Change Request Form & Method of Procedure

On-Prem to AWS Site-to-Site VPN Connectivity

CHANGE REQUEST SUMMARY

Change Request No.: AWS-2026-02

Project: Hybrid On-Prem/AWS Connectivity — Reusable Template

Requested By: Justin K. Bowden, Network Engineer I

Department: Network Engineering

Change Priority: Medium

Change Impact: Major

Environments Impacted: On-prem core network; target AWS VPC

DESCRIPTION OF CHANGE

Establish a site-to-site IPsec VPN connection between on-prem network infrastructure and a target AWS VPC to support a cloud-connected workload, with routing configured for bidirectional reachability.

REASON FOR CHANGE

- Provide secure, encrypted connectivity to a cloud-hosted workload
- Avoid exposing AWS resources to the public internet
- Produce a documented, reusable pattern for future hybrid connectivity requests

CHANGE IMPACT EVALUATION

Change Type	Impacted
Network	Yes
Security	Yes
Cloud Infrastructure	Yes
Procedures	Yes

RESOURCE REQUIREMENTS

Personnel: 1 Network Engineer, 1 Cloud/Systems reviewer. Hardware/Software: AWS console access (VPC, VPN Gateway), on-prem VPN-capable router/firewall, IPsec pre-shared key material.

METHOD OF PROCEDURE

1. Diagram the target topology, including on-prem VPN device, AWS Virtual Private Gateway, and VPC subnet(s) to be reached.
2. Create the Customer Gateway object in AWS, specifying the on-prem device's public IP and routing type.
3. Create the Virtual Private Gateway and attach it to the target VPC.
4. Create the Site-to-Site VPN Connection in AWS, linking the Customer Gateway and Virtual Private Gateway.
5. Download the AWS-generated configuration and apply matching IPsec Phase 1/Phase 2 parameters on the on-prem device.
6. Bring up the tunnel(s) and confirm IKE/IPsec negotiation succeeds on both AWS and on-prem sides.
7. Configure routing: static routes or BGP (if using a Virtual Private Gateway with dynamic routing) so the VPC subnet is reachable internally.
8. Update on-prem routing tables/ACLs as needed to permit the new traffic path.
9. Validate connectivity from an on-prem host to a resource in the target VPC subnet, and vice versa.
10. Package the topology diagram, AWS configuration export, and MOP as a reusable template for future hybrid connectivity requests.

TEST / VERIFICATION PLAN

- Verify VPN tunnel status shows UP in the AWS console

- Verify routing propagation in both directions (on-prem → VPC and VPC → on-prem)
- Verify application/host connectivity across the tunnel
- Confirm no unintended exposure of VPC resources outside the tunnel

ROLLBACK PLAN

- Delete or disable the Site-to-Site VPN Connection in AWS
- Remove the corresponding on-prem VPN configuration and routes
- Confirm no dependent services were relying on the connection before final teardown
- Notify stakeholders that rollback is complete

Note: Change numbers and environment labels shown here are illustrative. Client-identifying details have been withheld in accordance with a signed NDA; the process and technical steps reflect the actual change performed.