Cloud Interconnect Provisioning Guide

1. AWS - Hosted Direct Connect Provisioning

Purpose

Establish a private Layer 2 or Layer 3 connection between on-prem infrastructure and AWS.

Workflow

Step 1: Gather Required Information
- Customer AWS Account ID
- Private /24 CIDR block (must not overlap with internal or AWS VPC ranges)
- AWS VPC subnets
- On-prem subnets
- Bandwidth requirement
- Preferred AWS Region

Step 2: Allocate Network Resources
- Reserve two VLANs (AWS-facing and customer-facing)
- Allocate /30 subnets from the /24
- Assign VRF, RD, RT, ASN, and BGP password

Step 3: AWS Console - Create Hosted Connection
- Use AWS Direct Connect -> Allocate Connection
- Enter connection name, customer AWS ID, VLAN, and bandwidth
- AWS sends invite for VIF creation

Step 4: Assist Customer with Virtual Interface
- Help customer accept the connection and configure a Private VIF
- Provide BGP details and IP assignments

Step 5: Configure On-Prem Router
(Example configuration included in full guide)

Step 6: Testing & Monitoring
- Verify BGP
- Run reachability tests
- Monitor via NMS or custom scripts

2. Google Cloud - Partner Interconnect Provisioning

Purpose

Establish private connectivity between enterprise networks and Google Cloud VPCs.

Workflow

Customer Side:
- Go to VLAN Attachments in GCP Console
- Create Partner Interconnect and share pairing key

Provider Side:
- Use gcloud CLI to create VLAN attachment using pairing key
- Retrieve IP configuration from GCP

Cloud Interconnect Provisioning Guide

- Configure router with assigned IPs and BGP to ASN 16550

3. Microsoft Azure - ExpressRoute Provisioning

Purpose
Establish private connectivity between a customer network and Microsoft Azure.

Workflow
Customer:
- Create ExpressRoute Circuit in Azure Portal
- Provide Service Key to provider

Provider:
- Use Equinix or Megaport portal to provision connection
- Configure primary and secondary peerings
- Assign VLANs and subnets
- Configure router BGP session with Azure ASN 12076

4. Monitoring & Troubleshooting

Monitoring Best Practices:
- Ping cloud router IPs
- Monitor BGP and prefix count
- Alert on tunnel/BGP failures

Troubleshooting:
- Verify BGP IPs, ASN, passwords
- Check MTU, firewall, prefix-lists
- Validate cloud-side configuration