Restructured LAN & Network Security for IT&DC

About IT & DC

A premier Training and consultancy company which provide hands-on training for corporate and individuals, also provide consultancy services for organization. It's head office is in New Delhi (Ashok Nagar) and branches all over across Delhi.

Summary of the project

Earlier IT & DC network was running on unmanaged Switches and unstructured cabling. They were having flat network only and the same IP schema was used for entire organization including mission critical Servers.

They were using mix products such as Linksys and D-Link for their network. No Security Gateway device was used at perimeter level and no restrictions were there for any traffic as, they were using Public IP on the servers directly to access the applications over internet for remote users/clients.

The whole network was running on Ethernet unstructured cabling and no other option was available in case of Ethernet connectivity issue to connect the network or to access the network resources i.e. Network printer, Servers etc...

IT&DC were also having few businesses critical Servers installed on which critical application were running i.e. Web Servers, Mail Servers etc. The IT Management and team were really suffering with the Network issues and the maintenance of the same was a big task /challenge for them.

Challenges

- Unmanaged, unstructured, & non-documented cabling
- Mixed Cables such as Cat 3,& 5

- No network diagram resulting in longer Turnaround time
- LAN security & management concern
- No wireless connectivity available for organization
- Servers and End users systems got Virus infected due to non-availability of security/UTM device in the network
- LAN/WAN users were unable to access internet due to internet bandwidth congestion
- No network segmentation (VLANs)
- No security in the Network

Preemptive Value Proposition

- Restructured, revamped the entire cabling
- Configured Fortinet UTM and Core Switches in High Available architecture mode to provide redundancy in the network in case of Hardware failure
- Configured Cisco 3750-X in stack mode at the core layer and 2960S at the Edge Layer of network
- Configured VLAN (as per the requirement), Inter VLAN routing, Spanning Tree Protocol (STP) to provide loop free network
- Configured FortiGate 200D Firewall at the perimeter of the Network to provide L4 security. Configured access lists to provide authorized access only between due to internet bandwidth choking
- Configured Forti Analyzer for complete reporting and visibility of user activities over web
- Configured wireless solution on Cisco to provide redundancy in case of Ethernet connectivity unavailable, implemented Wireless controller with 10 Access Points

Benefits to Customer

- Perimeter security & core switching on redundancy for high availability of the network
- Proper documentation of entire Network
- Easy troubleshooting, management for active & passive devices
- Easy to move & add changes in the network