**Shoeb Ali**

**Professional** **Summary**

* Experience with enterprise-wide network and security administration as well as implementation & support.
* Experience with Cisco ASA and Checkpoint firewalls.
* Experienced with Palo Alto Networks Firewall systems, Cisco routers, switches, (to include 2600, 2500, 3600, 3800 series) Pix 515 and ASA 5510 series firewalls, and Voice over IP telephony using Cisco Call Manager 4.3
* Proven analytical, decision making, and problem-solving abilities.
* Self-motivated with ability to work independently/work together in Team environment.
* Excellent understanding of network security architectures, network topologies, data flow, data encryption at rest and in motion, and other relevant network security domains.
* Capable of quickly learning new technologies and adapting to new environments.
* Experience in Firewalls like Cisco, Dell SonicWALL, Juniper, etc., establishing site-to-site VPN's, Troubleshooting VPN issues
* Complete knowledge of network equipment such as switches (Cisco, Extreme, etc. ), routers, hubs, Wi-Fi Controller (Cisco, Ruckus), Wi-Fi Access Points, Firewalls and associated equipment and how to construct and maintain networks

**Education**

- Master’s in Information Systems Security from University of the Cumberlands (GPA 3.7)

- Master’s in Computer Science from University of Illinois at Springfield (GPA 3.3)

**Technical Summary**

***Hardware Platforms*:** Cisco ASA Firewalls including ASA 5585, 5555, 5540, 5520 and Firepower series as well as Cisco VPN Concentrators. IDSM and NAM modules on Cisco 6500 Switches. Cisco AIP-SSM Modules on ASA 500 Series appliances, IDSM Modules on Cisco 6500 Switches. IDS 42XX Devices. Cisco Networking Hardware 7600, 7200, 3800, 3600, 2800 Series Routers and Cisco 6500, 4900, 4500, 3750, 3560, 2900 series switches. Juniper ISG 1000, NS 5400, SSG Firewalls and NSM 2007 and 2010 for management. Check Point Gaia R80.10, R77.30, R76, R75 etc., Multi Domain Server MDS/Provider-1 NGX with multiple CMA.

***Operating Systems*:** Cisco IOS 9.x, 8.x. for Firewalls, Cisco IPS OS 5.X, 6.X, 7.X Cisco Catalyst OS and IOS 12.x, FWSM 3.X Cisco CSM 4.X. IPSO 4.x, 6.x, SPLAT, Check Point R80.10, R77.30, R76, R75

*LAN & WAN*: OSI Layer, TCP/IP, WAN Routing Protocols RIP V2, EIGRP, OSPF, BGP. Layer 2 WAN Protocols MPLS, Frame Relay. High Availability configurations including HSRP, VRRP and Spanning Tree Protocols STP, RSTP, MST. Dot1q Trunk. Server Technologies like Windows 2008, 2012, Red Hat Linux, HP-UX, Solaris and Active Directory, DNS, DHCP. Network Management Protocols including SNMP, SYSLOG. Sniffer tools like Wire Shark, Packet Capture, Tracer.

***Security*:** RSA Two Factor Authentication using RSA ACE Server (both Native and Radius Mode). Work on Cisco Security Manager CSM Configuration, Event, Health & Performance and Report Manager. Security Implementations including multiple Zones ( DMZ, Third-party, ASZ etc.) Centralized policy management as well as signature updates through Cisco CSM. Advanced NAT including Identity, Static and Policy based etc.

**Certifications:**

CCNA

**Professional Experience:**

3M

(July 2023 - Present)

Network and Security Engineer

Remote

* Planning, Design, Implementation and Troubleshooting of Checkpoint Firewalls in the network.
* Migration of IPsec B2B VPN tunnels from one platform to another between Cisco ASA and Checkpoint.
* Checkpoint Appliances include 21K, 15K and 13K series running Gaia as well as Management Platform on Smart1 appliances and Provider-1 NGX with multiple CMA.
* Configuring Static and dynamic routing on Security Gateway using OSPF and BGP on Checkpoint.
* Build and Configure Checkpoint Provider -1 and work with Global objects and policies.
* Integrate various 3rd party applications with Checkpoint using OPSEC client.
* Provide day-to-day operational support for all firewall and VPN platforms including Checkpoint and Palo alto firewalls and ITIL Based Service Delivery and Management.
* Day-to-day work involves changes on the Checkpoint Firewall using the Smart Dashboard R80 software and connecting via Smart Center management.
* Implementation of high availability on Checkpoint security gateways using ClusterXL and Palo alto firewalls.
* Working with advanced blades on checkpoints including IPS, Anti-virus, Anti-Bot and Threat emulation.
* Provide day-to-day operational support for all firewall and VPN platforms including Checkpoint and Palo alto firewalls and ITIL Based Service Delivery and Management.

Cira Managed Service - CCMH Project (Comanche County Memorial Hospital)

(Jan 2023 to July 2023)

Network and Security Engineer

Client has 25 firewalls which include: Palo Alto networks, Cisco ASA and VMware NSX - ( Software defined networking).

* Installation and configuration of Cisco ASA Firewalls including X series running 9.4 IOS.
* Configure High Availability using Active/Standby mode with stateful replication.
* Configure Active-Active failover in Multiple Context Mode ASA
* ASA firewall upgrades and migration from one platform to another
* Experience working with both Pre 8.3 and Post 8.3 NAT and objects and inspection policies.
* Implementation experience on IPsec Site to site and Remote access VPN (ANYCONNECT) on ASA.
* Firewall Policy provisioning on ASA using Cisco Security Manager CSM 4.x
* Build Site to Site VPN with 3rd party and ensure proper NAT and Access list is in place.
* Troubleshooting Phase 1 and Phase 2 issues on the B2B VPN Tunnels between various business partners.
* Firewall Policy provisioning on PAN devices using the Panorama Management platform.
* Security Policy configuration and Policy administration on Palo Alto firewalls PA-5060, PA-3K and PA-200,220,800 Series.
* Configured HA on Palo-Alto in Active and Passive mode.
* Perform upgrades on PAN OS devices in High Availability pair.
* Work on User-ID, APP-ID, Wildfire, security profile, Threat prevention.
* Configure and implement URL Filtering on Palo Alto Firewalls.
* Working with Panorama including Device Groups and Templates
* Configure Panorama for Shared Policy and Reporting as well as log collection.
* Responsible for the operational support and project initiatives involving our Citrix Remote Access environment.
* Responsible for providing maintenance, support, and enhancements to the remote access systems including all published business critical applications and virtual desktops.
* Experience bringing customers from NSX-V to NSX-T

Comcast Cable Corporation

(September 2018 to December 2022)

Network and Security Engineer

West Chester, PA

* Responsible for the execution, upkeep and day-to-day support of network security technologies:  
  Third-Party VPN, Bluecoat, UTM, Gigamon, Black-Hole, F5 VPN, Aruba, Arbor, Cisco Stealthwatch, iBoss Proxy, Remote Access Points, Firewall, and Xfinity Store Networking
* Extensive Experience with SD-WAN Velo Cloud deployment & administration.
* Installation, configuration, and documentation of Fortinet products (3000D, 1000D, 1200D, 3600C, 300E, 2000E, 1500D running FortiOS 5.x & 6.x)
* Assisting client staff with day-to-day Fortinet products operation/ support
* SD-WAN Infrastructure, life cycle management of HW / SW, network migrations, new builds
* Administered firewall policies on Fortinet platforms.
* VPN technologies including both Site to Site and Remote Access including SSL VPN technologies such as Cisco ANYCONNECT, Juniper SA VPN ( Now Pulse Secure ) and Global-Protect on PAN firewalls.
* Support Juniper Netscreen as well as SRX 1400 and 1500 Firewalls
* Configure Chassis Cluster, NSRP on Juniper SRX and ISG firewalls.
* Experience in Planning, designing of Corporate Firewalls architecture and implementing in distributed environment i.e., configuring & troubleshooting – Checkpoint, Cisco ASA, FWSM & Juniper Firewalls.
* Planning, Design, Implementation and Troubleshooting of Palo Alto, Checkpoint and Cisco ASA Firewalls in the network.
* Hardware upgrades includes migrating PA-5050/5060 to PA-5220 and PA-5060 to PA-7050 in multi-vsys.
* Configured global protect portal, gateways, certificates, SSL/TLS profiles.
* Configured HA on Palo-Alto in Active and Passive mode.
* Perform migration from Websense URL filtering to PANDB URL filtering.
* Perform software upgrades on PA firewalls and Panorama in High Availability pair.
* Configuring Palo Alto Firewalls with multiple zones based with traffic segregation requirements.
* Work on User-ID, APP-ID, Wildfire, security profile, Threat prevention.
* Working with Panorama including Device Groups and Templates
* Configure Panorama for Shared Policy and Reporting as well as log collection
* Creating Data-filtering profiles in PAN devices which helps to prevent sensitive information.
* Configuring and support different types of NAT on PAN devices. Source/Destination based NAT, U-Turn NAT.
* Troubleshoot security policy, high availability, Global Protect on PAN devices.
* Firewall Policy provisioning on PAN devices using the Panorama Management platform.
* Security Policy configuration and Policy administration on Palo Alto firewalls PA-7000, PA-5200, PA-5000, PA-3000 and PA-200,220,800 Series.
* Provide day-to-day operational support for all firewall and VPN platforms including Checkpoint and Palo alto firewalls and ITIL Based Service Delivery and Management.
* Security Policy configuration and Policy administration on Palo Alto firewalls PA-7000, PA-5200, PA-5000, PA-3000 and PA-200,220,800 Series.
* SCCM OS deployment (example, Windows 10) Software package deployment (example, Office 2016) Update package deployment (example, MS security updates) Citrix or RDS Stand up the infrastructure to support a Citrix XenApp/XenDesktop and Microsoft RDS environments.
* Documentation and draw network diagrams using MS Visio and use SharePoint portal as site repository.

USPROSERV

(January 2016 to August 2018)

Network and Security Engineer

Atlanta, GA

* Part of Network and Security team responsible for managing Internet and Extranet segment of the hosted environment in the data center for multiple clients including AAA California, Hitachi, TRW Automotive, IPP of America etc. and responsibilities include:
* Assigned with the setup, configuration and installation of 16 Palo Alto 5060's and 3020's globally and also develop scripts for Panorama templates and configuration to improve proficiency in deployments.
* Configured, troubleshooted, and monitored Tipping Point event flows including the integration of Tipping Point data into a SIEM for use by cyber intrusion analysts
* Installation Configuration and Troubleshooting of Cisco ASA and Check Point Firewalls in the network.
* Day to Day work involves implementation of firewalls for new clients as well as managing and administering Cisco ASA and Check Point Firewalls at various zones including DMZ, Extranet (Various Business Partners and 3rd party) and ASZ supporting different clients’ environments.
* Creating VLANs and managing Spanning tree for the network and inter VLAN routing. Use Dynamic Routing Protocols including OSPF, EIGRP and BGP.
* Provided Tier 2/3 troubleshooting for Tipping Point issues, within the tool or as part of an integrated team of professionals addressing larger issues
* Configured and supported FWSM Firewall Blade modules on Cisco 6509 Switches
* Configure CSM Cisco Security Manager 4.x to manage all the Cisco ASA Firewalls for Policy Provisioning.
* Administer Checkpoint firewalls with cluster gateways including pushing policies and processing user requests to allow access through the firewall using Smart Center based Smart Dashboard.
* Monitor the health and logs using Smart view tracker and smart monitor on the Checkpoint firewall.
* Troubleshoot firewall logs from Smart view tracker as well as Command Line of Security Gateway.
* Creating object, groups, updating access-lists on Check Point Firewall, apply static, hide NAT.
* Creating and managing RSA ACE Profiles in Native mode as well as Radius Mode.
* Configure and update Intrusion Detection and Prevention systems through CSM for centralized management of Signature updates.
* Firewall OS upgrades and Maintenance of OS updates as part of addressing Vulnerabilities on Firewalls.
* Manage and support IDS/IPS including AIP SSM Modules on Cisco ASA Firewalls, IDSM Modules on 6500 Switch, IDS 4200 Series. Firewall OS upgrades as well as Signature updates and event management.
* Work with users to verify connectivity and troubleshoot Firewall related connectivity issues.
* Identify Firewall Ports required for application using CSM as well as CLI logging feature as well as use Packet Tracer to verity Access Policy, NAT and Routing.
* Upgrade PIX 535 Firewalls to ASA 5540 and 5550 Firewalls which includes hardware and OS upgrade.
* Juniper NetScreen and ISG Firewall configuration and support through NSM 2010 (Network Security Manager).
* Follow change management process using HP Service Manager to schedule changes.
* Firewall Policy Optimization and access list management using Tufin and syslog using Log Logic tool.
* Push the policies on CheckPoint using Smart Dashboard and work with users to verify connectivity and troubleshoot Firewall related issues using smart view tracker as well as CLI command line.
* Perform Firewall and Hardware upgrades including IPSO image upgrades, upgrade security gateways.
* Review Firewall rule conflicts and misconfigurations as well as redundant rules using Tufin.
* Compiled and analyzed network traffic reports and logs in support of subordinate compiling incident response and disseminating analysis reports at the appropriate classification level
* Identify unused rules and schedule change to mark it for permanent deletion at later point of time.
* Create firewall audit reports and compliance metrics.
* Primary responsibility for the implementation, administration, and maintenance of infrastructure security solutions in the organization, with a focus on Web Content Filtering.
* Support routing protocols including BGP and OSPF routing, High availability using HSRP, VRRP, load balancing/failover configurations, GRE Tunnel Configurations, VRF configuration and support on the routers.
* Experience setting up all features on the Palo Alto's such as: Site to Site VPN's, Global protect, Mind Meld, Aperture, Panorama, Dynamic Access Lists, many others.
* Strong understanding for routing and switching in relation to Checkpoint
* Building and supporting Site to Site IPSec based VPN Tunnels for all Extranet and 3rd party communications.
* Configuring DMVPN tunneling between the branches. Hands on in deployment of GRE tunneling, SSL, Site-Site IPSEC VPN and DMVPN.