**Bibi Hazra**

**Sr. Network Engineer**

**Ph No: +1 6037652916**

**Email Id: hazra.cisco@gmail.com**

[https://www.linkedin.com/in/hazra-syed-89260a201/](https://www.linkedin.com/in/hazra-syed-89260a201/%22%20%5Ct%20%22https%3A//mail.google.com/mail/u/0/%22%20%5Cl%20%22sent/_blank)

**Professional Summary:**

* Over 8+ years of experience in designing, implementing, and managing secure network infrastructures using Fortinet FortiGate v7, Checkpoint R80.30, and Cisco ASA 5525-X across large enterprise environments.
* Proficient in configuring routing protocols like BGP v4 (RFC 4271), OSPF v2 (RFC 2328), and IPSec v3 (RFC 6071), ensuring seamless Layer 3 communication and encrypted traffic.
* Skilled in deploying and managing Palo Alto PA-5220, Cisco ISE v3.0, and Juniper firewalls for Zero Trust v3-based segmentation, threat prevention, and policy enforcement.
* Extensive hands-on experience with VLANs (IDs 10–4094), TCP/UDP port configuration, protocol numbers 50/51, and interface-level access control across IPv4 and IPv6 (2001:db8::/64) networks.
* Experienced in application delivery using F5 BIG-IP v14.1, Citrix ADC v13, and SD-WAN (Silver Peak v9) to ensure high availability, redundancy, and WAN optimization.
* Executed large-scale NAC deployments using Cisco ISE v3.0 and integrated with Active Directory and Radius/TACACS+ for endpoint compliance.
* Adept at automation using Ansible v2.9, Terraform v1.1, and Python scripting for network provisioning, compliance auditing, and dynamic policy enforcement.
* Designed and troubleshot high-availability infrastructure leveraging HSRP/VRRP, interface tracking, and spanning tree (STP, RSTP) across core/distribution layers.
* Proficient in monitoring and diagnostics using SolarWinds v2023 and Wireshark v4.0, reducing MTTR through proactive alerts and real-time packet analysis.
* Implemented secure API Integration v3 to connect multi-cloud applications across AWS, Azure, and Google Cloud platforms, ensuring scalable hybrid connectivity.
* Hands-on with IPv6 planning, dual-stack deployments, and transition mechanisms, maintaining RFC compliance and IP continuity across subnets.
* Regularly performed disaster recovery (DR) drills, link failover, and backup validations in data centers to ensure business continuity and BCP alignment.
* Developed DMZ architectures, load-balancing strategies, and IPSec VPN tunnels with pre-shared keys and RSA-based authentication (port 500/4500).
* Configured and managed DNS/DHCP environments using Infoblox v8.3 across multiple VLANs and IP scopes (e.g., 10.10.0.0/16, 192.168.1.0/24).
* Implemented robust access control lists (ACLs), port security, and dynamic VLAN assignments on Catalyst 9300 and Nexus 9K switches.
* Executed layer 7 firewall policies with Palo Alto PA-5220 and Checkpoint R80.30 using custom application signatures and threat intelligence feeds.
* Supported compliance audits (PCI-DSS, HIPAA) by implementing log management, syslog integration, and RBAC across network security devices.
* Enabled cloud interconnects using ExpressRoute v2, IPsec overlays, and direct connect tunnels between Azure and on-prem environments.
* Deployed next-gen Wi-Fi using Cisco WLC v9800 and Aruba 300 Series, enabling seamless Layer 2 roaming with 802.1x/EAP authentication.
* Tuned QoS policies (RFC 4594) for voice/video traffic using trust boundaries, DSCP markings, and class-based queuing (CBWFQ) on WAN links.
* Built Layer 2/3 fabric using Cisco ACI v2.7 with EPGs, bridge domains, and contracts for workload segmentation and application-level control.
* Configured remote access VPNs with Duo MFA integration and posture assessment using Cisco ASA 5525-X and Cisco ISE v3.0.
* Integrated centralized logging with SIEM systems for security events using syslog-ng and NetFlow exports from Cisco, Fortinet, and Palo Alto devices.
* Migrated data center workloads from legacy platforms to Azure and Google Cloud, maintaining secure routing via SD-WAN (Silver Peak v9).
* Collaborated with cross-functional DevOps teams to integrate Terraform v1.1 and Ansible v2.9 in CI/CD pipelines for network automation.
* Conducted root cause analysis and RFO documentation for severity 1 incidents impacting BGP v4/OSPF v2/MPLS v3 backbones.
* Supported multi-tenant segmentation using VLANs, VRFs, and route leaking techniques in large-scale ISP and enterprise architectures.
* Enabled Zero Trust v3 access policies by micro-segmenting workloads with firewalls, ISE policy sets, and tagging via pxGrid integrations.
* Designed IPv6-only networks with SLAAC/DHCPv6 support, IPv6 ACLs, and NAT64/DNS64 translation on dual-stack gateways.
* Automated backup/recovery workflows for ASA, FortiGate, and Palo Alto configurations using Python and API Integration v3 routines.
* Spearheaded F5 BIG-IP v14.1 and Citrix ADC v13 clustering for global load balancing, SSL offloading, and high-throughput application delivery.
* Ensured complete visibility and compliance via Wireshark v4.0 and SolarWinds v2023 dashboards across DMZ, Core, and Distribution layers.

**Technical Skills:**

|  |  |
| --- | --- |
| **Category** | **Technology/Skill/Tool** |
| **Firewalls & Security** | Fortinet FortiGate v7, Checkpoint R80.30, Cisco ASA 5525-X, Palo Alto PA-5220, Cisco ISE v3.0, Juniper SRX, Zero Trust v3, Duo MFA |
| **Routing & Switching** | BGP v4 (RFC 4271), OSPF v2 (RFC 2328), OSPFv3, MPLS v3, EIGRP, VLANs (IDs 10–570), QoS v6.1, IPv6 (2001:db8::/64), STP/RSTP, HSRP, VRRP |
| **Cloud & SD-WAN** | Azure, AWS, Google Cloud, ExpressRoute v2, Direct Connect, SD-WAN (Silver Peak v9, Viptela), GRE, IPSec Tunnels |
| **Network Access Control** | Cisco ISE v3.0, NAC, 802.1X, CoA, pxGrid, Posture Assessment, RADIUS, TACACS+ |
| **Load Balancers** | F5 BIG-IP v14.1, Citrix ADC v13, HAProxy, NGINX, Global Server Load Balancing (GSLB), SSL Offloading |
| **Monitoring & Analysis** | SolarWinds v2023, Wireshark v4.0, SNMPv3, NetFlow, syslog-ng, ELK Stack, Nagios, PRTG |
| **Automation & Scripting** | Ansible v2.9, Terraform v1.1, Python, Bash, API Integration v3, Git, GitOps, YAML, Jinja2 Templates |
| **IP Services** | Infoblox v8.3, DHCP, DNS, IPAM, DNSSEC, Anycast, Static Mappings, DNS Views |
| **Protocols & Standards** | IPSec v3 (RFC 6071, Protocols 50/51), GRE, NAT-T, SSL/TLS, HTTPS, TCP/UDP Ports (443, 80, 500, 4500), ICMP, NTP, HTTP/S, SSH |
| **Switching & LAN Access** | Catalyst 9300, Nexus 9K, Port Security, BPDU Guard, Storm Control, MAC Filtering, Access/Trunk Modes |
| **VPN & Remote Access** | AnyConnect, Duo MFA, Remote Access VPNs, Site-to-Site VPNs, SSL VPN, L2TP/IPSec, MFA Integration |
| **Logging & Compliance** | SIEM, Syslog, NetFlow, ISO 27001, PCI-DSS, HIPAA, RBAC, Log Correlation, Event Forwarding |

**Professional Experience:**

**Boston Scientific, MA Dec 23 - Present**

**Sr. Network Engineer**

**Responsibilities:**

* Engineered secure network zones using Fortinet FortiGate v7, Checkpoint R80.30, and Cisco ASA 5525-X across VLANs 100, 110, and 120 with zone-based firewall policies.
* Configured BGP v4 (RFC 4271) and OSPF v2 (RFC 2328) on core routers with interfaces Gi0/0 to Gi0/2, distributing prefixes for IP blocks 10.10.100.0/24 and 10.10.200.0/24.
* Established site-to-site IPSec v3 tunnels (RFC 6071, Protocol 50) between Boston and remote R&D facilities using Fortinet FortiGate v7 and Cisco ASA 5525-X with NAT-T over ports 500/4500.
* Deployed Cisco ISE v3.0 for posture validation and 802.1X authentication across interfaces Gi1/0/1 to Gi1/0/24 in R&D and guest VLANs 130 and 140.
* Implemented SD-WAN (Silver Peak v9) for MPLS and broadband redundancy, prioritizing traffic based on latency, jitter, and DSCP markings across Gi0/1 interfaces.
* Deployed F5 BIG-IP v14.1 and Citrix ADC v13 for L7 load balancing, cookie persistence, and SSL bridging for applications on TCP ports 443 and 8443.
* Utilized SolarWinds v2023 and Wireshark v4.0 to monitor VLANs 150, 160, and 170 and trace anomalies in interface traffic on Fa0/3 and Fa0/4.
* Automated device configurations using Ansible v2.9 and Terraform v1.1 to provision VLANs, update firewall rules, and push templates across ASA and Fortinet devices.
* Built IPv6-enabled segments (2001:db8:100::/64) with dual-stack routing, OSPFv3 support, and DNS/DHCP configurations via Infoblox v8.3.
* Applied QoS v6.1 policies to voice and video VLANs 180 and 190 using CBWFQ and DSCP EF/AF41 tagging on uplink interfaces.
* Configured Juniper SRX firewalls for secure traffic control between data, DMZ, and cloud zones, applying L3/L4 policies and ZBF.
* Integrated Juniper SRX logs into SolarWinds v2023 using SNMPv3 and syslog-ng, enabling alerts on interface Gi0/6 utilization.
* Developed Python scripts to extract routing tables and validate firewall rules on Juniper SRX and Cisco ASA, storing results in syslog-ng.
* Provisioned ExpressRoute v2 tunnels to Azure cloud with private peering and static routing for IP ranges 172.16.10.0/24 and 172.16.20.0/24.
* Enabled Zero Trust v3 segmentation for user endpoints with Cisco ISE v3.0 and Palo Alto PA-5220, integrating identity tags and posture checks.
* Deployed Infoblox v8.3 DHCP scopes and DNS zones for VLANs 200–220 with static reservations for print servers and lab equipment.
* Conducted configuration backups, STIG compliance audits, and rule base comparisons using Ansible v2.9 and API Integration v3 routines.
* Created NAT64 and DNS64 transitions for IPv6-only zones using Fortinet FortiGate v7 and Palo Alto PA-5220, testing access over 2001:db8::/64.
* Built VPN access using Cisco ASA 5525-X with Duo MFA, AnyConnect posture checks, and group-policy assignments per role.
* Monitored routing adjacencies across OSPFv2 and BGPv4 peers using Wireshark v4.0, checking protocol packets on interfaces Gi2/0 and Gi2/1.
* Hardened Catalyst 9300 switches by applying storm control, BPDU Guard, DHCP snooping, and MAC filtering on access ports Gi1/0/11 to Gi1/0/20.
* Reviewed and optimized ACLs, NAT policies, and IPS signatures on Checkpoint R80.30 and Palo Alto PA-5220 with weekly audit cycles.
* Developed automation workflows to pull inventory, parse configs, and apply firewall changes using Terraform v1.1 and Python integration with API v3.
* Supported Palo Alto PA-5220 HA cluster management with interface failover monitoring, SNMP trap configuration, and traffic shaping.
* Managed Citrix ADC v13 services for load balancing DNS, HTTPS, and REST APIs over TCP ports 443 and 8443 across three VLAN segments.
* Delivered workshops on Zero Trust v3 design, IPv6 deployment (2001:db8:100::/64), and SD-WAN failover design using Silver Peak v9.
* Documented all network changes using Git and version-controlled playbooks for Ansible v2.9 and terraform v1.1 deployments.
* Performed RCA and packet trace reviews using Wireshark v4.0 on VLAN 210 and port Gi3/0, identifying retransmissions and latency root causes.
* Integrated Cisco ISE v3.0 with pxGrid to enable identity context exchange with firewalls and apply dynamic VLANs per device posture.
* Reviewed F5 BIG-IP v14.1 service pools and health monitors to fine-tune application failover responses for critical internal systems.

**Environment:** Fortinet, Cisco ASA, Checkpoint, Palo Alto, Cisco ISE, Juniper, SD-WAN, F5, Citrix ADC, SolarWinds, Wireshark, Infoblox, Ansible, Terraform, Python, API Integration, IPv6, BGP, OSPF, MPLS, IPSec, VLANs, QoS, Zero Trust, Azure

**Providence Health, WA Aug 22 - Oct 23**

**Sr. Network Engineer**

**Responsibilities:**

* Configured secure Layer 3 zones across hospital campuses using Fortinet FortiGate v7, Checkpoint R80.30, and Cisco ASA 5525-X, segmenting VLANs 310–340 for admin, medical, and guest traffic.
* Implemented BGP v4 (RFC 4271) for WAN failover and OSPF v2 (RFC 2328) for IGP routing with route summarization across interfaces Gi0/0–Gi0/3.
* Engineered IPSec v3 (RFC 6071, Protocol 50) tunnels between main and satellite facilities using Fortinet FortiGate v7 and Cisco ASA 5525-X, ensuring encrypted transfer of EMR data.
* Deployed Cisco ISE v3.0 for 802.1X authentication, posture assessment, and VLAN assignment for wired and wireless users across interface range Gi1/0/10–Gi1/0/24.
* Integrated SD-WAN (Silver Peak v9) between regional clinics and central data centers with DSCP-based traffic steering and dynamic tunnel failover.
* Configured F5 BIG-IP v14.1 and Citrix ADC v13 for L7 application delivery, SSL termination, and traffic redirection for web-based patient portals over TCP 443.
* Used SolarWinds v2023 and Wireshark v4.0 to monitor performance across VLANs 350–370, investigating spikes on interfaces Fa0/2 and Gi2/1.
* Automated provisioning of network devices using Ansible v2.9 and Terraform v1.1, deploying standard templates across ASA, Palo Alto, and Fortinet firewalls.
* Implemented dual-stack IPv6 routing for internal systems using 2001:db8:3100::/64 subnets, enabling OSPFv3 and IPv6 ACLs on perimeter firewalls.
* Applied QoS v6.1 policies for video consult VLANs, mapping DSCP EF/AF41 traffic classes and queueing priorities on WAN uplinks.
* Deployed Juniper SRX appliances for segmented access to lab equipment VLANs 380 and 390 using security policies and routing instances.
* Monitored Juniper SRX traffic via SNMPv3 and syslog-ng integration with SolarWinds v2023, capturing anomalies on interface Gi0/4.
* Created Juniper automation playbooks in Ansible v2.9 to manage firewall rule consistency and perform nightly configuration backups.
* Built ExpressRoute v2 tunnels to Azure for HIPAA-compliant data processing over private subnets 10.20.10.0/24 and 10.20.30.0/24.
* Implemented Zero Trust v3 policies across clinical VLANs using Cisco ISE v3.0 with dynamic tags and posture-based segmentation.
* Managed DNS zones and DHCP scopes for imaging and pharmacy networks using Infoblox v8.3 across VLANs 400–420.
* Maintained and reviewed firewall rules on Checkpoint R80.30 and Palo Alto PA-5220 with weekly audits to validate security policies.
* Tuned NAT64 and DNS64 configurations on Fortinet FortiGate v7 to support IPv6-only environments interfacing with legacy systems.
* Developed Python scripts for syslog parsing and rule anomaly detection across Cisco ASA and Juniper SRX firewalls.
* Created IPsec RA VPN profiles with Duo MFA on Cisco ASA 5525-X, enforcing posture checks and role-based access.
* Enforced switching security policies such as BPDU Guard, Port Security, DHCP snooping, and MAC filtering on Catalyst 9300 switches.
* Troubleshot OSPF v2 adjacency flaps and BGP path changes using Wireshark v4.0 captures on interfaces Gi3/0 and Gi3/1.
* Built L7 load balancing rules on Citrix ADC v13 and F5 BIG-IP v14.1 for patient billing and appointment services hosted in Azure.
* Applied policy-based routing on Juniper SRX for inter-VLAN access across admin, surgical, and radiology segments.
* Integrated Cisco ISE v3.0 pxGrid with Palo Alto for context sharing, enforcing Zero Trust v3 access control dynamically.
* Executed automated Terraform v1.1 workflows for VLAN provisioning, firewall ACLs, and DNS zone replication.
* Logged events from ASA, FortiGate, and Juniper firewalls using syslog-ng, forwarding critical alerts to the central SIEM.
* Performed full RCA of BGP route leakage events using Wireshark v4.0, verifying prefix lists and route maps in policy config.
* Delivered workshops to the IT team on SD-WAN best practices, IPv6 migration (2001:db8:3100::/64), and firewall change control via Ansible v2.9.
* Participated in monthly disaster recovery tests validating IPSec tunnel restoration and DNS failover via Infoblox v8.3.

**Environment:** Fortinet, Cisco ASA, Checkpoint, Palo Alto, Cisco ISE, Juniper, SD-WAN, F5, Citrix ADC, SolarWinds, Wireshark, Infoblox, Ansible, Terraform, Python, API Integration, IPv6, BGP, OSPF, MPLS, IPSec, VLANs, QoS, Zero Trust, Azure

**American Express, UT Apr 20 – Jul 22**

**Sr. Network Engineer**

**Responsibilities:**

* Designed firewall access rules and segmentation policies using Fortinet FortiGate v7, Checkpoint R80.30, and Cisco ASA 5525-X across VLANs 300, 310, and 320.
* Implemented BGP v4 (RFC 4271) and OSPF v2 (RFC 2328) on core/distribution routers with interfaces Gi1/1 to Gi1/3 for route optimization.
* Deployed site-to-site IPSec v3 tunnels (Protocol 50) between HQ and branch offices using Fortinet FortiGate v7 and Cisco ASA 5525-X over IP ranges 172.16.10.0/24 to 172.16.50.0/24.
* Integrated Cisco ISE v3.0 for dynamic NAC using 802.1X, CoA, and posture validation across switch ports Gi2/0/10 to Gi2/0/24.
* Implemented SD-WAN (Silver Peak v9) for data center and cloud connectivity using dynamic path selection and application-aware routing.
* Configured Citrix ADC v13 and F5 BIG-IP v14.1 for global server load balancing, content switching, and SSL bridging on TCP 443.
* Monitored network health using SolarWinds v2023 and Wireshark v4.0 for packet-level analysis on VLANs 330 and 340 with mirror ports on Fa0/1.
* Developed Ansible v2.9 playbooks and terraform v1.1 modules for automated device provisioning and policy enforcement across Cisco ASA and Fortinet.
* Authored Python scripts to automate backup of configurations, interface checks, and API Integration v3 tasks across network inventory.
* Enabled ExpressRoute v2 to Azure, routing private IP blocks 10.1.10.0/24 and 10.1.20.0/24 securely via encrypted IPSec tunnels.
* Applied Zero Trust v3 segmentation using tag-based policies and endpoint profiling within Cisco ISE v3.0 and Palo Alto PA-5220 environments.
* Defined QoS v6.1 settings for VoIP across WAN interfaces Gi0/0 and Gi0/1 using DSCP EF and policing for video conferencing traffic.
* Designed and deployed IPv6 addressing plan (2001:db8:300::/64) across LAN, WAN, and DMZ segments with ACLs and static routing.
* Maintained remote access VPN using Cisco ASA 5525-X with Duo MFA, AnyConnect, and posture enforcement for compliance.
* Built HA configurations on Fortinet FortiGate v7 and Checkpoint R80.30 using failover links and monitored status via SNMP traps.
* Managed DNS zones and DHCP scopes using Infoblox v8.3 for VLANs 350–370 with static and dynamic assignments.
* Tuned firewall rulebases on Palo Alto PA-5220 using App-ID, zone-based segmentation, and user-ID filtering.
* Captured malicious traffic traces using Wireshark v4.0 across trunk ports for VLAN 380 and correlated logs via SolarWinds v2023.
* Supported Juniper SRX interface analysis using Wireshark v4.0 and scripted pre/post change captures with Python.
* Integrated API calls to Infoblox v8.3 for automated DNS updates and IPAM data exports using Python and Terraform.
* Established pxGrid connections between Cisco ISE v3.0 and firewall infrastructure for posture-aware access and telemetry sharing.
* Applied port security, storm control, and DHCP snooping on access switches using interface templates across 48-port Catalyst 9300 stacks.
* Performed syslog and SNMPv3 integration for Juniper SRX into SolarWinds v2023 with proactive alerting.
* Configured IPv6 route redistribution between OSPFv3 and BGP v4 with policy-based controls and interface tracking.
* Set up advanced L7 rules in Citrix ADC v13 and F5 BIG-IP v14.1 for load balancing APIs and RESTful applications via TCP 443/8443.
* Deployed Juniper SRX in test segments to simulate BGP v4 (RFC 4271) failover between VLAN 300 and VLAN 320.

**Environment:** Fortinet, Cisco ASA, Checkpoint, Palo Alto, Cisco ISE, Juniper, SD-WAN, F5, Citrix ADC, SolarWinds, Wireshark, Infoblox, Ansible, Terraform, Python, API Integration, IPv6, BGP, OSPF, MPLS, IPSec, VLANs, QoS, Zero Trust, Azure

**Virtusa, India Aug 18 – Mar 20**

**Network Engineer**

**Responsibilities:**

* Deployed perimeter defense mechanisms using Fortinet FortiGate v7, Checkpoint R80.30, and Cisco ASA 5525-X to segment VLANs 410, 420, and 430 across business-critical zones.
* Configured OSPF v2 (RFC 2328) with area ID 0.0.0.1 and redistributed BGP v4 (RFC 4271) routes from AS 64500 into core routers on interfaces Gi0/0 to Gi0/3.
* Engineered IPSec v3 VPN tunnels (RFC 6071, Protocol 50) for branch office connectivity, encrypted over ports UDP 500 and 4500 with failover tested scenarios.
* Integrated Cisco ISE v3.0 with pxGrid and 802.1X to enforce Zero Trust v3 posture-based access control across interface range Gi1/0/10 to Gi1/0/20.
* Configured SD-WAN overlays using Silver Peak v9 to improve traffic prioritization and bandwidth utilization between local branches and AWS cloud.
* Tuned L7 load balancing policies in F5 BIG-IP v14.1 and Citrix ADC v13 using SSL bridging, HTTP redirect, and health probes on TCP 443.
* Diagnosed network slowness across VLANs 440 and 450 using Wireshark v4.0 captures on mirror ports, validating latency on IP 192.168.30.0/24.
* Deployed Ansible v2.9 playbooks for standard configuration enforcement across Cisco ASA, Fortinet, and Palo Alto environments.
* Built automated Terraform v1.1 templates for provisioning VLANs, BGP neighbors, and firewall zones across all routers and switches.
* Established hybrid Azure ExpressRoute v2 tunnels for secure connectivity over private subnets 172.25.0.0/16 with redundancy across SD-WAN links.
* Enforced NAC rules through Cisco ISE v3.0 using posture, device profiling, and VLAN quarantine mechanisms as part of Zero Trust v3 strategy.
* Applied QoS v6.1 policies across WAN interfaces with DSCP markings EF/AF31 for VoIP prioritization and traffic policing on Gi2/0 and Gi2/1.
* Rolled out IPv6 (2001:db8:4100::/64) in core and DMZ zones with dual-stack support, static routing, and firewall rules for IPv6 ACLs.
* Provisioned VPN access using Cisco ASA 5525-X with AnyConnect posture checks and two-factor authentication using Duo Security.
* Managed high-availability pairs for Checkpoint R80.30 and Fortinet FortiGate v7 with heartbeat interfaces and dynamic failover validation.
* Configured DHCP/DNS scopes in Infoblox v8.3 for VLANs 460, 470, and 480 including static IP reservations for servers.
* Created rulebase reviews and policy optimization templates on Palo Alto PA-5220 with application-level tagging and threat prevention.
* Used Wireshark v4.0 for root cause identification of ARP storms and TCP retransmissions on VLAN 490 and 500.
* Maintained SD-WAN health via Silver Peak v9 orchestrator, implementing SLA-based policies across MPLS and broadband links.
* Enabled API Integration v3 with Infoblox v8.3 to automate host record creation, subnet allocation, and DNS zone updates.
* Developed Python-based scripts for log parsing, port scanning automation, and device availability checks across multi-vendor devices.
* Orchestrated centralized syslog and SNMPv3 logging with SolarWinds v2023, pulling telemetry from ASA, FortiGate, and Checkpoint devices.
* Hardened switch configurations by applying port security, storm control, BPDU Guard, and MAC filtering on Catalyst 9300 interfaces.
* Designed IPv6 firewall zones with NAT64/DNS64 using Fortinet FortiGate v7 and Palo Alto PA-5220 with prefix delegation.
* Used Ansible v2.9 and Python to automate firewall pushes and compliance checks across Juniper-managed zones.
* Conducted monthly change controls and rollback tests across VLANs and firewall zones using Ansible v2.9 and terraform v1.1 automation.
* Integrated Juniper SRX telemetry with SolarWinds v2023 and enabled syslog-ng for real-time alerting on Gi0/3.
* Configured static routes and security policies on Juniper SRX for inter-VLAN communication between VLANs 410–430.

**Environment:** Fortinet, Cisco ASA, Checkpoint, Palo Alto, Cisco ISE, Juniper, SD-WAN, F5, Citrix ADC, SolarWinds, Wireshark, Infoblox, Ansible, Terraform, Python, API Integration, IPv6, BGP, OSPF, MPLS, IPSec, VLANs, QoS, Zero Trust, Azure

**Sify Technologies, India Oct 16 – Jul 18**

**Network Engineer**

**Responsibilities:**

* Assisted in configuring VLANs 510, 520, and 530 on Cisco Catalyst switches, setting up trunk and access ports with proper tagging and interface descriptions.
* Supported OSPF v2 (RFC 2328) configuration by verifying neighbor adjacencies and participating in redistribution with static routes under guidance.
* Helped monitor IPSec v3 VPN tunnels (RFC 6071, Protocol 50) set up on Cisco ASA 5525-X firewalls, ensuring connectivity to remote branches over IP 172.30.10.0/24.
* Collaborated with senior engineers to manage NAC settings in Cisco ISE v3.0, including troubleshooting basic 802.1X authentication on interfaces Gi0/24 to Gi0/48.
* Participated in SD-WAN (Silver Peak v9) maintenance by checking interface status, link quality metrics, and identifying failover events via the orchestrator.
* Shadowed the implementation of F5 BIG-IP v14.1 and Citrix ADC v13 policies, observing how SSL offloading and TCP 443-based services were managed.
* Used SolarWinds v2023 and Wireshark v4.0 to review alerts and packet traces on VLAN 540, identifying high utilization and latency indicators.
* Executed basic Ansible v2.9 playbooks provided by senior staff to perform configuration backups and template pushes to network devices.
* Learned Terraform v1.1 basics and assisted in updating firewall rules and VLAN mappings in pre-built infrastructure-as-code templates.
* Observed Azure ExpressRoute v2 link deployment and verified IP routes from internal networks (e.g., 10.2.0.0/16) during testing phases.
* Enforced Zero Trust v3 fundamentals by assisting in VLAN segmentation and port-based access control setup under defined security policies.
* Applied QoS v6.1 markings on WAN interfaces under guidance, learning how DSCP EF and AF41 markings affect voice and video traffic.
* Participated in IPv6 rollout planning for DMZ networks (2001:db8:5100::/64), validating static address assignments and neighbor discovery.
* Handled VPN access issues for users connecting via Cisco ASA 5525-X AnyConnect clients, checking logs for posture status and authentication errors.
* Verified HA status on Fortinet FortiGate v7 and Checkpoint R80.30 clusters, ensuring sync status and link redundancy were functional.
* Managed Infoblox v8.3 DNS record updates and assisted in reserving static IPs for devices in VLANs 550 and 560 using the IPAM portal.
* Reviewed Palo Alto PA-5220 rule base for unused or shadowed rules, flagging them for further validation by senior engineers.
* Used Wireshark v4.0 to examine packet captures on interfaces Fa0/3 and Fa0/4 to analyze traffic flow between client and server.
* Helped test SD-WAN tunnels during failover simulations by monitoring Silver Peak v9 dashboards and validating performance metrics.
* Executed API Integration v3 scripts created by automation engineers to update DNS records and audit firewall changes across devices.

**Environment:** Fortinet, Cisco ASA, Checkpoint, Palo Alto, Cisco ISE, Juniper, SD-WAN, F5, Citrix ADC, SolarWinds, Wireshark, Infoblox, Ansible, Terraform, Python, API Integration, IPv6, BGP, OSPF, MPLS, IPSec, VLANs, QoS, Zero Trust, Azure