Service Name

AWS VPN

Service Overview

AWS VPN is comprised of two services: AWS Site-to-Site VPN and AWS Client VPN. AWS Site-to-Site VPN is a fully-managed service that creates secure IPsec VPN connections between on-premises networks or branch offices and AWS resources using IP Security (IPSec) tunnels. AWS Client VPN is a fully-managed remote access VPN solution that enables secure access to resources within both AWS and on-premises networks for remote workforces. Both services provide encrypted connectivity, high availability, and automatic scaling to support hybrid cloud architectures and remote work scenarios.

Key Use Cases

- Hybrid connectivity: Securely extend on-premises networks to AWS cloud resources using Site-to-Site VPN with IPsec tunnels for application migration and multi-site communication
- Remote workforce access: Enable secure remote access for employees to both AWS and on-premises resources using Client VPN with OpenVPN protocol and multi-device support
- Multi-site networking: Connect distributed branch offices and remote locations through VPN CloudHub for hub-and-spoke topology or VPN Concentrator for cost-effective multi-site connectivity

Features

- **Site-to-Site VPN**: IPsec VPN connections with dual tunnels for high availability, supporting up to 5 Gbps per tunnel with accelerated options using AWS Global Accelerator
- **Client VPN**: OpenVPN-based remote access with mutual authentication, SAML/Active Directory integration, and support for multiple operating systems including Windows, macOS, Linux, iOS, and Android
- **VPN Concentrator**: Cost-effective multi-site connectivity allowing up to 100 remote sites per concentrator with shared bandwidth up to 100 Mbps per tunnel
- **Advanced Security**: Certificate-based authentication, Network Address Translation (NAT) traversal, private IP VPN support, and integration with AWS security services
- **Monitoring and Management**: CloudWatch metrics, connection logging, AWS Console management, and integration with AWS monitoring tools for visibility and troubleshooting

Value Proposition

AWS VPN provides fully-managed, highly available VPN services that eliminate the need for customers to deploy and maintain their own VPN infrastructure. Key advantages include automatic scaling and failover, built-in redundancy with dual tunnels, seamless integration with AWS services like Transit Gateway and Direct Connect, and pay-as-you-go pricing with no upfront costs:

- The service offers enterprise-grade security with IPsec encryption, supports high throughput up to 5 Gbps per tunnel, and provides comprehensive monitoring through CloudWatch
- AWS VPN integrates natively with AWS security and networking services, reducing operational complexity while maintaining industry-standard security protocols

Service Integration

AWS VPN integrates deeply with core AWS networking services including Amazon VPC for secure network isolation, AWS Transit Gateway for centralized connectivity hub supporting ECMP routing, and AWS Direct Connect for hybrid encrypted connections. Security integrations include AWS Certificate Manager (ACM) for SSL/TLS certificate management, AWS IAM for authentication and authorization, Amazon CloudWatch for monitoring and metrics, and AWS CloudTrail for API logging. Additional integrations include AWS Global Accelerator for Site-to-Site VPN acceleration, AWS Directory Service for Active Directory authentication with Client VPN, and AWS Network Firewall for traffic inspection at the network perimeter.

Onboarding and Offboarding

Customers can start with AWS VPN using the AWS Management Console, AWS CLI, or APIs. For Site-to-Site VPN, the process involves creating a customer gateway representing the on-premises device, creating a virtual private gateway or Transit Gateway attachment, configuring routing, and downloading configuration files for the customer gateway device:

- For Client VPN, setup requires generating server and client certificates using OpenVPN easy-rsa utility, importing certificates to AWS Certificate Manager, creating a Client VPN endpoint, associating target networks, and configuring authorization rules
- AWS provides comprehensive documentation, sample configurations for supported devices, and getting started guides for both services

Getting Started Guide:
https://docs.aws.amazon.com/vpn/latest/s2svpn/SetUpVPNConnections.html

Data Removal

To offboard from AWS VPN, customers can delete VPN connections, Client VPN endpoints, and associated resources through the AWS Console, CLI, or API. For Site-to-Site VPN, this involves deleting VPN connections, customer gateways, and virtual private gateways. For Client VPN, customers delete endpoints, revoke client certificates, and remove associated target networks. All connection logs stored in CloudWatch Logs and configuration data are automatically removed when resources are deleted, ensuring complete data cleanup during service termination.

Backup/Restore and Disaster Recovery

AWS VPN provides inherent redundancy with dual IPsec tunnels per connection for automatic failover, but does not offer traditional backup/restore capabilities as it's a connectivity service. Configuration data is stored in the AWS control plane with built-in redundancy. For disaster recovery, customers can deploy VPN connections across multiple AWS regions and use multiple tunnel configurations with Transit Gateway ECMP routing for high availability and fault tolerance across geographic regions.

Backup Capabilities

AWS VPN does not integrate with AWS Backup as it is a network connectivity service rather than a data storage service. The service configuration is automatically maintained by AWS with built-in redundancy:

- However, customers should backup their customer gateway device configurations and VPN connection settings outside of AWS
- Client VPN configuration files and certificates should be securely stored and backed up by customers to ensure service continuity

Disaster Recovery

AWS VPN does not integrate with AWS Elastic Disaster Recovery as it provides connectivity rather than compute instance recovery. However, VPN connections support disaster recovery architectures through dual tunnels, multi-region deployments, and integration with Transit Gateway for automatic failover. Customers can establish VPN connections in multiple AWS regions and use routing policies to achieve cross-region disaster recovery for their hybrid network connectivity requirements.

Recovery Objectives

AWS VPN supports low RTO through automatic tunnel failover (typically under 30 seconds), multiple tunnel configurations with ECMP routing, and multi-region VPN deployments. For RPO, the service provides continuous connectivity without data loss during failover events. Accelerated Site-to-Site VPN reduces convergence time by routing through AWS Global

Accelerator edge locations. Customers can achieve sub-minute RTO by implementing proper routing configurations and monitoring tunnel health through CloudWatch metrics.

Service Constraints

Service Quotas: https://docs.aws.amazon.com/vpn/latest/s2svpn/vpn-limits.html

FAQ: https://aws.amazon.com/vpn/faqs/

Technical Requirements

Service Documentation: https://docs.aws.amazon.com/vpn/

User Guide: https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html

API Reference: https://docs.aws.amazon.com/AWSEC2/latest/APIReference/OperationList-query-vpc.html

Pricing Overview

Please see the AWS UK G Cloud 15 Pricing Document accompanying this service in the Digital Marketplace.

Public Pricing: https://aws.amazon.com/vpn/pricing/

Cost Optimization

AWS VPN offers several cost optimization strategies including VPN Concentrator for multi-site deployments that reduces per-site costs by sharing bandwidth across up to 100 sites. Customers can optimize costs by rightsizing tunnel bandwidth (choosing standard 1.25 Gbps vs:

- large 5 Gbps based on actual needs), using unaccelerated VPN for non-critical workloads, and implementing proper routing to minimize data transfer costs
- Terminating VPN on Transit Gateway instead of Virtual Private Gateway enables ECMP routing for better bandwidth utilization
- Customers can also leverage AWS Direct Connect with VPN backup for cost-effective hybrid connectivity while maintaining redundancy

Savings Considerations

Primary cost savings come from eliminating on-premises VPN infrastructure costs including hardware, maintenance, and operational overhead. Pay-as-you-go pricing model eliminates upfront capital expenditure with billing based on connection-hours and data transfer:

- VPN Concentrator reduces costs for multi-site deployments by up to 50% compared to individual connections
- Using standard tunnels instead of accelerated VPN saves on Global Accelerator charges for non-critical workloads
- Customers can achieve additional savings by optimizing data transfer patterns, implementing efficient routing policies, and using Regional Data Transfer pricing
- The fully-managed nature eliminates staffing costs for VPN infrastructure management and maintenance