Company Profile:-

We at Netplace Technologies Pvt. Ltd., hold over 25 years of experience as industry experts merged with world-leading technology vendors that deliver an integrated range of solutions for complete IT Systems, Cybersecurity, and Physical safety & security with building management systems and related lifecycle management.

We are a company thriving on changing the way organizations think about IT infrastructure and smart building solutions. We are experts in wired and wireless networking solutions for mobility, Network security, and management on both on-premises and cloud platforms. These technology solutions are provided by combining the best products from various OEMs and Netplace's partnered services covering resourcing, consulting, and assessment managed by our skilled Customer Experience (CX) and Project Management (PM) teams.

Being in business since 1998, we have catered to Omni-sector organizations across Pan India with a personalized & customized networking solution.

Website- www.netplace.in

Designation- Network Security Engineer
Location: Andheri East, Mumbai
Office time- 10.00 am to 7.00 pm
Working days- Monday to Saturday full day working, only 03rd Saturday will be full day Off.

Position Summary:
We are seeking a skilled IT Network Security Engineer specializing in firewall technologies to join our team. The ideal candidate will have deep expertise in configuring, deploying, and managing enterprise-grade firewalls, ensuring the security, performance, and integrity of our network systems. This role will focus on firewall deployment and configuration, troubleshooting network security issues, and maintaining secure communication across our enterprise network.

Primary Duties and Responsibilities:

- **Firewall Configuration & Management:**
  - Configure, deploy, and manage various firewall technologies, including **Cisco**, **Palo Alto**, **FortiGate**, and others, to protect the organization's network infrastructure from potential threats.
  - Design and implement security policies and firewall rules to safeguard business applications, network devices, and sensitive data.
  - Ensure proper configuration of **VPN concentrators** and security appliances for secure remote access.
- **Network Security Design & Implementation:**
  - Design and implement comprehensive network security solutions, focusing on firewalls, intrusion detection/prevention systems (IDS/IPS), and related security appliances.
  - Set up and configure secure **wireless networks** and **switching environments** to ensure secure communication across the organization.
- **Troubleshooting & Incident Response:**
  - Troubleshoot firewall-related issues, including connectivity problems, firewall rule misconfigurations, and potential security breaches.
  - Monitor firewall logs and alerts to detect unauthorized access attempts or vulnerabilities, and take corrective action when necessary.
  - Respond to security incidents promptly and work to mitigate any impact on the network, including providing detailed post-incident analysis.
- **Firewall Performance Monitoring & Optimization:**
  - Continuously monitor firewall performance and security posture to ensure optimal functionality.
  - Conduct regular performance tuning and maintenance to enhance the efficiency of firewall systems and ensure compliance with industry standards and best practices.
- **Documentation & Reporting:**
  - Maintain up-to-date documentation of firewall configurations, security policies, and network security architecture.
  - Generate periodic reports on firewall performance, security incidents, and recommendations for improvements.
- **Collaboration & Technical Support:**
  - Work closely with other IT teams to troubleshoot network issues and design integrated network security solutions.

    - Respond to inquiries and provide support related to network security and firewall configurations to internal teams, external vendors.
    - Coordination with OEMs.
- **Continuous Improvement & Learning:**
    - Stay up-to-date with the latest advancements in firewall technologies and network security threats to enhance the company's security posture.
    - Participate in training and certification programs to continuously improve skills and expertise in firewall technologies.

Required Qualifications:

- Proven experience with configuring and managing **firewall technologies** such as **Cisco**, **Palo Alto**, **FortiGate**, and **Check Point**.
- Strong understanding of **network security principles**, including VPNs, IDS/IPS, NAT, routing, and network segmentation.
- Expertise in creating and implementing **firewall rules**, security policies, and access control lists (ACLs) to manage network traffic securely.
- Proficient in troubleshooting firewall-related network issues and security breaches.
- Experience with monitoring firewall logs, analyzing security events, and taking proactive steps to secure the network.
- Ability to design, implement, and optimize complex **network security infrastructures** to support business requirements.

Preferred Qualifications:

- Certifications in **Cisco (CCNA, CCNP Security)**, **Palo Alto Networks (PCNSE)**, **Fortinet (FCNSA/FCNSP)**, or similar.
- Hands-on experience with **Next-Generation Firewalls (NGFW)** and technologies such as **Cisco Firepower**, **Palo Alto PAN-OS**, or **FortiGate**.
- Familiarity with **cloud security** concepts (e.g., AWS, Azure) and the integration of firewall policies in a cloud environment.
- Experience with **intrusion prevention systems (IPS)** and network segmentation for improved security.