****

**Abhilash Bandari**

**Email: abhilashb1327@gmail.com**

**Phone: 413-341-9226**

**Professional Summary:**

* Network 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 (NGX R65, R70, R71, R75 and R77), **Juniper Firewalls** (SRX5400, SRX5600and SRX5800), **Cisco Firewalls** (ASA 5505, 5506-X, 5585), **Palo Alto Networks Firewall models** (PA-2k, PA-3kand PA-5 k).
* Provide scalable, supportable military grade **TCP/IP** security solutions along with expert TCP/IP network designs that enable business functionality.
* Configured and Implemented **Cisco Identity Services Engine (ISE)** with connectivity to Microsoft Active directory for Authentication including Certificate Based Authentication.
* Performed support, configuration, testing and documentation for **ISE** rollout for Center Point Energy which includes making configuration changes in access and distribution layer switches, wireless controllers and **ISE nodes.**
* 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.
* Deployed **Cisco ACI** Network for several years in enterprise data centers.
* Working experience on tools and devices like **Gigamon, Sourcefire, Fire eye, Aruba, Cisco ASA, Cisco ISE.**
* Collaborated & Managed with various project teams consist of 8 to 22 resources to deliver Panorama program projects and Developed group and individual timelines and assessed/identified potential bottlenecks various work streams in each project/program process.
* 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.
* Managed all network and devices to include Cisco routers, switches, VPNs, SSL, Check Point, Cisco PIX, Cisco ASA, Cisco FWSM as well as content delivery networks (CSS, Citrix NetScaler and F5 Big IP LTM and GTM 1600 and 3400 load balancers) enterprise environment.
* Knowledge of web application firewalls and data loss prevention technologies.
* Configuration and troubleshooting of **CISCO** & **ARUBA** wireless devices
* Aruba Airwave Manager, ClearPass Policy Manager Server
* Worked on **Juniper Net Screen Firewalls** NS50, SSG 550M, SSG520M, ISG 1000, ISG 200 and Cisco PIX 535, 520, 515, ASA -5500 and 5505.
* Experience in Deployed Check Point Provider-1 NGX and configured CMAs
* Responsible for Checkpoint and Cisco firewall administration across global networks
* 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 LoadBalancer LTM**.
* Creating Virtual Servers, Nodes, Pools and **iRules on BIG-IP F5 in LTM module**.
* Experience with Firewall migrations from PIX firewall to **Cisco ASA** and **Juniper SRX** firewall appliances
* 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. Experienced in Installation, Configuration, and Troubleshooting VMware ESX & ESXi, 6.5, 6.0, .5.5, 5.1, 5.0, 4.1, 4.0, 3.5, vSphere 5.5, 5.1, 5.0, 4.1, 4.0, vMotion and Virtual Center 5.1, 5.0, 4.1, 4.0, Hypervisor.
* 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.
* Hands on experience with **Microsoft Azure** Cloud services, Storage Accounts and Virtual Networks.
* Knowledge of DDOS protection/Terminal functionality, Windows XP/7/8, iOS devices, Unix/Linux, Perl/Python, Nmap, ESXI 5.1, VMware vSphere 5.0, Metasploit with Armitage, Penetration Testing, and usage of Qualys Guard Vulnerability Management/Policy Compliance/WAS/ Asset Management / PCI.
* Excellent knowledge in Routing, Switching, Firewall and Gateway technologies, system design, wireless design, data network design, capacity management and network growth.
* Experience on ITSM modules (Incident/Problem/Change/Service Level/Service Request Management) regarding installations and operations.
* Deployed the Cisco 3500 Access Points using Cisco Wireless controllers 5500 and 2500 and WCS System.
* Experience in working with Cisco Nexus Switches and Virtual Port Channel Configuration.
* Experience with Checkpoint VSX, including virtual systems, routers and switches.
* Experience with **DNS/DFS/DHCP/WINS** Standardizations and Implementations.
* Extensive understanding of networking concepts, (IE. Configuration of networks, router configuration and wireless security, **TCP/IP, VPN, Content Filtering, VLANs and routing in LAN/WAN, Ethernet Port, Patch Panel and wireless networks.**
* Experience with management platforms such as **Panorama, Juniper NSM** and **Smart Center**.
* Configuration of Network and Security devices such as Cisco routers and switches **(Cisco 7600/3500/Nexus 7K/5K), Firewall (Checkpoint R75/Gaia and Cisco FWSM), Load Balancers and DNS and IP Manager (Infoblox)**
* Black listing and White listing of web URL on Blue Coat Proxy Servers.
* Administration of production Windows Servers infrastructure that includes Domain Controllers, IIS Web Servers, SharePoint, File and Print and FTP/SFTP servers.
* Experienced with routing protocols **(RIPv1/2, IGRP, EIGRP, OSPF, BGP), switching (VLANS, VTP Domains, STP and trunking),**
* Extensive experience in Windows 2008 R2/2008/2003 Wintel Servers at single or multi-domain platforms.
* Provide consultancy services to customers on a variety of network security products including firewalls, VPNs, authentication, load-balancing, data loss prevention and security information and event management.
* Wrote Python scripts to parse XML documents and load the data in database.
* Proficient in installing and configuring **Windows Server 2003, 2008, 2012 and Windows XP, 7 & 8Professional Client Operating Systems**
* IDS and IPS event management using CSM including signature updates for SSM Modules, IDSM.
* Provides management level reporting of firewall and Intrusion Protection System (IPS) activity on a periodic basis.
* Optimize, secure and control the delivery of all enterprise and cloud services and maximize the end user experience for all users including mobile clients using NetScaler.

|  |
| --- |
| **TECHNICAL SKILLS** |

|  |  |
| --- | --- |
| **Networking** | **OSI, TCP/IP, Cisco IOS, IOS-XR, LAN/WAN interconnection, Frame-Relay, ISDN, RIP, OSPF, EIGRP, IS-IS, BGP, MPLS, STP, RSTP, MST, VTP, NAT, ACLs, VPN, IP-Sec** |
| **Hardware Routers** | **Cisco (1800/2600/3600/3800/7200/7600 series), Cisco ASR 9Ks)** |
| **Switches** | **Cisco (2900/3500/3700/5500/6500 Series, Nexus 7k, 9k)** |
| **Firewalls** | **Cisco ASA (5510,5540), Checkpoint R65, R70, R75, R77 Gaia, Juniper SSG, SRX, Palo Alto** |
| **Other Tools** | **Tufin Secure Track, ForeScout CounterACT, F5 Big IP (LTM/GTM/ASM), DNS, Bluecoat Proxy, Solar Wind, Wireshark, BMC Remedy, Citrix NetScaler, Cisco Prime, VMware, proxies, firewalls, IDS/IPS, DLP** |
| **Network Monitor Tool** | **Wireshark** |
| **Lan and Wan Protocols** | **Ethernet, TCP/IP, CDP, STP, RSTP, VTP, Fast Ethernet, Frame Relay, PPP, HDLC.** |
| **Routing Protocols** | **OSPF, EIGRP, BGP, RIP** |
| **Load Balancer** | **Citrix, F5 Load Balancer** |
| **Application Protocols** | **SNMP, Telnet, SSH, DHCP, DNS, ARP, HTTP, FTP, TFTP** |
| **AAA Architecture** | **TACACS+, RADIUS, Cisco ACS** |
| **Operating Systems** | **Win 95/98, NT, XP, VISTA, LINUX, UNIX** |

**Professional Experience:**

**Client: At&T, Austin, TX Jan 2019 – Present**

**Role: Sr. Systems Engineer**

**Responsibilities**:

* Responsible in Massive project Migrating current Brocade Infrastructure to F5 Infrastructure.
* Worked to optimize current data center leveraging best practices for aging technology until the upgrade plan is executed.
* Work across multiple customers including internal and external constituents ultimately supporting the whole Infrastructure.
* Creating Ansible Playbooks for each and every instance in the migration plan
* Developed Ansible scripts for Setup and Configuration of F5 virtual instances.
* Advised management on current state and future state recommendations.
* Providing all varieties of services over Layer-2, Layer-3 and SME on F5 and Brocade Load Balancer’s.
* Analyze and provide the best practices using Stats on the ports or of the network using various Networking Monitoring tools.
* Providing end-to-end infra support for development, staging and production environments.
* Configuring GSLB policies for virtual servers on existing brocade Load balancers.
* Manage VCMP’s on physical F5 device and setting up them separately for Dev and QA instances.
* Running ansible playbooks on remote linux server and testing them by migrating the virtual servers to F5.
* Maintain and support Network Architecture Post-Migration.
* Configured F5 LTM solutions on various virtual Instances, which includes Wide IP, Pool Load Balancing Methods, probers and monitors.
* Setup and configured LTM instance from the scratch.
* Installed and configured high availability Big IP F5 LTM and GTM load balancers 11800 to provide uninterrupted service to customer applications and monitoring the availability.
* Created multiple instances for helping the Migration plan to be Implemented successfully.
* Implemented security policies utilizing F5 ASM to Secure At&T’s web applications.
* Participate in application delivery environment, build activities including creation of virtual servers, SSL profiles, pools, encryption policies and iRules based on customer requirements.

**Environment:** Brocade ServerIron ADX, Big IP F5 LTM, Ansible, Server management.

**Client: Schlumberger, Houston, TX June 2016 – Dec 2018**

**Role: Sr. Network Security Engineer**

**Responsibilities**:

* Modify pilot ISE environment for production scaling and performance
* 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.
* Configured, implemented and troubleshooting issues on Checkpoint **R77.10 Gaia, R75, Cisco ASA 5540, 5000** series firewalls for the client environment.
* Contribute to the development and overall strategy of the penetration testing program
* Manage project task to migrate from **Cisco ASA firewalls** to Check Point firewalls.
* Configured **Cisco ISE** for Wireless and Wired 802.1x Authentication on Cisco Wireless LAN
* Configuration and Integration of Cisco Identity Services Engine **(ISE)**
* Worked on **VPN configuration, routing, NAT, access-list, security contexts and failover in ASA firewalls.**
* 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**.
* Configuring, Administering and troubleshooting the Checkpoint, Palo Alto and ASA firewall.
* Configured IPSec VPN (Site-Site to Remote Access) on Cisco ASA (5200) series firewalls.
* Working with the rule base and its configuration in Cisco ASA, Palo Alto, Juniper and Checkpoint firewalls.
* Deploying ISE Wired and Wireless Authentication, Authorization and Accounting.
* 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.
* Hands-on experience on Tufin Secure Track to reduce risk while increasing compliance and efficiency.
* Installation and configuration of Splunk product at different environments. Configured Splunk Searching and Reporting modules, Knowledge Objects, Administration, Add-On's, Dashboards, Clustering and Forwarder Management.
* 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.
* Worked on manual Penetration testing of client systems, web sites and discovered network vulnerabilities.
* 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.
* 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**.
* Applied security enhancement by implementing certificates and RSA keys for authentication.
* Installed and administered RSA Secure ID token authentication servers.
* 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
* Configured F5 GTM solutions, which includes Wide IP, Pool Load Balancing Methods, probers and monitors.
* Designed and developed **Azure** **Cloud**Service projects and deployed to Web Apps, PaaS, and IaaS.
* Work with the **Cisco Meraki** Sales team and on strategic sales initiatives like customer outreach and channel training to grow business in targeted regions.
* 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.
* Responsible for resolving customer issues involving Routing & Switching, SD-WAN services, Router configuration, and managing field technician dispatches
* Worked on Cisco Nexus 9000 family of switches whose hardware is based on **Cisco ACI**
* Physically deployed new Cisco Nexus devices, Catalyst and Nexus replacement blades, **FWSMs, Cisco ASAs, Citrix NetScaler MPX and SDX chassis.**
* Verify Firewall status with Checkpoint Monitor. Creation and implementation of Application delivery architectures which includes load balancing on F5 BIG IP modules.
* Worked with F5 Load balancing, IDS/IPS, Bluecoat proxy servers and Administrating.
* Use of Web application firewall providing reverse proxy-based protection for applications deployed in physical, virtual / public cloud environments.
* Involved in the deployment and decommission of VLANs on core ASR 9K, Nexus 7K, 5K and its downstream devices.
* Involved in F5 LTM GTM and ASM planning, designing and implementation. Actively involved in F5 ASM policy configuration and deployment. Troubleshoot and Worked with Security issues related to Cisco ASA/PIX, Checkpoint, IDS/IPS and Juniper Net screen firewalls
* Configured High availability, User ID on Palo Alto firewall.
* 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.
* Integrating Cisco Stealthwatch with other Cisco Security services such as Firepower and Cisco Identity Services Engine (ISE)
* Stateful firewall, VLAN to VLAN routing, Link bonding / failover, 3G / 4G failover, Traffic shaping / prioritization, WAN optimization, Site-to-site VPN, Client VPN, MPLS to VPN Failover, Active Directory and LDAP integration.
* Responsible for investigating Data Loss Prevention using Symantec DLP.
* 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
* Configure and troubleshoot Routing protocols such as OSPF and EIGRP for routing internally and BGP for external routing. Configuring and maintaining virtual server environment using VMWARE ESXi, VSphere, VCenter, VBlock.
* Worked and maintained various network, application monitoring tools like Solar Winds, Cisco Prime, **ForeScout, Wireshark, TCP Dump.**
* To monitor, track and report changes for all firewalls, routers and switches in the organization by using the Tufin secure track
* Supply documentation and training based articles on different aspects of StealthWatch and NetFlow.
* **ForeScout CounterACT- NAC**, endpoint compliance, real-time intelligence and policy-based control.
* Experience with Monitoring wireless networks and performing site surveys.
* Involved in Troubleshooting IP Addressing Issues and Updating IOS Images using **TFT**.
* Managed multiple projects resource allocation (in-house, offshore & virtual), leveling & planning for current and future Panorama Program projects using integrated project plans as well as negotiating with multiple teams, resource managers for maximizing resource talents.

**Environment:** Cisco ASA5580/5540/5520, CheckpointR70, R75, R77.20 Gaia, Palo AltoPA-5000/3000, Juniper SSG, SRX, Big IP F5 LTM/GTM, Nexus switches, Routers, TCP/IP, VPN, Bluecoat Proxy servers, IDS/IPS. SIEM and monitoring, BMC Remedy, Cisco Prime, ForeScout CounterACT, Tufin.

**Client: CITADEL, CT December 2014 –May2016**

**Role: Sr. Network Security Engineer**

**Responsibilities**:

* Implementing Security Solutions using **PaloAltoPA-5000/3000, Cisco 5580/5540/5520, Checkpoint firewalls R70, R75, R77.20Gaia 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.
* Monitors the network traffic and maintain the records with the help of SPLUNK.
* Knowledge of **Cisco ASA firewall, VPN, GRE over IPSec tunnel** configuration and Route-maps.
* 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.
* Create and validate SMOPS for upgrade, replace, add and remove Cisco VOD equipment.
* Work with Load Balancing to build connectivity to production & disaster recovery servers through **Citrix NetScaler.**
* Provided engineering support and technical assistance by ensuring the Cisco ISE server is correctly installed and licenses are applied.
* Vulnerability scanning using IBM Endpoint Manager & Nessus
* Vulnerability security patching using IBM Endpoint Manager, **SCCM & WSUS**
* 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.
* 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.
* Handling Modern related issue like that of RAD & Aruba.
* 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 5580-20, ASA 5540, ASA 5520, ASA 5510** 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.
* Monitoring Traffic and Connections in Checkpoint and ASA Firewall.
* Manage project task to migrate from Cisco ASA firewalls to Check Point firewalls.
* Configuring and troubleshooting site-to-site IPSEC VPN tunnels using Cisco ASA 5540 for third-party connectivity.
* Served a platform for other services that are required within the data center or cloud environment using **Cisco ACI**.
* 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.
* Placed in charge of control and maintenance of the SD-WAN laboratory environments, performing version updating before user client official updating.
* 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.
* Configuration and Integration of Cisco Identity Services Engine (ISE).
* Consisted of ISE Deployment, Authentication with Active Directory and Microsoft Certificate Authority.
* 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.
* Worked on F5 solutions/support for migration work of applications and websites from Cisco CSS Load Balancers to the F5 BigIP Load Balancers.
* Configure and Monitor **Cisco Sourcefire** IPS for alerts.
* 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.
* Provide support to help desk for complex/major network problems. Build the rules for the application access across the IPSEC VPN tunnel
* Implemented configuration back-ups using WinSCP, cyberfusion to automate the back-up systems with the help of public and private keys.
* 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.
* Monitor Intrusion Detection Systems (IDS) console for active alerts and determine priority of response.
* Actively use SIEM technology for searching and monitoring real-time events for network security and compliance.
* Review daily log data gathered from various resources such as sensors, alert logs, firewall logs, content filtering logs.
* Experience with converting Cisco 6500 IOS to Cisco Nexus NX-OS in the data center environment.
* Working on day-to-day service tickets to solve troubleshooting issues.
* Experience using Service Now ticketing tool.

**Environment**: Cisco ASA5580/5540/5520, CheckpointR70, R75, R77.20 Gaia, Palo AltoPA-5000/3000, Big IP F5 LTM/GTM, Nexus switches, TCP/IP, VPN, Bluecoat Proxy servers, IDS/IPS. SIEM and Monitoring, Service Now.

**Client: Rukus wireless, CA May 2012 – November 2014**

**Role: 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.
* Provide VOD Method of Procedures documentation to customer for software upgrade downgrade release.
* Maintained the following Cisco platforms **7600, 7500, 7200, 7000, 3560, 2900, 2801, 2000, ASA5500, Catalyst 6500, 4500, 3560 and 2900.**
* Experience as a Sales QA Representative in Production Environment for Network Based Firewall Based Wireline Applications and interact with Net bond team who establishes a firewall connection on a VPN to the Cloud Portal.
* Participate in the installation and configuration of new VOD equipment.
* Configured and utilized many different protocols such as OSPF, ISIS, BGP/MP-BGP, OER, MPLS, LDP, juniper cast, IPv4/IPv6 protocols.
* Utilized knowledge of Spanning Tree Protocol, BGP, MPLS, OSI model layers 1-2 to create network layouts.
* Acts as local liaison to identify, correlate, communicate and verify customer impact for nationally managed care team events impacting Video, VOD, network transport, or related IP services.
* 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 (5585, 5550 and 5540) 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.
* Firewall policy provisioning on Fortinet FortiGate appliances using FortiManager.
* 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.
* FWSM configurations in single/multiple contexts with routed and transparent modes.
* Support Data Center Migration Project involving physical re-locations.

**Environment**: Juniper (SRX, JUNOS, ScreenOS, Net Screen SSG), Cisco (CheckPoint, ASA Firewalls), Palo Alto Firewalls, Big IP F5 LTM/GTM, TCP/IP, FortiGate, Service Now.

**Client: Pluribus Networks, Bengaluru, India May 2010 – March 2012**

**Role: Network Engineer**

**Responsibilities**:

* Firewall Policy Provisioning and troubleshoot connectivity issues through firewall.
* Performed penetration testing internally for our clients.
* I 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 Wire shark 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.
* Configuring VPN both B2B and remote access SSL and centralized policy administration using Fort Manager, building FortiGATE High Availability using FortiGATE Clustering Protocol (FGCP).
* 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.
* Deployed Jenkins user documentation 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.

**Environment**: CISCO routers and switches, Access Control Server, RIP V2, OSPF, EIGRP, VLAN, Trunk Protocols, CISCO ASA, DHCP, DNS, Spanning tree, Nimsoft.