**Akshaya K**

**akothlap@gmail.com**

**703-594-6362 , Fairfax, VA**

**Professional Summary:**

* Network Security Engineer with Over 8+ years of experience in testing, troubleshooting, implementing, optimizing and maintaining enterprise data network and service provider systems.
* Implementation, Configuration and Support of Checkpoint (R75, R77.30, R80.10 and R80.20), Juniper Firewalls (SRX5400, SRX5600and SRX5800), Cisco Firewalls (ASA 5505, 5506-X, 5585), Palo Alto Networks Firewall models (PA-2k, PA-3k, PA-5k and PA-7k).
* Provide scalable, supportable TCP/IP security solutions along with expert TCP/IP network designs that enable business functionality.
* Excellent Hands on experience with Cisco ISE and the Migration of Wireless and TACACs to ISE
* Good knowledge on Endpoint incorporates a rules-based firewall, as well as an anti-malware technique
* Worked on F5 LTM/GTM, BIG-IP, load balancing, I Rules and WAN acceleration.
* Administration, Engineering and Support for various technologies including proficiency in LAN/WAN routing, switching, security, application load balancing and wireless.
* Working experience on tools and devices like Gigamon, Sourcefire, Fire eye, Aruba, Cisco ASA, Cisco ISE.
* Experience in creating User/Group Accounts and attaching policies to User/Group Accounts using AWS IAM service.
* Provide ISE deployment services for migration of users from Cisco NAC to Cisco ISE platform for the following locations.
* Knowledge of web application firewalls and data loss prevention technologies.
* Configuration and troubleshooting of CISCO & ARUBA wireless devices
* Worked on Juniper Net Screen Firewalls NS50, SSG 550M, SSG520M, ISG 1000, ISG 200 and Cisco PIX 535, 520, 515, ASA -5500 and 5505.
* Responsible for Checkpoint and Cisco firewall administration across global networks.
* Expert Level Experience in Cisco ASA, Fortinet, PaloAlto, VMware NSX, Check Point and Juniper SRX/Netscreen Firewalls
* Configured and deployed the NGFW Firewall Features in Fortinet, like App control, Web Filter, FSSO, Proxy, and DNS, PS/IDS.
* Review requirements and migrate clients ’s application and servers to either Azure or on-premise from old Datacenters.
* Troubleshoot and deploy servers in Azure
* Responsible for deploying Palo Alto firewall in one datacenter and Azure Environment.
* Network connectivity design for AWS and Azure connectivity with best security practice including micro-segmentation, transport encryption and complete Account/VPC/VNET/AZ/Subnet design using AWS Transit Gateway & Transit Hubazur.
* Worked on Cisco Catalyst Switches 6500/4500/3500 series.
* Policy development and planning/programming on IT Security, Network Support and Administration.
* Experience in Configuring and Troubleshooting BIG-IP F5 LTM Load Balancer.
* Experience in analyzing security logs generated by Intrusion Detection/Prevention Systems (IDS/IPS), firewalls, network flow systems, Anti-Virus and/or other security logging sources.
* Monitor SIEM and IDS/IPS feeds to identify possible enterprise threats. Actively investigate, respond to and remediate security incidents.
* Experience in implementation of F5 GTM based on topology load balancing methods.
* Experience in migration of data to cloud environment. Good working knowledge of Azure and AWS.
* Experience with Bluecoat Proxy servers, LAN & WAN management.
* Excellent knowledge in Routing, Switching, Firewall and Gateway technologies, system design, wireless design, data network design, capacity management and network growth.
* Experience in working with Cisco Nexus Switches and Virtual Port Channel Configuration.
* Black listing and White listing of web URL on Blue Coat Proxy Servers.
* Provides management level reporting of firewall and Intrusion Protection System (IPS) activity on a periodic basis.
* Experience in installing, configuring, and maintaining Cisco Switches (2960, 3500, 3750, 3850, 4500, and 6500) in enterprise Environment and Nexus 2k, 3k, 5k, 7k and 9k in Data Center Environment.
* Expertise in installing, configuring and troubleshooting Juniper EX Switches (EX2200, EX2500, EX3200, EX4200, EX4500, EX8200 series).

**Education:**

* B.Tech in EEE from JNTU Hyderabad , 2013

**Certifications:**

* Cisco Certified Network Associate (CCNA)
* Checkpoint Certified Security Administrator (CCSA)
* PCNSA and PCNSE \*

**Professional Experience:**

**Afees, Remote Jun 2020 – Present**

**Sr. Network Security Engineer**

**Responsibilities**:

* Experience in creating multiple policies and pushing them into Checkpoint Firewall (Gateways) and hands-on experience in managing the Checkpoint Management Server and Gaia operating system.
* Experience working with Palo Alto firewalls managed through Panorama management platform.
* Configure High Availability on Palo Alto firewalls.
* Configured High availability, User ID on Palo Alto firewall.
* Palo Alto design and installation (Application and URL filtering, Threat Prevention, Data Filtering).
* Configured and maintained IPSEC and SSL VPN's on Palo Alto, Cisco ASA Firewalls.
* Working with the rule base and its configuration in Cisco ASA, Palo Alto and Checkpoint firewalls.
* Configuring, Administering and troubleshooting the Checkpoint, Palo Alto and ASA firewall.
* Configured, implemented and troubleshooting issues on Checkpoint R80.40 Gaia, Cisco ASA 5540, 5000 series firewalls for the client environment.
* Configure all Fortinet Networks Firewall models (100E, 200E, 600D, 900D, 1500D, 3980E, 5001E etc) as well as a FortiManager to manage large scale firewall deployments and FortiAnalyzer to collect logs from all FortiGate firewalls.
* Configuring and Implementing Security rules as per the business needs in Palo Alto Firewalls, Fortigate Firewall, Cisco ASA Firewall and Juniper SRX.
* Managed the security infrastructure of the service provider which includes Fortinet Firewalls, Cisco ASA’s, Juniper SRX, and PaloAlto.
* Provide support and for Tier-3 firewall architecture, which includes Fortigate, Juniper, Cisco ASA and Palo-Alto firewalls.
* Contribute to the development and overall strategy of the penetration testing program
* Manage project task to migrate from Cisco ASA firewalls to Palo Alto firewalls using Expedition tool.
* Defining, tracking and maintaining the standard baselines and configuration sets of security devices and implementing industry best practices with regards to **Firewall, IDS/IPS, IPsec VPN, SSL VPN**.
* Modify pilot ISE environment for production scaling and performance
* Work closely with the team and with cross functional (Security and telecom) teams as required.
* Resolve tickets submitted to the networking team on day-to-day basis and participate in monthly on-call rotation schedule.
* Worked on projects like configuring access points on the Controller and Cisco Prime for entire Bronson Battle creek buildings.
* Manage S2S VPN giving access to remote tunneling using cisco ASA firewalls including troubleshooting end user VPN issues as required.
* Submitted change control to software upgrade entire Bronson wireless network controllers.
* Worked with Bronson Vendors like Patient point to ensure client connectivity as required.
* Managed the network using SNMP based solutions using Solarwinds.
* Designed and configured Azure Virtual Networks (VNets), subnets, Azure network settings, DHCP address blocks, DNS settings, and security policies and routing.
* Works with client engineering groups to create, document, implement, validate and manage policies, procedures and standards that ensure confidentiality, availability, integrity and privacy of information.
* Researched, designed and replaced aging Cisco ASA firewall architecture with new next generation Palo Alto appliances serving as firewalls and URL and application inspection.
* Executing RADIUS pre-deployment tasks like ISE setup, loading templates into Cisco Prime.
* Performed site refreshes on Cisco switching and Aruba wireless infrastructure at several locations.
* Worked on VPN configuration, routing, NAT, access-list, security contexts and failover in ASA firewalls.
* Configured IPSec VPN (Site-Site to Remote Access) on Cisco ASA (5540) series firewalls.
* Deployment of Cisco ASA firewalls and migration of end of life ASA firewalls to New ASA firewalls
* Cisco Firewalls include ASA 5585x, 5580, 5550 Series Hardware managed through CLI, ASDM as well as CSM.
* Responsible for maintaining availability, reporting and communication of the SIEM between it, its event-sources and the endpoints.
* Configuring & Administration of the Checkpoint Firewall that includes creating Hosts, Nodes, Networks, Static & Hide NAT's.
* Experience with configuring WAF, P2S/S2S VPNs, Azure Firewalls, Application Gateways, NSGs, VNets, and VMs.
* Contributed and collaborated with multiple Azure Teams to resolve customer outages.
* Support Citrix NetScaler F5 platform, configuring, implementing, & troubleshooting Citrix NetScaler VIP configuration with health check, policy configurations Access Gateway, & content switching configuration solutions.
* Coordinate and evaluate vendors and associated products/tools in facilitating the Penetration Testing initiatives
* Defined AWS Security Groups which acted as virtual firewalls that controls the incoming traffic and configured the traffic allowing reaching one or more AWS EC2 instances Virtual private cloud (VPC), subnets, Internet Gateways.
* Involved in the deployment and decommission of VLANs on core ASR 9K, Nexus 7K, 5K and its downstream devices.
* Configured EIGRP routing and BGP route maps to allow traffic from subnets out to the core to Datacenter on the ASR 1002 devices.
* Implementation and configuration of Cisco L3 switches 3750, 4500, 6500 in multi VLAN environment with the use of inter-VLAN routing, dot1Q trunk, ether channel

**Con Edison, New York, NY May 2017 – June 2020**

**Network Security Engineer**

**Responsibilities**:

* Implementing Security Solutions using PaloAltoPA-5000/3000, Cisco 5580/5540/5520, Checkpoint firewalls R77.30 Gaia and Provider-1/MDM.
* Configuration and administration of firewalls, which includes Checkpoint, Juniper and Cisco ASA firewalls.
* Configured and maintained rule sets in the firewalls and updated them on the daily basis.
* Knowledge of Cisco ASA firewall, VPN, GRE over IPSec tunnel configuration and Route-maps.
* Configuring High Availability using Cluster XL on Checkpoint as well as VRRP and monitor the Sync status for state full replication of traffic between active and standby member.
* 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.
* Configuration and upgrading the IOS in the FortiGate firewalls, PaloAlto, Cisco ASA, Juniper SRX and Pulse Mag Devices.
* Configuring and deploying the Fortigate firewall. And managed by Forti Manager, Deployed Forti authenticator and Analyzer.
* Design, configure, maintain and administer on-prem / Azure cloud hybrid network and related computing environment using HP G5-G9 Server hardware, Azure Vnet, Azure VM’s,Azure DR VM’s, Azure VPN, Cisco ASR1001 Router, Cisco 2960/2960G switches, Windows 2008, 2008R2, 2012, 2012R2 server OS, SonicWall NSA 4600 firewall, assorted HP LaserJet Networked printers, Xerox Docucolor printers (including Fiery server), a multitude of server applications (listed below), and assist with all desktop configurations.
* Configured and deployed the NGFW Firewall Features in Fortinet, like App control, Web Filter, FSSO, Proxy, and DNS, IPS/IDS
* Implemented IPSEC Site-to-Site in Fortigate Firewall, Cisco ASA.
* Configured & maintain SSL VPN in Fortigate and Juniper Pulse secure MAG’s.
* Configuration, Troubleshooting and Maintenance of Fortigate, Cisco ASA, Juniper SRX, Pulse MAG.
* Researched, designed and replaced Checkpoint firewall architecture with new next generation Palo Alto PA3000 and PA5000 appliances serving as firewalls and URL and application inspection.
* Extensive knowledge of and experience configuring and troubleshooting layer 3 routing protocols (EIGRP, OSPF, RIP, BGP) and High Availability on Cisco devices.
* Designed AWS Cloud Formation templates to create custom sized VPC, subnets, NAT to ensure successful deployment of Web applications and database templates.
* Vulnerability scanning using IBM Endpoint Manager & Nessus
* Vulnerability security patching using IBM Endpoint Manager, SCCM & WSUS
* Responsible for the deployment and associated tasks for the implementation of the
* Tanium Endpoint Security and Systems Management product.
* Configuring rules and maintaining Palo Alto Firewalls& Analysis of firewall logs using Panorama.
* Successfully installed Palo Alto PA-3000/PA-5000 firewalls to protect Data Center and provided L3 support for routers/switches/firewalls.
* Configured and maintained IPSEC and SSL VPN's on Palo Alto Firewalls and also implemented Zone-Based Firewall and Security Rules on the Palo Alto Firewall.
* Exposure to wild fire feature of Palo Alto.
* Configuration and Maintenance of Cisco ASA 5540 series firewalls.
* Hands on Experience with Cisco Wireless Controllers 5500's and 2500's and coming to access points, worked on 3700's, 3500's and 1142 access points.
* Configured and installed Cisco routers 2500, 2600, 3601 and 4000 series. 2950 Switches & Link sys wireless access points.
* Configuring and install hardware and software required to conduct network penetration testing.
* Configure Syslog server in the network for capturing and logs from firewalls.
* Provided tier 3 support for CheckPoint and Cisco ASA Firewalls to support customers, Backup and restore of Checkpoint and Cisco ASA Firewall policies.
* Configuring and troubleshooting site-to-site IPSEC VPN tunnels using Cisco ASA 5540 for third-party connectivity.
* Installed and configured a variety of Cisco devices like Cisco Routers (1841, 1900, 2600, 2800, 3800, ASRs and more), Cisco switches (3560, 3750, 4507 catalysts, 6500 catalyst Switch and more) and Nexus 7000 series, Nexus 5000 series, Nexus 2K Fabric Extenders and F5 appliances.
* Applied knowledge of Ethernet switch and router configuration to configuration/design MPLS connections.
* Understanding of Layer2/3 VPN's, MPLS, Metro Ethernet and LAN switching.
* Creating object, groups, updating access-lists on Check Point Firewall, apply static, hide NAT using smart dashboard.
* Installed and configured high availability Big IP F5 LTM and GTM load balancers like 6600, 6800 to provide uninterrupted service to customer applications and monitoring the availability.
* Identified opportunities for implementation of network best practices, particularly F5 load balancer implementations.
* Configuring F5 Load Balancers: Adding virtual IPs, nodes, pools and health monitoring.
* F5 Big IP iRule programming and troubleshooting.
* Working with different teams to gather info for the new request and troubleshoot for any connectivity issues by capturing traffic using TCPDUMP and smart view tracker.
* Worked on VPN configuration, routing, NAT, access-list, security contexts and failover in ASA firewalls.
* Deployment and Management of Bluecoat proxies in forward proxy scenario as well as for security in reverse proxy scenario.
* Worked on Blue Coat Proxy SG to safeguard web applications in extremely untrusted environments such as guest Wi-Fi zones.
* Performing URL filtering and content filtering by adding URL’s in Bluecoat Proxy SG’s.
* Working on the network team to re-route BGP routes during maintenance and FW upgrades.
* Running vulnerability scan reports using Nessus tool.
* Use of Citrix NetScaler for the application delivery control.
* Configure B2B VPN with various business partners and 3rd parties and troubleshoot VPN Phase 1 and Phase 2 connectivity issues including crypto map, encryption domain, psk etc.
* Provided administration and support on Bluecoat Proxy for content filtering and internet access to primary, remote site offices and VPN client users
* Follow information security policies, methods, standards, NIST standards and practices to organize information systems, IT reference material and interpret regulations.

**Citi Group, Irving, TX Jun 2015 – May 2017**

**Network Security Engineer**

**Responsibilities**:

* Day-to-Day work involves scheduling firewall policy provisioning and working with users to identify connectivity related issues and troubleshoot using both Smart Utilities and CLI.
* Managing and administering Juniper SRX and Checkpoint Firewalls at various zones including DMZ, Extranet (Various Business Partners) and ASZ and internal.
* Implementing Security Solutions in Juniper SRX and Net Screen SSG firewalls by using NSM.
* Juniper Firewall Policy Management using NSM and Screen OS CLI.
* Maintained the following Cisco platforms 7600, 7500, 7200, 7000, 3560, 2900, 2801, 2000, ASA5500, Catalyst 6500, 4500, 3560 and 2900.
* Design, configure and troubleshoot FortiAnalyzer, Fortimail, Fortiweb, Fort client, Forti DDOS, Forti sandbox, Forti SIEM, Forti authenticator and Forti ADC.
* Utilize FortiManager, Forticlient and FortiAnalyzer to maintain and optimize FortiGate firewalls.
* Incorporated web-filtering and intrusion prevention solutions for Fortinet Clients in order to meet surf control policy and industry standards
* Configured and utilized many different protocols such as OSPF, ISIS, BGP/MP-BGP, OER, MPLS, LDP, Multicast, IPv4/IPv6 protocols.
* Utilized knowledge of Spanning Tree Protocol, BGP, MPLS, OSI model layers 1-2 to create network layouts.
* Daily technical hands-on experience in the configuration, troubleshooting of Juniper SRX firewalls as well as experience working directly with customer in a service/support environment.
* Troubleshooting Firewall Connectivity related issues using Smart view tracker on Checkpoint, NSM Log viewer for Juniper Firewalls.
* Creating and Provisioning Juniper SRX firewall policies.
* Configure and administer Cisco ASA Firewalls and use command line CLI, Cisco CSM, ASDM for day-to-day administration.
* Active/Standby and Active/Active HA configuration on Cisco ASA Firewalls.
* 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.
* Configuring rules and maintaining Palo Alto firewalls and analysis of firewall logs using various tools.
* Experience on ASA firewall upgrades to 9.x.
* Configured Panorama web-based management for multiple firewalls.
* Worked on configuration, maintenance and administration of Palo Alto PA3000 Firewalls and migrating customers from Cisco ASA to Palo Alto in HA network.
* Configuring rules and maintaining Palo Alto Firewalls& Analysis of firewall logs using various tools.
* Network hands-on installation experience of (Cisco routers, switches, ASA 5505 firewall, VPN)
* Understand the flow of traffic through the Check Point Security Gateway cluster and troubleshoot connectivity issues using advanced troubleshooting from Command Line Utilities.
* Use Tools such as SKYBOX for Firewall Policy optimization and rule base Clean up.
* Build and configure Active/Standby Failover on Cisco ASA with stateful replication.
* Configure and tweak the inspection policies on Firewall to allow legacy application traffic.
* Understand different types of NAT on Cisco ASA firewalls and apply them.
* Support Blue Coat Proxy in explicit mode for users trying to access the Internet from Corp Network.
* Troubleshooting connectivity issues through Blue coat as well writing and editing web policies.
* Involved in Upgrading Bluecoat proxy servers from SG900-10s to SG 9000-20B.
* Administration Big IP F5 LTM for all Local Load balancing and use GTM for load balancing across Data Centers.

**Publix, Lakeland, FL Jan 2014 – Jun 2015**

**Network Engineer**

**Responsibilities**:

* Firewall Policy Provisioning and troubleshoot connectivity issues through firewall.
* Performed penetration testing internally for our clients.
* Worked on Check Point Security Gateways and Cisco ASA Firewall.
* Firewall Clustering and High Availability Services using Cluster XL on Check Point.
* Configuring and tweaking Core XL and Secure XL acceleration on Check Point gateways.
* Troubleshoot User connectivity issues on Checkpoint and Cisco ASA using CLI utilities.
* Packet capture on firewalls and analyzing the traffic using Wireshark utilities.
* Troubleshot Clustering issues on Check Point and Sync issues monitoring and fix.
* Upgrade of Checkpoint Gateways in Cluster with Minimal downtime.
* Implemented Active/ Standby HA configuration on Cisco ASA Firewalls.
* Configuring Cisco ASA firewalls in Single and Multiple Context Mode firewalls.
* Upgrade of Cisco ASA Firewall in Active/Standby mode with no down time.
* Firewall Compliance and Rule remediation for compliance such as SAS 70 Audit.
* LAN/WAN level 3 support (diagnose and troubleshoot layer 1, 2, 3 problems)
* Vlan design and implementation, Spanning Tree Implementation and support using PVST, R-PVST and MSTP to avoid loops in the network. Trunking and Port channels creation.
* Working with OSPF as internal routing protocol and BGP as exterior gateway routing protocol.
* Configuring static NAT, dynamic NAT, Inside Global Address Overloading, TCP overload distribution, Overlapping Address Translation on Cisco ASA Firewalls.
* Deployed a Syslog server to allow proactive network monitoring.
* Implemented VLANS between different departments and connected them using trunk by keeping one VLAN under server mode and rest falling under client modes.
* Configured Firewall logging, DMZs and related security policies and monitoring.
* Switching related tasks included implementing VLANS and configuring ISL trunk on Fast-Ethernet channel between switches.
* Documentation and Project Management along with drawing network diagrams using MSVISIO.