

VPN Site-to-Site



Overview

JioCloud VPN Site-to-Site creates a private, encrypted tunnel between your data center and JioCloud. Traffic stays protected with IPsec, and the connection stays up — ideal for hybrid applications, data sync, backups, or disaster recovery. You don't need to rip out your existing routers or firewalls. This works with what you already have. And with rapid provisioning and built-in failover, it's reliable enough for production — but flexible enough to grow with you.

Key Features

- **Encrypted IPsec tunnel**
Secures all traffic using AES-256 encryption and SHA-based authentication.
- **Always-on connection**
Keeps cloud and on-prem systems linked, with no manual re-establishment needed.
- **Built-in redundancy**
Configure failover tunnels and gateways, so connections don't drop if a device or link fails.
- **Works with existing hardware**
Compatible with most enterprise routers and firewalls — no vendor lock-in or box replacements.
- **Scales without re-architecting**
Add more tunnels or increase throughput as your needs grow.
- **Quick setup via console or API**
Skip long provisioning cycles and deploy VPN tunnels in minutes.

Benefits

- Secure, encrypted cloud connectivity – without public internet exposure.
- Fast, scalable extension of your private network to the cloud.
- Reduced cost and complexity compared to traditional leased lines.
- Compliance-ready setup with audit visibility and policy-based control.
- A hybrid-ready foundation for migration, DR, and data replication.

Use Case

- **Enable hybrid cloud**

Bridge on-premise systems and cloud apps for secure data exchange, backups, and migrations.

- **Migrate without disruption**

Move services to cloud gradually – with persistent, policy-driven connectivity.

- **Protect sensitive workloads**

Avoid internet exposure by tunneling traffic directly over encrypted, private paths.

- **Stay resilient**

Ensure availability with redundant tunnels and failover configurations built for business continuity.