**Kumar Battula**

Email: battulash1@gmail.com

Phone: (719)-470-0999

**NETWORK SECURITY ENGINEER**

**PROFESSIONAL SUMMARY:**

* 9+ years of extensive knowledge on Network & Information Security. Solid understanding of Design, Implementation, Administration, Operational and troubleshooting of enterprise data networks.
* Strong hands-on experience on **Palo Alto**, **IBM QRadar**, **RSA Net witness, Proof Point, Rapid7,** **Checkpoint Firewall**, and **Cisco ASA** firewalls.
* Involved in migration of 22 different log sources from IBM QRadar to RSA Netwitness by working with multiple vendor companies.
* Expertise in Configuring Policies and Maintaining PaloAlto Firewalls along with troubleshooting using firewall logs.
* Expert level knowledge in firewall rule audit and optimization using **Tufin Secure Track**.
* Migration of the firewall rules from Cisco ASA, Checkpoint to Palo Alto firewalls using migration tool from Pan.
* Strong knowledge on mitigation of **DoS** attacks on Cisco and Palo Alto firewalls.
* Extensive knowledge on Security breach analysis using Kill Chain process.
* Extensive knowledge on utilizing Wildfire for mitigating zero-day attacks.
* PaloAlto design and installation (**Application** and **URL filtering (PAN-DB)**, **Threat Prevention**, **Data Filtering**).
* Implementation of **IPSEC** and **SSL VPN's** on PaloAlto, Cisco ASA Firewall.
* Profound knowledge in **AAA** configuration using **TACACS+ & RADIUS** server.
* Managed all network hardware and dealt with the **DOS** attacks and zone flooding attacks.
* Configured Cisco ISE for Wireless and Wired 802.1x Authentication on Cisco Wireless LAN Controllers, Catalyst Switches, and Cisco ASA Firewalls.
* Decent knowledge of operations within **AWS** **(EC2, S3, IAM, VPC**, Direct Connect, Route53).
* Worked on F5 BIG-IP LTM 8900, Citrix NetScaler configured profiles, provided and ensured high availability.
* Implementing security policies using **ACL** in Switches, Routers.
* Experience in implementing site-to-site and remote access **VPN** Technologies using **GRE, IPSEC & MPLS**.
* Responsible for designing and deploying various network security & high availability products like **Cisco ASA**.
* Design and Implementation of **LAN, WAN, VLANs**, **VTP**, Spanning Tree (**STP**), **Trunking** and Ether channel.
* Implemented various **Switch Port Security** features as per the company's policy.
* Decent knowledge with **SOC** (Security operation Center) operations, and **NOC** **(**Network operation Center**)** operations, especially resolving a ticket raised by the security team.
* Resolved tickets raised by the **SOC** teams by analyzing the traffic with the help of SIEM tools like QRADAR, SPLUNK, RSA Netwitness.
* Solid knowledge on Proxy Servers (Forward Proxy, Reverse proxy) such as Bluecoat Proxy Server.
* Decent knowledge on the upcoming concepts of **IoT** (Internet of Things). And usage of Infoblox to identify all the connected devices to the network.
* Expert level knowledge of Cisco network security (**IDS, NIPS ASA** 5500 Firewall), network redundancy (**HSRP, GLBP** and **VRRP**).
* Worked on network monitoring tools such as Solar Winds.
* Extensive experience in configuring Layer3 routing and layer2/3 switching of Cisco based nexus 7K,5K,2K& 800ISR series Switches & routers.
* Extensive experience as systems administrator supporting and maintaining **Citrix VPN** enterprise environments, including **Citrix XenApp** and **XenDesktop 7.6**.
* Experienced in implementing and managing the **XenApp**, **XenDesktop 4, 5, 5.5, 5.6, 7, 7.1, 7.5, 7.6, 7.7, 7.8,** **NetScaler** architecture including managing and creating the **Delivery Groups, machine catalogs, and Storefront**, applications, and users.
* Responsible for the deployment of web services, containers, and other components within the middleware domain.
* Expertise on maintaining system health, performance, and availability of middleware environment by engaging in high priority incidents to identify the root cause, restore service as quickly as possible, and identifying opportunities for future prevention.
* Experienced in deploying and supporting web, middle-tier, and 3rd-party systems across on-prem and cloud platforms.
* Troubleshooting platform and routing issues within on-prem and cloud environment. And also automating repetitive operational tasks to increase efficiencies, productivity, and to enable delegation of support tasks.
* Experienced with configuration management tools like Puppet, Ansible. Good knowledge of VMware virtualization (vSphere, vRealize Automation).

**Technical Skills**

|  |  |
| --- | --- |
| NETWORKING CONCEPTS | OSI, TCP/IP, UDP, IPV4, IPV6, VLSM, FLSM, CIDR. |
| SWITCHING PROTOCOLS | VLAN, VTP, STP, PVST, MVST, INTER VLAN, LAYER 2,3. |
| ROUTING PROTOCOLS | BGP (IBGP, EBGP), STATIC, DYNAMIC (RIP, EIGRP, OSPF, ISIS ) |
| LOAD BALANCERS | F5(LTM, GTM), F5(BIG -IP) |
| REDUNDANCY PROTOCOLS | FHRP (HSRP, VRRP, GLBP) |
| WAN | MPLS, GRE, MGRE, VPN, DMVPN |
| FIREWALL | PALOALTO, CISCO ASA, CHECKPOINT |
| SECURITY | IKE, IPSEC, SHA-2, PSK, SSL-VPN |
| TOOLS | SIEM (QRADAR, RSA Netwitness SPLUNK, HPARCSIGHT) WIRESHARK, TCPDUMP, SOLARWINDS,  |
| LANGUAGES | IOS, PANOS, MATLAB, HTML, PYTHON |
| AUTHENTICATION  | TACACS+, RADIUS, AAA |
| OPERATING SYSTEM | WINDOWS 7,8,10, LINUX. JUNOS, IOS |

**Educational Information:**

* Master of Science from Texas A&M University Kingsville in Electrical Engineering.
* Bachelor of Technology from Jawaharlal Nehru Technological University Hyderabad in Electrical & Electronics Engineering.

**Certifications:**

* Proof Point Accredited Administrator: Information Protection.
* Proof Point Accredited Administrator: Email Protection.

**NETWORK SECURITY ENGINEER August 2019- Present**

**The TJX Companies- Marlborough, MA**

**Responsibilities:**

* Deploying the Palo Alto Firewalls 800, 3k, 5k series from the scratch for new sites.
* Operational maintenance on the firewalls- Dynamic updates, OS version upgrades, security profiles etc.
* Expertise on architecting the new templates and template stack for the new sites and its hierarchy.
* Writing the Security polices, NAT rules, SSL decryption, URL filtering rules.
* Assisting in troubleshooting the issues related to NAT and routing issues.
* Global deployments for around 170 firewalls on configuring the SSL Certificate profiles for decryption and management purposes.
* Upgrading all the firewalls to the latest preferred versions in order to avoid the vulnerabilities.
* Expertise in deploying the ISE servers from the scratch and testing with the various vendors to integrate them to ISE.
* Deployment for the Air Defense central controllers on the wireless activity, such as writing the rules and sanctioning the devices and clearing the rogue activities.
* Creating and documenting the JIRA stories and maintain the confluence pages for security team.
* Working on migrating the ASA configurations to Palo with the help of Expedition tool.
* Deploying Cisco Meraki wireless devices for new sites architecture along with Fortinet equipment for SD-WAN.
* Completed the Prisma SaaS and Armis-IOT trainings and working on onboarding the new tools and integrating with existing tools in the organization.
* Deploying the site to site vpn tunnels between Palo Alto firewalls and Cisco ASA firewalls.
* Worked with VMware teams in building the NSX servers, Expedition on private clusters. Worked on multiple VMware server network troubleshooting issues.
* Expert knowledge on building new sites with the help of Visio.

**Environment:** Palo Alto Networks, Air Defense, Cisco Meraki, Cisco ISE, Cisco Routers and Switches. F5 load balancer, BluCat IPAM, Splunk, Prisma SaaS, Armis.

**NETWORK ENGINEER May 2019- August 2019**

**Bose Corporation- Stow, MA**

**Responsibilities:**

* Developed a Document for Vulnerability Management Process.
* Working with the network teams located globally in remediating the Network Vulnerabilities.
* Running the vulnerability scans with the help of Qualys, reporting to management on the top vulnerabilities and remediation procedures.
* Investigating the Network Devices which are not authenticating the Qualys to run a vulnerability Scan internally on that device.
* Performing the IOS version upgrades on the Devices which are prone to Compromise.

**Environment:** Qualys, Cisco Switches and Routers.

**SECURITY ANALYST August 2017- May 2019**

**Ahold Delhaize (Food Lion)- Charlotte, NC**

**Responsibilities:**

* Developing the migration sequence for log sources to be moved to **RSA Netwitness** from **IBM QRadar**.
* Performing the Pilot tests before moving the log sources from QRadar to RSA Netwitness with the help of QA teams and validating the Parser issues for each log source.
* Validating all the logs coming from multiple logs sources to RSA Netwitness with the help of **ESA**.
* Running all the system and health reports and making the custom rules for triggering alerts.
* Responsible for raising all the firewall change tickets in the information security department and working with the Network/network Security teams to get them done.
* Scanning entire environment for SQL injections of malware, spam, and viruses by using the **Appspider** application.
* Performing vulnerability scanning using **Rapid7** to identify the potential vulnerabilities across the environment and informing the concerned departments to act on it.
* Running the weekly and monthly reports, scanning the entire environment on weekly, monthly basis and pushing all the reports to management.
* Scanning all the inbound and outbound emails for malwares, spam, virus and quarantining the infected emails by using the Proof Point.
* Configuring threat response and auto pull(**TRAP**) for identifying potential threats in the emails and integrating that to Proof Point.
* Performing the health check of RSA Netwitness with the help of professional services from EMC2.
* Configuring Blue Coat Content Analysis and malware Analysis, scanning all the packets passing through the proxies.
* Developing Validation procedures for migration of QRadar data to Splunk.
* Developing Validation procedures for back out of failed migration of QRadar data to Splunk.
* Determining the migration sequence for log sources to be moved.
* Analyzing QRadar rules and building blocks to determine rule dependences and requirements.
* Analyzing QRadar rules to improve functionality.
* Performing a comparison of QRadar log sources and HIPAA devices to determine if any HIPAA devices were not reporting to QRadar (39,000 QRadar log sources and 3000 Compliance log sources) over 1000 devices were missing from QRadar.
* Collecting QRadar data from 22 device types and over 2000 event types to determine what data should be filtered at the Splunk syslog server.
* Creating the regular expressions to be used by Splunk to filter QRadar events.
* Collecting several weeks of QRadar events to be used to show the reduction of events going to QRadar after the migration.
* Performing on going analysis of QRadar events to find additional events that should be filtered by Splunk.
* Participating in tests of Splunk to QRadar data transmission to help troubleshoot Splunk issues.
* Worked with Palo Alto firewalls PA3060, PA5060 using Panorama servers, performing changes to monitor/

block/allow the traffic on the firewall.

* Configuring rules and Maintaining **Palo Alto Firewalls** & Analysis of firewall logs using various tools.
* Configured routes on Palo Alto firewalls 3060, 5060, 7050.
* Configuring **TACACS+, LDAP**, and **RADIUS** for Cisco ASA and Palo Alto firewalls.
* Integrating **Panorama** with Palo Alto firewalls, managing multiple Palo Alto firewalls using Panorama.
* Palo Alto App ID migration from the legacy based port rules for PA 5060, 7050.
* Palo Alto **SSL** decryption installation and configuration on PA 3060,5060, and 7050.
* Successfully installed Palo Alto PA-3060 firewalls to protect Data Center and provided L3 support for routers/ switches/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 Firewalls.
* Implemented **Zone Based Firewalling** and Security Rules on the Palo Alto Firewall.
* Configure policies on the Bluecoat VPM, local database and PAC files to filter the traffic flow by creating

custom rules, URL filters (PAN-DB) and routing policies.

* Implementing and configuring **F5 LTM's** for **VIP**'s and Virtual servers as per application and business requirements.
* F5 configuration, installation, and monitoring with **F5 APM.**
* Administration on **Big IP F5 LTM** for all Local Load balancing and use **GTM** for load balancing across Data Centers.
* configuring the DNS server to delegate wide IP-related requests to the BIG-IP GTM for name resolution.
* Experienced in implementing and managing the **XenApp**, **XenDesktop 4, 5, 5.5, 5.6, 7, 7.1, 7.5, 7.6, 7.7, 7.8,** **Netscaler** architecture including managing and creating the **Delivery Groups ,machine catalogs, and Storefront**, applications, and users.
* Setting up **NetScaler** and configure all the basic NetScaler Settings including **on NetScaler for Back-end Servers and Traffic, Network-related Settings, Load Balancing, SSL Offloading, Acceleration and Optimization of Traffic-handling, NetScaler licenses**.
* Installing and configuring **Citrix Receiver with registry settings for desktop launches.**
* Citrix Certified Professional
* Perform application installations and updates to the **Citrix environment**. Work with internal and external personnel to implement new applications.
* Experienced in Monitor all components **of Citrix infrastructure** to maintain performance and reliability.
* Responsible for the deployment of web services, containers, and other components within the middleware domain.
* Experienced with configuration management tools like Puppet, Ansible. good knowledge of VMware virtualization (vSphere, vRealize Automation).

**Environment:** IBM QRadar, RSA Netwitness, Splunk, Proof Point, rapid7, Appspider, Carbon Black, Palo Alto, Blue Coat Proxies, F5, ServiceNow.

**SR. NETWORK SECURITY ENGINEER January 2016- 2107July**

**CenterPoint Energy- Houston, TX**

**Responsibilities:**

* Responsible for firewall rule set migration from Cisco ASA, Checkpoint to newly implemented Palo Alto.
* Worked with Palo Alto firewalls PA3060, PA5060 using Panorama servers, performing changes to monitor/

block/allow the traffic on the firewall.

* Configuring rules and Maintaining **PaloAlto Firewalls** & Analysis of firewall logs using various tools.
* Configured routes on PaloAlto firewalls 3060, 5060, 7050.
* Configuring **TACACS+, LDAP**, and **RADIUS** for Cisco ASA and PaloAlto firewalls.
* Integrating **Panorama** with PaloAlto firewalls, managing multiple PaloAlto firewalls using Panorama.
* PaloAlto App ID migration from the legacy based port rules for PA 5060, 7050.
* PaloAlto **SSL** decryption installation and configuration on PA 3060,5060, and 7050.
* Addition and removal of services from virtual server configuration on Citrix Netscalar load-balancer.
* Configuring and integrating Network Access Devices(NAD), profiles and polices on Cisco ISE.
* Configuration of High Availability (HA) for inline Cisco ISE appliances.
* Maintaining SSL certificate on Citrix Netscalar load balancer and managing the virtual servers
* Diagnose and analyze escalated incident requests pertaining to endpoints accessing hosted and managed applications via Citrix XenApp (5.0, 6.5), two factor authentication and Web VPN to meet Service Level Agreements.
* Implemented Positive Enforcement Model with the help of PaloAlto Networks.
* Researched, designed, and replaced aging Checkpoint firewall architecture with new next generation PaloAlto appliances serving as firewalls and URL and application inspection.
* Successfully installed Palo Alto PA-3060 firewalls to protect Data Center and provided L3 support for routers/ switches/firewalls.
* Responsible for setting up the infrastructure environment with majority of Cisco & PaloAlto appliances apart from various other equipment.
* PaloAlto user-identification implementation with **KIWI** server user PaloAlto user-id agents.
* PaloAlto integration with **VMware** Virtual Desktop infrastructure.
* PaloAlto upgradation and degradation.
* Exposure to **wild fire** feature of PaloAlto.
* Configured **VLAN** trunking with PaloAlto interface.
* PaloAlto design and installation (**Application** and **URL filtering**, **Threat Prevention**, **Data Filtering**).
* Configured and maintained **IPSEC** and **SSL VPN**'s on PaloAlto Firewalls.
* Implemented **Zone Based Firewalling** and Security Rules on the PaloAlto Firewall.
* Configuring, Administering, and troubleshooting the Checkpoint, PaloAlto, Imperva and ASA firewall.
* Configure policies on the Bluecoat VPM, local database and PAC files to filter the traffic flow by creating

custom rules, URL filters (PAN-DB) and routing policies.

* Build and configure Active/Standby Failover on Cisco ASA with Stateful replication.
* Writing the rules and policies for IBM QRadar.
* Validating the Building blocks of QRadar and monitoring the Network activity and log activity.
* Troubleshooting various network security related issues using Cisco SDM.
* Managing networks and servers in **AWS**. Specifically creating **VPC**’s, launching **EC2** instances and creating private and public subnets, Auto Scaling, **ELB, S3**, Cloud Front, **Route 53**, Cloud Watch, Cloud Formation, **SQS, SNS.**
* Working on the project of **F5 LTM** and **GTM** code upgrade project, doing couple of them every week.
* Worked on F5 **VIPRION** 4800 series BIG IP devices, configured VIP's with HTTP/SSL profiles, pools,

configured iRules and ensured high availability.

* Balancing traffic to tune and distribute server load on the network for scalability in Local Traffic management.
* Off-loading standard server tasks, such as HTTP data compression, SSL authentication, and SSL encryption to improve server performance. Monitoring the health and performance of servers on the network for availability in LTM.
* configuring the DNS server to delegate wide IP-related requests to the BIG-IP GTM for name resolution.
* Review and Provide Subject Matter Expert guidance in the design and installation and implementation of two data center rollout of the Sourcefire NGIDS/IPS.
* Oversee and coordinate all activities of SOC personnel supporting the security of critical production environments using Nitro, Sourcefire, Proxy, IaaS/SaaS.
* Inspection, URL filtering, and configuration and troubleshooting of Sourcefire /Firepower products.
* creating A record, NS record, CNAME (canonical name) records for web application in global traffic management.
* Configured AFM (Advanced Firewall Manager) a licensed module for the BIGIP appliance that provides stateful firewalling along with reporting and DoS protection.
* Worked on FireEye for inspection of common attacks that enter our network.
* Experienced working with design and deployment of **MPLS** Layer 3 **VPN** cloud, involving **VRF**, Route Distinguisher (**RD**), Route Target (**RT**), Label Distribution Protocol.
* Implementing and configuring **F5 LTM's** for **VIP**'s and Virtual servers as per application and business requirements.
* F5 configuration, installation, and monitoring with **F5 APM.**
* Configured **VLANs** with **802.1q** tagging. Configured Trunk groups, ether channels, and Spanning tree for creating Access/distribution and core layer switching architecture.
* Configured **HSRP** and VLAN trucking 802.1Q, VLAN Routing on Catalyst 6500 switches.
* Responsible for company’s Cisco ASA firewall administration across our global networks.
* Provided Level-3 Network support for Cisco Switches and **Cisco ASA 5500** Series Security Appliances.
* Configuring and Troubleshooting Cisco Firewall/ASA, Checkpoint FW, Bluecoat ProxySG and Cisco IronPort.
* Installed and tested Cisco router and switching operations using **OSPF** routing protocol, ASA Firewalls, and **MPLS** switching for stable **VPNs.**
* Worked in **NOC, SOC** teams to solve the network issues. Resolved the issues raised by the network and security teams with the help of SIEM tools.
* Worked on **SIEM tools** (IBM QRadar/HP Arcsight) to protect organization from threats and cybersecurity attacks.
* Experienced on analyzing the enterprise logs with the help of security information and event management technologies.
* Configured Virtual Chassis for Juniper switches EX-4200, Firewalls SRX-210.
* Supported on Cisco Nexus 5000 and Nexus 7000 Series Switch fabric links.
* Designed a Citrix **XenApp** Farm of 180 virtual servers on **Windows Server** using VMware vCenter. Responsible for installing in-house and 3rd party applications on **Citrix Termina**l Servers and publishing to users through Citrix Delivery console .
* Manage and maintain Citrix Presentation **Server 6.5** Farms and also plan, test, install, configure and manage different applications.
* Installation, configuration and administration of multiple **XenApp** farms.
* Responsible for administering and supporting 350 Citrix server environments on Windows Server 2003/2008.
* Installed **Citrix XenApp 6.5 on VMware Servers. Configuration of Citrix migration work 4.5 to 6.5.**
* Planning and testing the application Virtualization for various new application releases using **Citrix** Streaming Profiler and publishing it to the Citrix Farm.
* Managing user accounts, networking and connectivity for **Citrix** connectivity.
* Implemented POCs for **NetScaler**, **XenDesktop**, **XenApp** and **XenServer**.
* Load Balancing Technology and Concepts - specifically the **Citrix** NetScaler platform
* Configured Network Security policies to ensure that all the network is segmented in the way that no data leak happens from one zone to another.
* Experience in configuring Network Security access control on switch infrastructure and apply policies like User Authentication.
* Designed and implemented IT security policies and networked backup systems.
* Configured route redistribution between **OSPF** and **EIGRP** in a multi-area OSPF network.
* Implemented Hot Standby Router Protocol (**HSRP**) by tuning parameters like preemption.
* Monitoring links and configuration management using Solar Winds and NMAP.
* Maintained, configured, and installed Cisco routers and switches: 7500/catalyst 6500/RV320/2960/catalyst 3550/12410, 12816, 1204 series, Nexus 7k and 5k, WLC, and ASA 5540.

**Environment**: Cisco routers and switches: 7500/catalyst 6500/RV320/2960/catalyst 3550/12410, 12816, 1204 series, Nexus 7k and 5k, WLC, and ASA 5540. PaloAlto firewalls 3060, 5060, 7050. Cisco Nexus 5000 and Nexus 7000 Series Switch.

**Sr. NETWORK & SECURITY ENGINEER September 2014- 2015 December**

**University of Pennsylvania- Philadelphia, PA**

**Responsibilities:**

* Implementing and maintenance of network design, structure, up gradation and configuration of routers and switches at the client server for 400+ users.
* PaloAlto installation, configuration, administration, monitoring and implementing the policies
* PaloAlto design and installation (**Application** and **URL filtering**, **Threat Prevention**, **Data Filtering**).
* Work on Checkpoint Platform including Provider Smart Domain Manager. Worked on configuring, managing, and supporting Checkpoint Gateways.
* Maintained, configured, and installed **Cisco ASA** 5520 Firewall.
* PaloAlto user-identification implementation with **KIWI** server’s user PaloAlto user-id agents.
* PaloAlto integration with **VMware** Virtual Desktop infrastructure.
* PaloAlto up gradation and degradation.
* Configured VLAN trunking with PaloAlto interface.
* Configured routes on PaloAlto firewalls 3060, 5060, 7050.
* Configuring **TACACS, LDAP**, and **RADIUS** for Cisco ASA and PaloAlto firewalls**.**
* Integrating Panorama with PaloAlto firewalls, managing multiple PaloAlto firewalls using Panorama.
* PaloAlto App ID migration from the legacy based port rules for PA 5060, 7050.
* PaloAlto **SSL** decryption installation and encryption.
* Monitoring the Log activity and working on the offenses developed in QRadar.
* Tuning the QRadar with advanced rules and policies, validating the global rules and local rules.
* Worked on Citrix NetScaler load balancer for load balancing and failover across data center and between web servers.
* Configuring rules and Maintaining PaloAlto Firewalls & Analysis of firewall logs using various tools.
* Implementing and configuring Static, **RIP** and **OSPF** protocols on Cisco Routers.
* Worked using routing protocols **EIGRP** and **BGP** based company network for resolving level 2 and 3 issues.
* Performed troubleshooting and management of **OSPF** and **BGP** protocols on routers.
* Maintaining redundancy on Cisco 2600, 2800 and 3600 routers with **HSRP**.
* Worked on IP addressing based on sub netting and Variable Length Subnet Mask.
* Supporting customers with the configuration and maintenance of **PIX** and **ASA** firewall systems.
* Installation, configuration and administration of multiple **XenApp** farms.
* Deploying and configuring **Citrix** Access Gateway to leverage connectivity for external users.
* Analyzing Client's environment, existing infrastructure and proposing a solution.
* Involved with change ticket, priority tickets and supporting on-call for **Citrix**, windows and virtual machines.
* Supported 100 applications for 5000-6000 concurrent users out of 15000 users daily by solving 15-18 tickets a day and actively involving in the critical issues and resolved them by finding out the root cause of the issue including printing, App Sense and Citrix   profile issues  XenApp 5.0 and   CitrixXenApp 6.5.
* Remote & telephonic support to the users. Managing & troubleshooting the issues with **Citrix** servers.
* Monitoring the routing traffic using Cisco 2000 and Wireshark.
* Configuring Spanning tree, **VSTP, VLAN, SNMP** on EX series switches.
* 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.
* Provided Tier2 **LAN** and **WAN** operational support to network call center, supporting the remote, domestic and international offices.
* Providing technical support in **LAN** and **WAN** connectivity and hardware issues in the complex network system.
* Connecting various routing and switching devices with **CAT 5/ 5E** cabling.
* Hands on experience on SIEM tools (IBM QRadar/HP Arcsight) to protect organization from threats and cybersecurity attacks.
* Experienced on analyzing the enterprise logs with the help of security information and event management technologies.
* Used **F-5Load balancers** to increase capacity (concurrent users) and reliability of applications.
* Experience with configuring Virtual Server and Configuring Load balancing methods in **F5 LTM**.
* Installing of **NOC** [Network Operation Center] monitoring server to establish a 99.9 uptime standard.
* Installing **SOC** (Security operation Center) and monitoring the traffic with SIEM tools. And resolved errors or tickets raised by the security department.

**Environment**: Cisco 2600, 2800 and 3600router. F-5Load balancers. PaloAlto firewalls 3060, 5060, 7050. Cisco ASA 5520 Firewall.

**NETWORK AND SECURITY ENGINEER- Apprentice February 2012- 2014 March**

**Xebia usa Inc- Boston, MA**

**Responsibilities:**

* Hands on experience on all software blades of checkpoint firewall.
* Configuring **VPN**, clustering, and **ISP** redundancy in Checkpoint firewall.
* Configuring, maintaining, and troubleshooting **IPS** and **IPS-1** in Checkpoint.
* Configured redundant interfaces, **DHCP** server, **DHCP** relay, ntp settings, and sub interfaces on firewalls.
* Built and support **VRRP** / Cluster based **HA** of Checkpoint firewalls.
* Perform Checkpoint and **PIX** firewall/**IDS, NIPS** design, integration, and implementation for Cyber Trap client networks.
* Perform advanced troubleshooting using **Packet tracer** and t**cpdump** on firewalls.
* Implement changes on switches, routers, load balancers (**F5** and **CSS**), wireless devices per engineer’s instructions and troubleshooting any related issues.
* Administration on **Big IP F5 LTM** for all Local Load balancing and use **GTM** for load balancing across Data Centers.
* Security Device - **PaloAlto/ASA** Firewalls, Sourcefire **IPS/IDS, NIPS, VPN**.
* Configuring ASA for **NAT** (Static **PAT**/Manual **NAT**) to enable remote access for sites by doing Port redirection. Configuring various **VPN**s like IPsec Site to Site, **SSL VPN**.
* Extract the logs, perform real time log analysis using **SIEM** technologies and Forensics Analysis of logs as per the request.
* Deploying Cisco WSA and Bluecoat ProxySG (Web Security Appliance) S170 for **URL Filtering** Policies.
* Configuring, Administering, and troubleshooting the Checkpoint, PaloAlto**, Imperva** and **ASA** firewall.
* Configuring rules and maintaining PaloAlto firewalls and analysis of firewall logs using various tools.
* Troubleshooting the **VPN** tunnels by analyzing the debug logs and packet captures.
* Automation of security operations and optimizing the usage of infrastructure.
* Configuring and testing Multicast for both **IPv4** and **IPv6** routing in Data Center Environment.
* Configuration of **SSL VPN** through access blade and up-gradation of Firewall.
* Participated in Pfizer Legacy Data Center Network Infrastructure Transition and Disaster Recovery Center transition for various locations.
* Works closely with Customers in determining the business needs for a Project and build Detail design which includes Data Flow diagram, Logical and Physical Diagram.
* Planning, designing and implementing a secure **ODC** Network setup for upcoming projects.
* Resolving the requests triggered by the network analysts with the help of tools such as BMC Remedy automatically or manually.

**Environment:** Checkpoint firewall. Cisco WSA and Bluecoat ProxySG (Web Security Appliance) S170. F5, CSS load balancers. ASA firewall. Big IP F5 LTM. DHCP server. Packet tracer and tcpdump.

 **NETWORK ENGINEER- Intern November 2009- 2012 January**

 **Genpact- Hyderabad, IND**

 **Responsibilities:**

* Deployed in building the Datacenter right from the scratch, turning up devices and getting into Production.
* Performing network deployment & troubleshooting tasks such as creation and management of **VLANs**, port security, trunking, **STP, RPVST**+, Inter-**VLAN** routing and **LAN** security.
* Working with Cisco catalysts switches that include 3750, 4500 and 6500 in multi VLAN environment for implementation of inter-**VLAN** routing, **802.1Q** trunking and Ether channel.
* Performing **OTV** to extend **L2 VLANs** between data centers over IP on Nexus7018 switches.
* Hands-on experience with **BGP** multi-homing and configuration of Peer-Groups, Route maps.
* Network Design and Deployment of MPLS cloud - Designed, constructed, implemented, tested and launched various network nodes featuring **BGP, OSPF, MPLS** and **VLANS** using **RSTP**, gateway redundancy protocols **HSRP, GLBP** and **VRRP**.
* Configuring/troubleshooting various routing protocols like **OSPF, EIGRP, BGP** on Cisco router series including2900, 3600, 3900, 7200, 7600.
* Expertise in installing, configuring and troubleshooting Juniper EX Switches (EX3200, EX4200, EX4500, EX8200) series.
* Managing and configuring of Access lists, configuring of Wide Area Networking Protocols, **HDLC, PPP**, Frame Relay, **NAT, HSRP** and **VPN**.
* Implementing redundancy with **HSRP**, Ether channel technology (**LACP, PAGP**) etc.
* Deploying Nexus 2248TP GE Fabric Extenders switches in Server Farm environment with **VPC&VDC** features.
* Performing Legacy Catalyst 6509 with SUP-720, Catalyst 4507 with SUP-6 switches migration to Nexus 7k with SUP-2E as part of the data center refresh.
* Configuring Cisco Catalyst 2900, 2960, 3560, 3750, 4500, 4900, 6500 series and Nexus 2248, 5548 and 7010 switches.
* Testing various BGP attributes like **AS Path**, local preference, MED, Weight and replicated customer issues in the testing environment lab.
* Overseeing the **VPN** configuration providing secure access to the users.
* Implementing Firewall policies on Cisco **ASA**5500.
* Working withF5 **BIG-IP LTM 3900**, configured profiles and ensured high availability.
* AAA implementation for network device management with **TACACS+** and Radius server.
* Implementing on Policy Base Routing (**PBR**).
* Preparing engineering documents and network diagrams in Microsoft Visio.

**Environment:** Cisco ASA5500. Cisco Catalyst 2900, 2960, 3560, 3750, 4500, 4900, 6500 series and Nexus 2248, 5548 and 7010 switches. Cisco router series including2900, 3600, 3900, 7200, 7600. Legacy Catalyst 6509 with SUP-720, Nexus 7k with SUP-2E.