Network Security Engineer Network Security Engineer Network Security Engineer Chicago, IL CCNA CCNP CERTIFIED professional with over 9+ years of experience in network design, implementation, and support. Routing, switching, windows server, mail server, firewall technologies, system design, implementation and troubleshooting of complex network systems. Extensive experience in configuring and troubleshooting of protocols RIP v1/v2, EIGRP, OSPF, BGP and MPLS. Expert in Juniper &Cisco network environments. Extensive knowledge with VLAN's, Trunking, RSTP, SNMP, SDN, Ether Channels,PortSecurity,HSRP,VRRP, GLBP,ISIS,ACL's, QoS, Traffic Policing, Shaping, EIGRP, OSPF, ECMP, PAT, Inspections, VPN's, DHCP, Wiresharketc. Expertise in configuring and troubleshooting of Palo Alto, Fortinet, Juniper Netscreen & SRX Firewalls and their implementation. Working Knowledge of Cisco IOS, IOS upgrade, JunOS, ONOS (Open Network Operating System)& basic Nexus (7K, 5K&2K). Switching tasks include VTP, ISL/ 802.1q, VLAN, Ether Channel, STP and RSTP. Strong hands on experience on Checkpoint Firewall, CiscoASA (5505/5510) Firewalls, and PIX (506, 515, 525, and 535). Implemented security policies using ACL, Firewall, IPSEC, GRE, SSL, VPN, IPS/IDS, AAA (TACACS+ & RADIUS). Experience inphysical cabling, IP addressing and Subnetting with VLSM, configuring and supporting TCP/IP, DNS, installing and configuring proxies. In-depth knowledge and hands-on experience in ISP Routing Policies, Network Architecture, IP Sub netting, VLSM, TCP/IP, NAT, DHCP, DNS, FT1 / T1 / FT3 / T3 SONET POS OCX / GigE circuits, load balancing, Firewalls. Experience in Cisco Prime Infrastructure, Solarwinds. Technology and Infrastructure consultant for Cisco and Juniper design and implementation projects. Build and move IT infrastructure related tasks include Integrated, Integrations, configurations, support and maintenance of routers and switches. Understanding and knowledge of configuring Cisco Meraki WLan controller. Well experienced in configuring HSRP, GLBP, ICMP, PPP, ISIS, PAP, CHAP and SNMP. Experience in installing and configuring DNS, DHCP server Expertise in installing, configuring, and maintaining Cisco Switches (2900, 3500 ,7600, 3700 series, 6500 series) Cisco Routers (4800, 3800, 3600, 2800, 2600, 2900, 1800, 1700, 800) Expertise in installing, configuring and troubleshooting Juniper Routers (J, M and MX-series). Administration and diagnostics of LAN

and WAN, in-depth knowledge of TCP/IP, NAT, PPP, ISDN, SDN (Software defined networking) and associates network protocols and services. Hands on Knowledge/experience on F5 load balancers, its methods, implementation and troubleshooting on LTMs and GTMs. Worked extensively on Fortinet, Palo Alto, Juniper Net screen and SRX Firewalls. Experience with design and deployment of MPLS Layer 3 VPN, MPLS Traffic Engineering, MPLSQOS and ECMP. Extensive experience in configuring Layer3 routing and layer2/3 switching of Juniper & Cisco based J2320,MX,EX,2950,2960,3600,3750,4500,6500,1700,1800,2600 and 3700 series routers & Switches. Troubleshooting & implementation of VLAN, STP, MSTP, RSTP, PVST, 802.1Q, DTP, HSRP, VRRP, GLBP, LACP, PAGP, AAA, SYSLOG, SNMP,TACACS, RADIUS, MD5, VTP & SVI. Proficient in setting up IT infrastructure including wide area networks (WAN), local area networks (LAN), security management systems network device administration. Experience working with Cisco IOS-XR on the ASR9000 devices for MPLS deployments IOS/JUNOS upgrade for Cisco & Juniper routers cum switches. Experience in testing Cisco & Juniper routers cum switches in laboratory scenarios and deploy on site for production. Expertise in windows based server 2003/2008, DNS, DHCP, IIS, Microsoft Exchange server configure, implementation and troubleshooting. Authorized to work in the US for any employer Work Experience Network Security Engineer ADTALEM Global Education - Chicago, IL October 2017 to September 2018 Responsibilities: Adding Rules and Monitoring Checkpoint Firewall traffic through Smart Dashboard and Smart View Tracker applications. Configuring Checkpoint Firewall in IPSO, Secure Platform and GAIA platforms. Implement network security for remote access. Tasks include configuring site to site and clients to site VPN tunnels through multiple Cisco VPN concentrators and Checkpoint firewalls, and maintaining access policies for remote users. Implementing and Managing VPN Networks of the Customer through Checkpoint R77/R80 firewalls. Managed Checkpoint Firewalls using Multi Smart Domain Manager, Juniper with Network Security Manager with Cisco ASDM. Centralized Checkpoint Firewall Policy Management using Provider -1 interfacing multiple CMA containing multiple security policies. Checkpoint Firewall Log review, TCP Dump and analysis and troubleshoot connectivity issues. Configuring HA on checkpoint security gateways using cluster XL

and VRRP. Upgrading checkpoint security gateways in cluster with minimal downtime. Configure and manage LDAP User management with Checkpoint Smart Directory. Checkpoint IPS protections to identify and prevent or mitigate malicious activity. Primary responsibility is also to maintain, monitor and make production changes on R77.30/R80.10 Checkpoint Firewall. Cisco ASA/Juniper NSM/Checkpoint Firewall troubleshooting and policy change requests for new IP segments that either come on line or that may have been altered during various planned network changes on the network. Experienced with AlgoSEC security policy analyzer centrally manages network security policies across multi-vendor hybrid cloud environments. Cleanup and optimize firewall policies quickly and efficiently, identify and mitigate risky firewall rules. Reduce firewall auditing time, visualize complex network with a dynamic network topology map. Responsible for creating, modifying, configuring, troubleshooting and monitoring of Checkpoint Firewall R77 VPN-1 NATs, Subnets, IPSec Tunnels, and VPN LDAP Groups for over 100+ business partners. Implement new Python test script and improve existing test script for the integration system testing. Placed in charge of control and maintenance of the SD-WAN laboratory environments, performing version updating before user client official updating. Worked on the Versa SD-WAN solution, designed the test automation infrastructure for the entire suite of SD-WAN features. Rearranging the stacks including Controllers and edge routers as per the requirement of the SD WAN. Configured the SD WAN controller for the entire network appliances. Monitoring the connections and flow of traffic between the SD-WAN Gateway and all the edges. Modified various configurations and changed policies using SD-WAN. Implemented Firewall security policies using ACL, NAC,NACL,IPSEC, SSL, VPN, IPS/IDS, AAA (TACACS+ & RADIUS) Worked on Checkpoint firewall for creating various firewall rules and NAT rules. Worked on Checkpoint firewall for creating object, data center object, dynamic object, network objects, assign dynamic object IP ranges. Update and configure the JSON file, configure and set parameter for python script file, Cron Job for update dynamic objects. Experience with incidence handling with checkpoint various issues, especially vSec issue, collect vSec logs, SetvSec debug command, install checkpoint Hot fix. Manage and administration multi-vendor security appliances including Check Point, Cisco,

Juniper, Netscreen, Palo-Alto, Cisco Firepower services. In-depth knowledge of Cisco Communication Manager,IOS, Cisco ASA and knowledge on Cisco FirePower. Experianced with Cisco ASA with FirePower NGIPS effective threat prevention services with AMP (Advanced Malware Protection). Define security intelligence, create access policy, URL policy, malware policy, balance IPS policy, enable portscan detection and DLP, SSL decryption. Configure NMAP host profile, HA Active/Standby failover test and spanned deployment. Experience with AWS infrastructure NextGen App which is an internal application that logs the customer data. Handled multiple AWS accounts with different VPC's for Prod and Non Prod environment. EC2 instances were configured and designed in all the environments to meet high availability and complete security. Setting up the CloudWatch alerts for EC2 instances and using in Auto scaling launch configuration and monitoring the traffic logs. Generated SSL certificates and installed into the Tomcat servers for the secured HTTPS protocol. IAM roles were created for the cross-account access and to send the Tomcat logs to CloudWatch. Developed build and deployment scripts using Maven as build tool in Jenkins to move from one environment to other environments. Built Elastic Load Balancers BigIQto distribute the incoming load to the EC2 instances in different availability zones. And installed certs on them with the use of Amazon Certificate Manager (ACM). Designed, built, and configured multi-AZ, private/public subnets, security groups, NACLs, NAT gateways, and bastion hosts to achieve required fault tolerance and security. Cloud Formation JSON Templates were written to setup and build AWS infrastructure with resources like VPC, EC2, S3, ELB, IAM, EBS, Security Groups, Auto Scaling and RDS automatically. Involved in everyday DC Migration meetings to ensure successful project forecasting and to discuss the roadblocks. Worked with our current application teams to understand our current applications and make migration recommendations and to-be architectures in AWS Services for clients. Network Security Engineer Morgan Stanley - New York, NY October 2016 to June 2017 SECOPS) Responsibilities: Assessment of risk to the network and creating security policy to counter the risks detected. Implementing the security policy and auditing the security policy at different times under different test circumstances to find vulnerabilities and modifying the security policy for better protection of the network. Manually

configuring security policies, policy properties and web application. Validate HTTP/TCP/UDP protocol compliance, Allow/Deny method and configuring security policy blocking. Understanding SOC environments and network types, components, and possible threats. Designing a firewall and user policy system to protect the components of network and the database from malicious people - hackers or employees. Implementing the security system by setting up firewall components and assigning rights to the users. In case of breach of security due to limitation of firewalls or any other reason, investigating the causes, providing for any loss arising out of the breach, and taking approaches, so that such breaches do not happen again. SECOPS (SOC) Scheduled or unscheduled testing of the security system under different scenarios to assess the strength of the network security and to assess the vulnerabilities. Modifying the network security for better protection of the network. Provide support infrastructure related requests and incidents within the firm. Analysis network trafficTCP/UDP, HTTP/HTTPS,SSL/TLS Decryption, FW staging, log search, Monitor the firm's security perimeter, core, and end point infrastructure. Experience with establish secure communication Handshake protocols, SSLv3 & TLS v1.0 decryption, PKI, CA self-sign cert assign. Linux/Unix Packet Capture and analysis, Detail analysis of OSI model (7 LAYER) and ACL with Wireshark appliances. Maintain Firewall policy and firewall plant migration.

Core Security (Kerberos, Radius, RSA, Encryption), End Point Security (Anti-virus, Device lockdown, End Point Encryption). Security Perimeter (VPN, Firewalls, Proxy, anti-spam, Data leakage). Manage firewall & Cluster Fortimgr, Juniper Space, NSM (NetscreenSecurity manager), IPFilter, IPtables. Hands on experience with Juniper SRX, Juniper QFX, Juniper EX, Juniper MX platforms and JUNOS Space and Network Director Platforms. Day-to-day monitoring of IT Security's Infrastructure technologies. Troubleshooting of possible network connectivity or infrastructure related problems. Outage Management: investigation, communication, triage and escalation Firewall related Task. Scripting experience with Bash and python. Sr. Network Engineer DTE Energy - Detroit, MI April 2016 to September 2016 Responsibilities: Experienced in Integration, configuration and maintenance of Cisco Router, Catalyst Switches and Firewalls. Configuring RIP, OSPF, EIGRP and Static routing on Juniper M and MX series Routers.

Datacenter upgrades from C6500s to Nexus 7k/5k/2k, VPC between distribution and access, single-VPC to servers. Responsible for all routing, switching, VPN, network security, and server load balancing. Using PBR with Route Maps for route manipulation/filtering. Troubleshooting routing issues like suboptimal routing and asymmetric routing. Implemented various EX, SRX & J series Juniper devices. Have created number of site to site IPSEC VPN tunnel with Checkpoint, Juniper Netscreen firewalls and Cisco ASA firewalls. Very good Experience in using and maintaining various network monitoring tools like Solarwinds, Splunk, Cisco Prime infrastructure, Cisco ISE. Expertise in the administration, support and operation of the OrionSolarwinds platform includingNetwork Performance Monitor (NPM), SYSLOG, SNMP, Server Application Monitor (SAM), IP Address Manager (IPAM), Storage Manager, physical and virtual storage infrastructure, Troubleshoot application performance issues, Network Configuration Manager (NCM),NetFlow Traffic Analyzer (NTA), Database Performance Analyzer, VPAT Storage Manager. Configuring User Identity Groups, Filtering, Adding, and Removing Endpoints in an Endpoint Identity Group, Configuring Data Access Permission, Configuring Menu Access Permissions, Configuring Network Access for User Accounts. Configure Cisco ACI L2 Connectivity, integrating with Hyper-V, remote authentication and deployment of AVS (Cisco Application virtual switch) with ACI. Configuring various advanced features (Profiles, monitors, I Rules, Redundancy, SSL Termination, Persistence, NAT/SNATs, HA on F5 BIGIP/BIGIQ appliances SSL termination and initiation, Persistence, Digital Certificates, Executed various migration/upgrade projects across F5 and hands on with F5 BIGIP/BIGIQ LTMs/EM, web application firewall module, attack signature, brute force prevention, authenticate VPN SSL module AFM/ASM/APM. Configured CIDR, IP, PPP, HDLC, EIGRP, MPLS, OSPF and BGP routing. Security policy review and configuration in Cisco ASA, Fortinet Firewall and Troubleshooting of CISCO routers like ping, trace route and basic issues. Implemented the Policy Rules, DMZ and Multiple VDOM's for Multiple Clients of the State on the FortiGate Firewall. Implemented the Inter VDOM Routing through the FortiGate Firewalls and also the Router. Implemented Zone Based Firewalling and Security Rules on the Fortinet Firewall. Implemented IPS, DLP and UTM features on the firewall for added security purposes. FortiGate load balancer,

FortiGate web proxy. VPN & remote connectivity with FortiGate Site to site VPN and IPsec. Improved network capabilities and reliability by evaluating, testing, purchasing, and implementing new SONET, SDH, DWDM, IP/MPLS, Ethernet, and wireless 802.1xtechnologies Configured Juniper MX480s, EX8200s, EX4500s, EX4200s, from scratch to match design. Has a good experience working with the Trouble Tickets on F5 Load balancers on LTM module. F5 stateful inspection and dynamic packet filtering through TMOS. Experience with F5 VIPRION and F5 Edge series appliances, F5 cluster to manage large number of application traffic. Switch experience includes Cisco Catalyst switches: CISCO 3750, 4500, 6500 series switches, IOS upgrade for Cisco router and switches. Configuration and maintenance of OSPF protocol, which was the enterprise IGP. Configuration included deploying of new branch locations or new network devices in the existing infrastructure. Creating Stub Areas & configuring Summarization for effective Routing. Install configure and manage Aruba network infrastructure, Cisco wireless controller, AP's Provided technical support for full setup, debugged the problems of OSPF, switching and HSRP. Implemented and used SDM to configure Cisco IOS security features and network connection. Create and test Cisco router and switching operations using OSPF routing protocol, ASA Firewalls for stable VPNs. Implementation and maintained intrusion detection/ prevention (IDS/IPS) system to protect enterprise network and sensitive corporate data. For Fine-tuning of TCP and UDP enabled IDS/IPS signatures in Firewall. Configuration the access-list rules, network object-service group based on well-known port the port i.e. FTP/SFTP, SSH,TCP/UDP, HTTPS/HTTPS (SSL) etc. Negotiate VPN tunnels using IPsec/GRE encryption standards and also configured and implemented site-to-site VPN, Remote Access VPN. Security policy review and configuration in Palo Alto and JuniperSRX Firewall in US offices and Datacenter. Working knowledge of the UNIX and CLI based command to implement the networking tools. Configured and monitored Firewall logging, DMZ's and related security policies. Responsible for service request tickets generated by the helpdesk in all phases such as troubleshooting, maintenance, upgrades, patches, fixes, and all around technical support of 24*7. Configuration of ACLs in Cisco 5540 series ASA firewall for Internet Access requests for servers in LAN and DMZ and also for special user requests as

authorized by management. Involved in L2/L3 Switching Technology Administration including creating and managing VLANs, Port security, Trouncing, STP, Inter-VLAN routing, LAN security. Network Administrator Robodh Contracting Company - Dubai, AE February 2012 to April 2014 Responsibilities: Configure and implementing Fortinet FortiGate (5.x) Security systems Firewall. Implemented the Policy Rules, DMZ and Multiple VDOM's for Multiple Clients of the State on the FortiGate Firewall. Implemented the Inter VDOM Routing through the FortiGate Firewalls and also the Router. Implemented Zone Based Firewalling and Security Rules on the Fortinet Firewall. Implemented IPS, DLP and UTM features on the firewall for added security purposes. Performed troubleshooting, while maintaining trouble ticket tracking, following internal/external escalation procedures and customer notifications. Configured Cisco Routers for OSPF, RIP, IGRP RIPv2, EIGRP, Static and default route. Configured the Cisco router as IP Firewall for NAT. Supporting Development team for the access to corporate network and outside world. Providing access to specific IP, Port filter and port access. Switching (Ethernet) related tasks included implementing VLANS and configuring ISL trunk on Fast-Ethernet channel between switches. Installation and maintenance of new network connections for the customers. Configuring all the required devices and equipment for remote vendors at various sites and plants. Installing new equipment to RADIUS and worked with MPLS-VPN and TACACS configurations. Installing and maintaining local as well as network printers. Validating existing infrastructure and suggesting new network designs. Working on creating new load balancing policies by employing BGP attributes including Local Preference, AS-Path, and Community, MED. Installing and maintaining Windows NT Workstations and Windows NT Server. Providing technical support to LAN & WAN systems. Monitoring Memory/CPU on various low end routers in a network. Monitor performance of network and servers to identify potential problems and bottleneck. Performed administrative support for RIP, OSPF routing protocol. Maintained redundancy on Cisco 2600, 2800 and 3600 router with HSRP. Real time monitoring and network management using Cisco Works LMS. Provided technical support on hardware and software related issues to remote production sites. Configuring routers and send it to Technical Consultants for new site activations and gives online support at the

time of activation. Support Engineer Bijoy Online Limited January 2010 to June 2012 Responsibilities: Configuration and support for Active Directory, LAN, Windows 2003 servers, IIS, Exchange,VMware ESX server, Windows XP for 200+ users. Experienced in Integration, configuration and maintenance of Fortinet Firewall System. Knowledge of troubleshooting, licensing, firewall configuration, VPN, antivirus, intrusion prevention (IPS), Web filtering, antispam, and traffic shaping, policy based rules. FortiGate ASIC-based multi-threat security systems utilize breakthroughs in networking, security monitoring Bandwidth and content analysis. Troubleshoot and maintain network, desktops, laptops and other computer equipment. Install and maintains local area network hardware and software. Coordinate purchasing and installation of hardware and software for users. IT projects assigned by supervisors. Coordinates network schedule, backups, and downtime to users. Monitor and maintain network stability. Transition and installation of new security tools such as firewalls and other network traffic filters. Network site development. Continually asses, revise, document and standardize hardware, software and keep update of existing documentation. Maintain and document ongoing periodic maintenance activities for department systems. Implement and take lead role in ongoing infrastructure activities via project management and state guidelines including purchasing software, hardware and contracting through CMAS and other state agency ordering processes. Consult on infrastructure configuration and implementation. Other required activities such as writing charters, project plans and management written reports. Education Bachelor's Skills Firewall (6 years), Lan (5 years), Radius (3 years), Security (6 years), Vpn (6 years) Additional Information Technical Skills: Protocols & Standards: LAN, WAN, WLAN, VRF, VDC, TCP/IP, NAT, PAT, SDN, MPLS, GETVPN, GDOI, DMVPN, IPv4, IPv6, OSPF, OSPFv3, EIGRP, BGPv4, VPN,L2TP, GRE/IPsec / ISAKMP, IKE, VoIP, VSS, VLANs, ACLs, Layer 3, Switching, ISIS, HSRP, GLBP, VRRP, ECMP, QoS, TACACS+, RADIUS, 802.1X, PKI, LDAP, POE. Cisco Platforms: Nexus 7K, 5K, 2K & 1K, Cisco routers (7600, 7200, 3900, 3600, 2800, 2600, 2500, 1800 series) & Cisco Catalyst switches (6500, 4900, 3750, 3500, 4500, 2900 series), Huawei AR Series Routers, Cisco prime infrastructure, Cisco ACI, Cisco ISE Juniper Platforms: M, EX, J and MX Series Routers, Netscreen& SRX series firewall Networking Concepts:

Access-lists, Routing, Switching, Subnetting, Designing, CSU/DSU, IPsec, VLAN, VPN and Wireless Technology Firewall: Palo Alto,Fortigate, Juniper Netscreen, Juniper SRX, Cisco ASA Network Tools: IBM ITNM, Splunk, StealthWatch, Solar Winds, SNMP, CiscoWorks, Wireshark Load Balancers: F5 Networks (Big-IP) WAN technologies: Frame Relay, ISDN, ATM, MPLS, leased lines & exposure to PPP, DS1, DS3, OC3, T1 /T3 & SONET LAN technologies: Ethernet, Fast Ethernet, Gigabit Ethernet, & 10 Gigabit Ethernet, Port- channel, VLANS, VTP, STP, RSTP, 802.1Q, 802.1x. Wireless Technology: Meraki,Aruba wireless infrastructure, Cisco WLAN controller 5520, 3500, 2500 Security Protocols: IKE, IPSEC, GRE, SSL-VPN Virtualization: Vmware, VSphere 6, Vim's-ESX Server, vCenter. Networking Protocols: RIP, OSPF, EIGRP, BGP, STP, RSTP, ISIS, VLANs, VTP, PAGP, LACP, MPLS, HSRP, VRRP, GLBP, TACACS+, Radius, AAA Operating System: Windows 7/XP, Windows Server 2003/2008, ONOS, Linux, UNIX. Programming concept: C, C++, Java, Python.

Name: Jennifer Banks

Email: amanda05@example.com

Phone: +1-808-885-2620x991