Sr. Network Security Engineer Sr. Network Security Engineer Sr. Network Security Engineer - Capital One Plano, TX   Network Security Engineer with 7+years of experience in design, install, configure, support, and troubleshoot including a broad range of LAN/WAN/MAN, Public/Private Cloud enterprise networks and security using Cisco routers/switches/firewalls.   Implementation, Configuration and Support of Checkpoint (R80, R77 Gaia, R75 and R71), VSX,MDM/MDS, Provider-1, Juniper Firewalls (SSG 550M, SSG520M, ISG 1000, ISG 200, SRX5400, SRX5600, and SRX5800), Cisco Firewalls (ASA 5505, 5506-X, 5585 with firepower), Palo Alto Networks Firewall models (Panorama M-100, PA-2k, PA-3k, and PA-5 k).   Hands on experience using Expedition Palo Alto networks migration tool to convert a configuration from Checkpoint or Cisco or any other vendor to a PAN-OS.   Implementing security policies using AAA, ACL's, NAT, Policy NAT, PBF/PBR, Route-maps, Distribution lists and IPsec VPN's on different series of routers and firewalls.   Involved in the integration of F5 Big-IP load balancers with CheckPoint firewalls for firewall load balancing and was responsible was troubleshooting and maintenance.   Experienced in Migration from Checkpoint and Cisco ASA Firewalls to Palo Alto.   Worked on Cisco ASA (5540/5550) Firewalls and firepower 2k and 4k. Implemented Security Policies using ACL, Firewall, IPSEC, SSL, VPN, IPS/IDS, AAA (TACACS+ & RADIUS).   Hands-on experience on Palo Alto Rule changes PA-2000/PA-4000 series, templates, object creation, planning, configuration changes, OS upgrades and CLI troubleshooting.   Proficient in using SolarWinds Network Management tools like Network Performance Monitor (NPM), NetFlow Traffic Analyzer, Network Configuration Manager (NCM), Server and Application Monitor (SAM), SolarWinds Web Performance Monitor and SolarWinds Virtualization Manager.   Planning, Designing, Installing, Configuring of Cisco 6500, 4500, 2900, 3500, 3750 XL series switches, Nexus 5k, 7k series switches, Cisco 1800, 2500, 2600, 2800, 3600, 3800, 7200 series Routers and Juniper EX Switches.   Hands on experience in implementation and deploying BIG-IP F5 LTM, GTM series like 6400, 6800, 8800 for load balancing and network traffic management for business applications.   Handling Break/Fix situations, monitor, configure, policy creation on Checkpoint's SmartCenter Server.   Deployed Site to Site and Client to Site VPNs utilizing Checkpoint Firewall-1/VPN-1 and Cisco ASA.   Working on network design for

new next-generation VPN solution, migration from Checkpoint VPN to Pulse Secure VPN from network prospect. Experienced in working on network monitoring tools like SolarWinds, Nagios, NetFlow, Sniffing tools like Wireshark, Splunk and TCPDUMP. Configuring, Monitoring and Troubleshooting Cisco's ASA 5500/PIX security appliance, Failover DMZ zoning & configuring VLANs/Routing/NAT with the firewalls as per design. Managed inventory of all network hardware, Management and Monitoring by use of SSH, Syslog, SNMP, NTP. Hands on experience with Blue Coat Proxy URL filtering, Splunk SIEM, IBM Qradar, Nessus, Infoblox, Tufin, Algosec, Firemon, CSM, NSM, ASDM, Source fire IPS/IDS. Hands on experience in configuring and supporting site-to-site and remote access Cisco, IPsec, VPN solutions using ASA/PIX firewalls, Cisco, B2B VPN client in addition to providing TACACS+ and RADIUS services. 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.) Extensive experience in configuring and troubleshooting of protocols RIP v1/v2, EIGRP, OSPF, BGP and MPLS. Basic knowledge on Wireless Access points of 802.11 a, b, g. Creating and maintaining network documentation, design drawings, security diagrams, procedures and policies using MS word and Visio. Worked on virtual Palo Alto firewalls integrated with Azure Cloud - VM PA-200, PA-300. Install, configure, Upgrade of Red Hat Linux 4.x/5.x,6.x, Solaris 9.x/10.x, CentOS operating systems, configure kick start server and implemented patches via Redhat Satellite server. Extensive experience in AWS Cloud native services like EC2, ELB, VPC, Auto Scaling, Security Groups, Subnets, Launch Configuration, S3, SNS, AWS Macie, IAM, CloudWatch, CloudTrail, Elastic IP's, so on. Experience in providing the security to the AWS Cloud services with Security and Compliance tools. Work Experience Sr. Network Security Engineer Capital One - Richmond, VA July 2017 to Present Responsibilities: In-depth expertise in the analysis, implementation, troubleshooting & documentation of LAN/WAN architecture and good experience on IP services. Managed rules on Cisco ASA, Checkpoint and Palo Alto NGX firewall Involved in configuring and implementing of composite Network models consists of Cisco7600, 7200, 3800 series routers and Cisco 2950, 3500, 5000, 6500 Series switches Security policy

review and configuration in Palo Alto, Cisco ASA firewalls in US offices and data centers. Joined troubleshooting call with multiple team to resolve any network security related issues. Experienced with Checkpoint Gaia, SecureXL, IPSO. Experienced with Checkpoint Cluster environment. Experienced with Checkpoint SmartView Monitor, SmartView Tracker, Smart Console, Smart DashBoard. Experienced with Checkpoint Provider 1 as well as Smart Domain Manager (SDM) Experienced with multiple log servers of Checkpoint. Experienced with both Clish and Expert mode in Checkpoint. Experienced with Staging rule on policy base with Tufin Secure Change. Working on analysis policy, compare policy with Tufin Secure Track. Experienced with troubleshooting any kind of Checkpoint related issue with multiple team (like server team or application team) as well as with Diamond Support Engineer of Checkpoint vendor. Experienced with Palo Alto specially on Panaroma, Global Protect, Template, Device Group. Hands on experienced on Global Protect implementation on Palo Alto, troubleshoot with user to determine the issue related with GP. Hands on experienced to upgrade PAN OS from 7.0 to 8.0. Experienced with Add rule, add network object, EDL (external dynamic list), app-id exception, scheduled rule and so on in Palo Alto. Hands on experienced on Monitor, Packet capture, Proxy configuration on Panaroma. Experienced on CLI of Palo Alto. Troubleshoot with multiple team any Palo Alto related issue as well as PAN support engineer after opening case with Palo Alto. Experience in implementing F5 BIG IP load balancers. OS upgrade in F5 BIG-IP from 10.4.0 to 11.5.3. In depth knowledge and hands on experienced in iRules and iApps, as well as SNAT, NAT, Auto map and HA (High Availability) Hands on experienced in TcpDupms. and analysis with WireShark 1.8.2. Creating persistence profile, one-connect profile in F5 BIG-IP. Working and implementing GA and Topology LB method in F5 GTM. Hands on experience in SyncGroup in F5 GTM. Expertise in creating custom Health monitors, VIP's, pools, nodes for F5 LTM/GTM Performing troubleshooting on VPN connectivity issues, slow network connectivity issues, identifying the root cause of the issues. Hands on experience to monitor Blue Coat proxy high bandwidth utilization, health status, Policy analysis. Worked with network services like DNS, DHCP, DDNS, IPv4, IPv6, IPsec, VPN etc. Worked with Infoblox for secure DNS, DHCP and IPAM with Infoblox.

Configured static NAT, dynamic NAT, dynamic NAT overloading   Configuring ACL on ISE for making policies.   Responsible in troubleshooting on Cisco ISE added new devices on network based on policies on ISE.   Work assigned tickets (HPSM and JIRA) to determine the point of failure and resolve problems remotely utilizing available tools and other Operation Center resources.   Documenting network configuration for all new equipment and creating equipment configuration backups and monitoring to work with existing network systems   Provide escalation support to L1/L2 members of network team.   Participating in testing of the internal network infrastructure in the new building and troubleshooting and remediating any issues.   Work & escalate problems effectively in order to meet customer SLA's (service level agreements)   Perform problem management and root cause analysis for P1/P2/P3/P4 incident.   Environment: Checkpoint R75, R77, PaloAlto, F5 LTM and GTM, Nexus 2k/5k, Cisco 6500/7500/7200 Routers, Cisco 3550/4500/6500 switches, LAN, WAN, OSPF, RIP, BGP, EIGRP, HSRP, PPP, VPN, Checkpoint, Cisco ASA, McAfee EPO, Cisco ISE, EOP, Trend Micro, Kemp. Checkpoint Engineer Capital One - Plano, TX June 2015 to June 2017 Responsibilities: Configure and implement security solutions for various clients as per their requirements in Checkpoint R80, R77, R75, R65, Provider-1, Palo Alto firewalls, Panorama, Cisco ASA firewalls, ASDM and in CSM.   Configured and Maintained rules on Palo Alto Firewalls (PA-220, PA3060) & Analysis of firewall logs using various tools.   Configured High availability, User ID, App-ID and Global protect on Palo Alto firewall.   Implemented failover (Active-standby and Active-Active) and clustering with ipv4 on ASA Firewall.   Converted Port based rules to APP ID based rules in Palo Alto firewalls.   Pushed Policies from Panorama to Firewall in Palo Alto, Configured and Maintained Palo Alto Firewalls.   Palo Alto design and installation (Application and URL filtering, Threat Prevention, Data Filtering).   Exposure to wildfire advance malware detection using IPS feature of Palo Alto.   Implemented Checkpoint FW Interface, NAT and VLAN using R77 GAIA Smart Dashboard.   Worked on different software blades of Checkpoint firewall like IPS, VPN and NAT.   Implemented two factor authentications for the users, third-party vendors connecting organization's network.   Perform configuration changes on Checkpoint R77 Gaia and Palo Alto on a large-scale environment.   Proficient in researching traffic patterns to identify false-positives

and/or malicious traffic within IDS, IPS, proxy (Bluecoat) and firewalls (CheckPoint, ASA, and Paloalto). Converted Checkpoint VPN rules over to the Cisco ASA solution. Migration and implementation of new solutions with Palo Alto Next-Generation Firewall series PA-3060 and PA-5060. Installed, configured and maintained Checkpoint R75-R77 Gaia/SPLAT. Identified and removed security policies that are no longer needed to reduce Checkpoint Firewall policy lookup. Configured necessary routing and NAT on the Firewall appliance to communicate with the internet. Backup Restore and Upgrade of Checkpoint Firewall appliance. Monitored Checkpoint VPN tunnel activities with Smart View Monitor and troubleshoot VPN issues with CLI. Optimize existing policies to improve security and performance. Identify and remove security policies that are not no longer needed to reduce CheckPoint Firewall policy lookup. Experience on working with Palo Alto Next Generation firewall with security, networking, and management features such as URL filtering, Anti-virus, IPsec VPN, SSL VPN, IPS, Log Management etc. Extracted the logs, perform real time log analysis using SIEM technologies and Forensics Analysis of logs as per the request. Manage and maintain CheckPoint Cluster XL, VSX, VPN-1 firewall, strong abilities in installation and configuration of Checkpoint security Gateway, SmartConsole and SmartCenter server. Installed and configured protocols like TCP/IP and Internet protocols including Local Area Networking, routing and HTTP. Perform Checkpoint and ASA firewalls design, integration and implementation of networks. Experience in using Smart Update, User Identity Management and Authentication in CheckPoint Firewall. Responsible for Checkpoint and Cisco ASA firewall administration across our global networks. Configure IP-SEC VPN, and SSL-VPN (Mobile Access) on Checkpoint Gaia based on user traffics that needs to be encrypted using Checkpoint. Configuring and troubleshooting Smartcenter HA as well as backup of firewall policies and database versions. Responsible for the design and implementation of the network architectures including firewalls, load balancers, IDS, VPN, DNS, switching, routing, wireless security, TCP/IP, VPN and Content Filtering. Policy Reviewing, Audit and cleanup of the un-used rule on the firewall using Tufin and Splunk. Provided tier 3 support for CheckPoint and Cisco ASA Firewalls to support customers, Backup and restore of checkpoint and Cisco ASA Firewall policies. Supported Bluecoat proxies for URL

filtering and content filtering. Monitoring Traffic and Connections in Checkpoint and ASA Firewall.

 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. Provided support for 2Tier and 3Tier firewall architecture, which includes various Checkpoint, Cisco ASA firewalls and Palo-Alto firewalls. Working with customers Site-to-Site and Remote Site VPNs using Cisco routers to Cisco routers, ASA Firewall to Palo Alto Firewall, Cisco Router to Palo Alto Firewall and troubleshoot and modify existing VPN. Configuring Big-IP F5 LTMs (virtual servers, pools, SNATs, health monitors, irules) and GTM's for managing the traffic and tuning the load on the network servers. Centrally managed all Palo Alto Firewalls using Palo Alto Panorama M-100 management server. Worked on ServiceNow to create Incidents tickets and change requests to apply the remediation identified. Network Security Engineer T-Mobile - Seattle, WA January 2014 to April 2015 Responsibilities: Supporting and troubleshooting Checkpoint (R77.10 Gaia, R77, R76, Provider-1, MDM/MDS, VSX, SPLAT and IPSO) and Cisco firewall (ASA 5550, 5540, 5520, PIX 525, 535, CSM and ASDM) technologies. Migration and implementation of new solutions with Palo Alto Next-Generation Firewall series PA-5060, PA-3060 and PA-500. Troubleshooting connectivity issues on the Checkpoint Firewall using smart view tracker, monitor health of the appliance using smart view monitor. Responsible for planning, documenting and implementation of complex Firewall and VPN solutions. Configured Juniper SRX and SSG firewalls using NSM and via CLI. Adding zone-based rules in Juniper SRX and SSG Netscreen (6500, 6000, 5400) firewalls as per client requirements. Experience in Designs and implements Cisco FirePower and Palo Alto firewalls. Palo Alto design and installation (Application and URL filtering, Threat Prevention, Data Filtering). Extracted the logs, perform real time log analysis using SIEM technologies and Forensics Analysis of logs as per the request. Engineered BLS Checkpoint infrastructure which consists of 500+ firewalls running different flavors of hardware and Checkpoint OS such as (R71, R75, R76 and R77). Converting Checkpoint VPN rules over to the Cisco ASA solution and migrating with both Checkpoint and Cisco ASA VPN. Implemented Site-to-Site VPNs between ASA Firewall and Router. Configured and maintained IPSEC and SSL VPNs on Palo Alto

Firewalls. Configuration and administration of Palo Alto Networks Firewall to manage large scale Firewall deployments.   Performing packet captures using TCPDUMP, fw monitor, Snoop, Wireshark and other network monitoring tools.   Worked with Checkpoint Firewall (SPLAT/Gaia) for management (Smart Dashboard, Smart Monitor), Logging (Smart Log, Smart View Tracker). Configuration of Fabric path and connectivity between Nexus 5K and Nexus 7k.   Involved in Datacenter build and support, Implementation, migrations network support, Interconnectivity between an old Datacenter and new Datacenter.   Worked on Juniper: EX-2200, EX-4200, EX-4500, MX-480, M Series, SRX210, SRX 240, SRX 1600 SSG 550.   Designed and configuring of OSPF, BGP on Juniper Routers and SRX Firewalls.   Worked on Bluecoat ProxySG to block list/ whitelist websites, URL Filtering and content filtering as per business request.   Configure Access List ACL to allow users all over the company to access different applications, Internet and compliance to the security policy and standards.   Worked with Nagios for monitoring of network services (SMTP, POP3, HTTP, NNTP, ICMP, SNMP, FTP, SSH). Network Security Engineer CNSI - Rockville, MD October 2012 to December 2013 Responsibilities: Designed, implemented, and managed network security countermeasures including firewalls and intrusion detection/prevention systems such as: Palo Alto, Pfsense, and Cisco's SourceFire   Responsible for maintaining multi-vendor network environment including Cisco ASA, Juniper JUNOS, Fortinet firewalls, Palo Alto PA-200 and configuring different policies to provide connectivity.   Firewall Policy Provisioning and troubleshoot connectivity issues through firewall.   Maintenance and Troubleshooting of connectivity problems using Ping, Traceroute.   Configured access control lists. Troubleshooting DNS/DHCP issues within the LAN network.   Experience configuring various networking protocols, specifically OSPF, BGP, EIGRP and troubleshooting issues with the network.   Configured and maintained IPSEC and SSL VPNs on Palo Alto Firewalls. Configuration and administration of Palo Alto Networks Firewall to manage large scale Firewall deployments.   Adding Websites to the URL filtering block list in Bluecoat Proxies and upgrading firmware on the bluecoat proxies.   Worked on cleanup of several legacy rules of ASA and checkpoint firewalls and created a migration path to Palo Alto.   Configure and maintain security policies on Fortinet firewall and manage Forti-Manager/

Forti-Analyzer. Expertise in IP subnetting and worked on various designing and allocating various classes of IP address to the domain. Modified internal infrastructure by adding switches to support server farms and added servers to existing DMZ environments to support new and existing application platforms. Configuring static NAT, dynamic NAT, inside Global Address Overloading, TCP overload distribution, Overlapping Address Translation on Cisco ASA Firewalls. Physical cabling, IP addressing, Wide Area Network configurations (Frame-relay). Switching related tasks included implementing VLANS and configuring ISL trunk on Fast-Ethernet channel between switches. Involved in troubleshooting network traffic and its diagnosis using tools like ping, traceroute, WireShark, TCPdump and Linux operating system servers. Documentation involved preparing Method of Procedures (MOPs) and Work Orders. Also creating and submitting Remedy tickets for user auditing. Network Security Analyst South Jersey Industries - Folsom, NJ August 2011 to September 2012 Responsibilities: Installation and Configuration of networks, router/switches configuration and wireless access point/router with security, TCP/IP, VPN, Content Filtering, Access Control Lists on router/switches, VLANs (port mapping, naming etc.), and routing IP address in both LAN/WAN and wireless networks. Interface directly with the client in business units to determine project objective, cost estimates and ensure customer satisfaction and timely delivery of services ordered. Worked on wide array of different projects, ranging from server installs / probes to configuring Layer 2 and Layer 3 devices, for implementation into new and existing switching blocks. Implementation of New Backbone, Core and MAN/WAN routers for the New Data center. Configure Cisco 6500 Layer 2 and Layer 3 and supervise equipment installation and cabling work. Worked on Visio Software, update client network diagrams. Worked with Network Operations with trouble tickets. Configuring DNS and DHCP configuration in Infoblox. Coordinating the implementation of switched networking infrastructure for server and client building blocks Supervise moves, additions and changes in LAN environment, and update DHI database. Preparing Client Machines for users with Operating Systems, Software, antivirus and required utilities and mailing clients etc. Migration of RIP V2 to OSPF, BGP routing protocols. Network Administrator Wyndham Worldwide - Orlando, FL April 2010 to July 2011 Responsibilities:

Designed and implemented IP Addressing, Subnetting, Route Summarization and Route Distributions. Implemented and configured LAN Protocols: Ethernet, VLANs, VTP and STP. Have ability to install and maintain Microsoft Exchange and worked extensively on different applications. Perform daily maintenance, troubleshooting, configuration, and installation of all network components. Worked on IGMP, PIM protocols for implementing IP multicast routing in the enterprise network. Configuration of CISCO Routers (2800, 3600 Series) and 2900, 3750 series switches. TCP/IP network planning, Implementation and Management with subnets. Enabled SNMP traps for our Cacti Monitoring tool to monitor traffic and check the regular health of Servers and Network Devices. Implemented and Configured IP Routing Protocols: OSPF, EIGRP, and RIPv2. Monitored network using SNORT. Upgrades and backups of Cisco router configuration file to a TFTP server. Configured SSH on all network switches and routers for secure management purposes. Configured and Implemented VLANS over the core Switch, configured VTP to manage VLAN database. Worked with Remedy Ticketing tool in maintaining and keep a track of logs/monitor. Education Bachelor's Additional Information TECHNICAL SKILLS: Management Tools: TCPDUMP, Solarwinds, Orion products, Snort (IDS), Netflow Analyzer, WhatsUP Gold, Wireshark, SPLUNK, Remedy, Service Now, HPSM, HP NAS, IBM Qradar, Splunk, Visio, Tufin, Algosec and Firemon. Firewall Products: Checkpoint R 80.10,77 GAIA, R75, R71, NGX R65/R60, Cisco PIX 525E, 535 & ASA 5510, 5520, 5540, Provider-1, SmartCenter Server, SPLAT, VSX, Juniper SRX and SSG, NSM, Jun OS, Screen OS, SPACE, ASDM, Cisco ACS, Palo Alto PA-7000, PA-5000, PA-3000, PA-2000, PA-850, PA-820, PA-220, PA-200, Panorama. Cloud Services: AWS - ELB, VPC, EC2, Subnets, Security Groups, S3, Route 53, Cloud Front, etc. Cisco Products: Routers (1800, 2500, 2600, 3200, 3600, 3700, 3800), Cisco L2 & L3 Switches (2900, 3560, 4500, 6500), Nexus 3000, 5000, 7000, 9000 series Switches. Protocols/Services: Routing Protocols (RIP, IGRP, EIGRP, OSPF, BGP), QOS, TCP/IP, IPSEC, MPLS, TACAS+, RADIUS, Cisco NAC WAN Technologies: CDP, Access Control List (ACL), Network Address Translation (NAT), PAT, Redistribution, OSPF Virtual Links and GRE Tunnel, VPN3000 Concentrator, Bluecoat SG Proxy

Name: Jennifer Smith

Email: bradvance@example.org

Phone: 001-452-381-5420