Engineering & Technology Group

Network Design Engineer – Security

Position:	Network Design Engineer – Security	**Type:**	Full Time
Hiring Mgr:	Director Network Engineering	**Onsite Status:**	Onsite or Hybrid
Location:	Kingston, NY	**Date Added:**	Feb 7, 2024

Position Summary

The Network Design Engineer - Security is part of Archtop Fiber's Network Engineering group, and the role will support a variety of design needs for our network infrastructure and will provide guidance to keep secure our service provider environment. This position will work closely with the Director Network Engineering and others to support our advanced 100% fiber optic communications network. The Network Design Engineer – Security will be an integral team member working to design and develop Archtop's IP/SR-MPLS backbone, XGS-PON access layer, internet peering, optical transport infrastructure, and other various network expansions and upgrades while providing security expertise to our multi-state fiber optic network.

What you'll do:

- Oversees the development and implementation of multi-layered network security policies, standards, guidelines, and generally accepted industry practices which ensure compliance and support 99.999% uptime.
- Create implementation designs and required documentation, including Methods of Procedures (MOPs), diagrams, drawings, and various instruction details.
- Identify risk factors, develop response plans to address these risks, and recommend processes and procedures to assess vulnerability and audit security integrity.
- Perform tasks of high complexity related to the design, maintenance, and problem analysis of IP network access and IP transport equipment.
- Provide turnup and test information for new network builds and augmentations.
- Monitor, create reports, and provide analysis based on customer traffic patterns and overall internet traffic flows by utilizing our carrier-class traffic monitoring and threat mitigation tools – provide recommendations for network augments, peering additions, etc. based upon findings.
- Maintain detailed documentation of network elements, topologies, and device deployments.
- Recommend methods and procedures for disaster recovery, logging, and reporting.
- Support process development, documentation and support as needed to other teams for implementation, troubleshooting, and repair of network connections and customer deployments.
- Support equipment/materials vendor selection and maintain strong relationships with Archtop's vendors.
- Recommend policy and procedure for all service provider security tasks, including configuration, documentation, and procedural guidance for NOC.
- Foster a resilient network design approach that ensures redundancy and ultrafast failover.
- Maintain a high level of confidentiality towards
- Develop customer service configurations that can be deployed via network automation and low-touch provisioning. Work collectively with Network Operations to ensure that configurations align with and meet the needs of provision platforms.
- Implement security requirements that align with Archtop's carrier-class network requirements, including protection against flooding, DDoS, unauthorized access, unauthorized monitoring, and others.

- Assist Network Operations team objectives such as network management/element management, performance measurement, fault management, access security, and others.
- Create and maintain Best Practice documentation to capture our design, and deployment methodologies, device configuration templates, and customer service configuration with dedicated focus and cybersecurity.
- Support technical product development and deployment, including Proof of Concept testing procedures without bias. Carry out Alpha and Beta testing by working with Network Operations team members and others.
- Participate in annual budget planning for network projects and improvements.
- Assimilate, analyze, and correlate large amounts of forensic data from various network devices, operating systems, applications, security devices, logs, and alerts by leveraging analytical and problem-solving skills.

What you'll bring:

- 4+ years of progressive experience in network engineering or network architecture roles in a large network environment. Experience in a Service Provider (ISP/CSP) environment is strongly desired.
- Four-year Engineering, Computer Science, or comparable technology degree from an accredited college or university. Equivalent professional experience also considered.
- Professional level networking certifications are strongly desired but not required – CCNP Security (or similar) preferred.
- Strongly working knowledge of all aspects of OSI layers 1-4 is required.
- Firewall and various VPN technology experience required.
- Experience with application security standards, cloud security standards, vulnerability management, data loss prevention, risk assessment, investigating security incidents, and developing security action plans.
- Demonstrated deployment of eBGP, iBGP, ISIS, OSPF, MPLS, and Segment Routing is preferred.
- Knowledge of FTTx design and PON access technology GPON, XGSPON, OLT, and ONU is a plus.
- Detailed knowledge of End-to-End QOS, including Layer 2 and Layer 3 approaches, MPLS EXP, classifying, packet marking, and queueing.
- Knowledge of network tools and protocols including SNMP, TACACs+, radius, syslog, DHCP, VLANs, Spanning Tree, EVPN, VPLS, IPsec, Pseudowire, VRFs, MC-LAG, EV-LAG, DNS, NAT, CGN, TCP, UDP, FQDN, SIP, MGCP, RTP, NTP, PTP, and others.
- Knowledge of network operating systems, such as IOS-XR, AOS, Linix.
- Ability to troubleshoot complex issues related to a service provider's network.
- Ability to troubleshoot complex issues related to a service provider's network.
- Must have a strong focus on quality and network sustainability (99.999% up time).
- Thorough knowledge and experience with network access control and authentication methodologies including Access Control Lists (ACLs), RPKI, RADIUS, TACACS+, 802.1X, MAC and certificate authentication.
- Applicants must be a US citizen.
- Maintain a valid state driver's license and safe driving record.

What we offer (acquisition specific):

- Competitive salary – range for this opportunity is $120k to $140k
- Heavily subsidized medical, dental, and vision
- Holidays, PTO, and Flexible work schedules
- 401(k) w/ generous match
- Employee Assistance Program (EAP)
- Life insurance, short- & long-term disability insurance
- Employee Referral Program
- Employee discount programs

Archtop Fiber is proud to be an Equal Opportunity Employer. We celebrate diversity and are committed to creating a welcoming and inclusive environment for all.

Please apply directly Careers@Archtopfiber.com