**Pradeep Reddy**

**Pradeep.checkpoint@gmail.com**

**(862) 218 - 0092**

**Summary:**

* Network Security Professional with 8 years’ experience in researching, implementing and administering network security solutions. Skilled in supporting and troubleshooting operational issues related to network security Infrastructure.
* Designing, Implementation and Operations of enterprise data networks as Network Security Administrator.
* Strong hands on experience in installing, configuring, and troubleshooting of Cisco 7600, 7200, 3800, 3600, 2800, 2600, 2500 and 1800 series Routers, Cisco Catalyst 6500, 4500, 3750, 2950 and 3500XL series switches.
* Implemented Positive Enforcement Model with the help of Palo Alto Networks.
* 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.
* Worked with the Audit team by using AlgoSec tool to analyze firewall and automating the auditing and analysis of firewalls, routers, VPNs and other security devices.
* Installation, configuration and maintenance of Palo Alto, Cisco ASA 5500, Juniper SRX Firewalls.
* Experience in installing, configuring and troubleshooting of Checkpoint Firewall and Juniper SSG series.
* Performs Tier III network support for enterprise network and solves escalated ticket issues to include Bluecoat proxy rule additions and Cisco firewall issues
* Provided administration and support on Bluecoat Proxy for content filtering and internet access to primary, remote site offices and VPN client users.
* Experience with Blue Coat URL filtering with whitelisting and blacklisting URL, creating rules for content filtering.
* Utilized the Blue Coat Proxy, SIEM, SOC, Tuffin, IPS/IDS.
* Provided administration and support on Bluecoat Proxy for content filtering and internet access to primary, remote site offices and VPN client users.
* Worked on Palo Alto design and installation (Application and URL filtering, Threat Prevention, Data Filtering).
* Configure all Palo Alto Networks Firewall models (PA-2k, PA-3k, PA-5k etc.) as well as a centralized management system (Panorama) to manage large scale Firewall deployments.
* Collaborated Palo Alto Application with the Splunk for advanced security reporting and analysis.
* Hands on experience in configuring and supporting site-to-site and remote access server, IPSec, VPN solutions using ASA/PIX firewalls, Cisco and VPN client.
* Experience in site to site VPN configurations using Cisco ASA 5500 series firewalls
* Responsible for Checkpoint and Cisco ASA firewall administration across global networks.
* Worked on F5 LTM, GTM series like 6400, 6800, 8800 for the corporate applications and their availability.
* Experienced with setting up all features on the Palo Alto's such as: Site to Site VPN's, Global protect, Mind Meld, Aperture, Panorama
* Work experience on Bluecoat Proxy SG for Content filtering and URL filtering.
* Worked on network topological and configurations, TCP/IP, UDP, Frame Relay, Token ring, ATM, bridges, routers, and Switches.
* Experience in configuring Client-to-Site VPN using IPSEC VPN on SRX series firewalls
* Experience in adding Rules and Monitoring Checkpoint Firewall traffic through Smart Dashboard and Smart View Tracker applications
* Experience in configuring, implementing and troubleshooting F5 load balancer in the enterprise network
* Worked on blue coat proxy server as part of recent integration into the project
* Experience with Bluecoat Proxy servers, LAN & WAN management.
* Excellent working knowledge of TCP/IP protocol suite and OSI layers.
* In-depth knowledge and hands-on experience on IP Addressing, Sub netting, VLSM, Summarization and ARP, reverse & proxy ARP and Ping Concepts
* Part for Risk Management Team for reviewing the Technical documentation its procedures and Standards.
* Excellent customer management/resolution, problem solving, debugging skills and capable of quickly learning, effectively analyzes results and implement and delivering solutions as an individual and as part of a team.
* Certified in Accredited Configuration Engineer (ACE) Exam - PAN-OS 7.0 Version

**Technical Skills:**

|  |  |
| --- | --- |
| **Routers** | 1800, 2500, 2600, 2800, 3600, 3750, 3800, 7200. |
| **Cisco Switches** | 2900, 3500, 4000, 4500, 5000, 5800, 6500, Nexus 2k, 3k, 5kand 7k, MSFC, MSFC2. |
| **Routing Protocol** | (BGP, OSPF, EIGRP, IGRP, IGMP, RIP), Routed Protocol TCP/IP, Multicasting (PIM). |
| **WAN Technology** | Frame Relay, WiSM Module in 6509, X.25, L2VPN, L3VPN, E1/T1/DS1/DS3,MPLS |
| **Load Balancers:** | F-5 BIG-IP LTM 2000, 3900, 5000, 6400, 6800 AND 8900, Bluecoat SG8100, AV 510. |
| **Operating systems** | Linux, UNIX, DOS, Windows XP/2007/8, Windows 2003 server and Windows 2008 server |
| **Firewalls** | Checkpoint R65/R70/R75/R77.20, ISA 2004/2006, Palo Alto PA-500/PA-2K/PA-3K/PA-5K, ASA 5585/5520/5510 |
| **SIEM TOOL** | Splunk (Configured with Palo Alto APP). |
| **Performance Tool** | Nagios XI (Using NSClient++ or NCPA Agent). |
| **Algosec** | Firewall Analyzer |

**Work Experience:**

**RBC Capital Markets, Jersey city, NJ. Sep’17 to Present**

**Network Security Engineer.**

**Responsibilities:**

* Experience in Designing, configuring and troubleshooting, security policies, Modular Policy Framework, Routing instances, Zone Based firewalls and implementing different failover mechanisms on Palo Alto & Checkpoint R77 firewalls.
* Expertise configuring and monitoring Checkpoint firewalls through Smart Dashboard and Smart View Tracker Applications.
* Proficient in researching traffic patterns to identify false-positives and/or malicious traffic within IDS (Intrushield, TippingPoint, etc), IPS (Snort), proxy (Bluecoat) and firewalls (CheckPoint, ASA, PIX, and Netscreen).
* Converted Checkpoint VPN rules over to the Cisco ASA solution.
* Migration with both Checkpoint and Cisco ASA VPN.
* Created and manage VPNs for managed service clients including medical community on Cisco, Netscreen and Fortinet Cisco PIX VPN devices
* Responsible for Design and Implement Security, Network and Monitoring System Infrastructure utilizing Fortinet Technology for customers
* Working experience on Blue Coat Proxy SG to safeguard web applications.
* Performs Tier III network support for enterprise network and solves escalated ticket issues to include Bluecoat proxy rule additions and Cisco firewall issues
* Provided administration and support on Bluecoat Proxy for content filtering and internet access to primary, remote site offices and VPN client users.
* Experience with Blue Coat URL filtering with whitelisting and blacklisting URL, creating rules for content filtering.
* 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.
* Design, Build and Implement various solutions on F5 Load balancers and F5 Global Traffic Managers (GTM), Check Point Firewalls, Blue Coat Proxies.
* Install and upgrade Bluecoat proxy SG (900, 810 and SG9000 series) and Proxy AV (510,810 and 1400series) in Datacentre environment with hands on experience on inspection, data loss prevention, content caching and bandwidth management using Blue Coat proxy.
* Support Blue Coat proxy in the explicit mode for users trying to access the Internet from Corp Network.
* Troubleshooting connectivity issues through Bluecoat as well writing and editing web policies.
* Involved in Upgrading Bluecoat proxy servers from SG900-10s to SG 9000-20B
* Deployed Bluecoat Packet Shaper to prioritze internet traffic and optimize WAN bandwidth at several remote offices.
* Used Bluecoat Proxy SG Appliances to effectively secure Web communications and accelerate delivery of business applications.
* Deployment and Management of Bluecoat proxies in forward proxy scenario as well as for security in reverse proxy scenario.
* Configuring rules and Maintaining Palo Alto Firewalls & Analysis of firewall logs using various tools.
* Implemented many number of security policy rules and NAT policy rules on Palo Alto, created Zones, Implemented Palo Alto Firewall interface, Palo Alto IDS and VLAN.
* Palo Alto firewall troubleshooting and configuring policy based on change request, allowing/denying communication between different segments of the network based on requested ports.
* Algosec: Log collection, Firewall online/ offline Audits; determining risky rules and implement to mitigate/ minimize the risk; Firewall rule search for the refreshing servers using AlgoSec firewall analyzing tool.
* Navigated through Algosec and Palo Alto, Checkpoint to find risky ports and unused firewall rules to help with firewall audit.
* Implemented and maintained AlgoSec Firewall Management. Worked on Algosec for firewall rule analysis and firewall rules cleanup.
* Giving Connection ID for the rules on the Palo Alto and Checkpoint based on the policy and Third party that belongs to.
* Generating the FireFlow tickets for the rules for which Connection ID already provided and RISK Rating the rules.
* Assisting with investigative discovery of firewall rules of 500 connectors
* Assisting with documentation of connectors and incorporating them into a larger framework for future automation
* Maintaining Users and Groups as well as Creation of new Users and Policies. Deployed and manage security controls such as DLP, IPS/HIPS, web content filtering.
* Advanced knowledge in TCP/IP suite, security architecture and routing protocols: OSPF, BGP, & EIGRP, IPSEC VPN design connection & protocols, IPSEC tunnel configuration, encryption and integrity protocols.
* Creating Private VLANs & preventing VLAN hopping attacks & mitigating spoofing with snooping & IP source guard
* Performed Security operations in terms of pushing new policies and deploying new rules. Performing security troubleshooting in terms of checking ACLs and ACEs and traffic flow analysis using packet capture features.
* Researched, designed, and replaced aging Checkpoint firewall architecture with new next generation Palo Alto appliances serving as firewalls and URL and application inspection.
* Implemented zone based firewalling and security rules on the Palo Alto Firewall.
* Experience with convert Palo Alto VPN rules over to the Cisco ASA solution. Migration with both Palo Alto and Cisco ASA VPN experience

**Moody’s Analytics, Omaha, NE Feb’17 to Aug’17**

**Network & Firewall Administrator**

**Responsibilities:**

* Working with engineering team to create, document, implement, validate, and manage policies, procedures, and standards that ensure confidentiality, availability, integrity, and privacy of information.
* Implemented Positive Enforcement Model with the help of Palo Alto Networks.
* Experience with Firewall Administration, Rule Analysis, Rule Modification.
* Performs Tier III network support for enterprise network and solves escalated ticket issues to include Bluecoat proxy rule additions and Cisco firewall issues
* Provided administration and support on Bluecoat Proxy for content filtering and internet access to primary, remote site offices and VPN client users.
* Experience with Blue Coat URL filtering with whitelisting and blacklisting URL, creating rules for content filtering.
* Deployment and Management of Bluecoat proxies in the 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.
* Implementing and troubleshooting Firewall rules in Palo Alto Pa-5000 series using Panorama, Checkpoint VSX, R75.40, R76 and R77.20 as per Business Requirements.
* Upgrading the PAN-OS to fix the bugs and any other monitoring issues.
* Done documentation for Rule Justification for Palo Alto Firewall.
* Installed and categorized URL filtering categories according to the environment requirements.
* Installed and configured Nagios XI performance tool in the servers for getting live performance of the servers (like CPU, Memory and Disk Usages).
* Collaborated Palo Alto App with Splunk for advanced security and analysis.
* Updating the daily URL Filtering reports for analysis from Splunk Palo Alto APP.
* Implementing and troubleshooting firewall rules in Checkpoint R75.40 and R77 Gaia as per the business requirements.
* Experience with configuring Virtual Server and Configuring Load balancing methods in F5 LTM.
* Application (Layer 7) Firewall. Configuring RIP, OSPF and Static routing on Juniper M and MX series Routers.
* Worked on Migrating from ASA 5540 to ASA 5585.
* Created Virtual Contexts, Vlans, and Interfaces in ASA 5585.
* LAN base as well as Cable base failover configuration on Cisco firewall.
* Configuring Vlans, Self IP's & Routes on F5 load balancers.
* Deployed and supported Bluecoat Proxy SGs, and Bluecoat ThreatPulse.
* Experience with devices Palo Alto Network firewalls such as security NAT, Threat prevention & URL filtering.
* Reviewing & creating the FW rules and monitoring the logs as per the security standards in Checkpoint and Net Screen Firewalls.
* Execute the Incident Management process tasks in adherence with global and local requirements
* Configuring and troubleshooting Cisco ASA firewalls, Palo Alto and Checkpoint Firewalls.
* Assist with various duties that will arise including: implementation, configuration, management.

**Staples, Minneapolis, MN Dec’15 to Jan’17**

**Network Security Engineer**

**Responsibilities:**

* Maintaining Checkpoint security policies including NAT, VPN and Secure Remote access, Configuring IPSEC VPN (Site-Site to Remote Access).
* Maintained Corporate Firewalls & Analysis of firewall logs using various tools.
* Implementation and troubleshooting of ASA firewall
* Adding security policies and security rules on Checkpoint and ASA firewall.
* Regular upgrade and maintenance of Infrastructure, Installing, configuring, and maintaining Cisco Switches (2900, 3500 ,7600, 3700 series, 6500 series) Cisco Routers (4800, 3800, 3600, 2800, 2600, 2900, 1800, 1700, 800) Cisco Router and Switches, Juniper Routers and Firewalls, Nexus 9K, 7k,5k & 2k, f5 BIG IP, Palo Alto Firewalls, BlueCoat Proxy and Riverbed Steelhead appliances
* Managed BlueCoat Proxy and Web Filter solution
* Security: McAfee Firewall Enterprise, Palo Alto Networks Firewall, McAfee Web Gateway, BlueCoat Proxy, STIG Compliance
* Manages BlueCoat Proxy appliance configuration and is NPC's proxy appliance administrator. He is responsible for analyzing data dealing with traffic composition, usage and throughput as well as blocking customer specified URL content.
* Responded to on-call pages for various connectivity issues representing Network/Proxy team
* Perform script review for change management
* Deploying Cisco WSA, Zscaler and Bluecoat Proxy SG (Web Security appliance) S170 for URL filtering policies.
* Worked on Blue Coat by adding websites to blocked list on the bluecoat proxies based upon business requirements.
* Configuring rules and Maintaining Palo Alto Firewalls & Analysis of firewall logs using various tools.
* Taking backup of checkpoint configuration, security policies, logs with policy package management, database revision controls, upgrade export and import, snapshot procedure on regular basis.
* Successfully installed Palo Alto PA-3060 firewalls to protects Data Centre and provided L3 support for routers/switches/firewalls
* Responsible for designing and implementation of customer’s network and Security infrastructure.
* Worked extensively in Configuring, Monitoring and Troubleshooting Cisco's ASA 5500/PIX security appliance, Failover DMZ zoning & configuring VLANs/routing/NATing with the firewalls as per the design.
* Black listing and White listing of web URL on Bluecoat Proxy servers.
* Configuring routers, switches, WLC, Access Points, Bluecoat Proxy Server, Cisco ASAs, etc.
* Configured Routing protocols such as RIP, OSPF, EIGRP, MPLS static routing and policy base routing.
* Experience on Checkpoint Smart Domain Manager NGX R60 & R70.
* Log analysis using Checkpoint Smart view tracker and SPLUNK.
* Configured HSRP and VLAN trucking 802.1Q, VLAN Routing on Catalyst 6500 switches.
* Managed the F5 BigIP GTM/LTM appliances to include writing iRules, SSL offload and everyday task of creating WIP and VIPs
* Involved in Troubleshooting of DHCP and other IP conflict problems.
* Performed Switching Technology Administration including VLANs, inter-VLAN Routing, Trunking, STP, RSTP and Port Aggregation & Link Negotiation.

**WEC Energy Group, Milwaukee, WI Jan’14 to Nov’15**

**Network Engineer**

**Responsibilities:**

* Provides day to day support for firewall engineering and operations tasks and level 1 & 2 on-call technical support for the Firewall Engineering and Operations team; including assisting peers with issues and escalation.
* Configured VLAN’s, Private VLAN’s and enabling inter-VLAN routing.
* Configuring routing protocols like EIGRP, OSPF & BGP and troubleshooting layer3 issues.
* Responsible for designing and implementation of customer’s network and Security infrastructure.
* Worked on Cisco 7200, 3800, 3600, 2800, 2600, 1800 series Routers and Cisco 2900, 3500, 4500, 5500, 6500 and Nexus 5K series switches
* Policy cleanup and re-organization/Code Upgrade/ Hardware refresh for bluecoat proxy
* Technologies include Cisco ASA Firewall, Checkpoint Firewall, Bluecoat proxy
* Create, Modify, and implement policy for Firewall and Proxy
* Software Upgrade for Palo Alto Devices and Integrating of Active Directory/LDAP with Palo Alto Next Generation Firewall.
* Integrated LDAP with Palo Alto rule base and Global Protect Client VPNs.
* Handle tickets related to Palo Alto to grant web access to company staff.
* Conducted and implement Network and software installations and upgrades.
* Configured Remote User VPN, Site to Site VPN, and Remote Access VPN, Easy VPN, SSL VPN for Client based and Clientless applications.
* Design and configuring of OSPF, BGP on Juniper Routers (MX960, MX480) and SRX Firewalls (SRX240, SRX550)
* Blocking malicious sites as required by the information security system using Bluecoat Proxies
* Content filtering using Bluecoat Proxy SG.
* Creating VPLS connection between H and NE40's depend on customer services such as (Internet, VoIP, L2vpn, L3vpn, IBGP and EBGP)
* Implementation of Cisco ACS server & integration with RSA for two factor authentication
* Worked on Disaster Recovery (DR) test plan and build an IPSEC tunnel site to site.
* Advanced knowledge, design, installation, configuration, maintenance and administration of Checkpoint Firewall R55 up to R77.
* Configured layer 2 and layer 3 Switch port, L3 router interface, VLAN interface, VRRP on cisco and juniper devices.
* Rollout of RSA 6.0 Ace Server and Client for Windows Logon & VPN Authentication.
* Configured OSPF redistribution and authentication with type 3 LSA filtering to prevent LSA flooding

**Ralium Infosystems, India June 09 to Oct’13**

**Network Engineer**

**Responsibilities:**

* Worked on network-based IT systems such as racking, stacking, and cabling.
* IOS upgrading of 1900, 2900, 3500 series Cisco Catalyst switches and 2500, 2600, 3600 series Cisco routers using TFTP.
* Supported a transparent proxy environment which includes BlueCoat Proxy, Proxy AV, Reporter
* Hardware upgrade - Bluecoat proxy and proxy AV from SG 810-10/AV810 to S400
* Performed policy comparison and merger on Bluecoat Proxy SG
* Updated policy for Checkpoint and juniper firewall. BlueCoat Proxy and Proventia IPS/IDS
* nstalled and performed repairs to hardware, software and Bluecoat Proxy
* Worked with F5 Lboad balancing, IDS/IPS, Bluecoat proxy servers and Administrating.
* Policy and Rule maintenance using Palo Alto Panorama device
* Served as a main escalation point of contact for level I team.
* Coordinated with higher-level support and external vendors for resolution.
* Maintained all servers & network equipment with current stable firmware, IOS images & access control lists.
* Installation and Configuration of Cisco Catalyst switches 6500, 3750 & 3550 series and configured routing protocol OSPF, BGP with Access Control lists implemented as per Network Design Document and followed the change process as per IT policy.
* Monitoring customer network (Internet, VoIP, L2vpn, L3vpn, IBGP and EBGP).
* Giving support and configuring Cisco Routers such as 800, 2801, 2850, 2950
* Maintained and configured all Extended Access Lists securing VLAN 802.1q trunks to W2003/8 servers, STP, OSPF, Port-Channels, Classes, Group, Objects, Load-Balancing, ACS, Wireless setup for corporate office and stores.
* Implemented strategies for operating systems, virus protection, mail systems and Internet services.
* Performed scheduled Virus Checks & Updates on all Servers & Desktops.