

Sr. Network Security Engineer Sr.Network Security Engineer Sr. Network Security Engineer -
Germania Insurance Topeka, KS 8+ years of experience in planning, design, implementation and
configuration of Network/Security devices Extensive experience with design, installation,
configuration, maintenance and administration of Check Point Firewall R55 up to R77 version,
Secure Platform Installation, VPN. Experience in installing, configuring and troubleshooting Juniper
SSG and SRX series Firewalls. Hands on experience in Installation, configuration, and
maintenance of Palo Alto PA-3k, PA-4K, PA-5K, Cisco ASA 5500 Firewalls. Advanced knowledge
of Cisco ASA and Palo Alto firewalls PA-5K and CMS. Experience in handling and installing Palo
Alto Firewalls with exposure to WildFire feature of Palo Alto Networks. Implemented Zone Based
Firewall and Security Rules on the Palo Alto Firewall using Panorama. Managed URL filtering, File
blocking, Data filtering by Palo Alto firewall. Experience in monitor and analysing network threats
through Palo Alto Panorama; run vulnerability assessment on machines with anomalous behaviour,
monitor firewall for incoming and outgoing threats. Implementing security Solutions using Palo Alto
PA 5020, Check Point Firewalls R75, R77.20 Gaia and Provider-1/MDM. Experience in adding
Rules and Monitoring Checkpoint Firewall traffic through Smart Dashboard and Smart View Tracker
applications. Hands on experience on all software blades of Check Point firewall. Using Smart
Update, User Management and Authentication in Check Point Firewall. Firewall technologies
including general configuration, risk analysis, security policy, rules creation and modification of
Check Point/Nokia Firewall VPN-1 FW-1 NGX R65, R70 & R75 Provider-1/Site Manager-1 R65,
R70.30 & R75.40 Smart Domain Manager command line & GUI. Experience in designing and
assisting in deploying enterprise wide Network SSL Security and High Availability Solutions for ASA.
Monitoring Traffic and Connections in Check Point and ASA Firewall. Juniper Firewall Policy
management using NSM and Screen OS CLI. 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. Assisted in the development
of DLP alerts and IPS alerts to maximize information value from each system. Experience with
IDS/IPS technologies and vulnerability assessments tools & monitoring. Network Security

Monitoring via Cisco Firepower Management Center(FMC). Knowledge of Intrusion Detection, DMZ, encryption, IPsec, proxy services, Site to Site VPN tunnels, MPLS/VPN, SSL/VPN. Auditing and testing of security loopholes through Wire shark. Monitored Network Activity using Cisco Prime 2.2, Splunk, Ops Manager, IPAM, Wire Shark,Tufin SecureTrack, ePo and HIPS.

Virtualization: VLAN, VxLAN, VPLS, PW, GRE. IPSEC, L2TP, EVPN, Link Aggregation, Linux Bridge, OVS, HSRP, VRRP, GLBP. Experience in F5 BiG-IP LTM/GTM Load balancers. Experience with GTM F5 component to provide high availability with providing services across data centers. Experience in configuring, implementing and troubleshooting F5 load balancer in the enterprise network. Provided application level redundancy and availability by deploying F5 load balancers LTM. Experience deploying BIG-IP F5LTM Load Balancers for load balancing and traffic management of business application. Troubleshooting the issues that were raised while upgrading the F5 LTM's from 10.2.3 to 11.3. In depth knowledge of IPv4 & IPv6 addressing and Subnetting.

Experience in Layer 3 Routing Protocol configurations: RIP, OSPF, BGP, EIGRP, MPLS and Cisco ACS protocols like RADIUS and TACACS. Experienced in installation, configuration and maintenance of Cisco Nexus 7K, 5K switches. Extensive experience in layer-3 Routing and layer-2 Switching. Dealt with Cisco router models like 7200, 3800, 3600, 2800, 2600, 2500 and 1800 series, Cisco catalyst 6500, 4500, 3750, 3500 and 2900 series switches. Worked extensively on Juniper MX Series Routers and EX series Switches. Understand the JUNOS platform and worked with IOS upgrade of Juniper devices. Network security including NAT/PAT, ACL, VPN Concentrator. Involved in migration including subnet migration, VPNs migration, network and security device configurations. Experience with handling DNS and DHCP servers. Configuring and managing Blue Coat Proxy Servers. Experience with Bluecoat Proxy and VPN Technologies including B2B and Remote. Provided administration and support on Bluecoat Proxy for content filtering and internet access between site and VPN client users. Worked on Blue Coat Proxy SG to safeguard web applications in extremely untrusted environments such as guest Wi-Fi zones

Authorized to work in the US for any employer

Work Experience Sr. Network Security Engineer Germania Insurance - Brenham, TX December 2016 to Present

Responsibilities Strong hands on and exposure to

Checkpoint&Palo Alto on a regular basis. Primary responsibility for the Core Security of the Network. Managing the entire Network Security Products deployed in the network such as Checkpoint (GAIA R75.40/77.20). Migrated multiple IPsec, site-to-site VPNs from Juniper SRX to Checkpoint. Palo Alto design and installation (Application and URL filtering, Threat Prevention, Data Filtering). Successfully installed Palo Alto PA 3060 firewalls to protect Data Center and provided L3 support for routers/switches/firewalls. Configuring rules and Maintaining Palo Alto Firewalls(PA 3020, PA-3060 and PA 5020)& Analysis of firewall logs using various tools. Configured and maintained IPSEC and SSL VPN's on Palo Alto Firewalls. Configuration of Palo Alto Firewall PA-5k and CMS. Experience with implementing malware protection, policy control, analysing logs and different reports using Palo Alto PA-5020. Monitoring Traffic and Connections in Checkpoint and Palo AltoFirewalls. Reviewing & creating the FW rules and monitoring the logs as per the security standards in Checkpoint and Net screen Firewalls. Configuring & Administration of the Checkpoint Firewall that includes creating Hosts, Nodes, Networks, Static & Hide NAT's. Experience with Check Point Firewall Management station operations. Maintained and Configured Check Point VSX with firewall virtualization. Developed and executed datacentre migration plan for all managed security services such as firewalls, IDS, VPNs and authentication servers with no impact on production environments. Migration from Cisco firewalls to Palo Alto firewalls platforms PA 4000 and PA 500 and PA- 200 firewalls. Experience on Check Point Firewalls NG, NGX, NGX, R61, R65, R70, R75, R77. Checkpoint Firewall upgrade from Checkpoint R65 to Checkpoint GAIA R77. Planning & implementing information security guidelines as per the security standards on the firewalls. Upgrade of Checkpoint firewalls and management servers from Splat R75.30 to Gaia R77.20 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. Configuration and troubleshooting of Site to Site as well as Remote Access VPN on Cisco ASA and Check Point firewalls. Had been part of Cloud project to implement VRFs for IaaS, PaaS, SaaS to segregate the various networks accessing different cloud platforms as required. Implemented Microsoft Azure in the datacentre by

establishing VPNs to production AZURE Cloud, for service hosting (DNS NTP Authentication etc)

Performed configuration and monitoring of iRules on F5 load balancer. Implemented F5 GTM configurations with adherence to company global IT and InfoSec standards and industry best practices. Implementing proxy rules in Bluecoat Proxy SG using blue coat director. Utilized the Blue Coat Proxy, SIEM, SOC, Tuffin, IPS/IDS. Deploying Cisco WSA and Bluecoat Proxy SG (Web Security Appliance) S170 for URL Filtering Policies. Worked on changing global objects and global rules to local objects and local rules for migration project. Environment: Cisco Routers 7600, 2600 and 3800, Cisco Nexus 7k, 5k and 2k, Cisco catalyst Switches 2960, 3560, 4510, 4507, 6509, Checkpoint R75, GAIA R77 and Palo Alto Firewalls PA 3060, 5020, Routing Policies, OSPF, EIGRP, HSRP, BGP, Load Balancer BIG-IP F5 LTM 6500, Sniffers, Resolving tickets, Microsoft Exchange server 2013 and LAN and WAN networks. Network Security Engineer SCAN Health Plan - Long Beach, CA December 2014 to November 2016 Responsibilities Coordinate with network and security team to resolve some issues on Network side. Monitor security events, analyse the results and escalate, when necessary, to the appropriate group for remediation. Experience working on Juniper based EX and QFX series switches, M, E and MX series routers, SRX 220 firewall. Expertise in installing, configuring and troubleshooting Juniper EX Switches (EX2200, EX2500, EX3200, EX4200, EX4500, EX8200 series) and QFX 3500s as Layer 3 switches to enable routing between VLANs. Hands on experience with ACI (Application Centric Infrastructure) with spine and leaf architecture. Train new employees on how to bring up the ACI fabric and Basic configurations of Tenants/BDs/EPGs/VMM Networking and OOB Management configurations of Leaf/Spine Switches. Worked on the migration project of Juniper SSG to Juniper SRX firewalls. Cisco ASA Unified Threat Management System and Endpoint Protection designing. Cisco ASA Firewall Deployment, Upgrade and Administration. Experienced in Cisco Security Gateway appliances. Perform installation, implementation and daily management of Cisco, Sourcefire Intrusion Prevention System (IPS) with FirePower advanced malware protection. Installed and Configured Checkpoint Firewall in Internet Edge. Monitoring the network traffic with the help of Qradar and Cisco IPS event viewer. Performed intrusion detection and intrusion prevention using

Cisco Sourcefire IDS/IPS. Ability to clearly relay technical knowledge to both technical and non-technical people, written and verbally. Enabled STP attack mitigation (BPDU Guard, Root Guard), using MD5 authentication for VTP, disabling all unused ports and putting them in unused VLAN and ensuring DHCP attack prevention where needed. Experience in information gathering, planning, and execution of large and complex network security projects such as migrations and/or upgrades is an absolute requirement. Superior knowledge, skills and experience with Cisco routing hardware, software, protocols etc. Managing and Troubleshooting Checkpoint Security Management appliances (Smart-1 series). Implementing Security Solutions in Juniper SRX and NetScreen SSG firewalls by using NSM. Hands on experience with JUNOS platform and worked with IOS upgrade of Juniper devices. TCP/IP networking and troubleshooting, protocol analysis. Worked on network devices include Cisco routers, switches, VPN, SSL, Cisco ASA Firewall. Validation of Intrusion Detection System and Intrusion Prevention systems (IDS/IPS) of Cisco network security ASA products, Cisco Firepower Management Center. Providing technical security proposals, security presentation, installing and configuring Checkpoint and Palo Alto firewalls, VPN networks and redesigning customer security architectures. Proficiency in configuration of VLAN setup on various Cisco Routers and Switches. Experienced in trouble-shooting both connectivity issues and hardware problems on cisco based networks. Involve in DNS, SMTP and FTP, Network & Security Protocols. Experience with LAN/WAN architecture and IP services. Implementing security rules on firewall. Migrated the firewalls from Crossbeams to Checkpoint. Experience in F5, Cisco ACE 4710 Load balancers. Configuring VLANs, Self IP's & Routes on F5 load balancers. SSL offloading on F5 LTM's worked on both the server SSL profiles and client SSL profiles. Data Center consolidation and migration of network and applications by migrating the F5 LTM. Involved in migrating from F5 Load Balancers to latest A10 load balancers and with rules updating process. Used F-5 Load balancers to increase capacity (concurrent users) and reliability of applications. Black listing and White listing of web URL on Blue Coat Proxy Servers. Creating user accounts in Active Directory for End Users and adding them into ACS Server and adding new devices into ACS Server. Performed in-depth risk analysis and audit of existing firewall rules,

optimized their placement based on factors like usage hits and acceleration. Installed and maintained the security infrastructure having IPS, IDS, security assessment systems and log management and migration to new VPN. Environment: CISCO ASA Firewalls 5510, 5520 and 5505, Juniper SRX 220, Checkpoint Firewall, Sourcefire(IPS), Cisco Firepower, Cisco Catalyst 3550, 3750, 4500 and 6509 switches, Juniper routers M 3200, VLANs, VTP, STP, RSTP, Trunking, RIP, EIGRP, OSPF, BGP, NAT, PAT, VPN, Blue Coat Proxy and DHCP. Network Firewall Engineer Wells Fargo - Charlotte, NC November 2014 to November 2014 Responsibilities Designed, installed, and maintained various WAN technologies and applications connecting remote sites to corporate headquarters. Configured, implemented, and troubleshoot routers and switches with various account settings, permissions, and parameters including security firewalls. Primary responsibility is to design and deploy various network security & High Availability products like Check Point, Cisco ASA and other security products Installed various network hardware including bridges, and hubs to establish communication connections with remote locations. Configured multiple domain name services (DNS), email services (Exchange Server), web, and file transfer protocol services (FTP) for various platforms including line leasing through DHCP servers. Extensively working with Authorization Information System to research current authorizations and debug authorization problems based on the incident in the HPSC Ticketing Tool. Maintains and troubleshoot problems with high speed internet access, DSL, T1 lines and DS0, long-distance telephone service and local telephone services. Design, procure parts and implement networks for LAN & WAN (IPsec, MPLS, Frame Relay, ISDN, and T1/E1/T3/E3 Lease Line). Migrated Distribution switches from cisco 6509 to Nexus 7010. Experience converting Cat OS to Cisco IOS on the Cisco 6500 switches. Experience with deployment of Fibre Channel over Ethernet (FCoE) between the Data Centers using Nexus 5548P Switch. Networking protocols worked with included but not limited to TCP/IP, DNS, DHCP, VPN, Terminal Services, Routing and Remote Access, Network Design, wiring and cabling. Cisco IOS experience on 3600/7200 class hardware in complex WAN environment and experience on Cisco OS and IOS on CAT6500 in a complex data centre environment Hands on experience installing Sup720 for Cisco 6509-E series and its Gigabit

Ethernet port deployment in the core network Configuring IP, RIP, EIGRP, OSPF and BGP in routers. Experience in deploying EIGRP/BGP redistribution and the changing the metrics for the primary and backup. Environment: Cisco Nexus 7K and 5K Series Switches, Cisco 6509, 4500, 3750 series Switches; Cisco 1900, 2900, 2950, 3500 series catalyst switches; Cisco 2500, 2600, 2800, 2900, 3600 series routers, EIGRP, OSPF, BGP, RIP, VPN, IPSEC, Check Point and Cisco ASA Firewall 5585. Network Administrator Prosum, Inc - El Segundo, CA January 2011 to December 2012 Responsibilities Configuring and resolving various OSPF issues in an OSPF multi area environment, implemented, configured BGP WAN routing, converting OSPF routes to BGP (OSPF in local routing). Expertise in maintenance of layer2 switching tasks which advocate VLAN, VTP, STP, RSTP, PVST, RPVST, configuring of ether channel with LACP and PAGP along with troubleshooting of inter-VLAN routing. Packet capturing, troubleshooting on network problems with Wireshark, identifying and fixing problems. Implementing, configuring, and troubleshooting various routing protocols like RIP, EIGRP, OSPF, BGP etc. Performing network monitoring, providing analysis using various tools like Wireshark, Solarwinds etc. Experience working in Datacenter environment, configuration changes as per the needs of company. Configured and performed troubleshooting on link state protocols like OSPF in single area and multiple areas. Application (Layer 7) Firewall. Configuring RIP, OSPF and Static routing on Juniper M and MX series Routers. Redesigned Internet connectivity infrastructure for meeting bandwidth requirements. Configuring, implementing and troubleshooting VLAN's, VTP, STP, Trunking, Ether channels. Configured and managed Cisco access layer routers and switches. Provided support for troubleshooting and resolving customer reported issues. Worked on F5 BIG-IP LTM 8900, configured profiles, provided and ensured high availability. Worked on F5 and CSM load balancers deploying many load balancing techniques with multiple components for efficient performance. Experience with convert Checkpoint VPN rules over to the Cisco ASA solution. Migration with Cisco ASA VPN experience. Involved in designing of LAN (Ethernet) and WAN infrastructure for the new Data Centre Using MS Visio. Configuring VPN for site-site and remote access. Designing and configuring IP address schemes. Associate Network Engineer Pacific Holding Company - Los Angeles, CA June 2009 to

December 2011 Responsibilities Configuration of Access List ACL (Std., Ext, Named) to allow users all over the company to access different applications and blocking others. Perform routine network maintenance checks as well as configure and manage printers, copiers, and other miscellaneous network equipment. Configuring of IP Allocation and sub netting for all applications and servers and other needs throughout company. Troubleshoot the issues related to routing protocols. Installing operating systems, software and hardware on computers. Assisting Junior and Senior Engineers, on-site management of cable-wiring technicians Troubleshoot problems on a day-to-day basis and documented every issue to share it with design teams. Worked with Network Design and implementation teams on various projects across related to Branch, Campus and Data Center. Implemented and maintained various WAN equipment such as Cisco 2800, 3800 and 7200 routers, ASR 1006. Experience working with Cisco 3750, 4948, 2811, 2600, 7200, 6500, series switches. Designing and deployment of Partner IPSEC VPN tunnels. Involved in the configuration & troubleshooting of routing protocols: MP-BGP, OSPF, LDP, EIGRP, RIP and BGP. Configured IP access filter policies. Deploying and decommissioning Cisco switches and their respective software upgrades. Experience with manipulating various BGP attributes such as Local Preference, MED, Extended Communities, Route-Reflector clusters, Route-maps and route policy implementation. Configured CIDR RIP and OSPF routing. Performed Break Fix support through driving to different buildings, identifying the root cause of the hardware issues with switches, routers.

Design, implementation and operational support of routing/switching protocols in complex environments including BGP, OSPF, EIGRP, Spanning Tree, 802.1q, etc. Performing troubleshooting on slow network connectivity issues, routing issues that involves OSPF, BGP and identifying the root cause of the issues. Configure Corporate, Wireless and Lab Devices which including Bandwidth Upgrade, Adding New Devices, Decommissioning the Devices. Troubleshoot the Network Issues onsite and remotely depending on the severity of the issues. Installed, configured and maintain with the latest updates on the 3700, 3800, 7200 and 7600 Cisco Routers and 2960, 3750, 3560, 6500 Switches. Monitoring the network, troubleshooting network problems, implementing changes, provided Cisco IOS. Education Bachelor's Skills BGP (6 years), Cisco (6

years), EIGRP (6 years), OSPF (6 years), VPN (6 years), Network Security, Information Security, Splunk, Cissp, Siem, PCI, It Security, Access Control, CCTV, McAfee, Qualys, Palo Alto, Cyber Security, Nessus Additional Information TECHNICAL SKILLS Firewalls: Checkpoint, Cisco ASA Checkpoint NGX Installation, Juniper SRX firewall, FortiGate, FortiManager mgmt. & dashboard. Command line configuration splat, Rules based policy, Nat rules, IPS and IDS external authentication, multicast, VoIP, Smart view, monitoring, backup & recovery & Cisco ASA Connectivity & Hardware: Cisco 2900, Cisco Catalyst Switches SRW 300, 1900, 2900, 6500, 3500, 3700, 4500, Cisco ASA 5500, Cisco WLC 2500, Cisco Nexus 7k, 5k, 2k Juniper M320, T640, MX960, EX4500, QFX 3500 M10i. Routers: Cisco routers (7600, 9000), Cisco Router 7200, 3700, 3600, 2800, 1600, 800 series, Juniper Routers like, M320 and MX480, MX960, J4350, J6350 Routing Protocols: RIP, RIPv2, OSPF, IGRP, EIGRP, BGP, IBGP, Static Routing Switching Technologies: VLAN, VTP, HSRP, VRRP, GLBP, Stacking, STP, Port-fast Network Technologies: CDP, Access Control List (ACL), Network Address Translation (NAT), Port Address Translation (PAT) Security Technologies: IPS/IDS, FirePower, Sourcefire, Firewall, VPN, Tunneling, ASA, Palo Alto Firewalls 500/2k/3k/5k, Juniper Netscreen 550, Juniper SRX650, IPSEC, GRE over IPsec, DMZ , Load Balancer F5 BIG-IP LTM 6900 series, GTM Monitoring Tools: Wireshark, SolarWinds, SNMP, Syslog, Nagios, OpManager Wireless LAN SonicWALL Firewall, Checkpoint Firewall Link Aggregation Groups (LAG).

Name: Michael Hall

Email: nicole01@example.net

Phone: 3212538752