**VPN Implementation for Corporate Sites**

**Project Overview**

This project aims to securely connect two corporate sites using a VPN (Virtual Private Network) and enhance the network's performance, reliability, and security by integrating VLANs, OSPF, HSRP, STP, DHCP, and using Cisco Packet Tracer for simulation.

**Objectives**

* Establish a secure site-to-site VPN connection using IPsec.
* Segment the network using VLANs for improved efficiency and security.
* Enable dynamic routing between sites with OSPF.
* Ensure network redundancy and high availability with HSRP.
* Prevent network loops with STP.
* Automate IP address allocation with DHCP.
* Enhance network security with firewalls.

**Network Topology**

* Site A: [Description of Site A, including network devices and IP addresses]
* Site B: [Description of Site B, including network devices and IP addresses]

**Protocols and Technologies**

* **IPsec (Internet Protocol Security)**: Secure communication between the two sites.
* **VLAN (Virtual Local Area Network)**: Network segmentation for efficiency and security.
* **OSPF (Open Shortest Path First)**: Dynamic routing protocol for optimal path selection.
* **HSRP (Hot Standby Router Protocol)**: Network redundancy and high availability.
* **STP (Spanning Tree Protocol)**: Prevention of network loops.
* **DHCP (Dynamic Host Configuration Protocol)**: Automated IP address allocation for network devices.
* **Firewall**: Enhanced network security by controlling incoming and outgoing traffic based on predefined security rules.

**Suggested Hardware**

* **Routers**: Cisco ISR (Integrated Services Routers) such as Cisco ISR 4300 Series
* **Switches**: Cisco Catalyst switches such as Cisco Catalyst 2960 or 3650 Series
* **Firewalls**: Cisco ASA (Adaptive Security Appliance) for enhanced security
* **Servers**: Dedicated DHCP servers or routers with DHCP capabilities

**Implementation Steps**

**1. Define Requirements**

* Determine the purpose and requirements for the VPN connection (bandwidth, security, availability).

**2. Choose VPN Protocol**

* Select IPsec for the site-to-site VPN.

**3. Select VPN Devices**

* Use appropriate devices for each site, such as Cisco routers or firewalls (e.g., Cisco ASA).

**4. Configure the VPN Gateway**

* Set up the VPN gateways on both sites with the IPsec settings.

**5. Set Up VLANs**

* Configure VLANs on switches and assign devices to the appropriate VLANs.
* Use 802.1Q for VLAN tagging.

**6. Enable OSPF**

* Configure OSPF on routers for dynamic routing between the sites.

**7. Configure HSRP**

* Set up HSRP on routers for redundancy and high availability.

**8. Implement STP**

* Configure STP on switches to prevent network loops.

**9. Set Up DHCP**

* Configure DHCP on routers or dedicated DHCP servers to automatically assign IP addresses to network devices.
* Define DHCP pools for each VLAN.

**10. Configure Firewalls**

* Set up firewalls to control incoming and outgoing traffic based on predefined security rules.
* Ensure that the firewall policies are aligned with the organization's security requirements.

**11. Test and Monitor**

* Verify connectivity, test the VPN tunnel, and monitor performance and availability.

**Simulation Using Cisco Packet Tracer**

* **Purpose**: Use Cisco Packet Tracer to simulate the network setup and configurations.
* **Application**: Create a virtual network topology in Packet Tracer, configure the protocols and devices, and test the connectivity and performance.

**Example Configuration**

**Site A Configuration**

! Site A Configuration

crypto isakmp policy 1

authentication pre-share

encryption aes

hash sha

group 2

lifetime 86400

crypto isakmp key YOUR\_SHARED\_KEY address SITE\_B\_IP

crypto ipsec transform-set MY\_TRANSFORM\_SET esp-aes esp-sha-hmac

crypto map MY\_CRYPTO\_MAP 10 ipsec-isakmp

set peer SITE\_B\_IP

set transform-set MY\_TRANSFORM\_SET

match address VPN\_ACL

interface GigabitEthernet0/0

ip address SITE\_A\_IP 255.255.255.0

crypto map MY\_CRYPTO\_MAP

access-list VPN\_ACL permit ip SITE\_A\_NETWORK 0.0.0.255 SITE\_B\_NETWORK 0.0.0.255

! DHCP Configuration

ip dhcp pool VLAN10

network 192.168.10.0 255.255.255.0

default-router 192.168.10.1

dns-server 8.8.8.8

ip dhcp pool VLAN20

network 192.168.20.0 255.255.255.0

default-router 192.168.20.1

dns-server 8.8.8.8

**Site B Configuration**

* Mirror the configuration of Site A with appropriate IP addresses and network details.

**Conclusion**

By following this project outline and implementing the specified protocols, you will create a secure, efficient, and reliable network connection between the two corporate sites. The use of Cisco Packet Tracer will help simulate and validate the network setup before deployment.