Network Design Proposal for Bank

Title : Network Design Proposal for Bank

Abstract :

A network proposal has to be developed for a bank. The bank has a main office , which is located in London, and has 5 branch offices located at Paris, California, India, Dubai and Qatar. The bank has an application server, which is used by it's customers across the world for online transactions. All the branches have high speed internet connection. There are approximately 100 users in each of the branch offices and 200 users in the main office.

Network requirements.

1. Identify the hardware components required to setup the network for the Bank
2. High availability should be available to the application server, which is accessible using https protocol.
3. The application server should be setup in a secure manner with network and host level protection.
4. All traffic into the application server should be scanned for security attacks.
5. IP network design for the branch and main offices.
6. IP addressing range for users and hardware components.
7. The users at different locations should be able to access each other, including the application server.
8. Identify the features and methodology which would be followed to achieve the solution.
9. Network Topology diagram.

Network requirement analysis

As the locations of the banks are spanned across different geographical locations, a VPN solution is recommended as it would be more economical as compared with a leased line solution. VPN appliances are required for the same.

The application server is recommended as Windows 2008 / Windows 2012, with appropriate failover clustering to provide high availability to the application. The application server should be setup on a DMZ, where only access to https protocol (TCP port 443), should be made available to users accessing from the outside. Antivirus with desktop firewall should be installed on the server, which would provide host level protection. An appliance, which would perform deep packet inspection, should be setup on the network, to filter incoming traffic to the application server. This would scan the traffic for security threats and attacks.

Hardware and software requirement analysis

1. At the main office, a VPN appliance would be required, which would have integrated firewall and deep packet inspection. The recommended VPN appliance is **Sonic wall NSA 220/W**, which has the capacity to support site to site VPN tunnels and also has deep packet inspection and firewall capabilities.

2. There are 200 users in the main office. A total of 5 nos of 48 port switches are recommended considering ports for servers, VPN appliance and expansion plan. The **Cisco Catalyst 2960S-48FPD-L** is recommended for the same.

3. At the branch offices, the **Sonicwall TZ105** series is recommended to establish site to site VPN connectivity with the main office.

4. There are a total of 100 users each at the branch office. A total of 3 nos of 48 port switches is recommended, which are **Cisco Catalyst 2960S-48FPD-L**, considering future expansion plans.

5. Windows 2008/2012 is recommended for the application server with server hardware.

Additional requirements

1. All the locations have high speed internet connection. At the main office, an additional public IP address would be required to host the application server. The IP address would be registered with a domain name, which would enable users on the outside world (internet), to access the application.

Feature and Services

1. VLAN

Two networks are required at the main office. One network would be for the LAN, where the offices users would be connected. The second network would be the DMZ network, where the application server is hosted. This is required since the application server would require access from outside. Two VLANS would be created which would be mapped with the LAN and DMZ network. VLANS would be configured on the Switches.

2. Access control lists.

Access control lists are configured on the VPN appliance at the main office. The ACLs are used to restrict communication from the internet to only the allowed port, which is TCP port 443 on the application server in the DMZ. ACL is also configured to allow all traffic from the branch office networks to the DMZ and LAN network in the main office.

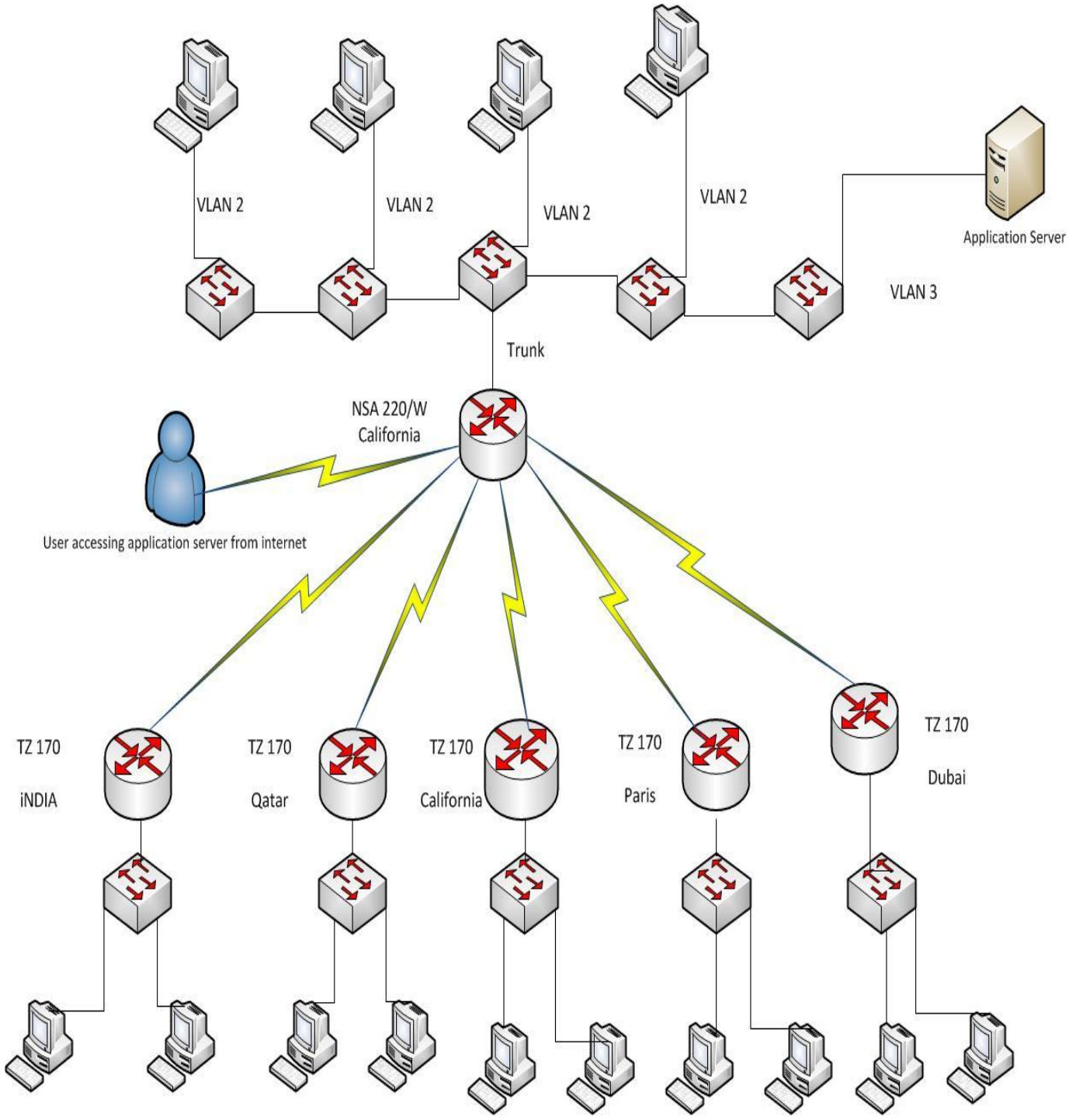
3. Static NAT

Static NAT is configured on the VPN Appliance to allow traffic from the public IP address of the application server, to the LAN IP address.

4. Failover cluster

Failover cluster is configured on the Windows 2008/2012, on which the application server is hosted. This would ensure that high availability is provided to the application.

Network Topology Diagram



Network Topology Diagram explanation

The main office is deployed with Sonic wall NSA 220/w appliance. The switches are configured with VLAN 2 and VLAN 3. VLAN 2 is mapped with the LAN network and VLAN 3 is mapped with the DMZ network. At the remote offices, TZ170 appliance is used to connect to the NSA 220/w appliance.

IP Network Design

Location	Network Address
Main office (LAN)	192.168.1.0/24
Main office (DMZ)	192.168.2.0/24
India (LAN)	192.168.3.0/24
Qatar(LAN)	192.168.4.0/24
California(LAN)	192.168.5.0/24
Paris (LAN)	192.168.6.0/24
Dubai(LAN)	192.168.7.0/24

IP address design

Location	IP address
Main office	LAN Users – 192.168.1.2 – 192.168.1.201 VLAN 2 Gateway (192.168.1.1) Application Server (192.168.2.2) VLAN 3 Gateway (192.168.2.1)
India	LAN Users – 192.168.3.2 – 192.168.3.101 Gateway address – 192.168.3.1
Qatar	LAN Users – 192.168.4.2 – 192.168.4.101 Gateway address – 192.168.4.1
California	LAN Users – 192.168.5.2 – 192.168.5.101 Gateway address – 192.168.5.1
Paris	LAN Users – 192.168.6.2 – 192.168.6.101 Gateway address – 192.168.6.1
Dubai	LAN Users – 192.168.7.2 – 192.168.7.101 Gateway address – 192.168.7.1

Network Design and configuration strategy

1. Connect the VPN appliances to the appropriate internet connections.
2. Configure VLANS , VLAN 2 and VLAN 3 on the switches at the main office.
3. Connect one of the ports on the switch to the trunk port on the NSA appliance.
4. Configure the VLAN 2 and VLAN 3 gateway on the NSA appliance as 192.168.1.1 and 192.168.2.1 respectively.
5. Configure site to site IPSEC tunnels between the TZ170 and NSA.
6. Configure static NAT on the NSA appliance to map the public IP address of the application server with the LAN IP address.
7. Configure ACL on the NSA appliance to allow only TCP port 443 (https) communication the application server. Configure ACL's to allow all traffic between the branch and main office networks.
8. Configure failover cluster on the application server, for high availability.

Hardware inventory list

Item	Model	Qty
VPN appliance	Sonic wall NSA 220/w	1
VPN appliance	Sonic wall TZ170	5
Switch	Cisco Catalyst 2960S-48FPD-L	20
Server	HP ProLiant ML350 G8 Server	1