**Vinay Kumar**

**Network Security Engineer**

**Professional Summary:**

* Over all **7 years** experience configuring, administrating and troubleshooting infrastructure with Cisco platform Routing, Switching and Security.
* **Black listing** and **White listing** of web URL on **Blue Coat Proxy Servers**.
* Strong knowledge on mitigation of DDoS attacks & SSL implementation on Cisco and Palo Alto firewalls.
* Working experience on Rapid 7 for vulnerability scanning on the network devices.
* 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.**
* Dealt with Cisco router models (7600, 7200, 3800, 3600, 2800, 2600, 2500, and 1800)series.
* Experience working with Cisco Nexus 2148 Fabric Extender and Nexus 5000 series to provide a flexible Access Solution for Data Center access architecture.
* Extensively worked on Cisco catalyst 6509 and implemented VSS along with VDC and VPC on Nexus 5505, 7009 switches.
* Experienced with routing protocols **(RIPv1/2, IGRP, EIGRP, OSPF, BGP),** switching **(VLANS, VTP Domains, STP**and **trunking)**,
* **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.
* Knowledge of AWS cloud computing platform such as VPC (Virtual private cloud), EC2 and load balancing with ELB using ECB.
* Experience working on Palo Alto Firewall
* Managed the F5 BIG-IP GTM/LTM appliances to include writing iRules, SSL offload and everyday task of creating WIP and VIPs. Wide experience in implementing and managing F5 BIG-IP loadbalancing.
* Responsible for Checkpoint and Cisco ASA firewall administration.
* Experience with management platforms such as **Panorama, Juniper NSM and SmartCenter.**

### 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)

* Server load-balancing utilizing F5 LTM-Big IP, including, APM and ASM modules.
* Administration of production Windows Servers infrastructure that includes **Domain Controllers, IIS Web Servers, SharePoint, File and Print and FTP/SFTPservers.**
* Experience working on Cisco Catalyst Series 3750, 3500, 4500, 4900, 6500, 2950; Nexus 2K, 5K, 6K and 7K series switches.
* Worked on administration and configuration of Check Point Firewall, Palo Alto Networks Firewall and Cisco ASA Firewall applied across global network.
* Experienced working with security issues related to Cisco ASR9K.
* Experience in risk analysis, security policy, rules creation and modification of Checkpoint, Cisco ASA, Palo Alto Firewall, Fortinetnetworks.
* Experience with **DNS/DFS/DHCP/WINS Standardizations** and Implementations
* Comprehensive expertise in the implementation of optimization, analysis, troubleshooting and documentation of LAN/WAN networking systems.
* Working knowledge on configuring access lists. Troubleshooting DNS/DHCP issues within the LAN network.
* Designed and configuring of OSPS, BGP and juniper routers and SRX firewall.
* Deep knowledge of AWS cloud computing platform such as VPC (Virtual private cloud), EC2 and load balancing with ELB using ECB.
* Experience working with Juniper EX series Ethernet switches and SRX series.
* Worked on ASR 901, 920, 903 and 9000 series Cisco routers

### Education & certifications:

* **Bachelors of Technology in Information Technology, India**.
* **Cisco Certified Network Associate(CCNA) – Routing and Switching**
* **Palo Alto Accredited Configuration Engineer ACE**

### Technical Skills:

|  |  |
| --- | --- |
| **Networking** | TCP/IP, Cisco IOS, IOS-XR, LAN/WAN interconnection, VPN, IP-Sec, Frame-Relay, ISDN, RIP, OSPF, EIGRP, IS-IS, BGP, MPLS, STP, RSTP,  MST, VTP, NAT, ACLs |
| **Cisco Routers** | Cisco (1800/2600/3600/3800/7200/7600 series), Cisco ASR 9Ks) |
| **Cisco Switches** | Cisco (2900/3500/3700/5500/6500 Series, Nexus 7k),Cisco Catalyst 6509, 6513, 3500, 5500, 5000, 2900(IOS- Version 12.4) |
| **Firewalls** | Cisco ASA (5510,5540), Checkpoint R65, R70, R75, R77 Gaia, Juniper  SSG,Checkpoint, Fortinet, Palo Alto |
| **Other Networking Tools** | F5 LTM (Big IP), GTM, 3 DNS, Bluecoat Proxy SG, Wireshark, Remedy,  Secure Track, CounterAct, Citrix Netscalar, SIEM, SCADA, Rapid 7 |
| **VPN** | Cisco IOS Firewall feature set (IOS 12.X) |
| **Routing** | OSPF, EIGRP, BGP, RIP-2, PBR, Route Filtering, Redistribution, Summarization, Static Routing |
| **Switching** | VLAN, VTP, STP, PVST+, RPVST+, Inter VLAN routing & Multi-Layer Switching, MulticastOperations, Layer 3 Switches, Ether channels, Transparent Bridging |
| **Operating Systems** | Win 95/98, NT, XP,VISTA, LINUX, UNIX |

### Professional Experience:

### Client: Humana Inc,Louisville, KY Feb 2018 – Present

**Role: Sr. Network Security Engineer**

**Humana Inc. (Humana),** incorporated on July 27, 1964, is a health and well-being company. The Company's segments include Retail, Group and Specialty, Healthcare Services and Individual Commercial. The Retail segment consists of Medicare benefits, as well as individual commercial fully insured medical benefits, including dental, vision, and other supplemental health products. The Group and Specialty segment consists administrative services only (ASO) products.

**Responsibilities**:

### Configured, implemented and troubleshooting issues on Checkpoint R77.10 Gaia, R75, Cisco ASA 5540 firewalls for the client environment.

### Setup/Configured/Supported Websense WSG Proxy. This included implementing SSL with WCCP.

### Designed/configured Websense DLP (Network and Endpoint).

### Configuring & Administration of the Checkpoint Firewall that includes creating Hosts, Nodes, Networks, Static & Hide NAT's.

### Experience in creating multiple policies and pushing them intoCheckpoint Firewall (Gateways) and hands-on experience in managing the Checkpoint Management Server and Gaia operating system.

### Applied security enhancement by implementing certificates and RSA keys for authentication.

### Installed and administered RSA Secure ID token authentication servers.

### Responsible for the integrity of PKI Infrastructure.

### Defined Security best practices, Security policies and security improvements on DDOS mitigation solution

### Setup testing labs to simulate DDoS Attacks in real-time

### Create & Present on ArcSight Enterprise Security Manager to newly hired Security Engineers.

### Configure ArcSight assets

### Forescout CounterAct- NAC, endpoint compliance, real-time intelligence, and policy-based control.

### Network Access Control and its implementation using Forescout CounterAct

### 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.

### Involved in Troubleshooting IP Addressing Issues and Updating IOS Images using TFTP.

### Experience with, but not limited to, the following Connectors/Agents: DNS, IIS, Syslog, WUC, WINC, McAfee EPO/AV, Symantec AV, Websense Proxy / DLP, Checkpoint FW, Sourcefire IDS, FireEye, Web Inspect, Nessus, Rapid7 Vulnerability Scanner

### 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.

### Performed site refreshes on Cisco switching and Aruba wireless infrastructure at several locations

### Configuration and troubleshooting of CISCO & ARUBA wireless devices

### Release and Patch management of different network devices, determining the vulnerabilities using Rapid 7 and its mitigation.

### Compliance check and administering network devices in Forescout CounterAct

### Monitoring network access rules usage on Tufin Secure Track.

### Policy Reviewing, Audit and cleanup of the un-used rule on the firewall using Tufin

### Configuring Tufin and network devices for monitoring network rules.

### Manage project task to migrate from Cisco ASA firewalls to Check Point firewalls.

### Maintain SIEM operations and document current network infrastructure and environment.

### Creation of technically detailed reports on the status of SIEM to include metrics on items as of number of logging sources, log collection and server performance.

### Worked on VPN configuration, routing, NAT, access-list, security contexts, and failover in ASA firewalls.

### Troubleshoot, conduct scans and assess Network issues, then patch vulnerabilities and mitigate DDoS attacks and other.

### Analysis and mitigation of DDoS (Distributed Denial of Service) attacks.

### Configuring IPSec VPN (Site-Site to Remote Access) on Cisco ASA series firewalls.

**Environment:**Cisco ASA5580/5540/5520, ArcSight, CheckpointR70, R75, R77.20 Gaia, Juniper SSG/SRX, Big IP F5 LTM, ASM, Nexus switches, TCP/IP, VPN, High Availability Bluecoat Proxy servers, IDS/IPS. SIEM and Monitoring, Tufin, Forescout CounterAct, Cisco Prime

### Client: Kroger, Cincinnati, OH Jan 16 –Jan 18

### Role: Sr. Network Engineer

**The Kroger Co.,** or simply Kroger, is an American retailing company founded by Bernard Kroger in 1883 in Cincinnati, Ohio. It is the United States' largest supermarket chain by revenue ($115.34 billion for fiscal year 2016), the second-largest general retailer (behind Walmart) and the seventeenth largest company in the United States. Kroger is also the fifth-largest retailer in the world and the third largest American-owner private employer in the United States. Kroger is ranked #17 on the Fortune 500 rankings of the largest United States corporations by total revenue.

### Responsibilities:

### Performed OSPF, BGP, DHCP Profile, HSRP, IPV6, Bundle Ethernet implementation on ASR redundant pair.

### Experience in Configuring, upgrading and verifying the NX-OS operation system.

### Upgraded Cisco 6500, 3750, 2960s, Nexus 5000, Nexus 2000, Nexus 7000 switch IOS software.

### Assisted in MPLS migrations, implemented a backup for the existing WAN connection using site-to-site IP sec VPN tunnels.

### Worked on Converting the Partner IPSEC VPN from one Data Center to Another Data Center.

### Deploying and decommission of VLANs on core ASR, Nexus 7K, 5K and its downstream devices.

### Experience configuring Virtual Device Context in Nexus 7010.

### Deployed & Implemented rules and created various zones in Palo Alto firewalls like PA2020, PA5020, PA5050.

### Configuring rules and Maintaining Palo Alto Firewalls & Analysis of firewall logs using various tools Editing and Changing Palo Alto Polices and Monitoring threats on firewalls.

### Experience in creating virtual domains for employing proxy servers on Fortinet firewalls. Configuring VPN both B2B and remote access SSL and centralized policy administration using Forti Manager, building Fortigate High Availability using Fortigate Clustering Protocol (FGCP).

### Configured application load balancing using F5 LTM. Experience with configuring VIP, Pools on F5 LTM and working with rule management on LTM.

### Strong experience in creating firewall policies as per the requirements on Palo Alto

### Worked on Layer 2 protocols such as STP, VTP, STP, RSTP, PVSTP+, MST and other VLAN troubleshooting issues and configuring switches from scratch and deployment

### Conversions to BGP WAN routing. Which will be to convert WAN routing from OSPF to BGP (OSPF is used for local routing only) which involves new wan links.

### Experience with design and implementation of Data center migration

### Implemented Changes on Existing configurations for the applications on F5 load balancer.

### Worked on Solar Winds NCM for pushing the config to Routers, Switches and Firewalls.

### Made DHCP and DNS changes through Infoblox.

### Configured DNS entries using Infoblox.

### Used Infoblox to create and manage newly created DHCP scopes.

### Worked on F5 Enterprise Manager 3.1 version to manage multiple F5 LTM devices from single-pane view.

### Configured rules and maintaining Palo Alto firewalls & analysis of firewall logs using various tools.

### Centrally managed all Palo Alto firewalls using Palo Alto, Panorama M-100 management server.

### Experience on Panorama firewall management tool which provides centralized monitoring and management of multiple Palo Alto devices from single window.

### Monitoring Network devices using Solar Winds.

### Performed Palo Alto firewall rule audit and optimization using Algosec.

### Configured and implemented Fortinet Security systems Firewall.

### Implemented Forti Manager 300D and Fortigate 600D cluster for deploying IPsec VPNs.

### Configured High availability, User ID on Palo Alto firewall.

### Configured Virtual server, service groups, Session persistence, Health monitors and Load balancing methods in new F5

### Worked on Data, VoIP, security as well as wireless installations and technologies

### Working on CISCO Prime and Wireless controller to manage all WAPs.

### Analyzed network health and performance issues using Solar Winds.

### Client: Tracfone Miami, FL Mar 2015 – Nov 2015

### Title: SecurityEngineer

**TracFone Wireless, Inc. (TFWI)** is America’s largest prepaid, no-contract cell phone provider. TFWI is a subsidiary of Mexico's largest telecommunications company, América Móvil, the leading provider of telecommunication services in Latin America, and offers products and services under several other brands. It operates as a mobile virtual network operator (MVNO), holding agreements with the United States' largest wireless network operators to provide service using their networks, including Verizon Wireless, AT&T Mobility, T-Mobile US, Sprint Corporation, and U.S. Cellular. TracFone Wireless had 25.668 million subscribers in 2015.

**Responsibilities**:

### Daily technical hands-on experience in the configuration, troubleshooting of JuniperSRXfirewallsas 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 JuniperFirewalls.

### Creating and ProvisioningJuniper SRX firewallpolicies.

### Day-to-Day work involves scheduling firewall policy provisioning and working with users to identify connectivity related issues and troubleshoot using both Smart Utilities andCLI.

### Support Data Center Migration Project involving physicalre-locations.

### Build and configure Active/Standby Failover on Cisco ASA with statefulreplication.

### 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.

### 24 x7 on call support.

### Configuring rules and Maintaining Palo Alto Firewalls& Analysis of firewall logs using various tools.

### Managing and administering JuniperSRXandCheckpointFirewalls at various zones including

### DMZ, Extranet (Various Business Partners) and ASZ and internal.

### Implementing Security Solutions in Juniper SRX and NetScreen SSG firewalls by usingNSM.

### Juniper Firewall Policy Management using NSM and Screen OS CLI.

### 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 ASAFirewalls.

### Understand the flow of traffic through the Check Point Security Gateway cluster and troubleshoot connectivity issues using advanced troubleshooting from Command LineUtilities.

### Use Tools such as SKYBOX for Firewall Policy optimization and rule base Clean up.

### Support Blue Coat Proxy in explicit mode for users trying to access the Internet from Corp Network.

### 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 to9.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.

### Troubleshooting connectivity issues through Blue coat as well writing and editing web policies.

### Involved in Upgrading Bluecoat proxy servers from SG900-10s to SG9000-20B.

### Administration Big IP F5 LTM for all Local Load balancing and use GTM for load balancing acrossData Centers.

### FWSM configurations in single/multiple contexts with routed and transparent modes.

### Environment:Juniper (SRX, JUNOS, ScreenOS, NetScreen SSG), Cisco (Checkpoint, ASA Firewalls), Palo Alto Firewalls, Big IP F5 LTM/GTM, TCP/IP, Fortigate.

### Client: Flipkart Pvt Ltd, India July2013 – Nov2014

### Role: Network Engineer

### Responsibilities

### Responsible for service request tickets generated by the helpdesk in all phases such as troubleshooting, maintenance, upgrades, patches and fixes with all around technical support

### Implementation and Configuration (Profiles, I Rules) of F5 Big-IP C2400 load balancers

### Involved in L2/L3 Switching Technology Administration including creating and managing VLANs, Port security, Trunking, STP, Inter-Vlan routing, LAN security.

### Worked on the security levels with RADIUS, TACACS+.

### Completed service requests (i.e. – IP readdressing, bandwidth upgrades, IOS/platform upgrades, etc.)

### EIGRP and BGP based PwC Supporting network by resolving level 2 &3 problems of internal teams & external customers of all locations.

### Configuring Big-IP F5 LTMs (virtual servers, pools, SNATs, health monitors, rules) for managing the traffic and tuning the load on the network servers.

### Upgrade Cisco Routers, Switches and Firewall (PIX) IOS using TFTP

### Identify, design and implement flexible, responsive, and secure technology services

### Performed load balancing and application level redundancy by deploying F5 BIG-IP LTM 3900.

### Configured switches with port security and 802.1x for enhancing customer’s security.

### Monitored network for optimum traffic distribution and load balancing using Solar winds.

### Created scripts to monitor CPU/Memory on various low end routers in the network.

### Handled Tech Support as it relates to LAN & WAN systems.

### Ensure Network, system and data availability and integrity through preventive maintenance and upgrade.

### Updated the HP open view map to reflect and changes made to any existing node/object.

### Handled SRST and implemented and configured the Gateways, Voice Gateways.

### Configuring HSRP between the 3845 router pairs for Gateway redundancy for the client desktops.

### Configuring STP for switching loop prevention and VLANs for data and voice along with Configuring port security for users connecting to the switches.

**Environment:**Net Flow, TACACS, EIGRP, RIP, OSPF, BGP, VPN, MPLS, CSM, Ether Channels, Cisco 7200/3845/3600/2800 routers, Cisco 6509/ 3750/3550/3500/2950 switches, Checkpoint firewalls (SPLAT).

### Client: Atria Convergence Technologies, India Oct 2012 – June 2013

### Role: Network Engineer

### Responsibilities:

### Performed troubleshooting, while maintaining trouble ticket tracking, following internal/external escalation procedures and customer notifications. Configured Cisco Routers for RIP, IGRP RIPv2, EIGRP, OSPF, Static and default route.

### Configured ASA 5510 appliance and VPN.

### Installed and configured PIX 520, 525, 535 series firewalls, configured standard and extended access-lists and policy- based filters.

### Implemented SNMP on Cisco routes to allow for network management. Completed the installation and configuration of T1, T3 & OC3 circuits.

### Troubleshoot TCP/IP problems and connectivity issues.

### Supporting Development team for the access to corporate network and outside world. Providing access to specific IP, Port filter and port access.

### Physical cabling, IP addressing, Wide Area Network configurations (Frame-relay and ATM).

### Configured the Cisco router as IP Firewall and for NATing.

### Worked with the Help Desk for circuit troubleshooting to give Support to the Tech persons at the site.

### Configuring routers and sending it to Technical Consultants for new site activations and giving online support at the time of activation.

### Switching (Ethernet) related tasks included implementing VLANS and configuring ISL trunk on Fast-Ethernet channel between switches.

**Environment:**Cisco 2990/3550/6550 switches, Cisco 7200/3845/3600/2800 routers, EIGRP, RIP, OSPF, BGP, VLAN, VPN, Ether Channels.