**Sathwik Patteti**

**Senior Network Security Engineer**

**pattetisathwik1@gmail.com**

**412-572-1745**

**Summary**

* 8+ years of experience in Networking, including hands-on experience in routing, switching, security and cloud technologies.
* Experienced with installing and managing IT services such as Active Directory, Site replication, DNS, SSH, DHCP, DNS, NAT and Terminal service.
* Experienced in troubleshooting and installation of Palo Alto firewall series link PA-7k (7050,7080), PA -5k (5430, 5420), PA -3k, PA-2700, PA-1200 and PA-800.
* Configured, installed and maintained Fortinet Firewalls device series such as (FortiGate 3000, 1800, and 1000).
* Expertise in configuring Datacenter switches Cisco Nexus 9k, 7k, 6k, 5k, 3k series as well as catalyst switches 3k, 4k, 6k series.
* Design and build SDN data center environment, including Cisco ACI.
* Enhanced level of experience in configuration &amp; troubleshooting of routing protocols: RIPv1, RIPv2, EIGRP, OSPF, MP-BGP, IS-IS BGPv4, LDP and MPLS.
* Experience working with Cisco ISE to design, implement and support cisco-based security as well as other providers.
* Working with AWS cloud platform and its various services, which include IAM, EC2, S3, ECS, CLI, SNS, RDS, Redshift and Cloud Formation etc.
* Experience with cisco ASR 9k/1k, cisco GSR, cisco CSR, cisco 7200vxr and cisco 7600, 7200, 6500, 4500, 4000, 3800, 3600 and 3200 routers.
* Involved in managing Viptela SD-WAN policies and traffic engineering rules, prioritizing essential applications for their optimal delivery.
* Worked on Network Monitoring using SNMP and other management tools (SPLUNK, Wireshark, and SolarWinds).

**TECHNICAL** **SKILLS**:

|  |  |
| --- | --- |
| **Firewalls** | Palo Alto (PA-7080, PA-7050, PA-7000, PA-5000, PA-3000 series ), Fortinet firewalls (FortiGate1000, FortiGate3000, FortiGAte3200, FortiGate7081F, FortiGAte6500F, FortiGate6300F, FortiManager, FortiAnalyzer), Cisco Firepower (4115, 4125, 4145 series), Cisco ASA 5506-X, 5508-X series, Checkpoint R77.30 and R80.0 |
| **Switches** | Nexus 2k/5k/7k, Arista switches and Juniper switches. |
| **Routing series** | Cisco ISR 4000, 1000, 900 and 800, Juniper MX480 and MX960 series. |
| **Routing Protocols** | OSPF, EIGRP, BGP, RIPv2, IS-IS, PBR, Route Filtering, Redistribution, Summarization, and Static Routing. |
| **Data Center** | Nexus (9300, 7000, 5000 series), Arista 7050SX3 and Juniper EX2200, EX2500, and EX3200 series |
| **Cloud** | AWS EC2, VPC, IAM, Lambda, S3, Cloud Front, RDS, DynamoDB, Elastic Cache, Route53, CloudWatch, Cloud Formation, Amazon Elastic Map Reduce (EMR). |
| **Load Balancers** | F5 BIG-IP i10000, and i5000 series, 5000, 6000 series and VIPRION 2400 Chassis A113 and Citrix load balancers. |
| **SD WAN Technology** | Cisco Viptela (vEdge, vManage, vSmart & vBond) Aruba S2500, 3800 and Meraki MR30H technology. |
| **Security** | IPsec, VPN Configuration, VPN Concentrator, Authentication AAA TACACS RADIUS Ethereal, Encryption technologies like DES, 3DES, IPS. |

**PROFESSIONAL EXPERIENCE:**

**Wells Fargo, Edison, NJ November 2023 – Present**

**Senior Network Security Engineer**

**Responsibilities:**

* Deployed and managed Palo Alto Networks firewalls (PA-7050, PA-5420, PA-3430, PA-7080, PAN-PA-7000-100G-NPC-A, PA-7000 series) in enterprise environments.
* Configured and managed **load balancing solutions** using **F5 BIG-IP (LTM, GTM), Citrix ADC (NetScaler), and AWS Elastic Load Balancer (ELB)** to optimize application performance.
* Integrated **SDN solutions with cloud platforms (AWS, Azure, GCP)** for hybrid cloud networking and automated network provisioning.
* Configured and managed **Cisco ASA firewalls (5500-X series, 9k, 8k, 7k)** to enhance enterprise network security.
* Configured and maintained Fortinet Firewalls (FortiGate 4800F, 4200F, 4400F, and 3000F), ensuring security best practices and compliance.
* Managed firewall policies and security profiles in Panorama M-500 and FortiGate devices to align with corporate security policies.
* Collaborated with network architects to design and implement resilient security solutions using Palo Alto, Fortinet, Cisco, and Juniper SRX firewalls.
* Architected and deployed Cisco ACI solutions for secure communication across data centre environments.
* Designed and deployed **secure, scalable, and highly available cloud infrastructure** on **AWS** using best practices.
* Implemented **traffic engineering policies** using **Viptela SD-WAN** to prioritize critical applications and optimize bandwidth utilization.
* Troubleshot **IPsec VPN issues,** including Phase 1 and Phase 2 negotiation failures, authentication mismatches, and encryption issues.
* Configured and secured wireless networks with WPA2 and WPA3, deploying Wi-Fi intrusion detection and prevention systems (WIDS/WIPS).
* Utilized IEEE 802.11e QoS standards for prioritizing network traffic and optimizing voice and video conferencing services.
* Deployed and configured AWS cloud infrastructure, managing services like VPC, Route 53, Elastic Load Balancing (ELB), and CloudFront.
* Managed SD-WAN policies, improving application delivery and user experience, with zero-touch provisioning (ZTP) for SD-WAN devices.
* Designed and maintained global voice systems (Cisco Call Manager, Cisco Unity voicemail systems, Cisco Emergency Responder) ensuring high availability and security.
* Monitored and optimized VOIP systems, proactively resolving potential security threats to maintain stable infrastructure.
* Implemented network security measures to achieve PCI DSS, SOX, HIPAA, and other regulatory compliance standards.
* Designed, deployed, and managed **SD-WAN solutions** using **Cisco Viptela, Fortinet, and VMware Velocloud** to enhance network agility and performance.
* Utilized FortiAnalyzer and other monitoring tools for ongoing compliance assessments.
* Directed continuous compliance monitoring for financial systems, ensuring adherence to NIST, SOX, PCI, and GLBA.
* Developed Python scripts to interact with network devices (routers, switches, firewalls), enabling automated configuration and analysis.
* Integrated Python scripts with network APIs to extract data for reporting and ensure consistency across devices.
* Integrated Illumio with SIEM and firewall management systems for enhanced network security visibility.
* Developed **Ansible roles and playbooks** for provisioning and managing **firewalls, routers, and switches** across multi-vendor environments (Cisco, Palo Alto, and Fortinet).
* Integrated Cisco ISE for identity management, authentication, and policy enforcement.
* Implemented OSPF, EIGRP, and BGP routing protocols to enhance network performance and security.
* Configured, deployed, and managed **Juniper SRX, MX, and EX series** for enterprise and data center networking.
* Designed, deployed, and managed **Cisco Application Centric Infrastructure (ACI)** to optimize **data center networking** and automation.
* Deployed F5 Advanced WAF, SSL interception, and application security policies to protect against DDoS and SQL injection attacks.
* Designed and deployed **Google Cloud networking solutions**, including **VPC, Cloud VPN, Interconnect, and Cloud Load Balancing** for secure and scalable cloud connectivity.
* Designed, deployed, and managed **Azure cloud infrastructure**, including **Azure Virtual Networks (VNet), NSGs, Load Balancers, and ExpressRoute** for secure and scalable networking.
* Fine-tuned ADC settings and implemented SSL encryption/decryption policies for secure communication.
* Deployed and managed **NetScout nGeniusONE** for real-time network performance monitoring, traffic analysis, and anomaly detection.
* Worked on the response to network security incidents, working with teams to resolve issues and mitigate risks.
* Used GIT for version control, managing network configurations and policies.
* Integrated security measures for SCADA-like systems in financial data centers, ensuring secure communication and monitoring.
* **Implemented IPsec encryption protocols** (IKEv1/IKEv2, ESP, AH) to ensure data confidentiality and integrity.
* Implemented **QoS (Quality of Service) policies and traffic shaping** to ensure optimal bandwidth allocation and minimize latency.
* Troubleshot and optimized **iRule performance** to ensure minimal latency and efficient request handling.
* Troubleshot **VPN connectivity issues**, including authentication failures, encryption mismatches, and latency concerns.
* Performed **packet capture and deep packet analysis** using **Wireshark** to troubleshoot network performance, latency, and security issues.
* **Optimized VLAN assignments** to enhance network scalability, reduce broadcast domains, and improve efficiency.
* Developed **Python scripts** for network automation, configuration management, and log analysis.

**Capital One, Mclean, VA September 2022 – October 2023**

**Senior Network Security Engineer**

**Responsibilities:**

* Worked on Palo alto PA-7K, PA-5K, PA-3K and implementing security policies and managing the traffic on Firewalls series.
* Implemented **IPsec and SSL VPNs** on Cisco ASA for secure remote and site-to-site connectivity.
* Integrated **NetScout with SIEM platforms and security tools** to enhance threat detection and incident response capabilities.
* Implemented **Layer 4 and Layer 7 load balancing** for high availability, scalability, and redundancy in enterprise environments.
* Configured, deployed, and managed **Aruba wireless controllers (Aruba Mobility Controllers, Aruba Instant, and Aruba Central)** for enterprise Wi-Fi solutions.
* Implemented and optimized **Juniper firewall security policies, NAT, IPSec VPNs, and UTM features** to enhance network security.
* Configured and managed **GCP IAM roles, service accounts, and identity federation** to enforce security and access control.
* Integrated **IPsec encryption with Viptela SD-WAN** to ensure secure site-to-site communication across branch offices.
* Configured and managed **AWS services** such as **EC2, S3, VPC, RDS, IAM, Route 53, Lambda, and Cloud Formation** for cloud-based networking and automation.
* Configured **SD-WAN policies** for **traffic engineering, application-aware routing, and dynamic path selection** to optimize network performance.
* Deployed and managed Palo Alto Networks firewalls (PA-7050, PA-5450, PA-5400-DPC-A, PA-3250) and configured security policies to protect enterprise environments.
* Used Prisma log aggregation and analysis to correlate security events, identify attack patterns, and uncover indicators of compromise (IOCs).
* Designed and deployed **SASE architecture** integrating **network security (FWaaS, SWG, CASB, ZTNA) and SD-WAN** for secure cloud connectivity.
* Integrated **IPsec with SD-WAN solutions (Cisco Viptela, Fortinet)** for optimized and secure network traffic routing.
* Designed and implemented **VLAN segmentation** to optimize network performance and enhance security across enterprise environments.
* Deployed **Cisco ISE TrustSec and pxGrid** to enhance security by segmenting and securing network access.
* Integrated **Ansible with Python and REST APIs** to automate security policies and network infrastructure updates.
* Integrated **Check Point firewalls with SIEM solutions (Splunk, QRadar) and centralized management using SmartConsole and SmartEvent** for real-time monitoring and analysis.
* Upgraded NX-OS on Cisco Nexus switches (9000, 7018, 7009, 5548, 5596), consolidating environments using VPC and VRF.
* Diagnosed and optimized Cisco Nexus switches and implemented redundancy features within the ACI fabric, including vPC, ISSU, and GIR for high availability.
* Used **Wireshark filters and dissectors** to diagnose application-layer issues and optimize network performance.
* Configured secure roaming in enterprise environments using IEEE 802.11r, 802.11k, and 802.11v to enhance performance and security for mobile devices.
* Implemented 802.1X-based secure authentication (EAP-TLS, EAP-PEAP) to enforce network access control policies.
* Developed **custom dashboards, alerts, and reports** using **Dynatrace AI-powered analytics** to monitor system health and optimize performance.
* Worked on Python and Ansible to automate network workflows, such as software upgrades, device provisioning, and configuration management.
* Utilized Python libraries (e.g., pandas, numpy) to analyze large network data sets for informed decision-making and troubleshooting.
* Integrated Cisco Firepower with external threat intelligence feeds for enhanced threat detection and utilized Firepower threat feeds to stay updated on security threats.
* Managed external vendor relationships, ensuring compliance with PCI DSS, SOX, GLBA, and other financial security regulations.
* Configured and optimized **Azure VPN Gateway, Virtual WAN, and Private Link** to establish secure hybrid cloud connectivity.
* Deployed and troubleshot **cable modem provisioning, DHCP, TFTP, and SNMP** for large-scale ISP environments.
* Managed **VLAN-based network segmentation** to enforce access control and mitigate security risks.
* Configured AWS Security Groups and Network ACLs to control traffic to instances, and set up AWS WAF for protection against web-based attacks.
* Configured High Availability (HA) solutions on Juniper SRX devices and conducted failover testing to ensure network continuity.
* Implemented zero-touch provisioning (ZTP) for Meraki devices, simplifying deployment and reducing configuration overhead.
* Integrated Spine-Leaf networks with Cisco ACI for dynamic provisioning and rapid adaptation, troubleshooting network issues using real-time monitoring tools.
* Configured and managed **SDN controllers (Cisco APIC, OpenDaylight, ONOS)** for centralized network policy enforcement and traffic engineering.
* **Integrated IPsec with firewalls** (Palo Alto, Fortinet, Cisco ASA) for enhanced network security.
* **Troubleshot VLAN connectivity issues** related to trunking, STP, and misconfigurations.

**BNY Mellon, New York, NY January 2019 – July 2022**

**Network Security Engineer**

**Responsibilities:**

* Configured and Troubleshoot issues with the following types of routers Cisco (PA- 4500, PA-2600 and 3500 series), to include: bridging, switching, routing, Ethernet, and DHCP, as well as assisting with customer LAN /WAN.
* Implemented and optimized **Aruba ClearPass Policy Manager (CPPm)** for network access control (NAC), authentication, and role-based access policies.
* Integrated **Juniper Mist AI and Junos Space Security Director** for network automation, monitoring, and centralized management.
* Configured and maintained **DOCSIS 3.0/3.1 CMTS (Cable Modem Termination System)** to optimize broadband service delivery and network performance.
* Configured, deployed, and managed **FortiGate Next-Generation Firewalls (NGFW)** for enterprise and data center security.
* Deployed, configured, and managed **Dynatrace Application Performance Monitoring (APM)** solutions for real-time observability and troubleshooting.
* Developed and optimized **iRules and iApps** on F5 load balancers for advanced traffic management and security enforcement.
* Configured, deployed, and managed **Check Point firewalls (NGFW, CloudGuard, Quantum Series)** to enhance network security and threat prevention.
* Deployed and optimized **AWS Security Groups, Network ACLs, and WAF** to enhance cloud security and compliance.
* Integrated **Cisco ASA with Cisco Firepower and ISE** for advanced threat protection and identity-based access control.
* Implemented **Azure Active Directory (AAD), Role-Based Access Control (RBAC), and Multi-Factor Authentication (MFA)** for identity and access management.
* Configured **ACI fabric components** including **APIC, spine, and leaf switches** for software-defined networking (SDN).
* Integrated **Dynatrace OneAgent** across cloud and on-prem environments, ensuring end-to-end visibility of application and network performance.
* Developed and optimized **F5 iRules** using **TCL scripting** to enforce advanced traffic management, security policies, and application routing.
* Implemented **IPsec tunnels and secure edge connectivity** in SD-WAN environments for encrypted site-to-site communication.
* Implemented **Palo Alto security policies, NAT, VPN (IPsec/SSL), and threat prevention** to safeguard enterprise networks.
* Performed troubleshooting, while maintaining trouble ticket tracking, following internal/external.
* Implemented procedures and customer notifications. Configured Cisco Routers for OSPF, RIP, IGRP, RIPv2, EIGRP, Static and default route.
* Troubleshot **Viptela SD-WAN connectivity, policy enforcement, and routing issues** using monitoring tools like NetScout and Wireshark.
* Troubleshot **VLAN misconfigurations, spanning-tree issues, and inter-VLAN routing** using network monitoring tools like **Wireshark and NetScout.**
* Configured VLANs with 802.1Q Tagging according to the Server team and requirements. Tested the Core routers via OSPF Areas.
* Deployed and managed **IPsec VPNs in cloud environments (AWS, Azure, GCP)** for secure hybrid cloud connectivity.
* Configured and managed **Site-to-Site and Remote Access VPNs** using **IPsec, SSL, and GRE tunnels** on Cisco ASA, Palo Alto, and Fortinet firewalls.
* Implemented **Ansible Tower/AWX** to streamline IT automation and enhance centralized management.
* Configured on Cisco Catalyst 6509 switches to have Redundancy.
* Worked on T1/ E1/T3 technologies and different LAN &amp; WAN technologies.
* Used various BGP Attributes and various Route-filters such as named Access-lists, Prefix lists, Route-maps to permit or deny routes and to change various attribute.
* Planned and implemented Subnetting, VLSM to conserve IP addresses.
* Implemented VTP and Trucking protocols (802.1q and ISL) on 3560, 3750 and 4500 series Cisco Catalyst switches.
* Configured STP for loop prevention and VTP for Inter-VLAN Routing.
* Configured ACL to allow user the company access different application and blocking others.
* Actively involved in switching technology Administration including creating and managing VLANS, Port security - 802.1x, Trucking 802.1Q, RPVST+, Inter-VLAN routing, and LAN security on Cisco Catalyst Switches 4507R+E, 6509-E and Cisco Nexus Switches 2232, 5596, 7009.
* Utilized **Python with APIs** to automate Cisco, Palo Alto, and Fortinet firewall configurations.
* Responsible for configuration, maintenance, and troubleshooting of dynamic routing protocols: BGP, OSPF &amp; (route redistribution, distribute lists, route-maps, offset-lists, prefix lists, route summarization, route-feedback, BGP attributes) on Cisco Routers 7613, 7201, and 3945E.
* Involved in configuring and managing F5 BIG-IP for Data centers, DNS Management and Integrated with DNS Vendors for DNS Security Management.
* Basic network troubleshooting (ping, traceroute, DNS, telnet to verify open ports).
* **Designed and configured VLANs** to segment network traffic and improve security and performance.

**PWC, India August 2017 - December 2018**

**Network Engineer**

**Responsibilities:**

* Worked as part of a team for Cisco Product Support. Troubleshooting by providing relevant knowledge base articles and other information.
* Network solutions for complex networks for VAR (Value added resellers) users for Cisco.
* Configured & maintained LAN, WAN, VPN, WLAN, and Firewalls on Cisco Routers for end users.
* Configuring MPLS, VPN (IPSEC, GRE) in VPN concentrators and QOS in integrated networks.
* Configuring IPS, IDS, VLAN, STP, Port Security, SPAN, Ether channel in Cisco Composite Networks.
* Configured routers and modems, troubleshot issues related to broadband technologies for Residential and Business Customers.

**Certifications:**

Cisco Certified Network Associate (CCNA)

Cisco Certified Network Professional (CCNP)

**Education:-**

Bachelors in Electrical, Electronics and engineering, India

Masters in Computer and Information Systems Security/ Auditing/ Information, Gannon University, PA, USA.