Site-to-Site VPN Setup Document Sample

1. Overview

This document outlines the configuration steps for establishing a Site-to-Site VPN connection between **Site A** and **Site B**.

2. Prerequisites

- VPN-capable routers/firewalls at both sites
- External static IP addresses for both sites
- Access to both devices' management interfaces

3. Network Information

Parameter	Site A	Site B
Public IP	198.51.100.10	203.0.113.20
LAN Subnet	10.1.0.0/24	10.2.0.0/24
Device Model	Cisco ASA 5506	Fortigate 60F

4. VPN Configuration Parameters

Parameter	Value
IKE Version	IKEv2
Pre-Shared Key	`sample-shared-key-1234`
Encryption	AES256
Authentication	SHA256
Diffie-Hellman Group	Group 14
Phase 1 Lifetime	28800 seconds
Phase 2 Lifetime	3600 seconds

5. Configuration Steps

Site A (Cisco ASA) Example CLI

```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 14
 lifetime 28800
crypto ikev2 enable outside
crypto ipsec ikev2 ipsec-proposal VPN-PROPOSAL
 protocol esp encryption aes-256
 protocol esp integrity sha256
tunnel-group 203.0.113.20 type ipsec-l2l
tunnel-group 203.0.113.20 ipsec-attributes
```

```
 ikev2 remote-authentication pre-shared-key sample-shared-key-1234
 ikev2 local-authentication pre-shared-key sample-shared-key-1234
access-list VPN-INTERESTING-TRAFFIC extended permit ip 10.1.0.0 255.255.255.0 10.2.0.0 255.255.255.0
```

Site B (Fortigate) Example Web GUI Steps

- Go to **VPN > IPsec Wizard**.
- Set **Remote Gateway** to `198.51.100.10`.
- Set pre-shared key to `sample-shared-key-1234`.
- Configure phase 1 and 2 settings to match above parameters.
- Add address groups for local `10.2.0.0/24` and remote `10.1.0.0/24` subnets.

6. Verification

- Check VPN tunnel status on both devices.
- Ping from one site to the other's LAN subnet.

7. Support Information

- Site A IT Contact: admin-a@example.com
- Site B IT Contact: admin-b@example.com