Security Engineer Security Engineer Security Engineer - Stemcor Inc Chicago, IL Over 10+ years of experience as a Network Security Engineer in Administration of LAN, WAN and Security Technologies. Experienced in design, installation, configuration, administration and troubleshooting of LAN/WAN infrastructure and security using Cisco routers/Switches/firewalls Configuration of Palo Alto Firewall PA-5k and CMS. Advanced knowledge, design, installation, configuration, maintenance and administration of Checkpoint Firewall R55 up to R77, Secure Platform Installation, VPN. Experience in configuring firewalls Fortinet, firefly. Advanced proficiency in designing, deploying, and maintaining perimeter security devices such as IPS, IDS, Radware, etc. Experienced Checkpoint Firewall, Security and Network Administrator. Good Knowledge on bluecoat Proxy (white listing, blocking URLs, PAC file changes etc.). Analyzed network traffic with Splunk and ArcSight tools on network traffic, firewall (Source Fire defense center) and AV (McAfee) logs. Configuring and managing Aruba Instant Access Points 215, 225 and troubleshoot network connectivity issues. Real-time experience in designing and assisting in deploying enterprise wide Network SSL Security and High Availability Solutions for ASA. Working knowledge with Infoblox appliances such as DNS, DNSSEC, DHCP, IPAM and TFTP. Advanced knowledge in design, installation and configuration of Juniper NetScreen Firewall ISG 1000/2000, SSG series and NSM Administration. Proficient in design, implementation, management and troubleshooting of Check Point firewalls, Check Point Provider-1 / VSX, Palo Alto IDS/IPS modules, Data Center Migration, F5 Load Balancers, Cyber Security and Bluecoat URL filtering & Packet Shaper systems. Proficient level in Voice Gateway & Gatekeepers (H.323, MGCP & SIP) Configured CUCM, Unity, CER, UCCX, VG's, CUCDM, TelePresence (servers and gateways) and 3945 voice gateways and 3750 switches Advanced knowledge in Cisco ASA 5000 series and PIX installation, configuration and maintenance. Upgrading the Imperva WAF and DAM module to the latest released version. Implementation and administration of Juniper WX/WXC devices for WAN Traffic acceleration Technical knowledge & proficiency in system administration, network maintenance, hardware maintenance, OS. Fulfilling routine change requests of Firewall and resolving trouble tickets, maintain and monitoring firewalls using scanning software Nesses

Knowledge of Intrusion Detection, DMZ, encryption, IPsec, proxy services, Site to Site VPN tunnels, MPLS/VPN, SSL/VPN. Juniper, Check Point Cisco ASA, Cisco PIX and Palo Alto Firewalls Administration. Experience in handling Infoblox tool for DHCP and DNS. Experienced in DHCP DNS, AD, NIS, NFS, SMTP, IMAP, ODBC, FTP, TCP/IP, LAN, WAN, LDAP, HP RDP, security management and system troubleshooting skills Experience in managing and migration of large scale enterprise networks, extensive knowledge in developing test plans, procedures and testing various LAN/WAN products and protocols Advanced knowledge in TCP/IP suite and routing protocols, such as OSPF, BGP, and EIGRP Manage network capacity in cooperation with the Network Operations Center (NOC) Worked on implementation strategies for the expansion of the MPLS VPN networks Work Experience Security Engineer Stemcor Inc - New York, NY February 2017 to Present Responsibilities: Design & Deploy Centralized AAA (RADIUS/TACACS+) solution with Cisco Identity Service Engine v2.3 patched with endpoint Profiling & Posturing, BYOD and AD integration with 802.1x. Configured NAD (Access Switches, AP, wLC and Cisco ASA) to work with Cisco ISE for Wired/Wireless/VPN users. CWA for Guest Access. TACACS+ for Device admin. Centralized Policy Enforcement with Policy Set and Conditions studio. Lead the team of engineers for a global Migration project of WatchGuard XT Firewall into Cisco 55XX Adaptive Security Appliances at 35 worldwide locations including North America/Europe/Africa and Asia. Responsible for creation, review, and update of current security policies, process, and procedures and migrate them to Cisco ASA policies with centralized Policy automation & control through Cisco ASA Policy Manager. Design and Implement Cisco FirePower services for Threat Centric. Design and Implement Data Center setup with Cisco Nexus 9k at NJ/London/Singapore location and connect them with Cisco VPN in Full -mesh and Site-to-Site with all 35 worldwide locations along with Fault Tolerance. Complete Design and Implement worldwide wireless solution with Cisco Meraki products and centralized Meraki Cloud based Dashboard management. Configured & Document entire security solution and draw worldwide schematic with Visio along with complete details of LAN (VLAN/OSPF) & WAN (BGP). Network Security Administrator Icahn Enterprises - New York, NY March 2014 to December 2016 Responsibilities: Manage firewall policy lifecycle

process from review, approval, implementation, publishing, verification and maintenance. Configure, manage, and upgrade FW, IDS, IVS, IPS, TAP's, Xstream load balancers (XLB), Encryption and a wide variety of other security products/appliances. Configuring and Troubleshooting Cisco Firewall/ASA, Checkpoint FW, Bluecoat Proxy SG. Installation of Palo Alto (Application and URL filtering, Threat Prevention, Data Filtering, WIldfire). Successfully installed Palo Alto PA-5060 Firewalls to protect Data Center. Deployed and configured VPN appliances including ASA 5500 for site-to-site VPN, DMVPN and Any Connect with LDAP based authentication and Cisco ISR 4451 for AWS, VPNs. Worked on Firemon with Security manager in providing reports or policy status for audits Firewall technologies including general configuration, optimization, security policy, rules creation and modification of Palo Alto and Juniper Firewall. Strong experience in checkpoint firewall and migration from Palo Alto, Juniper and Cisco to checkpoint. Installation of Palo Alto (Web Application and URL filtering, Threat Prevention, Data Filtering) Implemented Zone Based Firewalling and Security Rules on the Palo Alto Firewall. Experience with working on Palo Alto Next-Generation firewalls security profiles and Cisco ASA VPN. Experience on working with migration with both Juniper and Palo Alto Next-Generation. Experience on working with migration with checkpoint and palo alto next generation firewall as well as virtualization of both VSX and VSYS. Day-to-day work involves changes on the Checkpoint Firewall using the Smart Dashboard NGX R70 software and connecting via Smart Center management. Authentication is done using an RSA SecurID. Maintains wireless infrastructure consisting of Cisco and Aruba solutions covering over 12 million square feet of tenant space in a multi-state environment. Performed Checkpoint firewall upgrade of 20 firewalls from R55 to R65.Administered Juniper 50, 200, 500, and SSG 520 firewalls. Managing Unified Call Manager (ver, 8.x) clusters, Cisco TelePresence Manager, Cisco TelePresence Multipoint Switch, IP Phones.

Proficient in Palo Alto Next-Generation Bluecoat web proxy, Splunk Enterprise, Wireshark and various internet tools to assist in analysis. Experience on Cyber Security & Penetration Testing tools such as SQL Map, Appscan, Nmap, Vulnerability Scanner and familiar with shell scripting Implementing and Managing VPN Networks of the Customer through Checkpoint R75 firewalls.

Analyze and review security threats from Firewall (FW), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Antivirus (AV), Radware, and other security threat data sources. Expertise in standardizing SIEM Splunk Forwarder deployment, configuration and maintenance across UNIX and windows platforms. Configured firewalls Fortinet, Palo alto, firefly etc. Worked on Citrix Netscalers for accelerating performance and ensuring that applications are always available and protected. Experience in creating multiple policies and pushing them in to Checkpoint Firewall (Gateways) and hands on experience in managing the Checkpoint Management Server with SPLAT operating system Performed system and network audits against FISMA and FIPS200 regulatory requirements Worked on Cisco 871 DSL, IAD, 1800, 1900, 3900, 7200 series routers Third Party VPN migration from old data center to new data center. Designed and implemented Windows networks and Active Directory (AD) and security group hierarchy based on delegation requirements Implement Cisco Secure Intrusion Detection Sensors, IDSM and CSPM to monitor network activities Cisco IP Telephony: Unified CME, Cisco Call Manager (6, 7, 8), IP Telephony Feature and Cisco Unity/Unity Connection. Call routing, feature, break-fix issues Configure and maintain Windows NT/2000 environment services, including Active Directory, DFS, WINS, DNS, DHCP, file replications and logon scripts. Configuration and maintenance of Juniper Net Screen SSG -550. Experience with working on cisco switches like 2960, 3750, 4500, 6500 Designing, Implementing and Troubleshooting Cisco Routers and Switches using different routing protocols like RIP, OSPF, EIGRP, BGP, ISIS & MPLS L3 VPN, VRF. Implement LAN protocols like STP, RSTP, VTP, VLAN and WAN protocols like Frame relay, PPP, port channels protocols like LACP, PAGP. Implemented VLAN, VTP domain, trunking and Ether Channel on Cisco 5500 switches. Firewall Specialist PG & E Corp - San Francisco, CA July 2012 to February 2014 Responsibilities: Troubleshooting complex CheckPoint issues, Site-to-Site VPN related Performed upgrades for all IP series firewalls from R65-R75. Support for all migrations, upgrades, PCI and SOX audit requirements, and vulnerability assessments Support for all firewalls and related environments Checkpoint firewall upgrade from R55 to R65 for remote sites. Supported Bluecoat proxies for URL filtering and content filtering. Good knowledge of SNMPv3, Syslog, Net

flow management protocols Assisted in troubleshooting complex layer 1, 2 and 3 connectivity using Wireshark protocol analyzer and recommended solution for better performance. Troubleshooting of AQM (Recording Server) issues. Implement SecuRemote VPN for high speed remote access. Monitoring Arcsight tool(SIEM) and managing logs. Troubleshooting and escalating security alerts like malware, Mcafee, Mssql, wintel, Unix, Oracle alerts. Risk assessments where done using Nessus, and Internet scanner, on a monthly basis to help ensure that risks to the network are mitigated in a timely manner. Worked on bluecoat Proxy servers from initial set-up till configuration. Propagate local changes from Infoblox members to master and vice versa using Infoblox grid. Experience on device-based policy for application access, automatically confirm compromised hosts with Palo Alto. Managed Smart Center Checkpoint management server (SmartView Tracker). Managed Checkpoint Firewalls from the command line (cpconfig and Sysconfig) Installing and setting up Firewall Analyzer product to facilitate consulting on an IDS deployment project, using my Cisco Nexus 7k/5k experience to place IDS devices globally. Working and commenting on global firewall polices. Used Palo Alto for Reporting and Logging and to Reduce Risk by Enabling Applications. Migration with both Checkpoint and Cisco ASA VPN experience. Worked extensively in Configuring, Monitoring and Troubleshooting Cisco's ASA 5500 Implemented and troubleshooting the Virtual firewalls solutions in ASA. Providing input on day-to-day security architecture policies and procedures. Firewalls are R65 and R70 clusters. Administration of Juniper firewalls at corporate and remote locations. Developing systems and process to protect, various user groups while accessing public Internet content from malicious hack attacks Maintained, upgraded, configured, and installed Cisco routers, Cisco Catalyst Switches Network migration from OSPF to EIGRP Network Security Engineer Synnex - Fremont, CA October 2011 to June 2012 Responsibilities: Configuring multiple Cisco 6509 with MSFC2, 3500, 2948G-L3 switches, 2600 and 3600 routers, Frame relay, dedicated T1s and ISDN lines Implement network security for remote access Configure and maintain Windows NT/2000 environment services, including Active Directory, DFS, WINS, DNS, DHCP, file replications and logon scripts. Worked on Cyber Security & penetration tools such as AppScan , SQL Map. Configured 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. Responsible for setting up Web Application Firewalls (WAF). Configuration and maintenance of ACL lists on Cisco routers Worked on Cyber Security & penetration testing tool such as Nmap. Responsibility includes regular maintenance, security patch update and troubleshooting Configuring Checkpoint Firewall in IPSO, Secure Platform and GAIA platforms Knowledge of Intrusion Detection, DMZ, encryption, IPsec, proxy services, Site to Site VPN tunnels, MPLS/VPN, SSL/VPN. Knowledge of Juniper environment including SRX, Junos Space and ScreenOS. Administration and management of all firewall environments. Supported F5 ASM and McAfee IPS in an eCommerce environment providing WAF security and IPS for over 90 public financial web applications. Management of each firewall is done remotely and onsite at client sites. Upgrading WAF (Web application firewall) and fixing hot fixes and patches. Managed network IP access via Dynamic Host Configuration Protocol (DHCP). Redistribution of routing protocols and Frame-Relay configuration Network Security Engineer United Nations, NY September 2010 to September 2011 Responsibilities: Worked as a security engineer for migrating the Cisco and FortiGate firewalls to next generation Palo Alto firewalls. Worked with Palo Alto firewalls using Panorama servers and performed changes to monitor/block/allow the traffic on the firewall. Responsible to evaluate, test, configure, propose and implement network, firewall and security solution with Palo Alto networks. Performed security audits on Cisco ASA, FortiGate and Palo Alto firewalls in Network and secured the network by bringing it to the present security standards. Troubleshooting and implementing changes on Cisco, Checkpoint, FortiGate firewalls, F5 load balancers, Blue Coat proxies, and Juniper SSL/VPN devices. Migration of the firewall from Cisco ASA to Palo Alto firewalls using migration tool from PAN. Managed firewall design with network access control, Large Scale VPN deployment, automated firewall Policy deployment utilizing Panorama to build and edit templates for remote sites.

Provided administration and support on Bluecoat Proxy for content filtering and internet access to head quarter, remote site offices and VPN client users. Successfully installed Palo Alto PA-3020, PA-3060, PA-5060 Firewalls to protect Data Centre and provided L3 support for

routers/switches/Firewalls and implemented Zone Based security rules on the Palo Alto Firewall. Scheduling of Weekly scans and monitoring, generating Vulnerability reports and sharing to appropriate groups or owners for Remediation along with recommendations. Load Balancing using F5 Networks Big IP and configured the Automatic policy builder using the deployment wizard tool in Application Security Manager. Created Route maps on F5 BIG-IP GTM to link various VIPs from different F5 BIG-IP LTM to GTM. Performed complete setup of new F5 BIG-IP LTM, GTM and APM device, including license activation, VLANs configurations, Device certificates etc. Performed numerous SSL certificate renewals for customer VIPs, maintaining and renewing of all Load Balancers Device certificates. Performed hardware refresh on existing F5 BIG-IP Load Balancers to replace with new F5 BIG-IP devices and bought the F5 devices into the network in an uninterrupted manner. On a daily basis, worked on clearing existing tickets regarding firewall policies, proxies, weekly policy updates and documenting these events and changes. Expanded Data Loss Prevention (DLP) program to include all the high-risk applications, protocols, platforms, and devices. Responsible for the daily monitoring and investigation of violated Data Loss Prevention (DLP) policies using the Forcepoint Triton Security Gateway. Network Technician Omar Co. LLC - Washington, DC May 2007 to August 2009 Responsibilities: Configuring and troubleshooting multi-customer ISP network environment. Setting up Checkpoint devices, configuring, maintaining and troubleshooting. Perform network security, administration, analysis, and problem resolution for networks, including NT 4.0, Windows 2000, UNIX (Solaris & BSD), CISCO, TCP/IP, and Checkpoint firewalls. Setting up Windows server 2000/2003 as domain controller & adding client machines to domain. Managing Agilent software and configuring it on LAN. Installation and configuration of Thin Client Pc's. Providing technical support to LAN & WAN systems. Provides technical expertise in configuration and troubleshooting of various IP routing protocols including OSPF, EIGRP, and BGP. Education Associate Degree in Specialized Technology in Specialized Technology CHI Institute - Southampton, PA Skills ACTIVE DIRECTORY, CATALYST, CISCO, E1, E3 Additional Information TECHNICAL SKILLS Protocols NAT, VTP, VLAN, TCP/IP, UDP, ARP, NTP, EIGRP, OSPF, RIP, SSL, VPN, HTTP, HTTPS, FTP,

POP3, SMTP, DNS, ICMP Switches Cisco Catalyst VSS 1440/2960/4900/6513 Routers Cisco Routers ASR 1002/2600/3945/7606 Firewalls Palo Alto PA 500/2k/3k/5k, Checkpoint R65/R70/R77/Firewall-1, Cisco ASA Languages C/C++, Java Operating Systems Windows XP/7, RHEL LAN Technologies VLAN, VTP,vPC, Inter-VLAN routing, STP, RSTP, PVST,Active Directory WAN Technologies Frame Relay, ISDN, PPP, ATM, MPLS, exposure to DS1, DS3, OC3, OC12, OC48, NAT, PAT, T1 /T3 & E1/E3 Network Security NAT/, Ingress & Egress Firewalls, VPN Configuration(L2 and L3), Internet, Content, Tenable Network Security, Filtering, Load Balancing, IDS/IPS, URL Filtering, MSS

Name: Matthew Morales

Email: qbailey@example.com

Phone: 349.694.4401x16040