**Perspective:** Distribution network, office network, corporate network, product portfolio and its whereabouts

|  |
| --- |
| Technology (Retail Distribution Network): Technology Architecture Planning & Deployment |
| Capacity planning, management, current report and future plan |
| Server zones, Application delivery zones, OTT Zones etc. |
| Separation of Back-office network, as Firewall is incoming for the server zone |
| Transmission design for: Video Stream, IPTSP, Application based Policy on transmissions, ERP etc. |
| Identity & access management with ACL optimization |
| Broadcast, Anycast, Multicast configuration requirements |
| Network Segmentation by Corporate & Retail |
| Cache, CGNAT, BNG, IIG, CDN Separation & improve COGS |
| Make the retail network ready for PPPoE, purchase an already established solution with Selfcare |
| Critical hardware: Identify, justify, approve, Purchase immediately |
| System hardening based on benchmark for CISCO and all relevant services |
| Technology planning & system architecture with zoning for DMZ, servers, storage, VPN, VLAN, DNS, NTP etc. |
| Tech system detail plan and improvement scope definition & requirements |
| Decentralization network design with service mapping |
| Privileged access management on devices and customer's VPN credentials |
| Datacenter Assessment: Cabling: Power/Fiber/UTP/PDU |
| Tech Server & Application systems detailed plan |
| Networked device licensing & deprecation requirements |
| Networked device OS Types, Upgradability & Extended Support Requirements |
| Networked device: OS patch management, firmware upgrade |
| Exposed IP list & remediation plan for a private network against purchased IP blocks, How many are assigned & free |
| Firewall requirement formulation (LB first: Firewall- 1 in 6 out model) (100G per port) |
| Firewall requirement: Physical Server requirements and develop BoQ |
| LDAP IPA based Installation |
| Linux servers credentials, application PEM, Integration with IPA |
| NTP Server and syncing throughout the infrastructure |
| DNS server syncing throughout the infrastructure |
| Device OEM Portal access list |
| NMS Dashboard Requirement list with end-to-end visibility |
| SSL Certificates & its portal access |
| APNIC portal access |
| Data Collection and Log Shipping Requirements mapping for Security Scanning |
| Initiate internal SMTP integration |
| Customer VPN Links credentials with public key assignment |
| Systemwide static IP removal and re-design the IP network |
| Customer Data Links list and credentials documentations |
| IPTSP customer link records or documentations, agreements |
| Enable 2FA for critical resources |
| Small scale security device for BTSs or where required for DDoS protection |
| Zoning requirements and mapping |
| Device configuration streamline |
| Device access streamline using SSH not Telnet, stop Telnet on all devices |
| Perimeter exposure reduction, by limiting exposed IP |
| Zero trust network access design & implementation |
| Establish & document customer's data links layer |
| Establish & document customer's VPN credentials |
| List of licenses on networked devices, OS, various other things |
| Online portal access list for networked devices |
| ITIL Based service management portfolio |
| Cryptographic keys alignment and develop a software vault for storing these keys |
| PoC for: Lithium-ion battery for UPS, DDoS, NMS etc. |
| SCOM Deployment provisioning |
| NAC deployment provisioning |
| Automated IP fabric |
| DDoS response plan with remediation |
| Online UPS testing and commission |
| Enable TACACS for Cisco & RADIUS for Mikrotik - Full IAM |
| Enable policy based services protocol-wise, Bongo, IPTSP etc. |
| SSL Certificate enrollment with enablement of end-to-end data transmission encryption |
| Policy based application traffic & protection |
| IIG & BDIX data movement |
| Network design security factors |
| Traffic engineering: Separation of Transit, IIG & CDN, CGNAT, BNG, BRAS |
| Device based configuration baseline |