Senior Network Security Engineer Lead Senior Network Security Engineer Lead Senior Network Security Engineer Lead - Conceras Inc Boyds, MD   U.S citizen with outstanding certifications which include Cisco Certified Network Associate (CCNA, Cisco Certified Network Professional (CCNP) Proven track record solving IP network issues in timely and cost efficient manner while maintaining client service level agreements (SLA).   Consistent in building strong business relationships with both clients and coworkers.   Strong leader with experience in training and advising technical groups on best practices.   Excellent communication, problem solving and interpersonal skills. Work Experience Senior Network Security Engineer Lead Conceras Inc - Washington, DC November 2016 to Present   Working as a Lead Network/Security Engineer in Department of State.   Builds, designs, tests and deploys parameter security systems to include firewalls and proxy devices Responsible for firewall rule changes by process that includes analysis of request, security recommendation, change control documentation and obtaining approval for implementation. Facilitates system implementation planning, providing review of firewall rules and security risk analysis.   Conducts troubleshooting of firewall and network application issues, providing root cause determination and recommend resolution options. Manage vendor ticket, information gathering, and troubleshooting in the event of a platform issue   Plans, documents, and implements hardware and software refresh and upgrade of Palo Alto perimeter devices.   Conducts periodic firewall rule set review and auditing for standards and use.   Competence with Linux and firewall command line interfaces.   Creates and maintains standard operating procedures and guides for new and/or existing perimeter hardware and software.   Attends weekly teleconferences, onsite meetings, and participates in working groups, as related to constant changing security environment.   Support outbound email traffic and DNS traffic through E3 Einstein (DHS) inspection suites.   Configure, manage and deploy the DMZ zones for various server farms handling agencies traffic via Vsys on Palo Alto firewalls and contexts on Cisco ASA firewalls.   Perform traffic analysis via Wireshark and Tcpdump file.   Develop high level and detailed network diagrams on Visio.   Perform application/Content ID and URL filtering on next generation Palo Alto firewalls as per the department policy.   Plan and engineer migration plans for next generation firewalls and network infrastructure

devices.   Deploy and troubleshoot Cisco Nexus routers and A10 appliances for SSL intercept traffic.   Handle daily operational issues on the network and security boundary in a 24x7 environment   Troubleshoot all network and security related issues on Cisco IronPort's, StoneGates, Palo Alto and Bluecoat appliances.   Engineer new security and network solutions as per customer requirement.   Engineer and maintain multiple Bluecoat proxy appliances for agency wide internet traffic Senior Network Security Engineer Lead GDIT - Germantown, MD April 2014 to November 2016   Worked in the cyber security operations division at Department of Energy. Configure, support and maintain Palo Alto firewalls on ISP TIC (Trusted Internet circuit) boundary. Actively work in the Incident Response team to address emergency requests.   Supported the Trusted Internet Connection (TIC) operations division for Department of Energy in a 24x7 environment.   Address and resolve various vulnerabilities and audit findings on different firewalls and proxy appliances.   Engineer and maintain multiple Bluecoat proxy appliances for agency wide internet traffic.   Support the Trusted Internet Circuit (TIC) with all security measures with URL and application layer filtering on NextGen firewalls.   Engineer firewall changes on Cisco ASA's and Cisco FWSM modules based on best practices.   Supported the routing and switching domain on enterprise network by providing industry standard Cisco best practices.   Develop IP address scheme for Server farm and DMZ zones. Segregated networks based on function and customer requirements.   Interacted with various customers for outstanding issues and provided outstanding customer service.   Addressed and resolved various vulnerabilities and audit findings on Cisco routers and security appliances.   Monitor operability of the TIC environment for unplanned outages and alarms. Reported the chain of command for any incidents   Followed stringent incident response procedures as per requirements   Develop detailed standard operating procedures (SOP's) for all network devices.   Provide training to Tier1 and Tier 2 team to mitigate various security threats.   Provide reports on the current infrastructure status and ticketing system. Engage different teams in the department to deliver/solve various network connectivity requirements as per industry standards.   Resolve tickets for team in order to meet defined Service Level Agreement (SLA   Perform log analysis on firewalls and via Wireshark PCAP's and system logs.

Troubleshoot and resolve any connectivity or firewall issues with various DOE departments. Create and modify Python Scripts to extract logs from Syslog servers. Engage different teams in the department to deliver/solve various network security requirements as per industry standards.

Senior Network Engineer Lockheed Martin - Rockville, MD July 2013 to April 2014 Supported Operations/Engineering for Department of Justice datacenter. Planned and developed a test bed for migrating department's core infrastructure from Cisco 6513 to Nexus 7010's. Major routing protocols like BGP, OSPF and MPLS are involved in emulating production environment on test bed for successful migration. Engineered and developed a test bed for site to site VPN traversing the trusted internet circuit (TIC) stack. Implemented and coordinated internet circuit migration from an OC12 to a 1G circuit on the edges. Deployed configuration changes and performed maintenances on MPLS L3VPN, BGP and IPSEC VPN technologies deployed in the TIC infrastructures. Maintain and upgrade the Cisco ASR 9000 and 1000 routers as per requirement. Troubleshoot BGP, MPLS L3 VPN and IPSEC VPN issues with different customers. Support Trusted Internet Circuit (TICAP) operations for entire department of Justice Internet traffic. Configured and maintained Fortigate (Fortinet) and Stonegate firewalls policies as per customer requirements. Perform Internet Protocol (IP) engineering support services to maintain the core IP network convergence. Engineer and modify load balancing requirements on Cisco ACE modules to support different DOJ component requirements. Work hand in hand with security team to address/analyze and assess known security vulnerabilities and purposing industry standard best practice solutions. Support Cisco firewall switch module (FWSM) operations as per agency requirements. Develop detailed standard operating procedures (SOP's) for all network devices as per requirements. Responsible for drafting procedural documents as guidance for deploying new network components, and executing problem resolution steps which meet the change management process. Introduce new switches and routers in the network with full redundancy based on hardware and software. Prepare network diagrams and drawings on Microsoft Visio for project implementation and test bed scenarios. Resolve network related issues and tickets. **Senior Network Engineer** Computer Sciences Corporation - Washington, DC September 2008 to May 2013 Worked with Pension Benefit

Guaranty Corporation (PBGC) federal site in Washington DC to support network operations for client.   Created an in-depth engineering assessment of the existing deployment and implemented an engineering plan to bring the backbone into industry and vendor's best practices   Engineered and migrated Bluecoat proxy environment from explicit to transparent deployment addressing various security audit findings.   Engineered and Migrated entire client data center from Legacy Cisco 6500 switches to Cisco Nexus data center architecture.   Migrated Bluecoat proxy SG510 to Bluecoat SG9000 proxies with HA redundancy to mitigate single point of failure events. Implemented and coordinated Trusted Internet Connections (TIC) circuit installs at client sites. Stringently follow ITIL processes implemented in PBGC for change management and actively prepare and submit RFCs (Request for Change) for upcoming network changes. Tasks include replacing defective Cisco 6500 switch blade, IOS upgrades, configuring port-channel load-balancing, Layer 3 links and configuring routing and switching on distribution and core layer devices.   Migrated legacy network infrastructure from a flat OSPF design to a STUB OSPF design to enhance performance in the network.   Effectively minimized the spanning-tree diameter within the network as per Cisco best practices.   Key contributor in implementing and supporting routing, switching in LAN and WAN environment in accordance with specified customer requirements. Consistently upgrade network gear and IOS on all end of lifecycle devices.   Designed and implemented an efficient IP address scheme within the network utilizing VLSM, Subnetting and CIDR for optimal network performance and aggregation.   Segregated the network on DMZ, external and internal interfaces on Cisco ASA devices. Manage security policies and global objects on Cisco ASA appliances as per requirement in the network. Successfully upgraded OS on Cisco ASA devices as required.   Responsible for drafting procedural documents as guidance for deploying new network components, and executing problem resolution steps which meet the change management process   Configure and maintain Bluecoat SG510 gateways for all HTTP and HTTPS traffic traversing the PBGC network. Effectively update the Visual Policy manager (VPM) as per required access by the client. Periodically upgrade the bluecoat devices to desired feature set OS level as required.   Assisted in designing and introducing basic QOS in the network through

Riverbed appliances for increased performance on mission critical application throughout PBGC which spanned multiple sites. Assisted in setting and migrating windows based RSA server to new RSA appliances with upgraded OS to support two factor authentications within the organization as per security requirements. Maintain and monitor RSA appliances for configured agents and users which comprises of token based authentication. Worked in setting up and configuring load balancing requirement for various internal applications on Cisco CSS 11500 and Brocade Switches.

Prepare data network diagrams and drawings on Microsoft Visio to document and assist in communicating current operation status of networks. Monitor and maintain performance of Juniper SA 6500 appliances for SSL access into the organization from external network. Monitor bandwidth and network activity by analyzing information provided by Scrutinizer net flow to ensure both efficient and effective network operation. Lead and performed network testing for all upcoming agency requirement. Tasks include, but are not limited to, acquiring hardware products from vendors, and testing several layer 2 and 3 functionalities, such as, switch stacking, link aggregation (LACP), 802.1q Trunking, VLANs , access control lists (ACLs), DHCP, SNMP and various spanning-tree (RSTP, MSTP), routing (RIPv2, OSPF), and routing redundancy (VRRP, HSRP) protocols. Effectively configure Cisco Nexus 7010, Nexus 7018, 6500, 4500, 3750 and 3550 switches with appropriate Vlans, Trunks and layer 3 interfaces as required in production environment. Coordinate change control process with change management groups to ensure proper network, application deployments, and problem resolutions were delivered on time, in scope.

Assisted in setting up and configuring Remote Authentication Dial-In User Service (RADIUS) on RSA Server. This also includes disabling Telnet, HTTP, and Cisco Discovery Protocol (CDP) services, enabling Secure Shell (SSH), and configuring ACLs per IA regulations. Perform monitoring and maintenance on all network elements which include Cisco 6500, 4500, 4000 switches; Cisco 3750, 3500, 2900 switches; Cisco 3700, 3600, 2800, 2600, 1600 routers, and IP networks, protocols to include but not limited to: TCP/IP, BGP, IGP, OSPF, EIGRP, Spanning-Tree, SNMP, SSH, IPSec, 802.1q. Manage and maintain Lucent QIP for IP Address allocation and RSA server for all authentication issues. Resolve tickets for networking team in order to meet defined

Service Level Agreement (SLA). Network Engineer Malviya Inc - New York, NY November 2006 to June 2008 USA.   Provided technical support on data networks and implemented approved course of action.   Assisted in implementing and maintaining networks such as LAN, WAN, in accordance with specified requirements.   Utilized Wireshark (Ethereal) to capture and filter TCP/IPdata for troubleshooting purposes with fellow IT members.   Performed network configurations on switches and network application servers to meet the requirement.   Effectively configured Cisco 3550 access layer switches with appropriate Vlans, Trunks in production environment.   Analyzed frequent network problems and consulted senior network staff to resolve networking issues.   Worked on network issues such as; packet loss, loss of connectivity, routing failures and troubleshoot using industry standard methods such as Ping to test circuit connectivity and Trace to show traffic path to device or destination.   Performed IOS upgrade and password recovery on all Cisco routers and switches when required.   Supported personnel with network install and troubleshooting efforts in the network.   Install and configure Windows Server 2003 active directory on servers. Network Administrator Indoswift Consultants - Delhi, Delhi February 2006 to September 2006 India   Created and maintained user accounts in a Windows 2003 domain using Active directory on Domain controllers.   Responsible for administration of network, help desk, hardware inventory, software inventory.   Configured AD system policies and group policies   Maintained basic data network hardware and systems; escalated network and hardware matters of significance to appropriate groups.   On a daily basis, responsible for devising wiring solutions using CAT 5.   Provided technical support and assisted in maintenance of network.   Installed approved software, assisted end-users with the software, and performed minor PC repairs. Network Technician First Call BPO - Delhi, Delhi January 2004 to February 2006 India   Provided technical tier 1 and tier 2 support to customers on Cisco router and switches.   Escalated the technical queries to the right department.   Documented every issue in order to facilitate record management.   LinkedIn Profile - www.linkedin.com/pub/gursaran-abott/10/81a/976/   Education   Bachelors   in   Engineering   in Engineering Board of technical education Skills Active directory, Cisco, Firewalls, Networking, Bgp Links http://www.linkedin.com/pub/gursaran-abott/10/81a/976 Additional Information TECHNICAL

PROFICIENCIES   Networking: Cisco Routers and Switches.   Bluecoat Proxy SG gateways.

Splunk   Cisco Nexus (NX-OS).   Palo Alto   Cisco IronPort's   A10   RSA appliances.   Riverbed

2050, 6050 and CMC Appliances.   Juniper SSL VPN SA6500 appliances.   CiscoWorks.   Routing

Protocols (RIP, OSPF, BGP, IGRP, IS-IS AND EIGRP).   Switching Technologies (Vlans, Trunking,

VTP & STP).   Access Lists.   IP Addressing (Subnetting & VLSM).   Active Directory Windows

2003 Server (AD).   Network Address Translation (NAT).   LAN/WAN (Ethernet/ Frame Relay)

Cisco Pix and ASA Firewalls and VPN.   MYSQL   Python   Fortigate and Stonegate firewalls

IPv6

Name: Gregory Mooney

Email: calebraymond@example.net

Phone: (904)594-8600x9783