sr. SR. SR. Network Security / Firewall Architect sr. SR. SR.Network Security / Firewall Architect sr. SR. SR. Network Security / Firewall Architect - Ameriprise Financial Inc Jersey City, NJ Network Security Professional with experience in researching, implementing and administering network security solutions. Skilled in supporting and troubleshooting operational issues related to network security Infrastructure. Designing, Implementation and Operations of enterprise data networks as Network Security Administrator. Strong hands on experience in installing, configuring , and troubleshooting of Cisco 7600, 7200, 3800, 3600, 2800, 2600, 2500 and 1800 series Routers, Cisco Catalyst 6500, 4500, 3750, 2950 and 3500XL series switches. Implemented Positive Enforcement Model with the help of Palo Alto Networks. 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. Worked with the Audit team by using AlgoSec tool to analyze firewall and automating the auditing and analysis of firewalls, routers, VPNs and other security devices. Installation, configuration and maintenance of Palo Alto, Cisco ASA 5500, Juniper SRX Firewalls. Experience in installing, configuring and troubleshooting of Checkpoint Firewall and Juniper SSG series. Worked on Palo Alto design and installation (Application and URL filtering, Threat Prevention, Data Filtering). Configure all Palo Alto Networks Firewall models (PA-2k, PA-3k, PA-5k etc.) as well as a centralized management system (Panorama) to manage large scale Firewall deployments. Collaborated Palo Alto Application with the Splunk for advanced security reporting and analysis. Hands on experience in configuring and supporting site-to-site and remote access server, IPSec, VPN solutions using ASA/PIX firewalls, Cisco and VPN client. Experience in site to site VPN configurations using Cisco ASA 5500 series firewalls Responsible for Checkpoint and Cisco ASA firewall administration across global networks. Worked on F5 LTM, GTM series like 6400, 6800, 8800 for the corporate applications and their availability. Implemented traffic filters using Standard and Extended access-lists, Distribute-Lists, and Route Maps. Work experience on Bluecoat Proxy SG for Content filtering and URL filtering. Worked on network topological and configurations, TCP/IP, UDP, Frame Relay, Token ring, ATM, bridges, routers, and Switches. Experience in configuring Client-to-Site VPN using IPSEC VPN on SRX series firewalls

Experience in adding Rules and Monitoring Checkpoint Firewall traffic through Smart Dashboard and Smart View Tracker applications Experience in configuring, implementing and troubleshooting F5 load balancer in the enterprise network Experience with Bluecoat Proxy servers, LAN & WAN management. Excellent working knowledge of TCP/IP protocol suite and OSI layers. Performing network monitoring, analysis using various tools like Wireshark, & Solarwinds, Dynatrace, Extrahop tool helped for tracking root cause problems. Collect and analyze test device logs using Wireshark, logcat, and tcpdump for setup and test Pass/Fail verification Used Wireshark to troubleshoot servers that were impacted due to vulnerability data to block the proper ports during vulnerability scan to minimize impact such as air flight delays & Tested for the encryption. Part for Risk Management Team for reviewing the Technical documentation its procedures and Standards. Excellent customer management/resolution, problem solving, debugging skills and capable of quickly learning, effectively analyzes results and implement and delivering solutions as an individual and as part of a team. Authorized to work in the US for any employer Work Experience sr. SR. SR. Network Security / Firewall Architect Ameriprise Financial Inc July 2017 to Present Responsibilities:

Researched, designed, and replaced aging Checkpoint firewall architecture with new next generation PaloAlto appliances serving as firewalls and URL and Application inspection. Configuration, deployment and Administration of Checkpoint, PaloAlto Firewalls to manage large scale firewall deployments. Configuring, testing, troubleshooting multiple vendor device platforms like Cisco switching, Juniper, Palo Alto, Checkpoint and Fortigate Firewalls. Configuring rules and Maintaining Checkpoint, PaloAlto & Analysis of firewall logs using various tools. Worked with Palo Alto Panorama management tool to manage all Palo Alto firewall and network from central location.

Adding and removing checkpoint firewall policies based on the requirements. Responsible for the migration of Checkpoint firewall from R77.30 to R80.10 version and making the firewall environment up to date. Administrated checkpoint firewalls of R77.30 and R80.10. Involved in Configuration of Access lists (ACL) on checkpoint firewall for the proper network routing for the B2B network connectivity. FireEye EX Email events, malicious threats, and malware Review IDS Tools (FireEye HX, NX) Suspicious Threat Events, IOC's, Foreign IP Detection Following up the

transmission project solution (Servers DB Hitless protection solution, BB IPMPLS, Ethernet Traffic protection) Deployment and management of the following firewalls: Fortinet 100D, Fortinet 60C, Fortinet 60E, Fortinet 60D, Fortinet 200E (HA), this includes the whole UTM (app control, Web Filter, IPS, DoS, DDoS, etc.Configuring, testing, troubleshooting multiple vendor device platforms like Cisco switching, Juniper, Palo Alto, Checkpoint and Fortigate Firewalls. Building networking racks and installing equipment in accordance with given schematics, such as HP switches, fortinet firewalls, rack safes, PDU's, etc. Upgrading Checkpoint GAIA from R77.30 to R80.10. Troubleshoot firewall and network issues using CLI for all devices managed as well as using GUIs such as: Juniper NSM, Check Point Smartview Tracker. Troubleshoot and monitor Firewall traffics/issues through command-line using CLI commands, GUI interface and Smart Console (SmartView Tracker, SmartLog and SmartView Monitor). Analyze Logs and make necessary network reports using Smart Reporter console application. Using Algosec for the audit of the rules on the firewall and Enhance existing change management system with intelligent network and security automation. Configuring routing protocols OSPF, EIGRP, RIP, MPBGP, LDP and BGPV4 DNS net names and IP management using Men and Mice. Network monitoring, packet captures and troubleshoot traffic passing through Firewall via logs. Join troubleshooting calls to provide visibility to the traffic or data flow. Worked with the DCM security team to review list of IP addresses in-scope for particular migration and record findings. Conducted POCs from start to finish on several Fortinet platforms including Fortinet's Secure Fostered partner relationships to strengthen Fortinet's foothold as a premier network security vendor in the market Perform backup, system upgrades, restore of Fortinet, Checkpoint, Palo Alto and Juniper Firewall appliances, emergency patch application and maintenance. Provided Tier-3 troubleshoot support for all managed devices and supported technologies such as FireEye EX/NX and Checkpoint. Perform backup, system upgrades, restore of Fortinet, Checkpoint, Palo Alto and Juniper Firewall appliances, emergency patch application and maintenance. Create necessary configurations to match the exact data flows that was present prior to the migration Follow-up approved processes for any production changes. Manage Cisco, Sourcefire, FirePower, FireEye, Lastline, Carbon

Black, and Tipping Point. Attend project meetings to understand work that needs to completed for a given week or sprint. 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. Network Security / Firewall Engineer Beckton Dickenson Technologies/HCL, RTP, Durham February 2016 to June 2017 Responsibilities: Experience in Designing, configuring and troubleshooting, security policies, Modular Policy Framework, Routing instances, Zone Based firewalls and implementing different failover mechanisms on Palo Alto & Checkpoint R77 firewalls. Expertise configuring and monitoring Checkpoint firewalls through Smart Dashboard and Smart View Tracker Applications. Successfully replaced Juniper and Cisco Firewall with Checkpoint R77.30. Configuring rules and Maintaining Palo Alto Firewalls & Analysis of firewall logs using various tools. Implemented many number of security policy rules and NAT policy rules on Palo Alto, created Zones, Implemented Palo Alto Firewall interface, Palo Alto IDS and VLAN. Maintain FireEye PX packet capture appliances Maintain FireEye IA, Investigation Analysis system that act as a data visualization system, based on Kibana Palo Alto firewall troubleshooting and configuring policy based on change request, allowing/denying communication between different segments of the network based on requested ports. Algosec: Log collection, Firewall online/ offline Audits; determining risky rules and implement to mitigate/ minimize the risk; Firewall rule search for the refreshing servers using AlgoSec firewall analyzing tool. Navigated through Algosec and Palo Alto, Checkpoint to find risky ports and unused firewall rules to help with firewall audit. Implemented and maintained AlgoSec Firewall Management. Worked on Algosec for firewall rule analysis and firewall rules cleanup. Giving Connection ID for the rules on the Palo Alto and Checkpoint based on the policy and Third party that belongs to. Generating the FireFlow tickets for the rules for which Connection ID already provided and RISK Rating the rules. Fortinet Fortigate 1500C, 3700D, Palo Alto PA-5050 Assisting with investigative discovery of firewall rules of 500 connectors Assisting with documentation of connectors and incorporating them into a larger framework for future automation

Product line manager for FireEye Platforms AX/EX/HX/NX/CMS - email, endpoint and network detention and malware analysis appliances Knowledge and experience BGP, OSPF, ISIS, IPMPLS, QoS, IPv6, Multicast related areas. Knowledge of Juniper environment including SRX/Junos Space. Configured and set up of Juniper SRX firewalls for policy mgmt. and Juniper SSL VPN's Performing firewall optimization using Tufin by removing unused rule, duplicate objects, fully shadowed rules, and disabled rules. Administered and maintained Cisco ASA, Juniper and Checkpoint Firewalls. Maintaining Users and Groups as well as Creation of new Users and Policies. Deployed and manage security controls such as DLP, IPS/HIPS, web content filtering. Configuring and troubleshooting routing protocols OSPF, EIGRP, RIP, MPBGP, and LDP.

Advanced knowledge in TCP/IP suite, security architecture and routing protocols: OSPF, BGP, & EIGRP, IPSEC VPN design connection & protocols, IPSEC tunnel configuration, encryption and integrity protocols. Creating Private VLANs & preventing VLAN hopping attacks & mitigating spoofing with snooping & IP source guard Worked on Fortinet firewall IPSEC and SSL VPN Configuration Analyze Fortinet firewall logs Configure Local accounts in Fortinet Firewall Implementing Security Solutions using PaloAltoPA-5000/3000, Cisco 5580/5540/5520, Checkpoint firewalls R70, R75, R77.20Gaia and Provider-1/MDM. Worked with FireEye, McAfee ePO and SIEM, Riverbed, SourceFire and Vectra Investigation of internal alerts & Performed payload analysis of packets using Wireshark. Analyzed the flow of packets for LAN and Wi-Fi interface on the computer using Wireshark. Analyzed DHCP, DNS, and ICMPv6 and TCP protocol packets. Researched, designed, and replaced aging Checkpoint firewall architecture with new next generation Palo Alto appliances serving as firewalls and URL and application inspection. Hands on experience in creating the policies (vulnerability, anti-virus, wildfire etc) Troubleshooting of protocol based policies on Palo Alto firewalls and changing the policies as per the requirement and as per traffic flow. Implemented zone based firewalling and security rules on the Palo Alto Firewall.

Experience with convert Palo Alto VPN rules over to the Cisco ASA solution. Migration with both Palo Alto and Cisco ASA VPN experience Network & Firewall Administrator BCBS - San Jose, CA November 2013 to January 2016 Responsibilities: Working with engineering team to create,

document, implement, validate, and manage policies, procedures, and standards that ensure confidentiality, availability, integrity, and privacy of information. Implemented Positive Enforcement Model with the help of Palo Alto Networks. Experience with Firewall Administration, Rule Analysis, Rule Modification. Implementing and troubleshooting Firewall rules in Palo Alto Pa-5000 series using Panorama, Checkpoint VSX, R75.40, R76 and R77.20 as per Business Requirements. Configuration of firewall (Palo Alto) access policies, security policies, Global protect VPN, Application & URL filtering, Data filtering and file blocking. Administered and maintained Cisco ASA, Juniper and Checkpoint Firewalls Experience working with Cisco, Meraki, Nexus, Microsoft, VMware, Fortinet, Extreme, and HP technologies Remediation for Palo Alto devices on Rule and URL Filtering. Conducted scheduled reviews regularly in the organization (Firewall-rule sets, VPN). Upgrading the PAN-OS to fix the bugs and any other monitoring issues. Done documentation for Rule Justification for Palo Alto Firewall. Installed and categorized URL filtering categories according to the environment requirements. Installed and configured Nagios XI performance tool in the servers for getting live performance of the servers (like CPU, Memory and Disk Usages). Collaborated Palo Alto App with Splunk for advanced security and analysis. Updating the daily URL Filtering reports for analysis from Splunk Palo Alto APP. Implementing and troubleshooting firewall rules in Checkpoint R75.40 and R77 Gaia as per the business requirements.

Involved in configuration of access-control lists on Juniper and Palo alto firewalls for proper network routing and B2B connectivity. Experience with configuring Virtual Server and Configuring Load balancing methods in F5 LTM. Experience with live packet traffic analysis and reviewing packet captures using Wireshark and tcpdump tools Experience with devices Palo Alto Network firewalls such as security NAT, Threat prevention & URL filtering. Reviewing & creating the FW rules and monitoring the logs as per the security standards in Checkpoint and Net screen Firewalls.

Execute the Incident Management process tasks in adherence with global and local requirements Configuring and troubleshooting Cisco ASA firewalls, Palo Alto and Checkpoint Firewalls. Assist with various duties that will arise including: implementation, configuration, management. Network Security Engineer DhakaTech Limited December 2009 to May 2013 Responsibilities: Maintaining

Checkpoint security policies including NAT, VPN and Secure Remote access, Configuring IPSEC VPN (Site-Site to Remote Access). Maintained Corporate Firewalls & Analysis of firewall logs using various tools. Implementation and troubleshooting of ASA firewall Adding security policies and security rules on checkpoint and ASA firewall. Configuring rules and Maintaining Palo Alto Firewalls & Analysis of firewall logs using various tools. Taking backup of checkpoint configuration, security policies, logs with policy package management, database revision controls, upgrade export and import, snapshot procedure on regular basis. Successfully installed Palo Alto PA-3060 firewalls to protects Data Centre and provided L3 support for routers/switches/firewalls Good knowledge on Juniper SRX240, SRX220 and SRX550 series Firewalls. Responsible for designing and implementation of customer's network and Security infrastructure. Worked extensively in Configuring, Monitoring and Troubleshooting Cisco's ASA 5500/PIX security appliance, Failover DMZ zoning & configuring VLANs/routing/NATing with the firewalls as per the design. Black listing and White listing of web URL on Bluecoat Proxy servers. Configuring routers, switches, WLC, Access Points, Bluecoat Proxy Server, Cisco ASAs, etc. Configured Routing protocols such as RIP, OSPF, EIGRP, MPLS static routing and policy base routing. Log analysis using Checkpoint Smart view tracker and SPLUNK. Configured HSRP and VLAN trucking 802.1Q, VLAN Routing on Catalyst 6500 switches. Managed the F5 BigIP GTM/LTM appliances to include writing iRules, SSL offload and everyday task of creating WIP and VIPs Involved in Troubleshooting of DHCP and other IP conflict problems. Performed Switching Technology Administration including VLANs, inter-VLAN Routing, Trunking, STP, RSTP and Port Aggregation & Link Negotiation. Education Master's Skills Bgp, Cisco, E1, Eigrp, Mpls, Ospf, Ds1, Ds3, T1, Tcp, Tcp/ip, Firewalls, Nagios, Firewall, Siem, Splunk, Frame relay, Igrp, Linux, Unix, Cyber Security, Information Security, It Security, Cybersecurity, Comptia, Information Assurance, Nist, Cissp, Active Directory, security, Vmware, Exchange, VPN Additional Information Technical Skills: Routers 1800, 2500, 2600, 2800, 3600, 3750, 3800, 7200. Cisco Switches 2900, 3500, 4000, 4500, 5000, 5800, 6500, Nexus 2k, 3k, 5kand 7k, MSFC, MSFC2. Routing Protocol (BGP, OSPF, EIGRP, IGRP, IGMP, RIP), Routed Protocol TCP/IP, Multicasting (PIM). WAN Technology Frame Relay, WiSM Module in 6509, X.25,

L2VPN, L3VPN, E1/T1/DS1/DS3,MPLS Operating systems Linux, UNIX, DOS, Windows XP/2007/8, Windows 2003 server and Windows 2008 server Firewalls Check Point R65/R70/R75/R77.20, ISA 2004/2006, Palo Alto PA-500/PA-2K/PA-3K/PA-5K, ASA 5585/5520/5510 SIEM TOOL Splunk (Configured with Palo Alto APP). Performance Tool Nagios XI (Using NSClient++ or NCPA Agent). Algosec Firewall Analyzer

Name: Madeline Perry

Email: garrettjohnson@example.com

Phone: 746-797-6631x5105