and BGP for external routing.
* Use BGP attributes such as AS-PATH prepending and communities to influence routing amongst different paths
* Worked and maintained various network, application monitoring tools like Solar Winds, Cisco Prime, Fore Scout, Wire shark, TCP Dump.
* Forescout Counter ACT- NAC, endpoint compliance, real-time intelligence and policy-based control.
* Experience with Monitoring wireless networks and performing site surveys.
* Involved in Troubleshooting IP Addressing Issues and Updating IOS Images using **TFTP**.
* Used BMC Remedy tool for ticketing purpose.

**Environment:** Cisco ASA5580/5540/5520, CheckpointR70, R75, R77.20 Gaia, Palo AltoPA-5000/3000, Juniper SSG, SRX, Big IP F5 LTM/GTM, Nexus switches, iRule, Routers, TCP/IP, VPN, Bluecoat Proxy servers, IDS/IPS. SIEM and monitoring, BMC Remedy, Cisco Prime, Forescout Counter ACT, Tufin.

**Network Security Engineer**

**T-Mobile - Richardson, TX May 2014 to June 2016**

**Responsibilities:**

* Implementing Security Solutions using **PaloAltoPA-5000/3000, Cisco 5580/5540/5520**, **Checkpoint firewalls R70, R75, R77.20Gaia and Provider-1/MDM.**
* Configuration and administration of firewalls, which includes **Checkpoint, Juniper** and **Cisco ASA firewalls.**
* Configured and maintained rule sets in the firewalls and updated them on the daily basis.
* Monitors the network traffic and maintain the records with the help of SPLUNK.
* Knowledge of Cisco ASA firewall, VPN, GRE over IPSec tunnel configuration and Route-maps.
* Extensive knowledge of and experience configuring and troubleshooting layer 3 routing protocols (EIGRP, OSPF, RIP, BGP)and High Availability on Cisco devices.
* Designed AWS Cloud Formation templates to create custom sized VPC, subnets, NAT to ensure successful deployment of Web applications and database templates.
* Create and validate SMOPS for upgrade, replace, add and remove Cisco VOD equipment.
* Work with Load Balancing to build connectivity to production & disaster recovery servers through Citrix Net scaler.
* Configuring High Availability using **Cluster XL on Checkpoint** as well as **VRRP and monitor the Sync** status for stateful replication of traffic between active and standby member.
* Innovated with support of Palo Alto for remote and mobile users and for analyzing files for malware in a separate (cloud-based) process that does not impact stream processing.
* Researched, designed and replaced **Checkpoint firewall architecture** with new next generation **Palo Alto PA3000 and PA5000** appliances serving as firewalls and URL and application inspection.
* Handling Modern related issue like that of RAD & Aruba.
* Experience on Code Upgrade for Cisco Routers including 7200, 3900, 2900, 881, 891 and Switches including 6500, 4500**, Nexus 9K, Nexus 7k, Nexus 6k, Nexus 5k, Nexus 4k, ASR 9K, ASR 1K**.
* Responsible for the deployment and associated tasks for the implementation of the tanium Endpoint Security and Systems Management product.
* Configuring rules and maintaining **Palo Alto Firewalls**& Analysis of firewall logs using Panorama.
* Successfully installed **Palo Alto PA-3000/PA-5000 firewalls** to protect Data Center and provided L3 support for routers/switches/firewalls.
* Configured and maintained **IPSEC and SSL VPN's** on Palo Alto Firewalls and also implemented Zone-Based Firewall and Security Rules on the **Palo Alto Firewall.**
* Exposure to wild fire feature of Palo Alto.
* Configuration and Maintenance of **Cisco ASA 5580-20, ASA 5540, ASA 5520, ASA 5510** series firewalls.
* Hands on Experience with Cisco Wireless Controllers 5500's and 2500's and coming to access points, worked on 3700's, 3500's and 1142 access points.
* Configured and installed Cisco routers 2500, 2600, 3601 and 4000 series. 2950 Switches & Link sys wireless access points.
* Configuring and install hardware and software required to conduct network penetration testing.
* Configure Syslog server in the network for capturing and logs from firewalls.
* Provided tier 3 support for **Check Point and Cisco ASA Firewalls** to support customers, Backup and restore of Checkpoint and Cisco ASA Firewall policies.
* Monitoring Traffic and **Connections in Checkpoint and ASA Firewall.**
* Manage project task to migrate from **Cisco ASA firewalls to Check Point firewalls.**
* Configuring and troubleshooting site-to-site **IPSEC VPN** tunnels using **Cisco ASA 5540** for third-party connectivity.
* Installed and configured a variety of Cisco devices like Cisco Routers (1841, 1900, 2600, 2800, 3800, ASRs and more), Cisco switches (3560, 3750, 4507 catalyst, 6500 catalyst Switch and more) and Nexus 7000 series, Nexus 5000 series, Nexus 2K Fabric Extenders and F5 appliances.
* Applied knowledge of Ethernet switch and router configuration to configuration/design MPLS connections.
* Understanding of Layer2/3 VPN's, MPLS, Metro Ethernet and LAN switching.
* Creating object, **groups, updating access-lists** on **Check Point Firewall,** apply **static, hide NAT** using smart dashboard.
* Installed and configured high availability **Big IP F5 LTM** and **GTM load balancers like 6600, 6800** to provide uninterrupted service to customer applications and monitoring the availability.
* Identified opportunities for implementation of **network best practices,** particularly **F5 load balancer implementations.**
* Configuring F5 Load Balancers: Adding **virtual IPs, nodes, pools** and **health monitoring.**
* **F5 BigIP iRule programming** and troubleshooting.
* Worked on **F5 solutions/support** for migration work of applications and websites from **Cisco CSS Load Balancers to the F5 BigIP Load Balancers.**
* Configure and **Monitor Cisco Source fire IPS** for alerts.
* Working with different teams to gather info for the new request and troubleshoot for any connectivity issues by capturing traffic using **TCPDUMP** and **smart view tracker.**
* Worked on **VPN configuration, routing, NAT, access-list, security contexts and** failover in **ASA firewalls.**
* Provide support to help desk for complex/major network problems. Build the rules for the application access across the **IPSEC VPN tunnel**
* Implemented configuration back-ups using **Win SCP, cyberfusion to automate the back-up systems** with the help of public and private keys.
* Deployment and Management of **Bluecoat proxies in forward proxy scenario** as well as for security in reverse proxy scenario.
* Worked on **Blue Coat Proxy SG** to **safeguard web applications** in extremely untrusted environments such as guest Wi-Fi zones.
* Performing URL filtering and content filtering by adding **URL’s in Bluecoat Proxy SG’s**.
* Working on the network team to **re-route BGP routes during maintenance** and FW upgrades.
* Running vulnerability scan reports using **Nessus tool.**
* Use of Citrix Net scalar for the application delivery control.
* Configure **B2B VPN** with various business partners and 3rd parties and troubleshoot VPN Phase 1 and Phase 2 connectivity issues **including crypto map, encryption domain, psk** etc.
* Provided administration and **support on Bluecoat Proxy** for content filtering and internet access to primary, **remote site offices and VPN client users**
* Follow information security policies, methods, **standards, NIST standards and** practices to organize information systems, IT reference material and interpret regulations.
* **Monitor Intrusion Detection Systems (IDS)** console for active alerts and determine priority of response.
* Configuration and Installation of **Cisco Nexus 9K, 7K, 5K, 6K, ASR 1000 series.**
* Actively use **SIEM technology** for searching and monitoring real-time events for network security and compliance.
* Review daily log data gathered from various resources such as **sensors, alert logs, firewall logs, content filtering logs.**
* **Monitor Intrusion Prevention System (IPS).**
* Experience with converting **Cisco 6500 IOS to Cisco Nexus NX-OS** in the data center environment.
* Install updates on new signatures.
* Working on day-to-day service tickets to solve troubleshooting issues.
* Experience using Service Now ticketing tool.
* 24x7 support.

**Environment**: Cisco ASA5580/5540/5520, CheckpointR70, R75, R77.20 Gaia, Palo AltoPA-5000/3000, Big IP F5 LTM/GTM, Nexus switches, TCP/IP, VPN, Bluecoat Proxy servers, IDS/IPS. SIEM and Monitoring, Servie Now

**Network Security Engineer**

**Citigroup - Regent Campus, Irving, TX Jan 2011 to Apr 2014**

**Responsibilities:**

* Responsible for implementing, engineering & level 2 support of existing network technologies / services & integration of new network technologies / services.
* Building large scale Network environment using routing protocols like **OSPF, EIGRP**, and **BGP.**
* Configuring route redistribution between **EIGRP** and **OSPF.**
* Involved in **Network Designing, Routing, DNS, IP Subnetting, TCP/IP** protocol.
* Performing Route Filtering and Route Manipulation by applying distribute-lists, route-maps & offset lists.
* Diagnose **MPLS** protocol problems including **VRF** and **COS** issues to full resolution.
* Providing Layer-3 redundancy by implementing HSRP in the network.
* Hands-on experience in implementation and troubleshooting of BGP version 4, OSPF, IPV4 and Ethernet Protocols.
* Managing various **VLANs, IP addressing** for various subnets, **VLAN** Trunking between various access-switches.
* Used Load Balancers **F5 Big-IP6900** and 3900between the servers inside the Network and in the Server Farm.
* Performance fine tuning and maintaining customer network devices to provide high availability for the applications, proper bandwidth utilization and to avoid network congestion.
* Configuring Standard and **Extended Access Control Lists (ACLs)** and Firewalls.
* Designing and Implementing **VPN** and remote access support.
* Pro-active Monitoring and Alerting of client's network for any alarms.
* Testing and validating new solutions in lab before deploying them to customers.

**Environment:** CISCO 3750/3550/3500/2960 switches and CISCO 12000/7200/3845/3600 routers, CISCO ASA5510, Checkpoint. Juniper firewalls 5GT, 208, SSG 5, 140, 550, 550M, NSM, IDS/IPS, Vulnerability Assessment tools like Nessus, Red Hat, Solaris, Juniper VPN's, SSL.